Integre ThreatConnect con Umbrella

Contenido

Introducción

Este documento describe cómo integrar ThreatConnect con Cisco Umbrella.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Un panel de ThreatConnect con acceso para actualizar la URL para las integraciones
- Derechos administrativos del panel general
- El panel de Umbrella debe tener habilitada la integración de ThreatConnect.

Componentes Utilizados

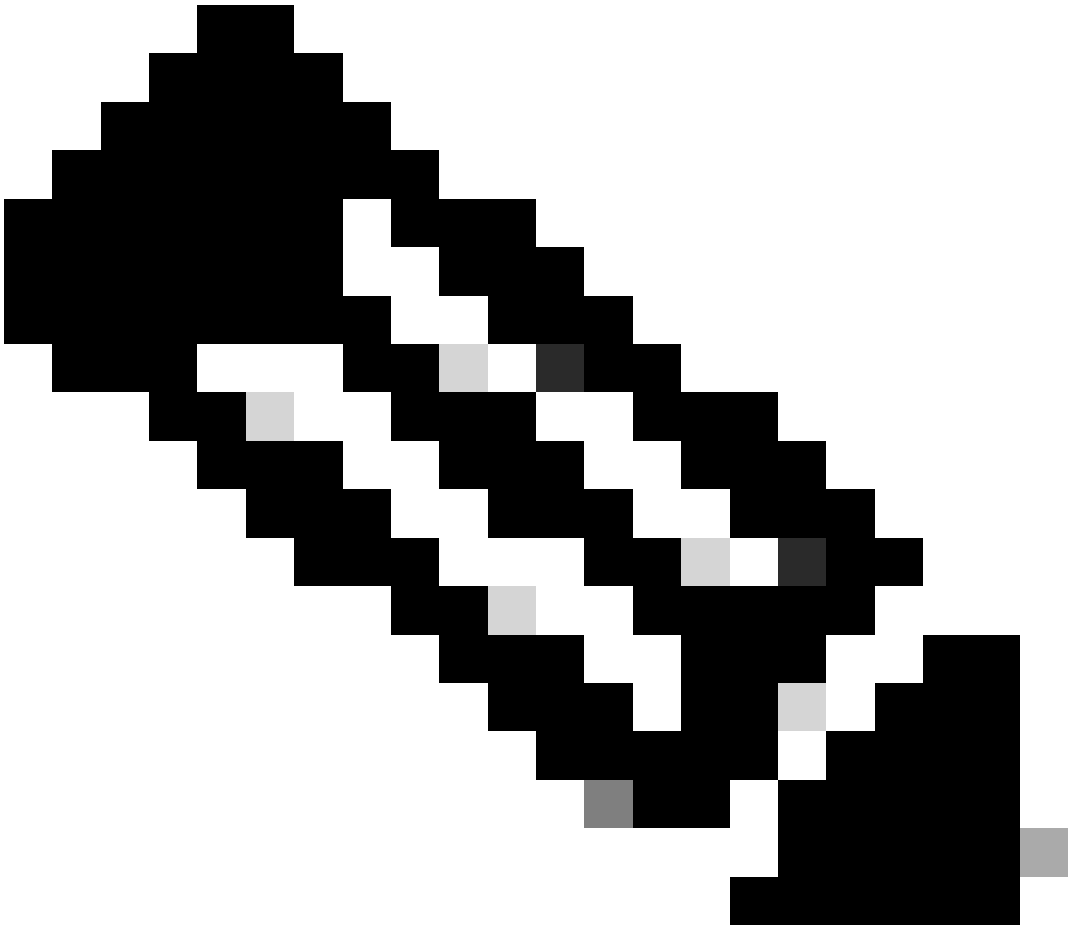
La información de este documento se basa en Cisco Umbrella.

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). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Descripción general de ThreatConnect y Cisco Umbrella Integration

Gracias a la integración de ThreatConnect con Cisco Umbrella, los responsables de seguridad y los administradores pueden ahora ampliar la protección frente a amenazas avanzadas a los portátiles, tablets o teléfonos en roaming, a la vez que proporcionan otro nivel de aplicación a una red corporativa distribuida.

Esta guía describe cómo configurar ThreatConnect para comunicarse con Umbrella de modo que los eventos de seguridad del TIP de ThreatConnect se integren en las políticas que se pueden aplicar a los clientes protegidos por Cisco Umbrella.

