Integre ThreatQ con Umbrella

Contenido

Introducción

Este documento describe cómo integrar ThreatQ con Cisco Umbrella.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

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

Componentes Utilizados

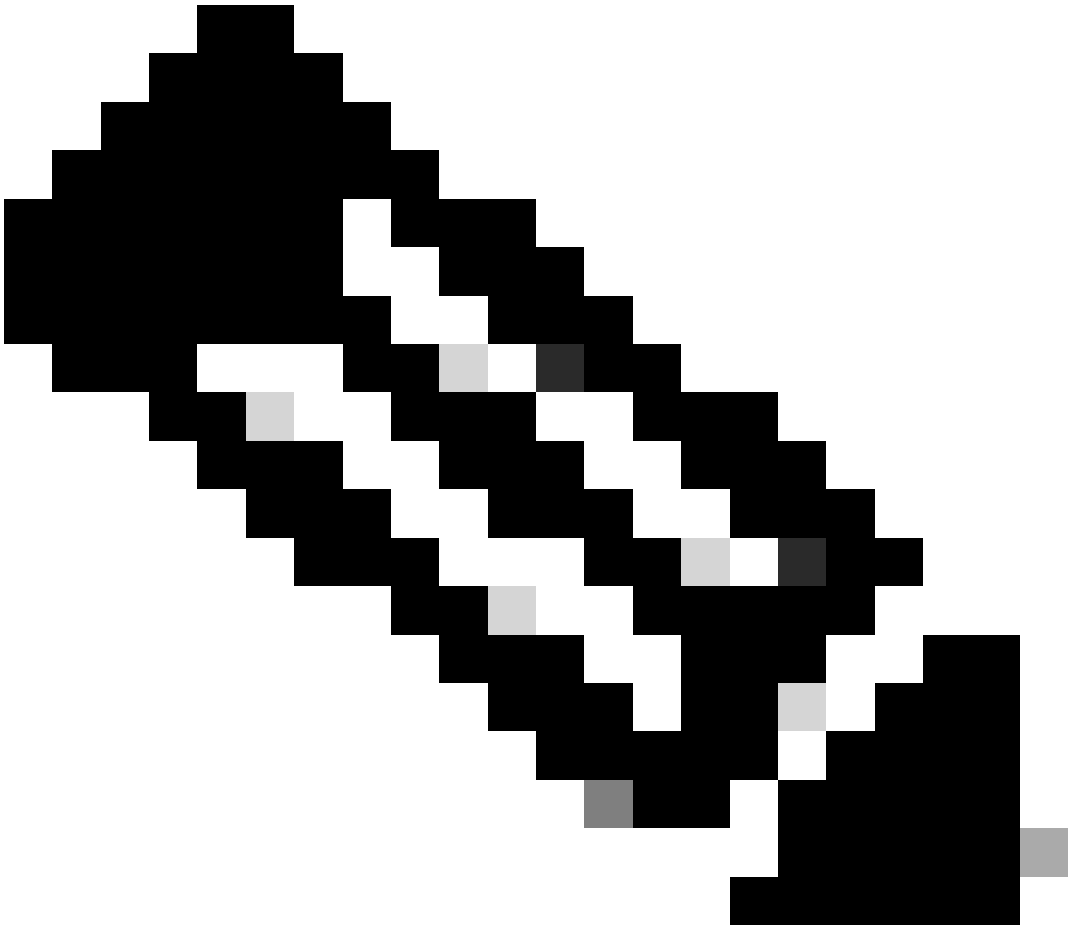
La información de este documento se basa en Cisco Umbrella.

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 la integración de ThreatQ y Cisco Umbrella

Al integrar ThreatQ con Cisco Umbrella, los responsables de seguridad y los administradores ahora pueden 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 ThreatQ para comunicarse con Umbrella de modo que los eventos de seguridad del TIP de ThreatQ se integren en las políticas que se pueden aplicar a los clientes protegidos por Cisco Umbrella.



