Integre Cisco SecureX con Cisco Umbrella

Contenido

Introducción

Prerequisites

- Requirements
- Componentes Utilizados

Antecedentes

Configurar

- Crear módulo
- Investigar API
- API de aplicación
- API de informes
- Guardar módulo
- Crear panel de SecureX

Verificación

- Investigar
- Aplicación
- Informes

Video

Información Relacionada

Introducción

Este documento describe el proceso para configurar y verificar la integración de Umbrella con SecureX con las 3 API disponibles.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Cisco Umbrella
- Cisco Secure X
- Cisco Threat Response

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Cuenta Umbrella con licencia de DNS Advantage
- X segura

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). If your network is live, make sure that you understand the potential impact of any command.

Antecedentes

Para configurar completamente esta integración con todas sus funcionalidades, necesita acceder a estas 3 API

- API de informes (incluida en todas las licencias)
- API de aplicación
- Investigar API

Para configurar la integración de Umbrella, primero debe recopilar información de sus instancias de Umbrella y luego completar el formulario Add New Umbrella Module.

Configurar

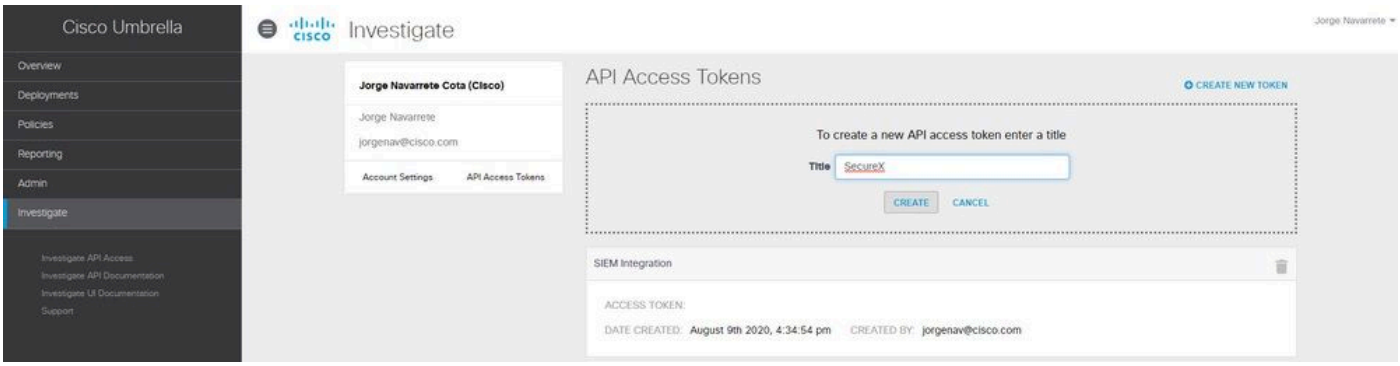
Crear módulo

1. Inicie sesión en su cuenta de Secure X. Si aún no tiene una cuenta, puede crear una con Cisco Secure Sign-On.
2. Vaya a Integraciones > Agregar nuevo módulo. En la página Integraciones disponibles, desplácese hasta la opción Paraguas y haga clic en Agregar nuevo módulo.

Utilice estos pasos para recopilar la información necesaria de su cuenta de Umbrella para enviarla en el formulario Agregar nuevo módulo de Umbrella.

