Integre o Cisco SecureX com o Cisco Umbrella

Contents

Introdução

Este documento descreve o processo para configurar e verificar a integração do Umbrella com o SecureX com as 3 APIs disponíveis.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Guarda-chuva da Cisco
- Cisco Secure X
- Cisco Threat Response

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Conta guarda-chuva com licença DNS Advantage
- X Seguro

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Informações de Apoio

Para configurar totalmente essa integração com todas as suas funcionalidades, você precisa acessar essas 3 APIs

- API de relatório (incluída em todas as licenças)
- API de Imposição
- Investigar API

Para configurar a integração do Umbrella, você deve primeiro coletar algumas informações de suas instâncias do Umbrella e, em seguida, preencher o formulário Adicionar novo módulo Umbrella.

Configurar

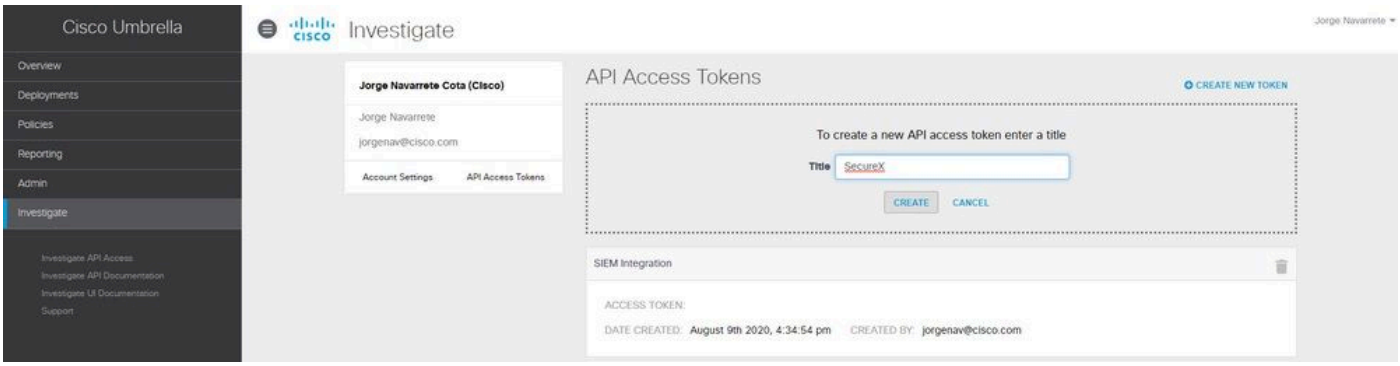
Criar módulo

1. Faça login na sua conta do Secure X. Se ainda não tiver uma conta, você poderá criar uma com o Cisco Secure Sign-On.
2. Navegue até Integrações > Adicionar novo módulo. Na página Integrações disponíveis, role para baixo até a opção Umbrella e clique em Adicionar novo módulo.

Siga estas etapas para coletar as informações necessárias de sua Conta Umbrella para enviar no formulário Adicionar Novo Módulo Umbrella.