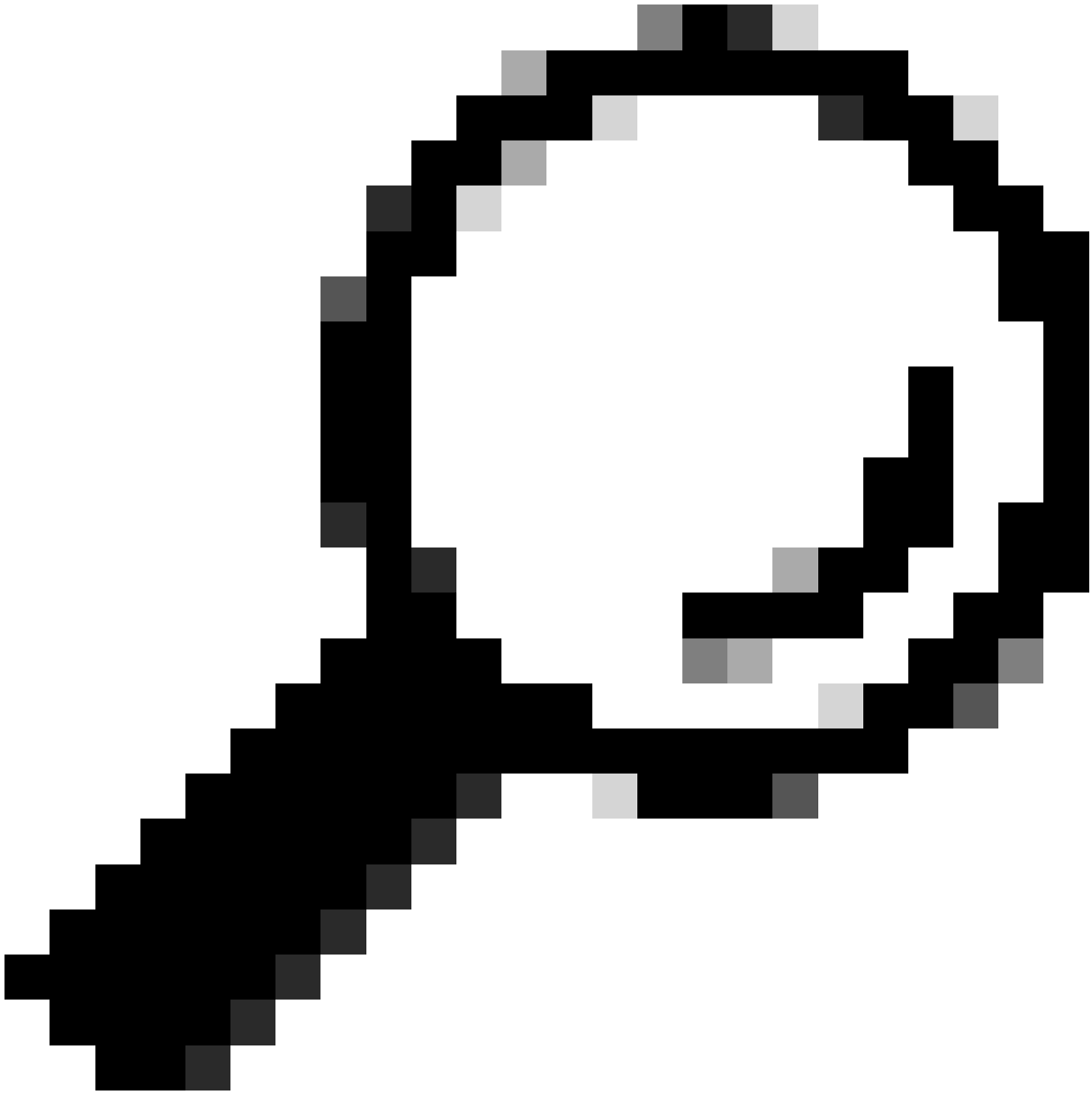


Nota: La integración de ThreatConnect solo se incluye en un determinado paquete de Cisco Umbrella. Si no dispone de un paquete que incluya esta integración, póngase en contacto con su representante de Cisco Umbrella para obtenerlo. Si tiene el paquete correcto pero no ve ThreatConnect como una integración para su panel, póngase en contacto con el servicio de asistencia de Cisco Umbrella.

En primer lugar, la plataforma ThreatConnect envía a Umbrella la inteligencia de amenazas cibernéticas que ha encontrado, como los dominios que alojan malware, comandos y control para sitios Botnet o de suplantación de identidad.

A continuación, Umbrella valida la amenaza para garantizar que se pueda agregar a una política. Si se confirma que la información de ThreatConnect es una amenaza, la dirección de dominio se agrega a la lista de destino de ThreatConnect como parte de una configuración de seguridad que se puede aplicar a cualquier política de Umbrella. Esta política se aplica inmediatamente a cualquier solicitud que se realice desde dispositivos que utilicen políticas con la lista de destino de ThreatConnect.

De cara al futuro, Umbrella analiza automáticamente las alertas de ThreatConnect y agrega sitios maliciosos a la lista de destino de ThreatConnect, ampliando la protección de ThreatConnect a todos los usuarios y dispositivos remotos y proporcionando otra capa de aplicación a su red corporativa.



Consejo: Aunque Umbrella hace todo lo posible por validar y permitir dominios que se sabe que son seguros en general (por ejemplo, Google y Salesforce), para evitar interrupciones no deseadas, Umbrella sugiere agregar dominios que no desea que se bloqueen a la Lista global de permitidos u otras listas de destinos según su política. Entre los ejemplos, se encuentran los siguientes:

- La página de inicio de su organización. Por ejemplo, mydomain.com.
- Dominios que representan los servicios proporcionados que pueden tener registros internos y externos. Por ejemplo, mail.myservicedomain.com y portal.myotherservicedomain.com.
- Aplicaciones en la nube menos conocidas de las que usted depende en gran medida, pero que Umbrella no reconoce ni incluye en su validación automática de dominio. Por ejemplo, localcloudservice.com.

La Lista global de permitidos se encuentra en Políticas > Listas de destino en Umbrella.