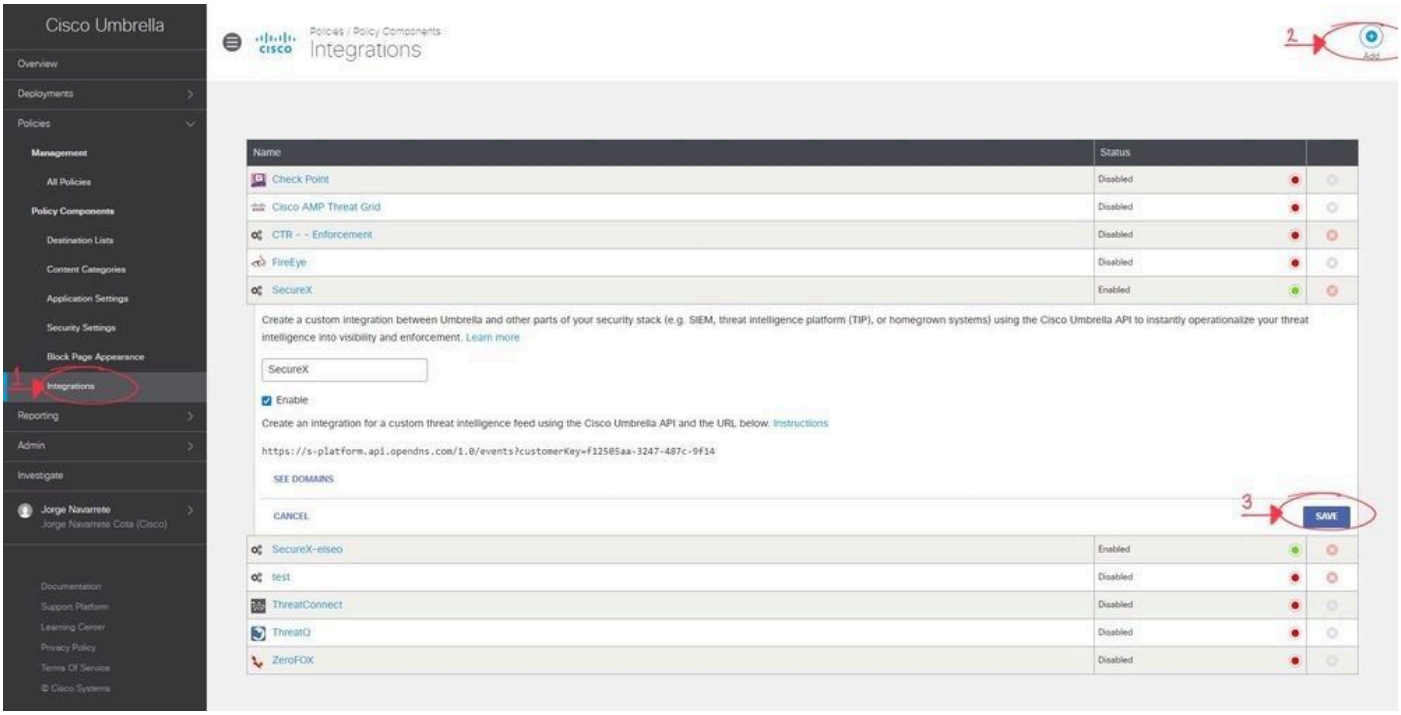
Investigar API

1. En Umbrella, navegue hasta Investigate > Investigate API Access, haga clic en Create New Token e ingrese un título para el token, y luego haga clic en Create New Token nuevamente.
2. Copie el valor del token de acceso en el campo Token de API del formulario Agregar nuevo módulo de paraguas.



API de aplicación

1. En Umbrella, navegue hasta Policies > Policy Components > Integrations, haga clic en Add e ingrese un nombre, y haga clic en Create.
2. Haga clic en el enlace nombre de integración recién creado, marque la casilla de verificación Enable y Save.
3. Haga clic en el nombre de integración para mostrar la URL de integración. Copie la URL de integración en el campo Custom Umbrella Integration en el formulario Add New Umbrella Module.



Nota: para integrar la API de aplicación de Umbrella, debe ser administrador de una organización independiente u organización secundaria de Umbrella en lugar de administrador de una consola de Umbrella.