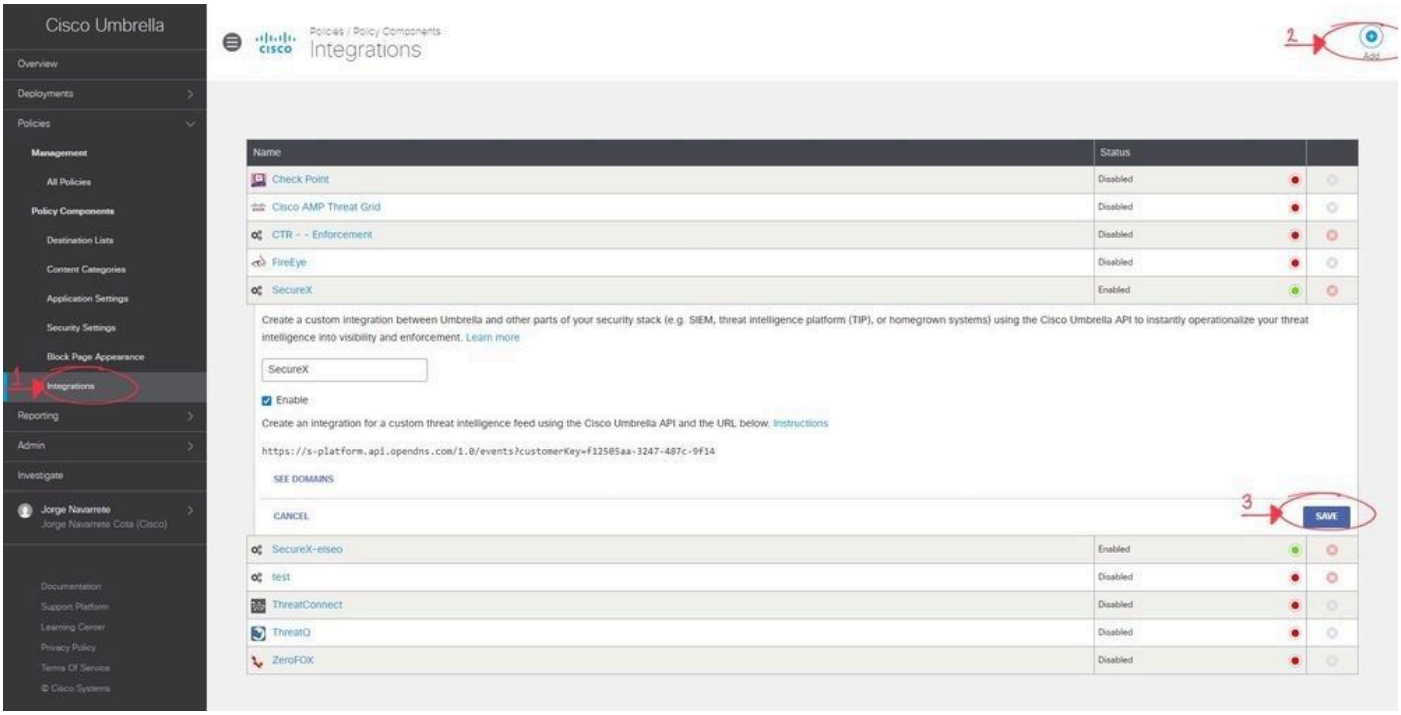
Investigar API

1. No Umbrella, navegue para Investigar > Investigar Acesso à API, clique em Criar Novo Token, insira um título para o token e clique em Criar Novo Token novamente.
2. Copie o valor do Access Token no campo API Token no formulário Adicionar novo módulo Umbrella.



API de Imposição

1. No Umbrella, navegue para Policies > Policy Components > Integrations, clique em Add e insira um nome e clique em Create.
2. Clique no link nome da integração recém-criado, marque as caixas de seleçãoHabilitar eSalvar.
3. Clique no nome da integração para exibir o URL da integração. Copie o URL de integração no campo URL de integração personalizada do Umbrella no formulário Adicionar novo módulo do Umbrella.



Observação: para integrar a API de aplicação do Umbrella, você deve ser um administrador em uma org autônoma ou org filho do Umbrella em vez de um administrador de um console do Umbrella.