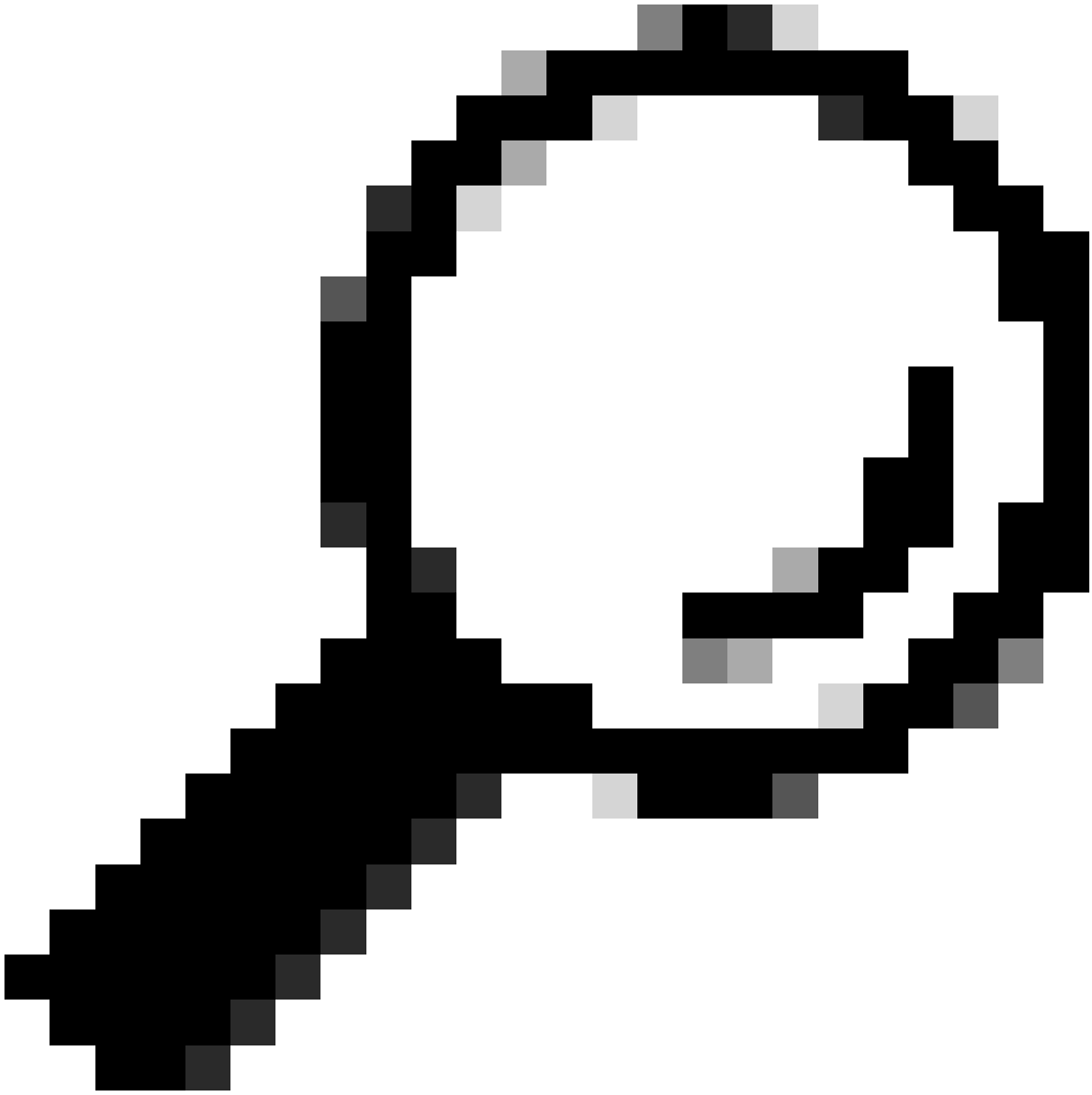
Nota: La integración de ThreatQ solo se incluye en determinados paquetes de Cisco Umbrella. Si no tiene el paquete necesario y desea la integración de ThreatQ, póngase en contacto con su representante de Cisco Umbrella. Si tiene el paquete Cisco Umbrella correcto pero no ve ThreatQ como una integración para su panel, póngase en contacto con el servicio de asistencia de Cisco Umbrella.

Funcionalidad de integración

La plataforma ThreatQ envía primero 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 ThreatQ es una amenaza, la dirección de dominio se agrega a la lista de destino de ThreatQ 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 ThreatQ.

De ahora en adelante, Umbrella analiza automáticamente las alertas de ThreatQ y agrega sitios malintencionados a la lista de destino de ThreatQ. Esto amplía la protección de ThreatQ a todos los usuarios y dispositivos remotos y proporciona otra capa de aplicación para su red corporativa.