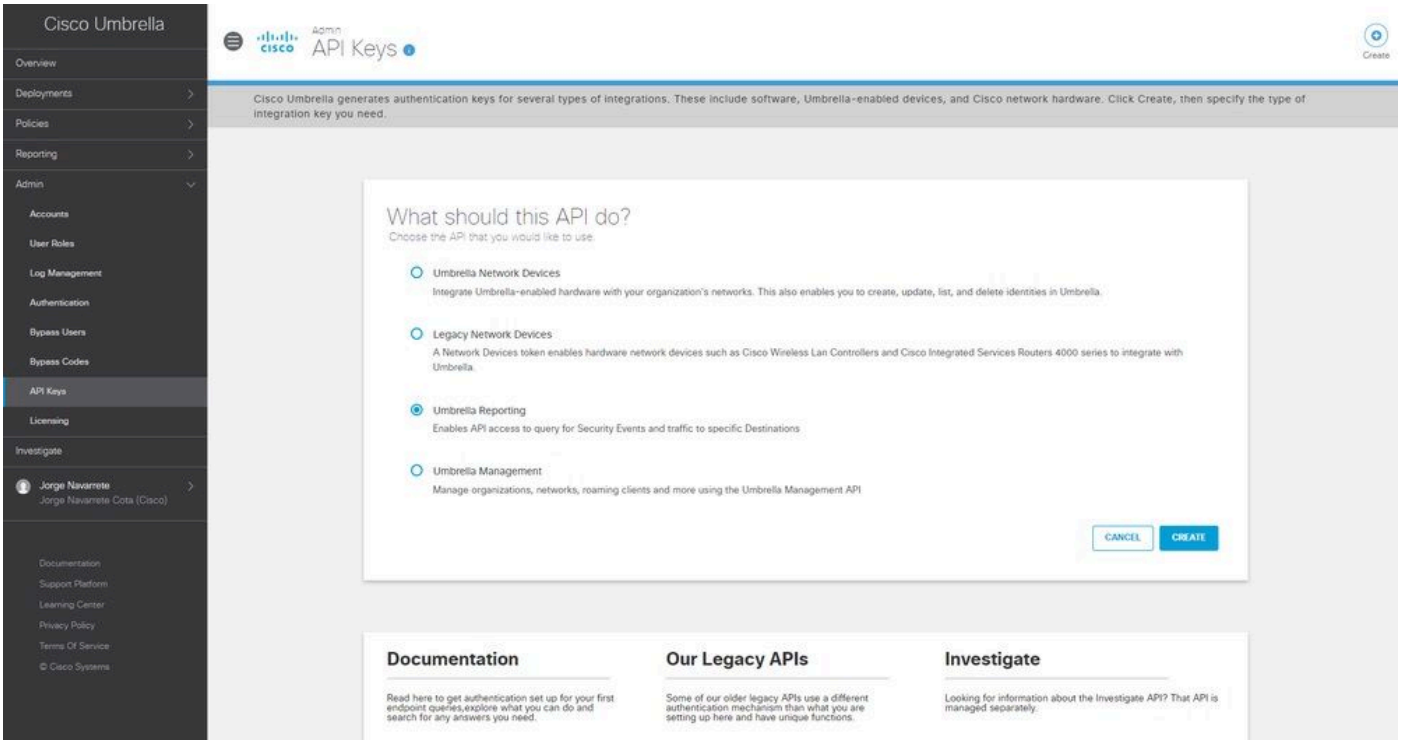
API de informes

1. En Umbrella, navegue hasta Admin > API Keys y haga clic en Create.
2. En ¿Qué debe hacer esta API?, haga clic en el botón de opción Umbrella Reporting y, a

continuación, haga clic en Create.