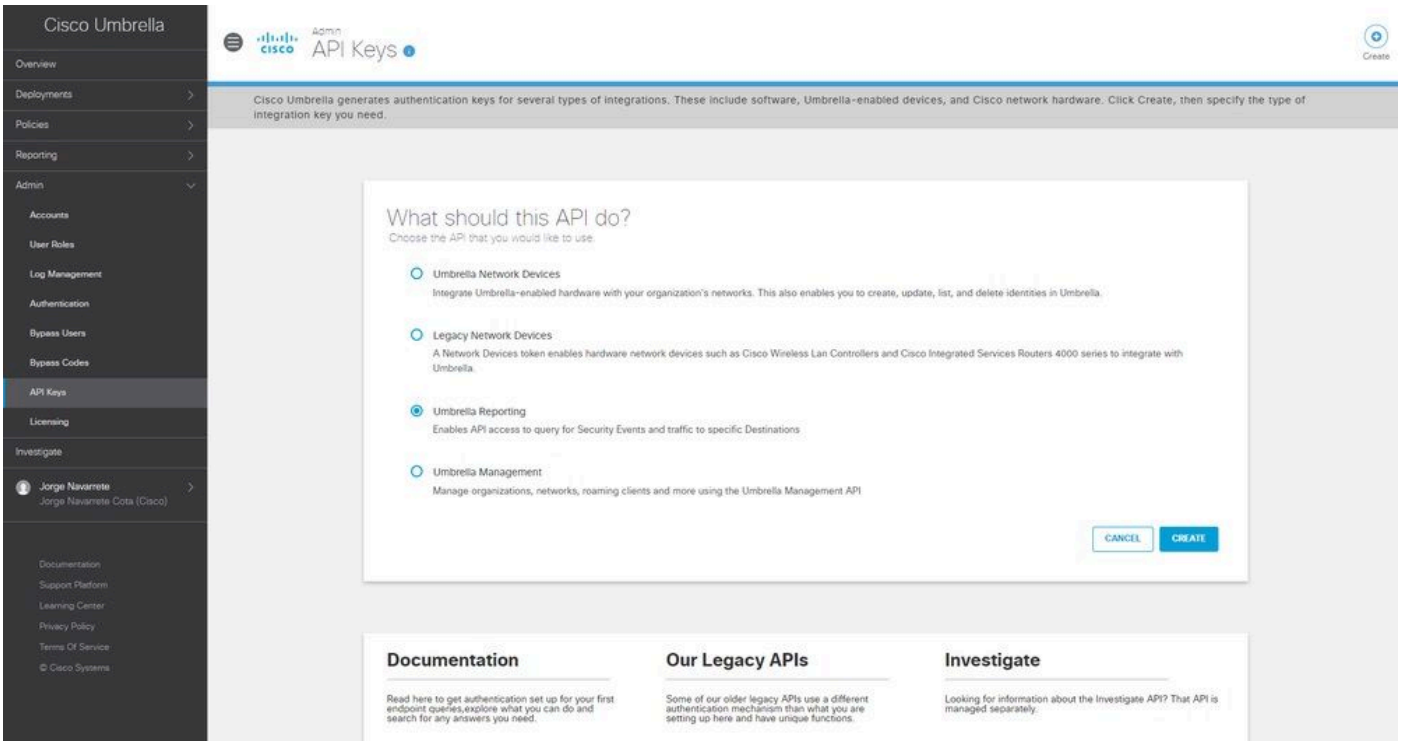
API de relatório

1. No Umbrella, navegue para Admin > API Keys e clique em Create.
2. Em What should this API do?, clique no botão de opção Umbrella Reporting e clique em

Create.

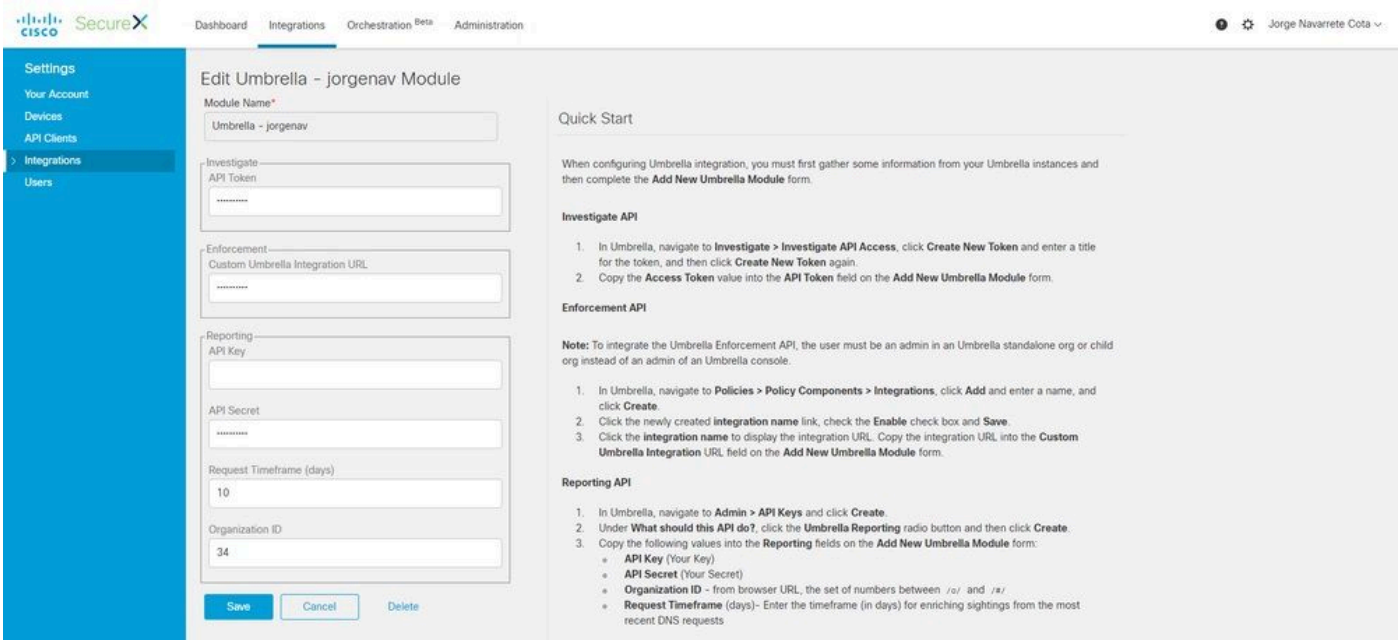
3. Copie os próximos valores nos campos Reporting no formulário Add New Umbrella Module:

   - Chave API (Sua Chave)
   - Segredo de API (Seu Segredo)
   - ID da organização - na URL do navegador, o conjunto de números entre `/o/e/#/`
   - Período de solicitação (dias) - Insira o período (em dias) para aprimorar avistamentos das solicitações de DNS mais recentes



Salvar módulo

1. Preencha as informações de API no seu Módulo Umbrella e clique em Salvar.

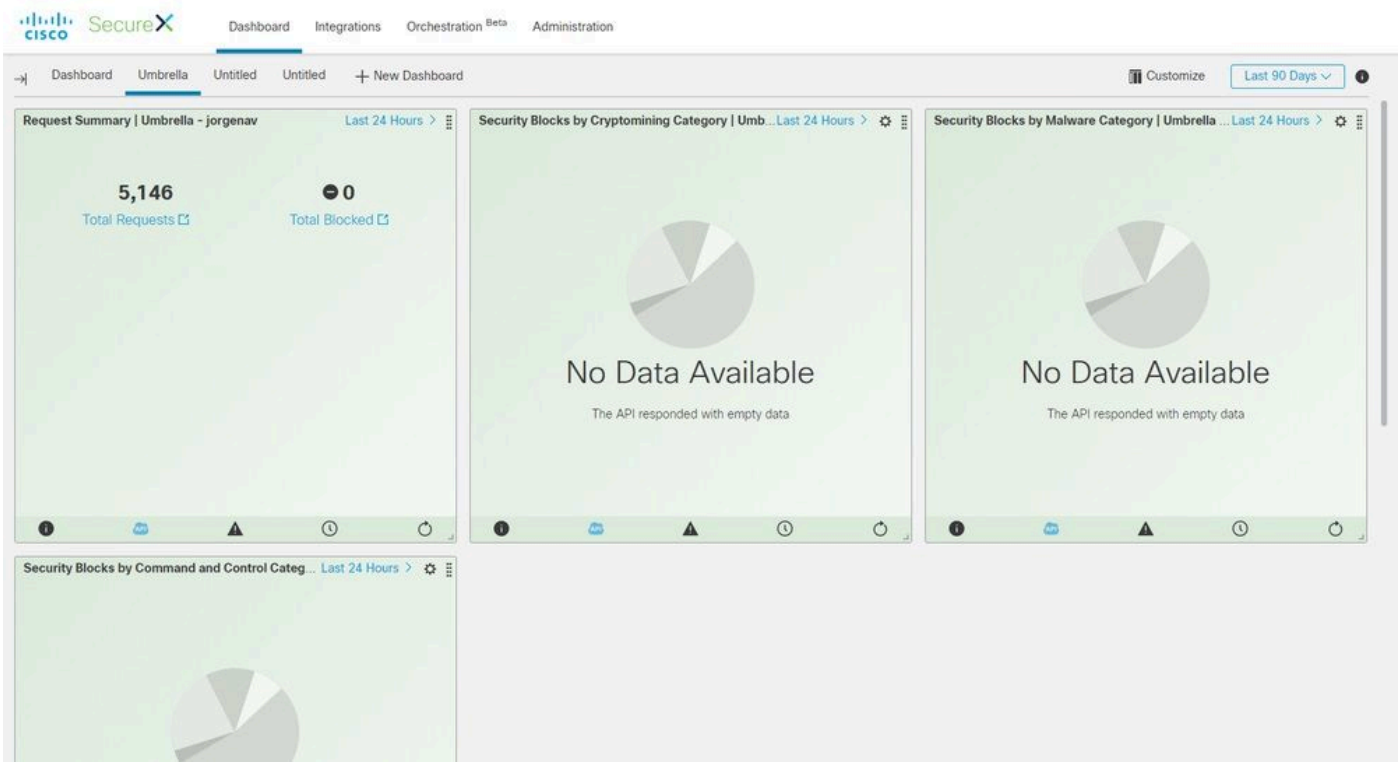


Criar painel SecureX

1. Depois de adicionar o módulo, você poderá navegar até o Secure X e criar um Novo Painel.

2. Nos Painéis disponíveis, selecione o módulo Umbrella e adicione as Categorias que você está interessado em ver.

