Integrar ZeroFOX con Umbrella

Contenido

Introducción

Este documento describe cómo integrar ZeroFOX Enterprise con Umbrella para que los eventos de seguridad puedan aplicarse a los clientes protegidos por Umbrella.

Descripción general de la integración de ZeroFOX Enterprise y Cisco Umbrella

Al integrar ZeroFOX Enterprise con Cisco Umbrella, los responsables de seguridad y los administradores pueden ampliar la protección frente a las amenazas actuales de las redes sociales a los portátiles, tablets o teléfonos en roaming, a la vez que proporcionan otro nivel de aplicación a una red corporativa distribuida.

Integración de Cisco Umbrella y ZeroFox: ¿Cómo funciona?

ZeroFOX Enterprise envía las amenazas que encuentra, como las amenazas cibernéticas basadas en redes sociales, incluido el malware selectivo, la suplantación de identidad (phishing), la ingeniería social, las suplantaciones y otras actividades fraudulentas o maliciosas a Cisco

Umbrella para su aplicación global.

A continuación, Umbrella valida la amenaza para garantizar que se pueda agregar a una política. Si se confirma que la información de ZeroFOX es una amenaza, la dirección de dominio se agrega a la lista de destino de ZeroFOX como parte de una configuración de seguridad que se puede aplicar a cualquier política de Umbrella. Esa política se aplica inmediatamente a cualquier solicitud realizada desde dispositivos asignados a esa política.

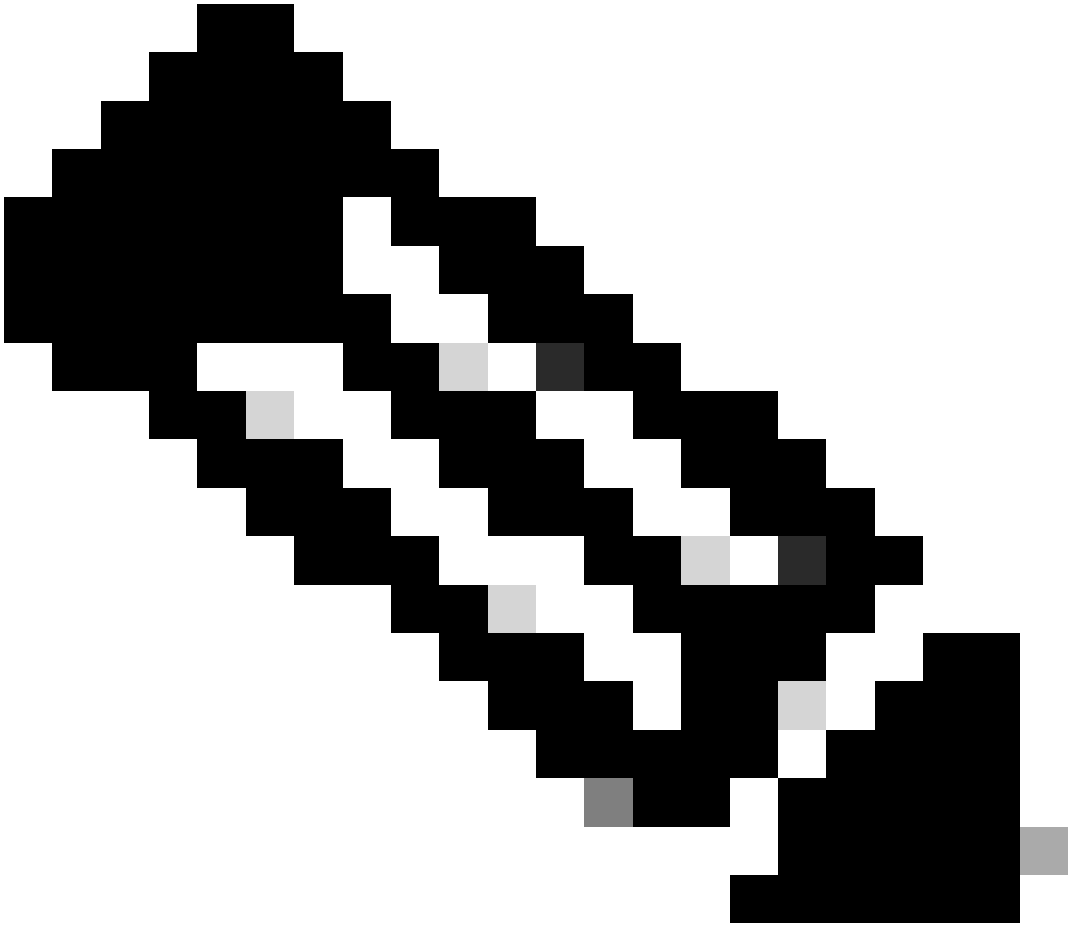
De cara al futuro, Cisco Umbrella analiza automáticamente las alertas de ZeroFOX y agrega sitios maliciosos a la lista de destino de ZeroFOX, ampliando la inteligencia de ZeroFOX a todos los usuarios y dispositivos remotos y proporcionando otra capa de aplicación a su red corporativa.