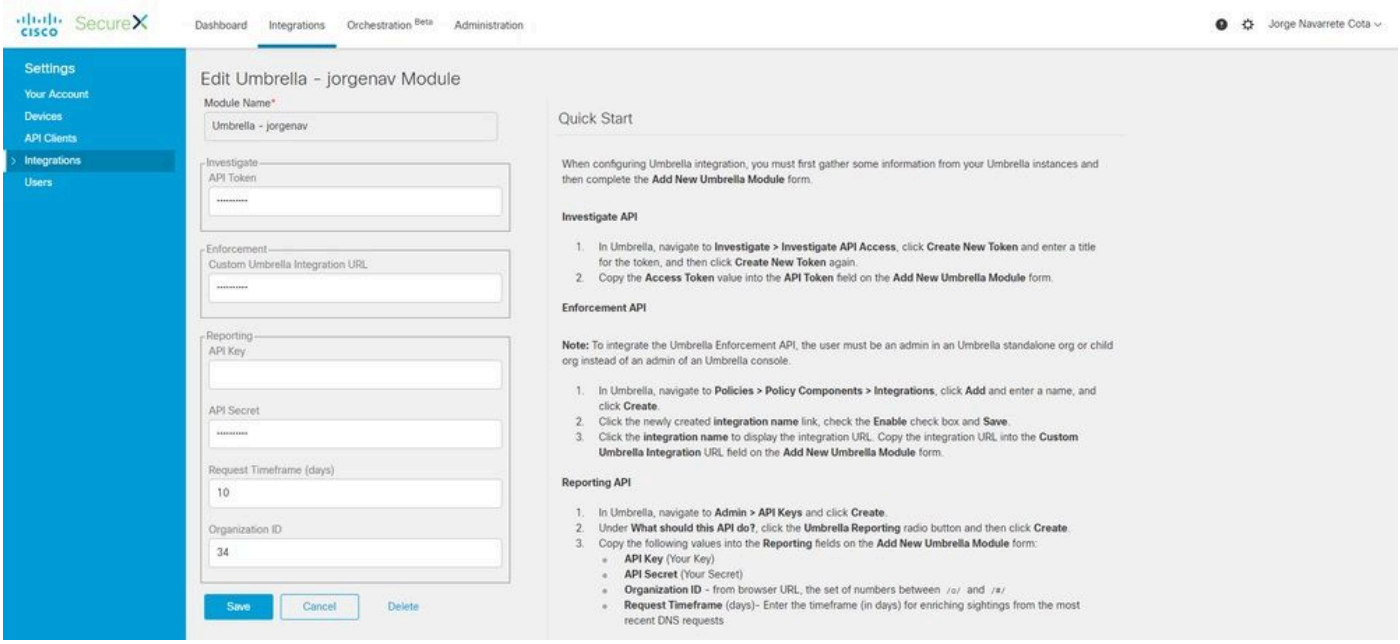
3. Copie los valores siguientes en los campos Reporting del formulario Add New Umbrella Module:

   - Clave de API (su clave)
   - Secreto de API (Su secreto)
   - ID de la organización: en la URL del navegador, el conjunto de números entre`/o/y/#/`
   - Período de tiempo de la solicitud (días): introduzca el período de tiempo (en días) para enriquecer los avistamientos de las solicitudes DNS más recientes