3. Clique em Salvar e veja suas informações preenchidas através da API.



Verificar

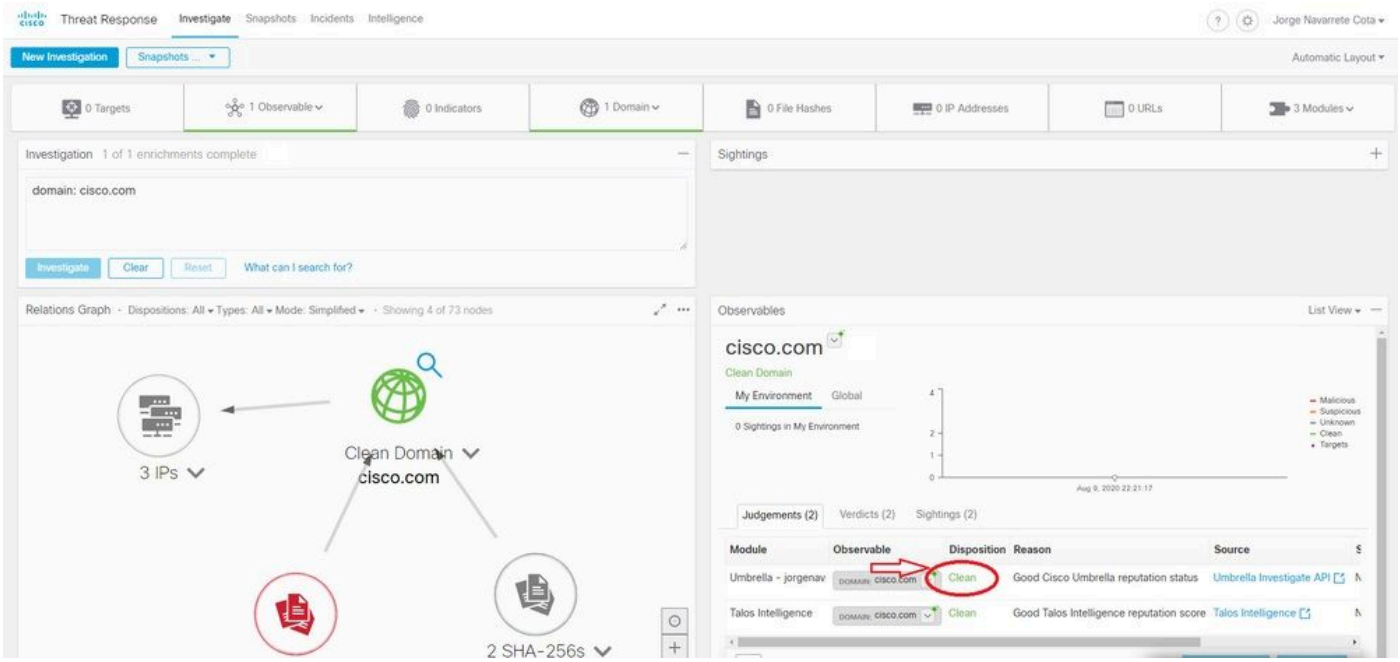
Use esta seção para confirmar se a sua configuração funciona corretamente.

Investigar

A API Investigar permite adicionar um feed a uma investigação CTR, para ver a disposição de um domínio e enriquecer a investigação com outros módulos.

1. Para verificar essa integração, faça uma nova investigação no Cisco Threat Response. Uma Disposição fornecida pelo Umbrella pode ser encontrada com uma pesquisa por um domínio conhecido, como cisco.com.

2. Se você clicar sob o domínio no Gráfico de Relações, também poderá girar a partir daí para o Painel Investigar no Umbrella.