Consejo: Aunque Cisco 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, le sugerimos que agregue dominios que nunca desee bloquear 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
- Dominios que representan los servicios proporcionados que pueden tener registros internos y externos. Por ejemplo, "mail.myservicedomain.com" y "portal.myotherservicedomain.com".
- Aplicaciones basadas en la nube menos conocidas de las que depende que Cisco Umbrella no incluya en la validación automática de dominios. Por ejemplo, "localcloudservice.com".

Estos dominios se pueden agregar a la Lista global de permitidos, que se encuentra en

Políticas > Listas de destino en Cisco Umbrella.

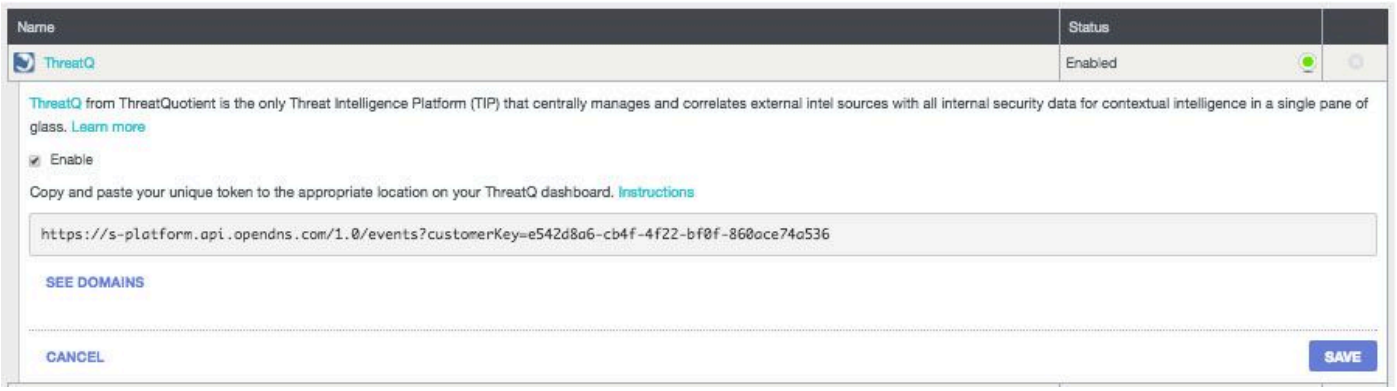
Generación de Umbrella Script y API Token

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. Navegue hasta Configuraciones > Integraciones y seleccione ThreatQ en la tabla para expandirla.

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



Necesita la URL más adelante cuando esté configurando ThreatQ para enviar datos a Umbrella, así que copie la URL y vaya a su panel de ThreatQ.

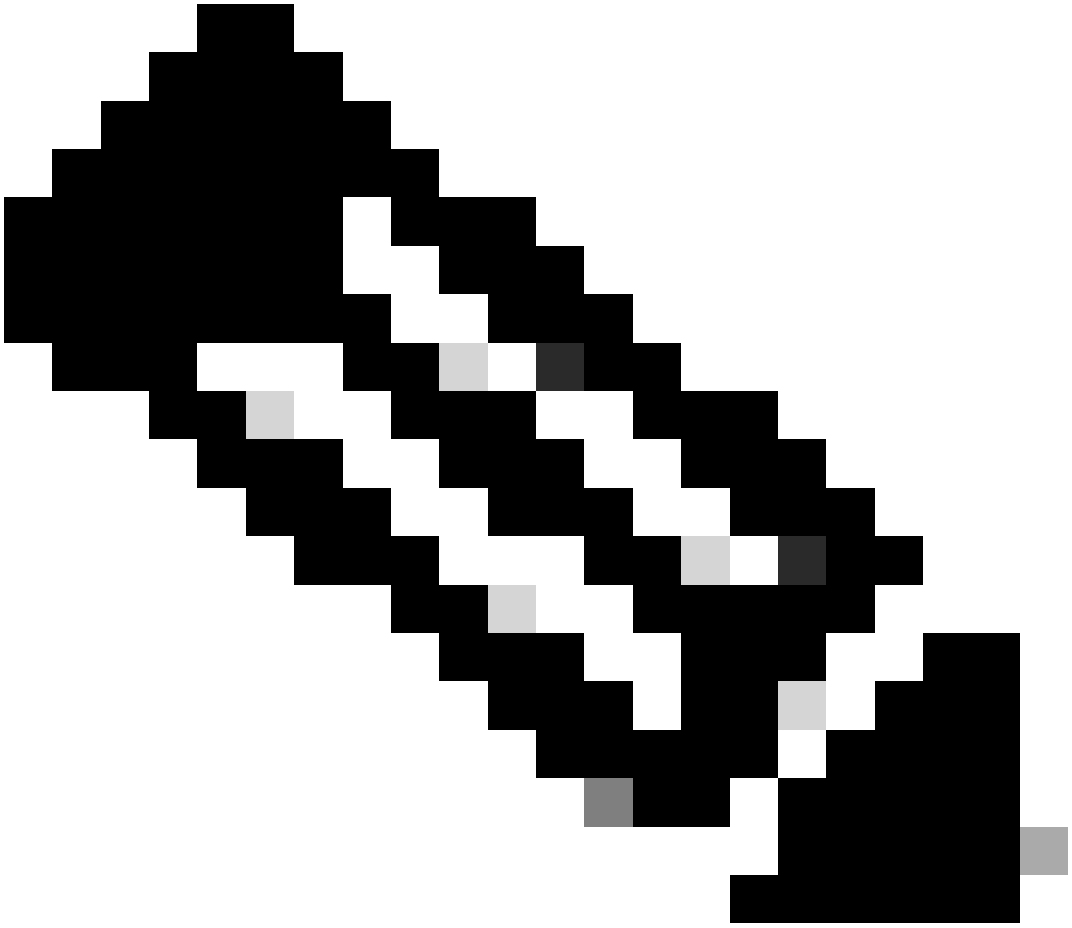
Cómo configurar ThreatQ para que se comunique con Umbrella