Guardar módulo

1. Rellene la información de la API en el módulo Umbrella y haga clic en Guardar.

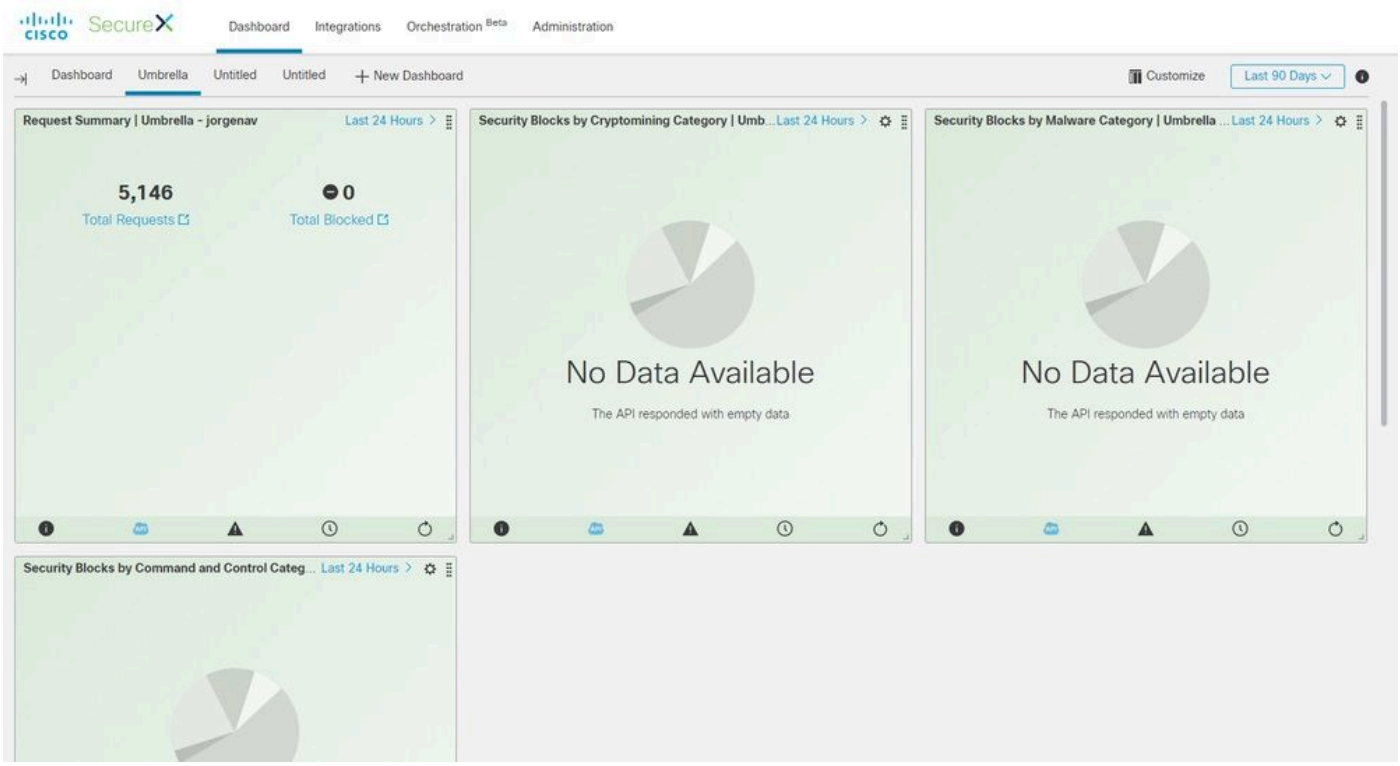


Crear panel de SecureX

1. Una vez agregado el módulo, puede navegar hasta Secure X y crear un nuevo panel.

2. En los paneles disponibles, seleccione el módulo Umbrella y agregue las categorías que le interese ver.

3. Haga clic en Guardar, y vea que su información se completa a través de la API.



Verificación

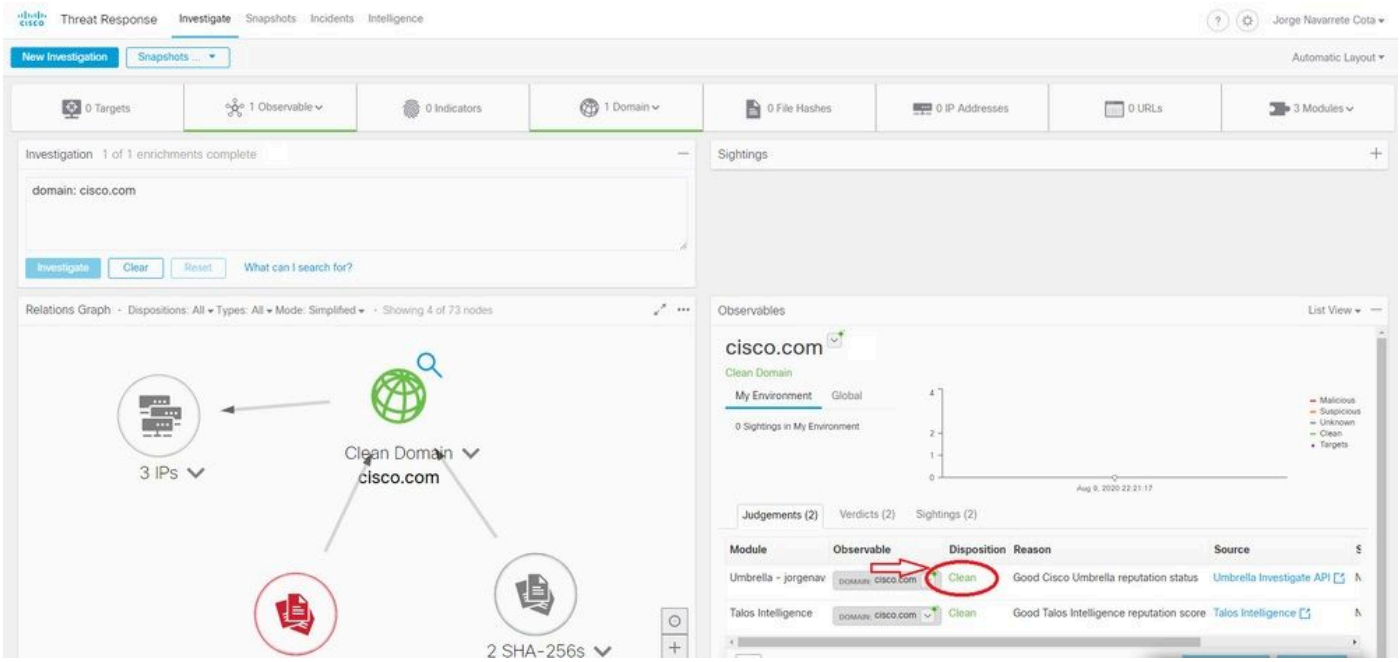
Utilize esta sección para confirmar que su configuración funcione correctamente.

Investigar

La API Investigate permite agregar una fuente a una investigación de CTR para ver la disposición de un dominio y enriquecer la investigación con otros módulos.

1. Para verificar esta integración, realice una nueva investigación en Cisco Threat Response. Una Disposición proporcionada por Umbrella se puede encontrar con una búsqueda de un dominio conocido, como cisco.com.

2. Si pulsa bajo el dominio en el Gráfico de relaciones, también podrá pivotar desde allí al tablero de mandos de investigación en Umbrella.