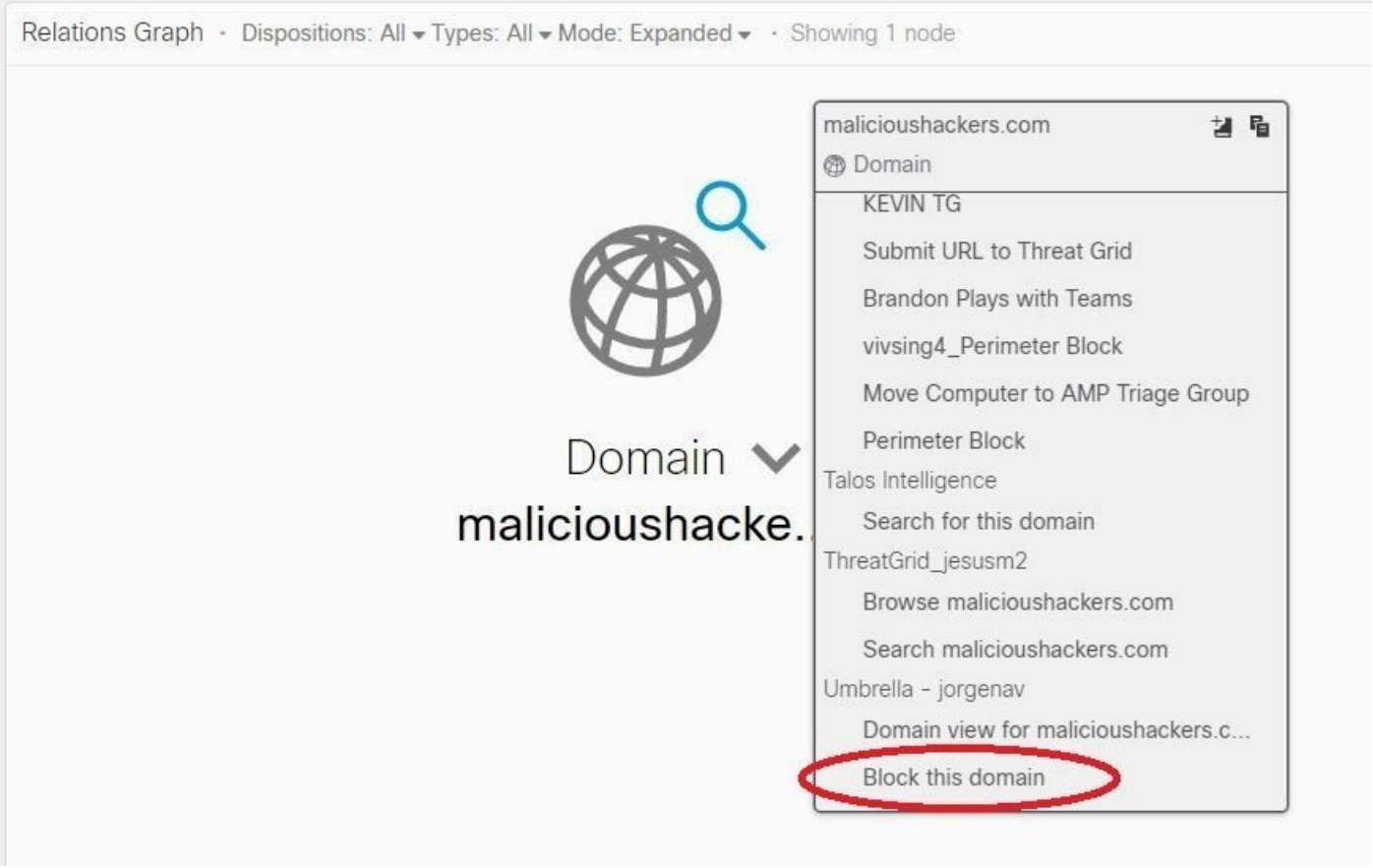


Aplicação

Com a API de aplicação, você pode bloquear ou desbloquear um domínio diretamente de uma investigação.

1. Para verificar se a API funciona, você pode bloquear um domínio visto em uma investigação e que adiciona o domínio à lista de bloqueios de política no Umbrella.

2. Para verificar se o URL foi adicionado à lista de bloqueio, navegue para Policies > Policy Components > Integrations. Selecione sua integração SecureX e clique em Ver domínios. Uma janela exibe os domínios adicionados do CTR.