Consulte la documentación para obtener más información: Administrar listas de destino

Configuración del panel de Umbrella para recibir eventos de ThreatConnect

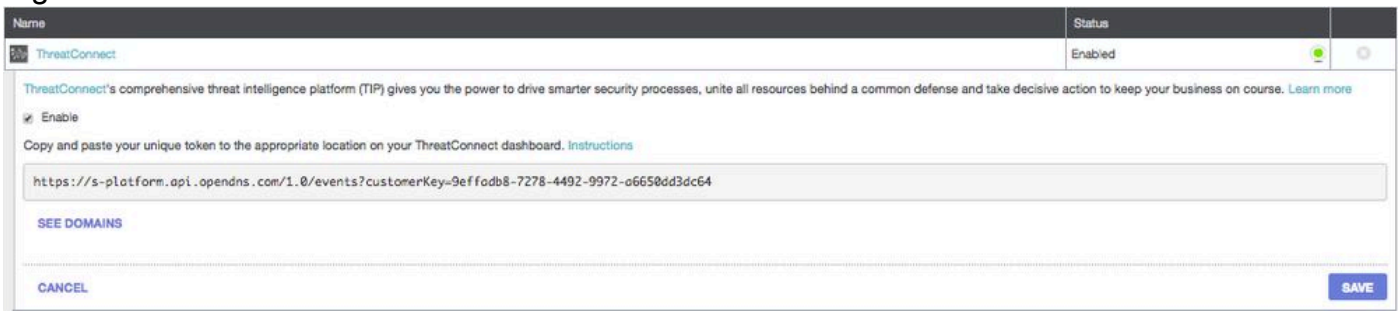
Empiece por encontrar su URL única en Umbrella para que el dispositivo ThreatQ se comunique con:

1. Inicie sesión en el panel de Umbrella.

2. Acceda a Políticas > Integraciones.

3. En la tabla, seleccione ThreatConnect para expandirlo.

4. Seleccione Activar y, a continuación, Guardar. Esto genera una URL única y específica para su organización dentro de Umbrella.



Necesita la URL más adelante en este artículo cuando configure ThreatConnect para enviar datos a Umbrella.

Configuración de ThreatConnect para comunicarse con Umbrella

Para comenzar a enviar tráfico desde ThreatConnect a Umbrella, debe configurar ThreatConnect con la información de URL generada en la primera sección de este artículo:

1. Inicie sesión en el panel de ThreatConnect.

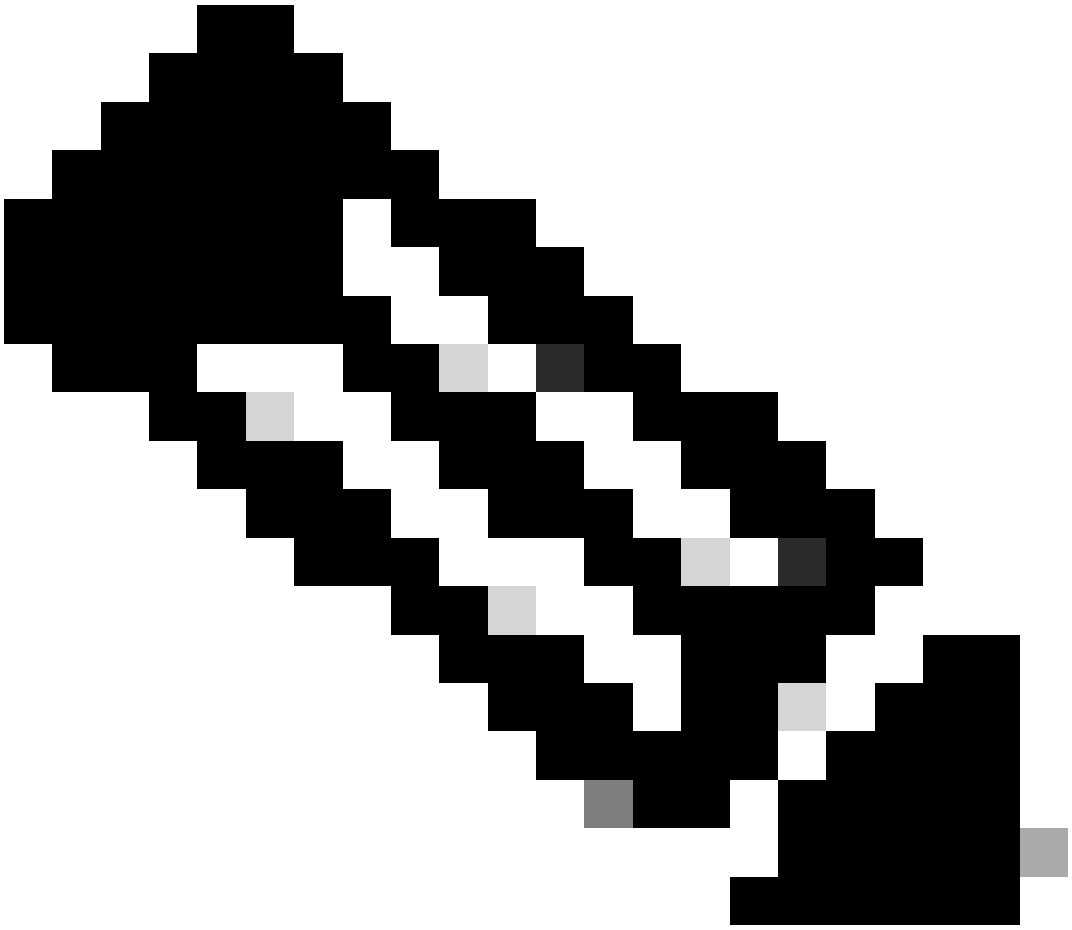
2. Agregue la URL en el área apropiada para conectarse con Umbrella.

Las instrucciones exactas varían y Umbrella sugiere ponerse en contacto con el soporte de ThreatConnect si no está seguro de cómo o dónde configurar las integraciones de API en ThreatConnect.