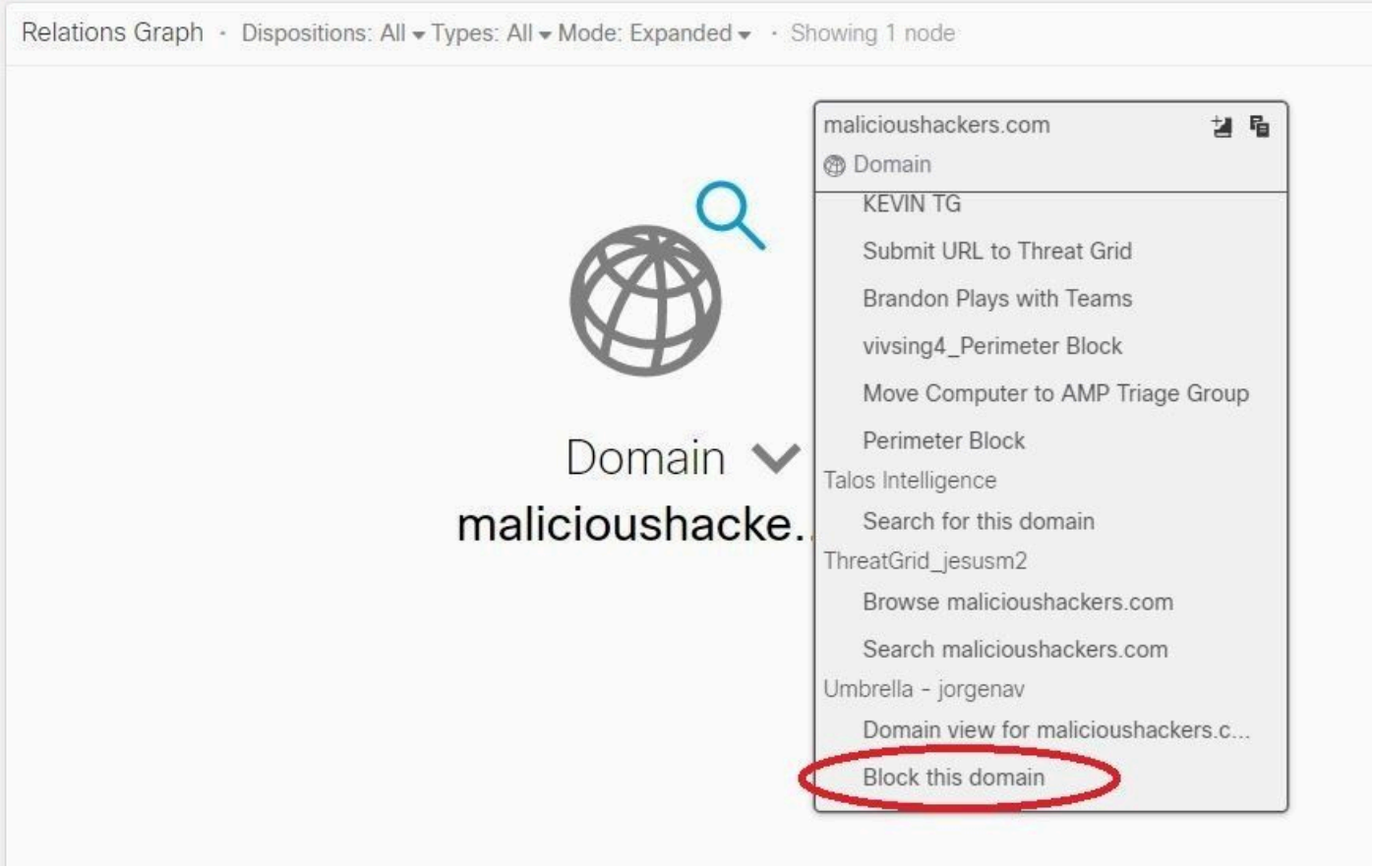


Aplicación

Con la API de aplicación, puede bloquear o desbloquear un dominio directamente de una investigación.

1. Para verificar que la API funciona, puede bloquear un dominio visto en una investigación y que agrega el dominio a la lista de bloqueo de políticas en Umbrella.

2. Para verificar que la URL se ha agregado a la lista de bloqueo, navegue hasta Políticas > Componentes de Política > Integraciones. Seleccione su integración de SecureX y haga clic en Ver dominios. Una ventana muestra los dominios agregados desde CTR.