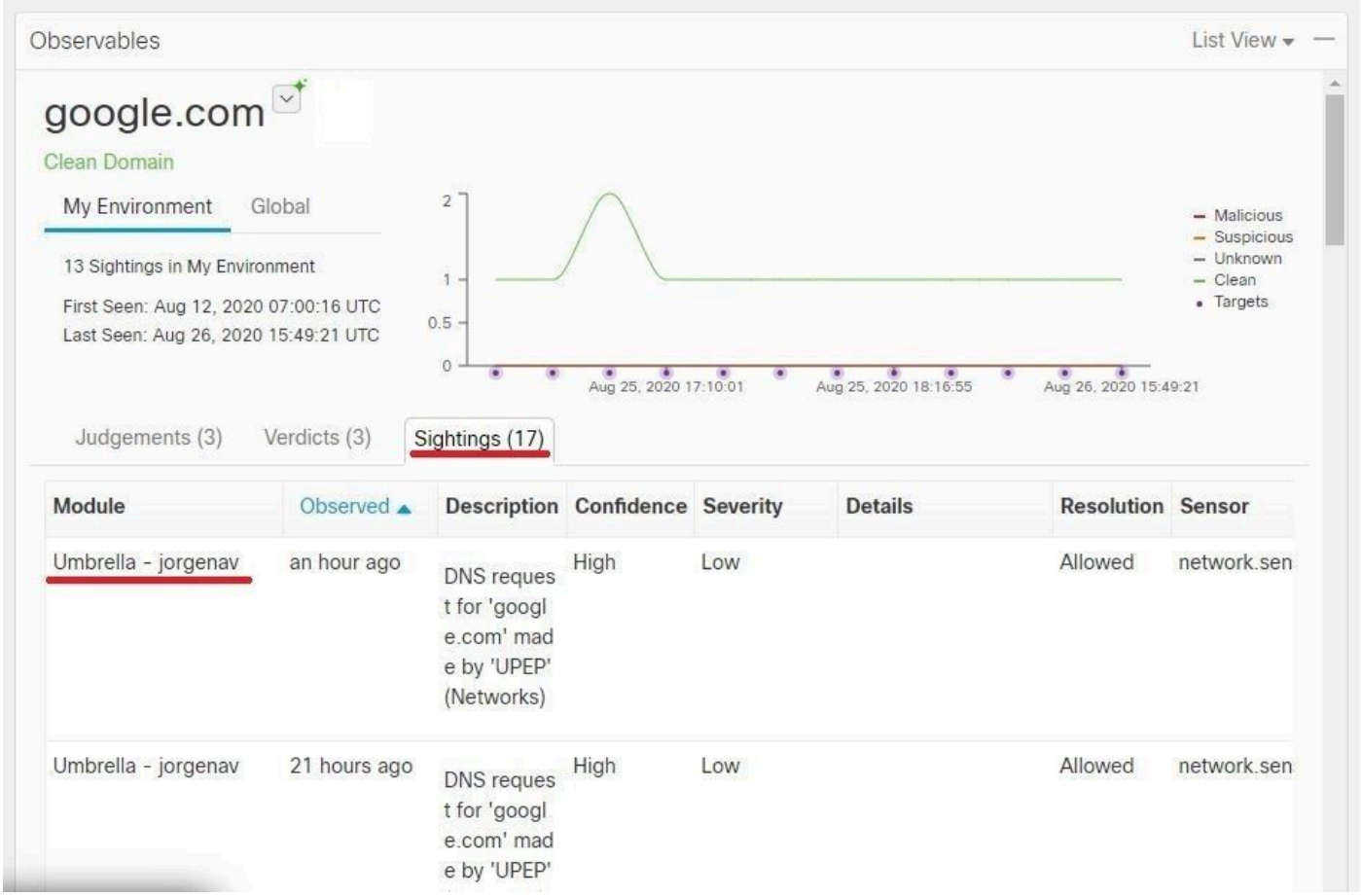
3. Se os domínios não estiverem bloqueados, no painel do Umbrella, navegue para Políticas > Componentes da Política > Configurações de Segurança. Em Integrações, certifique-se de ter aplicado a lista desejada.

Relatórios

A API de relatórios permite que você veja as informações de suas implantações do Umbrella no SecureX.

Você pode verificar a integração com uma investigação de um domínio que você sabe que foi visto em seu ambiente no CTR.

Na Investigação CTR, a lista de computadores que acessaram um domínio específico é exibida em Avisos.



Vídeo

Você pode encontrar as informações de configuração contidas neste artigo neste vídeo.

Informações Relacionadas

- Suporte Técnico e Documentação - Cisco Systems

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.