Inicie sesión en el panel de ThreatQ y agregue la URL en el área adecuada para conectarse a Umbrella.

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

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

Con el tiempo, los eventos del panel de ThreatQ comienzan a rellenar una lista de destinos específica que se puede aplicar a las políticas como categoría de seguridad de ThreatQ. 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 ninguna política y no pueden dar lugar a ningún cambio en las políticas de Umbrella existentes.



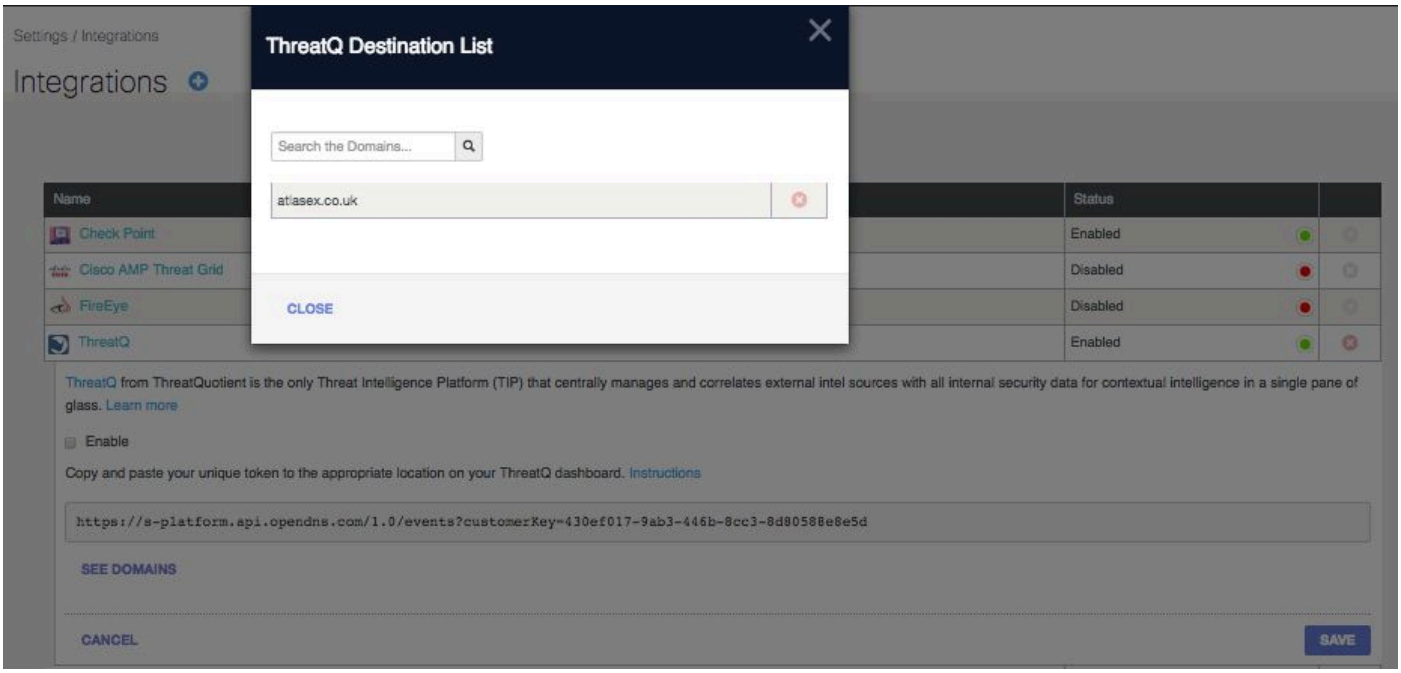
Nota: El modo de auditoría se puede activar durante el tiempo que sea necesario en función del perfil de implementación y la configuración de red.