Observación de eventos agregados a la categoría de seguridad de ThreatConnect en modo auditoría

Con el tiempo, los eventos del panel de ThreatConnect pueden empezar a rellenar una lista de destinos específica que se puede aplicar a las políticas como una categoría de seguridad de

ThreatConnect. De forma predeterminada, la lista de destinos y la categoría de seguridad se encuentran en modo Auditoría, lo que significa que no se aplican a las políticas y no provocan ningún cambio en las políticas de Umbrella existentes.



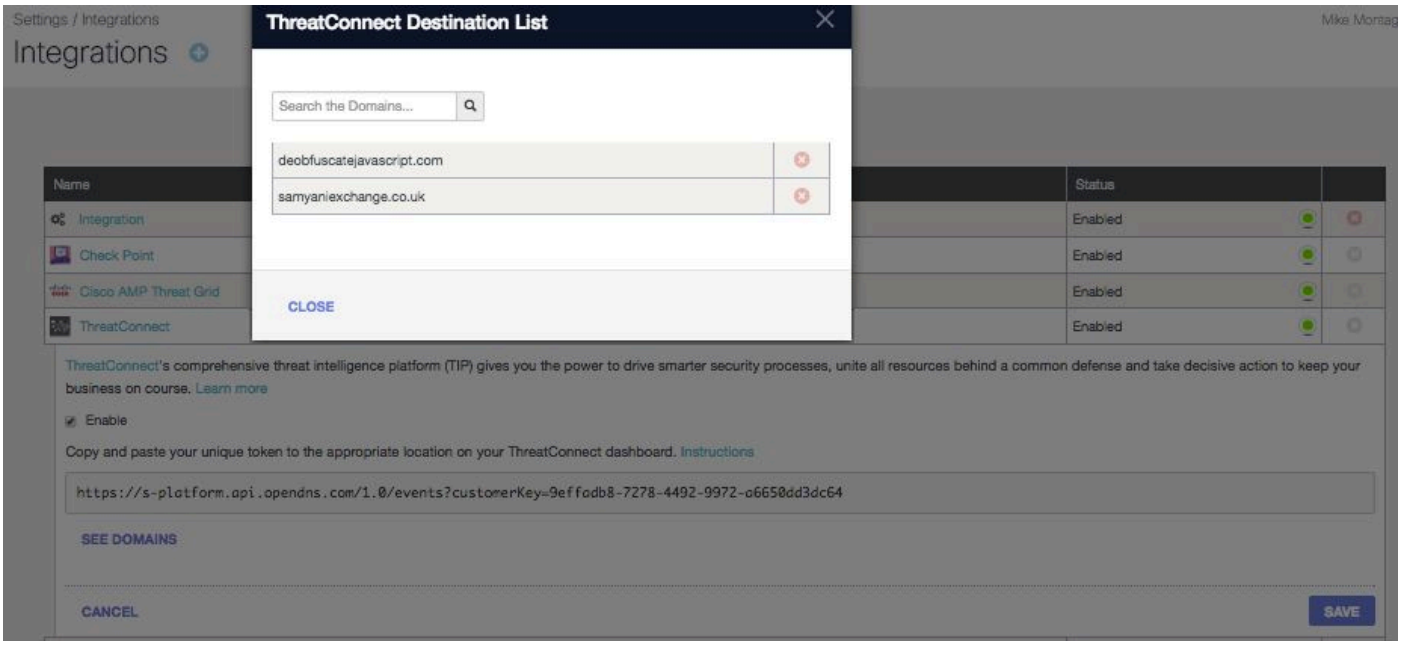
> Nota: El modo de auditoría se puede activar durante el tiempo que sea necesario en función del perfil de implementación y la configuración de red.

Revisar lista de destinos

Puede revisar la lista de destinos de ThreatConnect en Umbrella en cualquier momento:

1. En el panel de Umbrella, navegue hasta Políticas > Integraciones.

2. En la tabla, expanda ThreatConnect y seleccione Ver dominios.



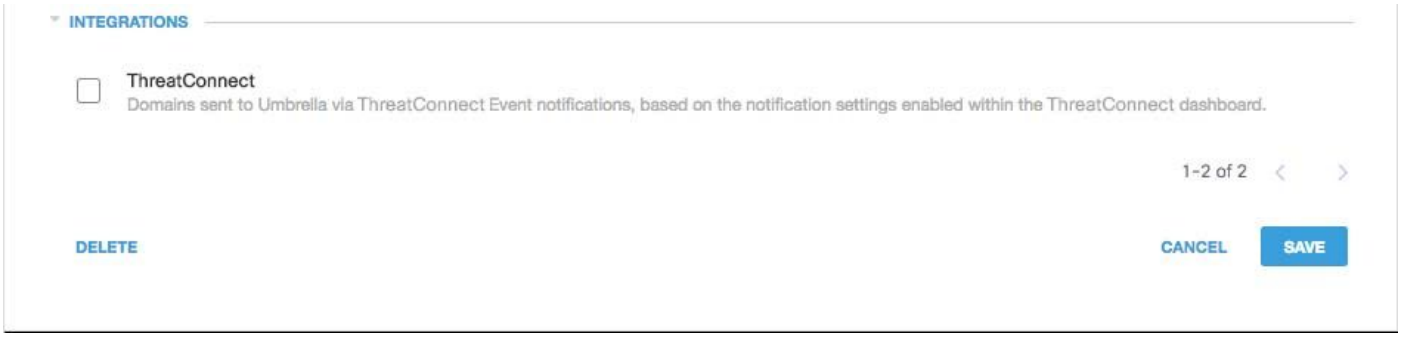
Revisar la configuración de seguridad de una directiva