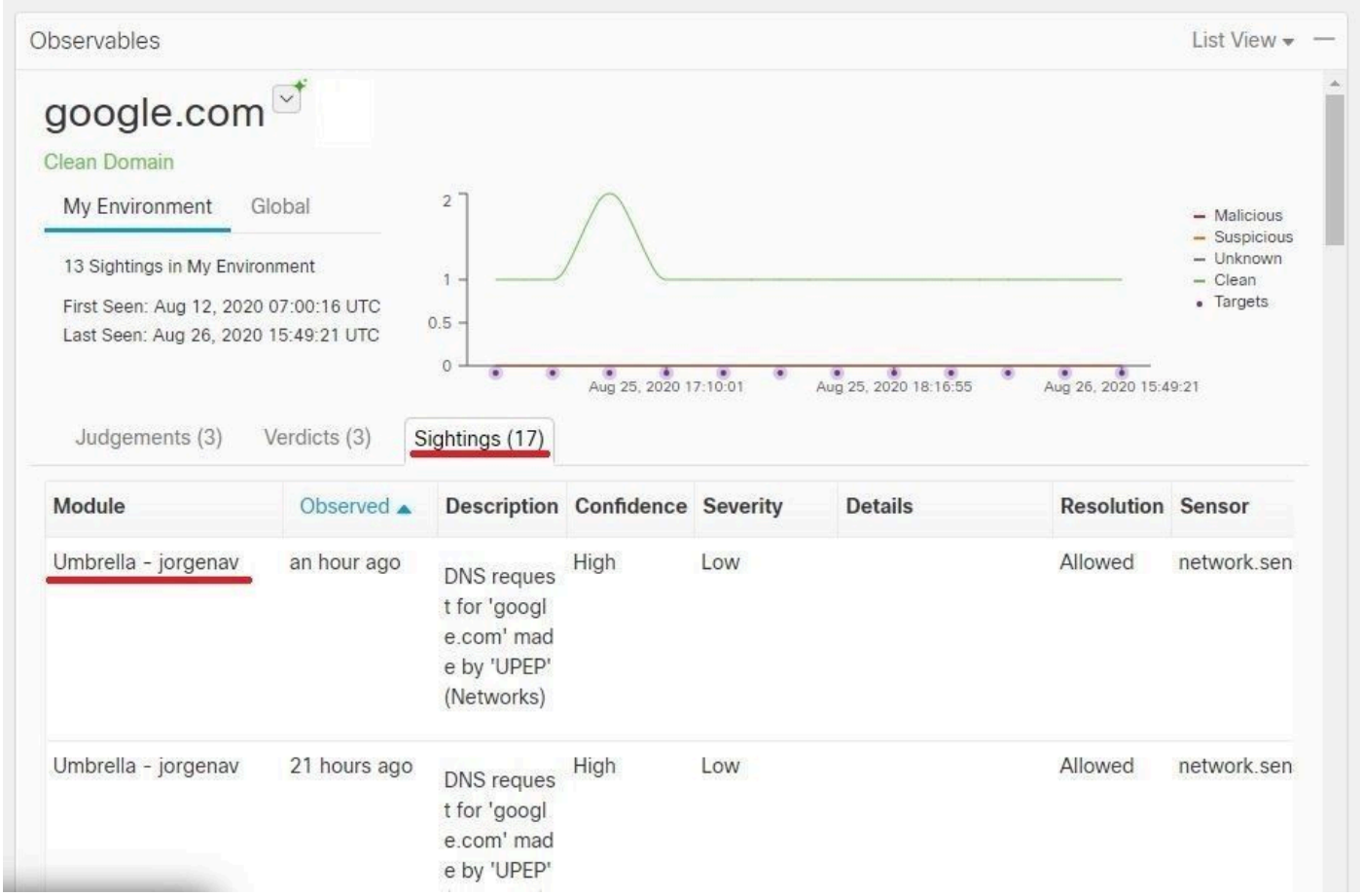
3. Si los dominios no están bloqueados, en el panel de Umbrella, navegue hasta Políticas > Componentes de política > Configuración de seguridad. En Integraciones asegúrese de que ha aplicado la lista deseada.

Informes

La API de informes le permite ver la información de sus implementaciones de Umbrella en SecureX.

Puede verificar la integración con una investigación de un dominio que sabe que se ha visto en su entorno en CTR.

En Investigación del CTR, la lista de equipos que han accedido a un dominio determinado se muestra en Avistamientos.



Video

En este vídeo puede encontrar la información de configuración que se incluye en este artículo.

Información Relacionada

- Soporte Técnico y Documentación - Cisco Systems

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).