Revisar lista de destinos

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

1. Navegue hasta Configuraciones > Integraciones.

2. Expanda ThreatQ en la tabla y seleccione Ver dominios.



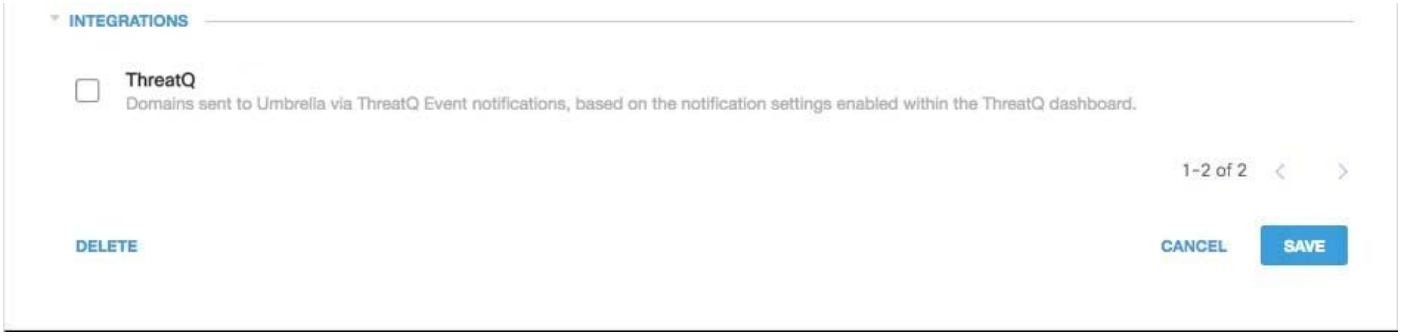
Revisar la configuración de seguridad de una directiva