Puede revisar la configuración de seguridad que se puede habilitar para una directiva en cualquier momento:

1. En el panel de Umbrella, navegue hasta Políticas > Configuración de seguridad.

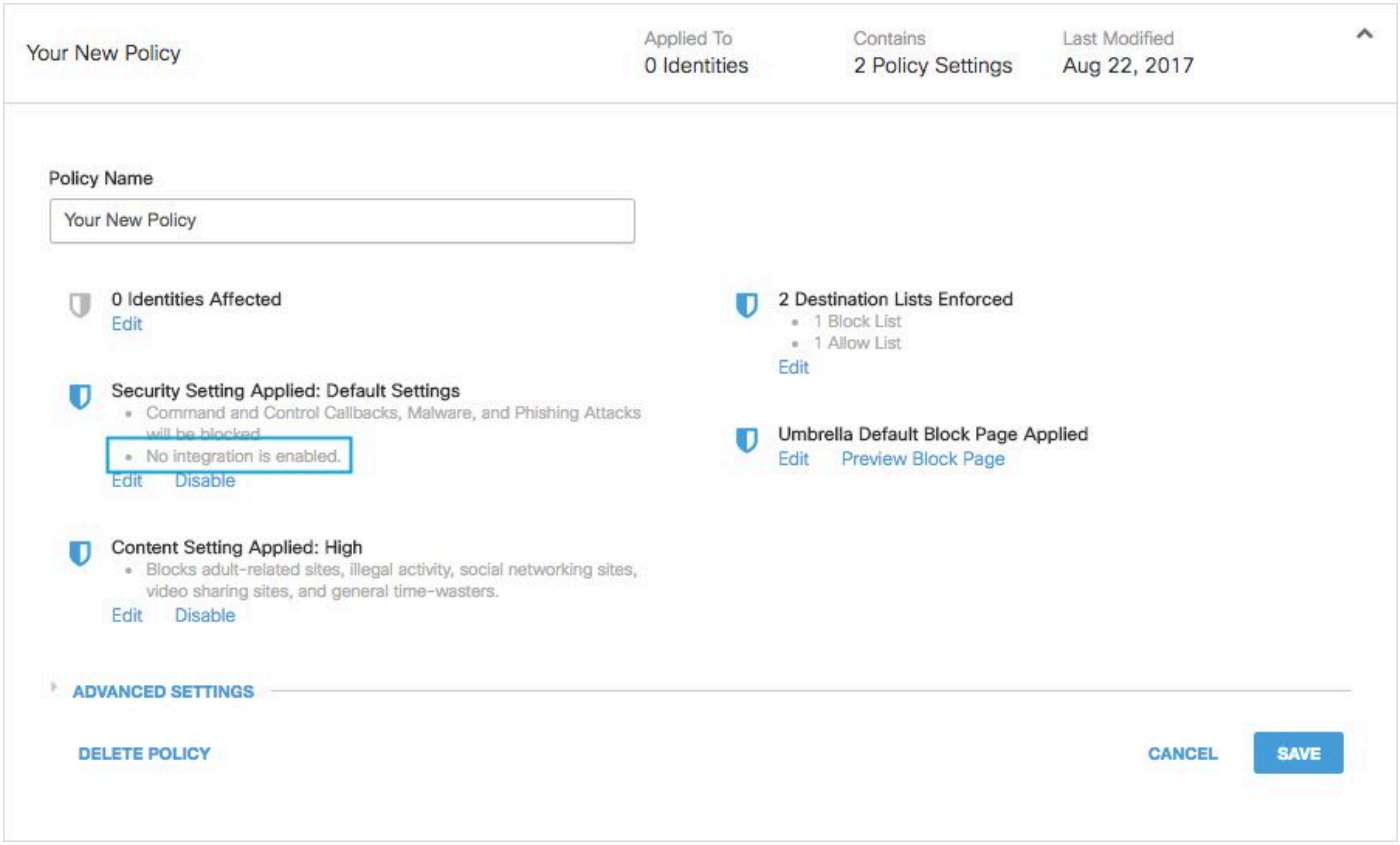
2. Seleccione una configuración de seguridad en la tabla para expandirla.

3. Desplácese hasta Integraciones para localizar el parámetro ThreatConnect.



115014036566

4. También puede revisar la información de integración en la página Resumen de Valores de Seguridad.



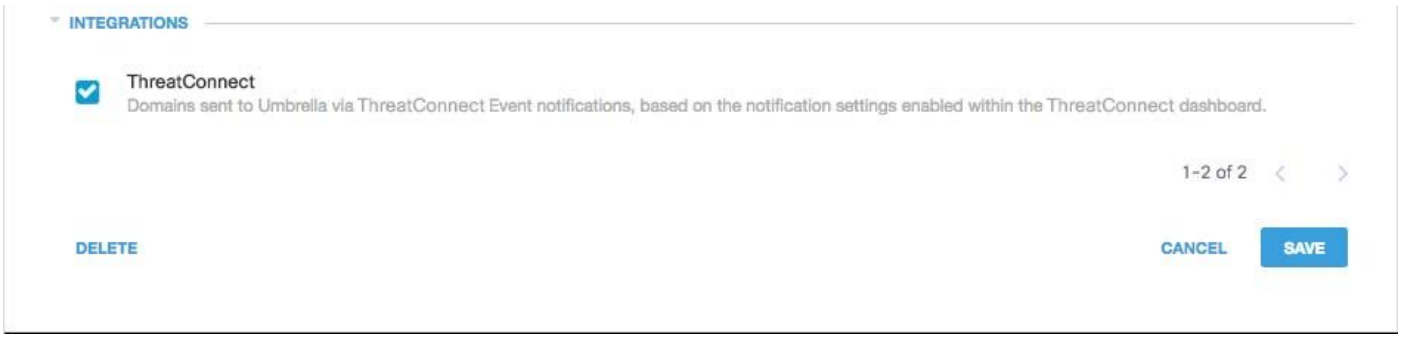
25464103885972

Aplicación de la configuración de seguridad de ThreatConnect en modo de bloqueo a una política para clientes gestionados

Una vez que esté listo para que los clientes administrados por Umbrella apliquen estas amenazas de seguridad adicionales, simplemente cambie la configuración de seguridad de una política existente o cree una nueva política que se sitúe por encima de la política predeterminada para asegurarse de que se aplica en primer lugar:

1. Vaya a Políticas > Configuración de seguridad.

2. En Integraciones, seleccione ThreatConnect y, a continuación, seleccione Guardar.



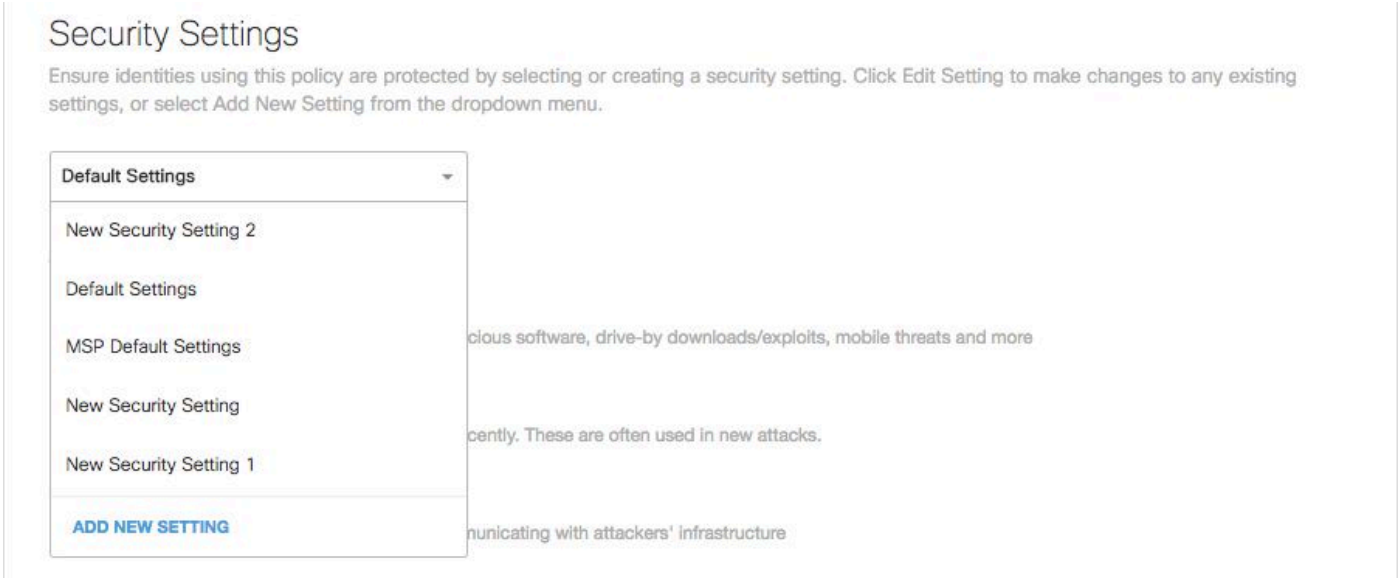
115014203703

A continuación, en el Asistente para directivas, agregue una configuración de seguridad a la directiva que está editando:

1. Acceda a Políticas > Lista de Políticas.

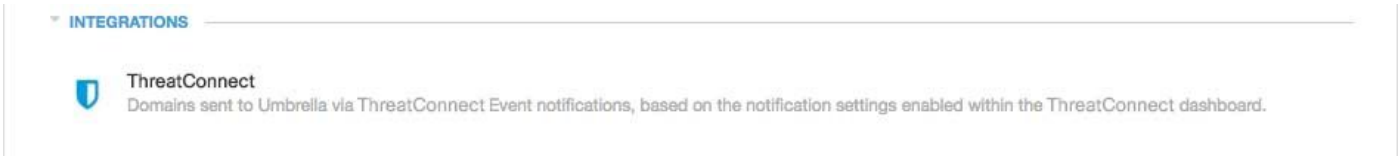
2. Expanda una directiva. En Configuración de seguridad aplicada, seleccione Editar.

3. En el menú desplegable Security Settings, seleccione una configuración de seguridad que incluya la configuración ThreatConnect.



25464103908884

El icono de escudo en Integraciones se actualiza a azul.



115014037666

4. Seleccione Establecer y devolver.

Los dominios de ThreatConnect incluidos en la configuración de seguridad de ThreatConnect se bloquean para las identidades que utilizan la directiva.