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

1. Vaya a Políticas > Configuración de seguridad.

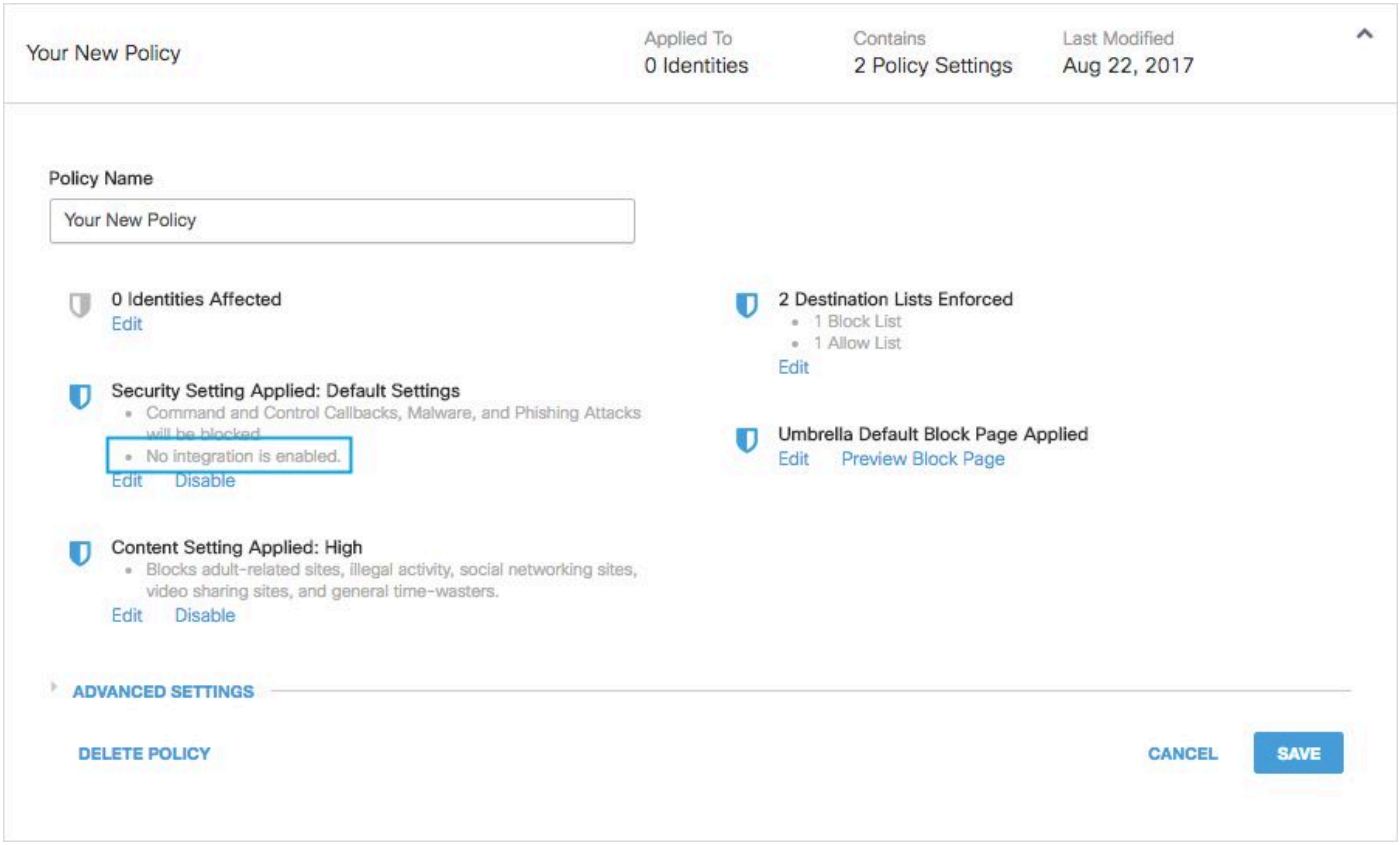
2. Seleccione una configuración de seguridad en la tabla para expandirla.

3. Desplácese hasta Integraciones para localizar el parámetro ThreatQ.



115014040286

También puede revisar la información de integración a través de la página Resumen de parámetros de seguridad.



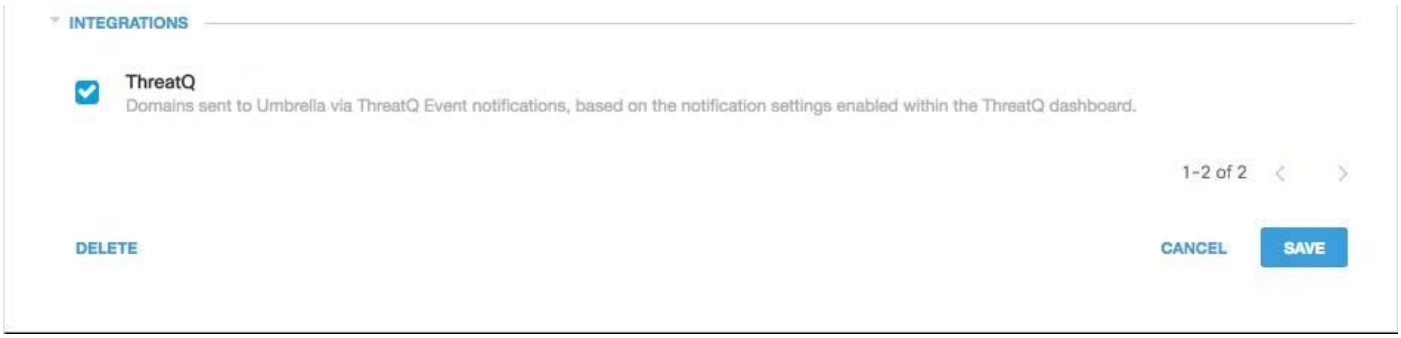
25464141748116

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

Una vez que esté listo para que los clientes que administra Umbrella apliquen estas amenazas de seguridad adicionales, puede cambiar la configuración de seguridad de una directiva existente o crear una nueva directiva superior a la predeterminada para asegurarse de que se aplica primero:

1. Vaya a Políticas > Configuración de seguridad.

2. En Integraciones, seleccione ThreatQ y Guardar.



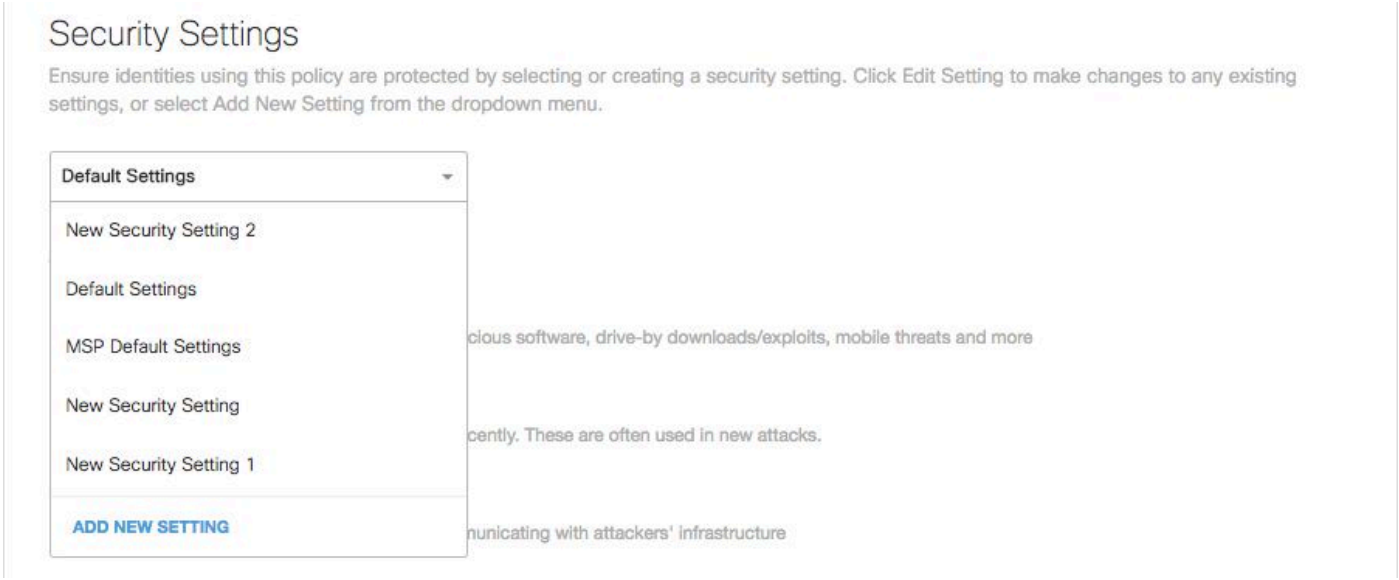
115014207403

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.

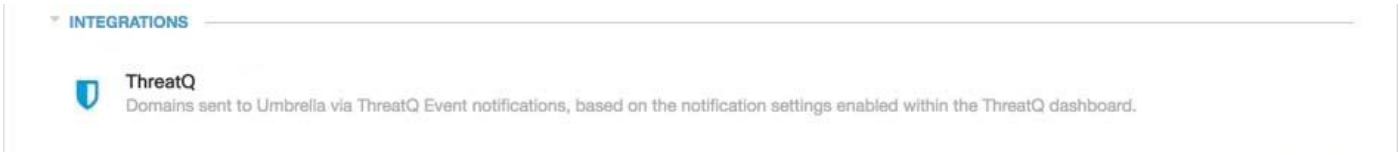
2. Expanda una política y seleccione Editar en Configuración de Seguridad Aplicada.

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



25464141787668

El icono de escudo de Integraciones se actualiza a azul.



115014040506

4. Seleccione Establecer y devolver.

Los dominios ThreatQ incluidos en la configuración de seguridad de ThreatQ se bloquean ahora para las identidades que utilizan la política.