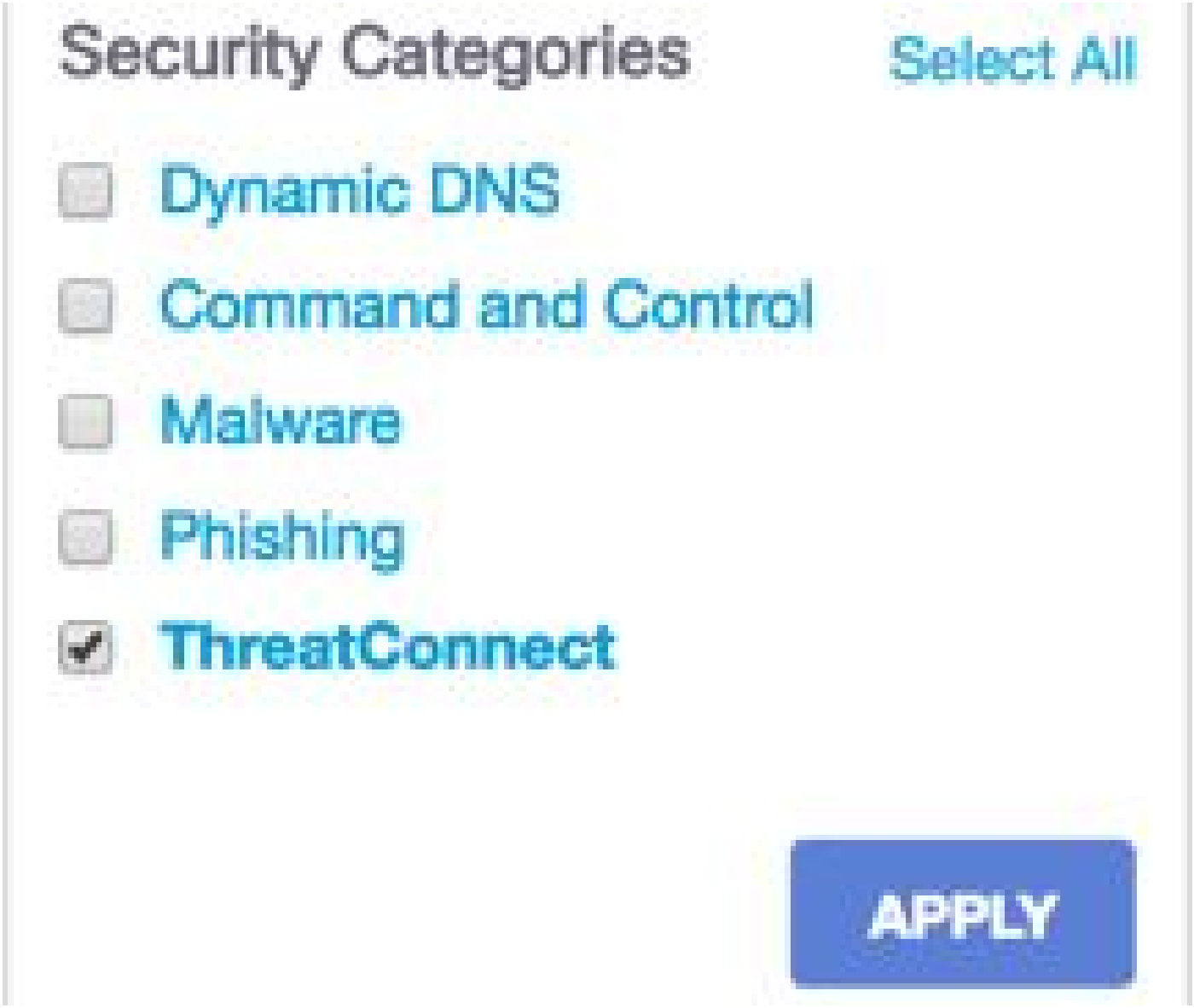
Generación de informes para los eventos de ThreatConnect