Generación de informes para los eventos de ThreatQ

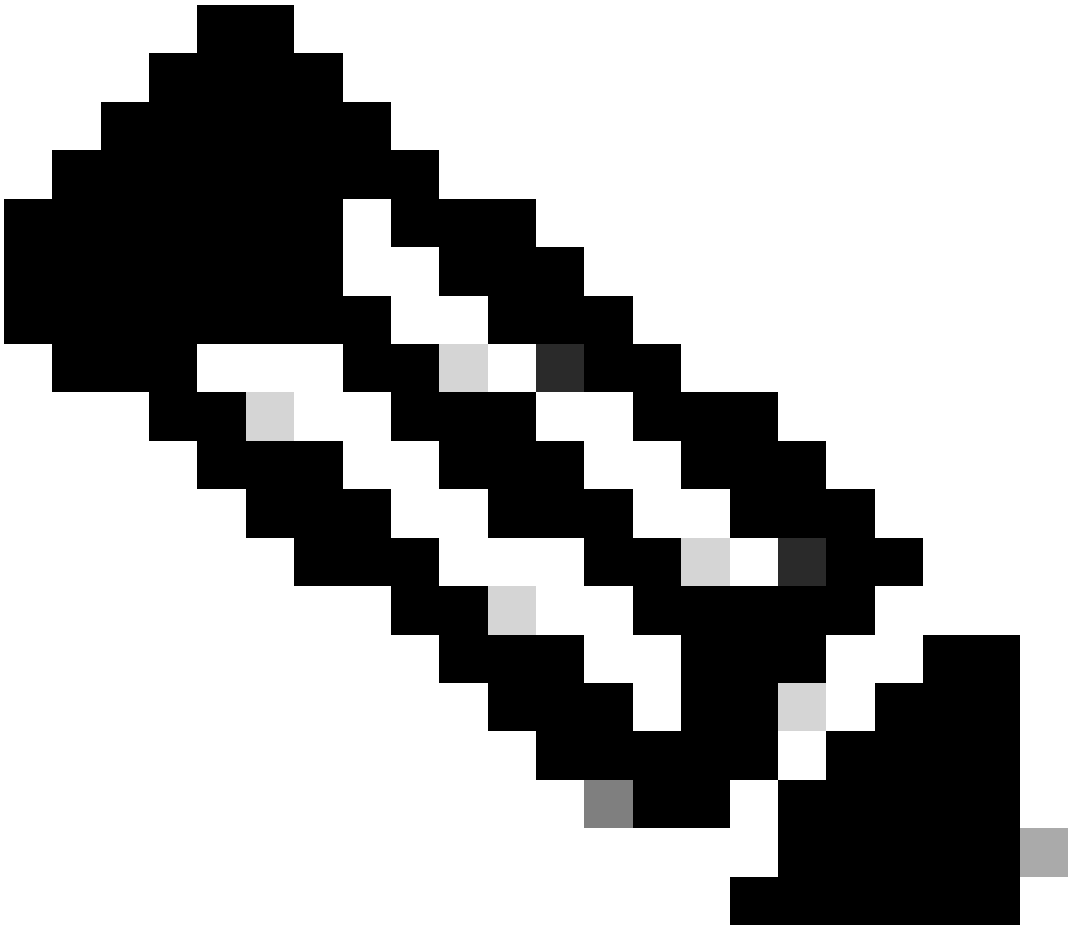
Informes sobre eventos de seguridad de ThreatQ

La lista de destinos de ThreatQ 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 ThreatQ.

1. Vaya a Informes > Búsqueda de actividad.

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

categoría de seguridad de ThreatQ.



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

115014207603

3. Seleccione Aplicar.

Informes sobre la adición de dominios a la lista de destinos de ThreatQ

El registro Umbrella Admin Audit incluye eventos del panel de ThreatQ a medida que agrega dominios a la lista de destino. Un usuario llamado "Cuenta ThreatQ", que también lleva el logotipo de ThreatQ, genera los eventos. Estos eventos incluyen el dominio que se agregó y la hora a la que se agregó. El registro Umbrella Admin Audit se puede encontrar en Reporting > Admin Audit Log.

Puede filtrar para incluir solo los cambios de ThreatQ aplicando un filtro para el usuario de la cuenta ThreatQ.

Gestión de detecciones no deseadas o falsos positivos

Permitir listas

Aunque es poco probable, es posible que los dominios agregados automáticamente por ThreatQ puedan activar un bloqueo no deseado que pueda impedir que los usuarios accedan a determinados sitios web. 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 ThreatQ tuviera que volver a agregar el dominio después de quitarlo, la lista de permitidos protege frente a los problemas que puedan causar.
- En segundo lugar, 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 ThreatQ en modo de bloqueo sólo se aplica a un subconjunto de las identidades de Umbrella administradas (por ejemplo, sólo 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 ThreatQ

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

Para eliminar un dominio:

1. Navegue hasta Configuraciones > Integraciones, luego seleccione ThreatQ para expandirlo.

2. Seleccione Consulte Dominios.

3. Busque el nombre de dominio que desea eliminar.

4. Seleccione el icono Suprimir.

5. Seleccione Cerrar.

6. Seleccione 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 ThreatQ. Posteriormente, puede eliminar el dominio de la lista de destinos de ThreatQ.

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).