Informes sobre eventos de seguridad de ThreatConnect

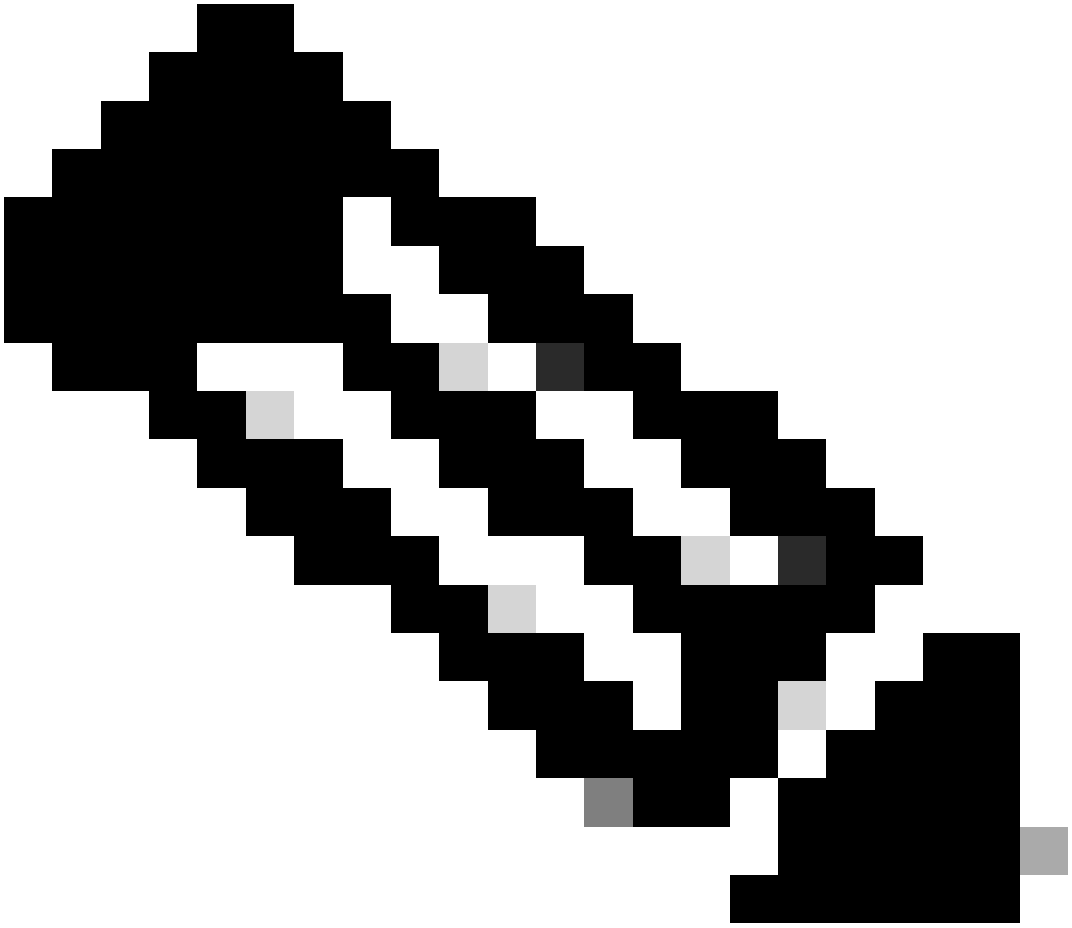
La lista de destinos de ThreatConnect es una de las listas de categorías de seguridad sobre las que puede informar. La mayoría de los informes, o todos ellos, utilizan las categorías de seguridad como filtro. Por ejemplo, puede filtrar las categorías de seguridad para mostrar solamente la actividad relacionada con ThreatConnect:

1. Vaya a Informes > Búsqueda de actividad.

2. En Categorías de seguridad, seleccione ThreatConnect para filtrar el informe y mostrar solo la categoría de seguridad de ThreatConnect.



115014206603



Nota: Si la integración de ThreatConnect está desactivada, no aparecerá en el filtro Categorías de seguridad.

3. Seleccione Aplicar.

Informes sobre cuándo se agregaron dominios a la lista de destino de ThreatConnect

El registro de auditoría de administración incluye los eventos del panel de ThreatConnect cuando agrega dominios a la lista de destino. Un usuario llamado "Cuenta de ThreatConnect", que también lleva la marca del logotipo de ThreatConnect, genera los eventos. Estos eventos incluyen el dominio que se agregó y la hora a la que se agregó.

Puede filtrar para incluir solo los cambios de ThreatConnect aplicando un filtro para el usuario "Cuenta de ThreatConnect".

Gestión de detecciones no deseadas o falsos positivos

Permitir listas

Aunque es poco probable, es posible que los dominios agregados automáticamente por ThreatConnect puedan desencadenar un bloqueo no deseado que impida a los usuarios acceder a sitios web concretos. En una situación como esta, Umbrella recomienda agregar los dominios a una lista de permitidos, que tiene prioridad sobre todos los demás tipos de listas de bloqueo, incluida la configuración de seguridad.

Hay dos razones por las que este enfoque es preferible:

- En primer lugar, en caso de que el panel de ThreatConnect vuelva a agregar el dominio después de quitarlo, la lista de permitidos protege frente a los problemas que puedan causar.
- Además, la lista de permitidos muestra un registro histórico de dominios problemáticos que se pueden utilizar para informes de diagnóstico o auditoría.

De forma predeterminada, existe una lista global de permitidos que se aplica a todas las políticas. Al agregar un dominio a la lista global de permitidos, el dominio se permite en todas las directivas.

Si la configuración de seguridad de ThreatConnect en modo de bloqueo sólo se aplica a un subconjunto de las identidades de Umbrella administradas (por ejemplo, solo se aplica a equipos móviles y a dispositivos móviles móviles), puede crear una lista de permitidos específica para esas identidades o políticas.

Para crear una lista de permitidos:

1. Navegue hasta Políticas > Listas de Destino y seleccione el icono Agregar (+).

2. Seleccione Permitir y agregue su dominio a la lista.

3. Seleccione Guardar.

Una vez guardada la lista de destinos, puede agregarla a una directiva existente que cubra los clientes afectados por el bloqueo no deseado.

Eliminación de dominios de la lista de destino de ThreatConnect

Junto a cada nombre de dominio de la lista de destino de ThreatConnect hay un icono Delete. La eliminación de dominios le permite limpiar la lista de destino de ThreatConnect en caso de que se produzca una detección no deseada. Sin embargo, la eliminación no es permanente si el panel de ThreatConnect vuelve a enviar el dominio a Umbrella.

Para eliminar un dominio:

1. Acceda a Políticas > Integraciones.

2. Seleccione ThreatConnect para expandirlo.

3. Seleccione Consulte Dominios.

4. Busque el nombre de dominio que desea eliminar.

5. Seleccione el icono Suprimir.

6. Seleccione Cerrar y, a continuación, Guardar.

En el caso de una detección no deseada o un falso positivo, Umbrella recomienda crear una lista de permitidos en Umbrella inmediatamente y, a continuación, remediar el falso positivo en el panel de ThreatConnect. Posteriormente, puede quitar el dominio de la lista de destinos de ThreatConnect.

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).