Esto se consigue mediante estos sencillos pasos de configuración:

1. Habilite la integración en Umbrella para generar un token de API.
2. Pegue ese token API en su cuenta ZeroFOX.
3. Establezca ZeroFOX para bloquear en la configuración de seguridad de las políticas deseadas

Prerequisites

- Derechos administrativos de ZeroFOX Enterprise
- Derechos administrativos del panel general
- El panel de Umbrella debe tener habilitada la integración de ZeroFOX



Nota: La integración de ZeroFOX solo se incluye en el paquete de la Plataforma de Umbrella. Si no tiene el paquete de la plataforma y le gustaría tener integración con ZeroFOX, póngase en contacto con su representante de Cisco Umbrella. Si tiene el paquete de la plataforma pero no ve ZeroFOX como una integración para su panel, por favor comuníquese con Soporte de Umbrella.

Importante: 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 cualquier interrupción no deseada, le sugerimos que agregue los dominios que no 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. 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 depende en gran medida que

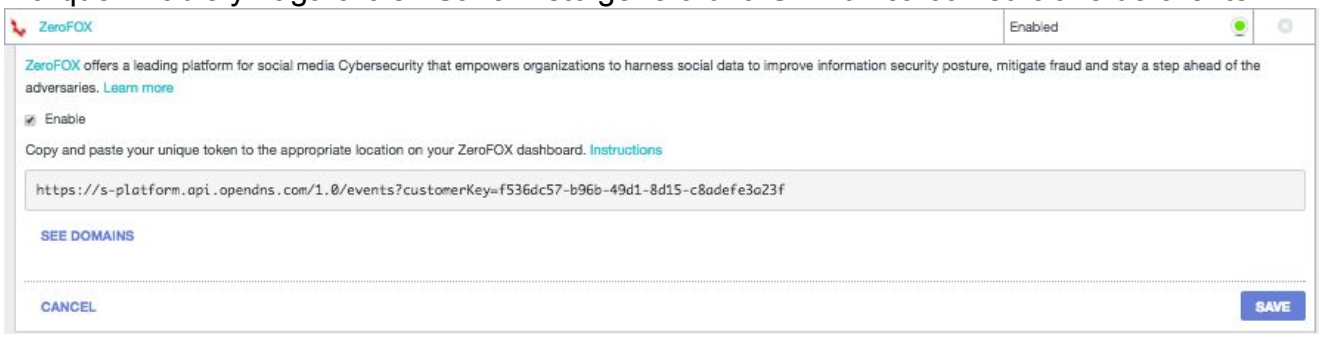
Umbrella no pueda detectar ni incluir en su validación automática de dominio. Por ejemplo, localcloudservice.com.

La Lista global de permitidos se encuentra en Políticas > Listas de Destino en Umbrella. Consulte nuestra documentación para obtener más información: Administrar listas de destino

Paso 1: Generación de Umbrella Script y API Token

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

1. Inicie sesión en el panel de Umbrella como administrador, navegue hasta Configuración > Integraciones y haga clic en "ZeroFOX" en la tabla para expandirlo.
2. Marque Enable y haga clic en Save. Esto genera una URL única con su clave de cliente.

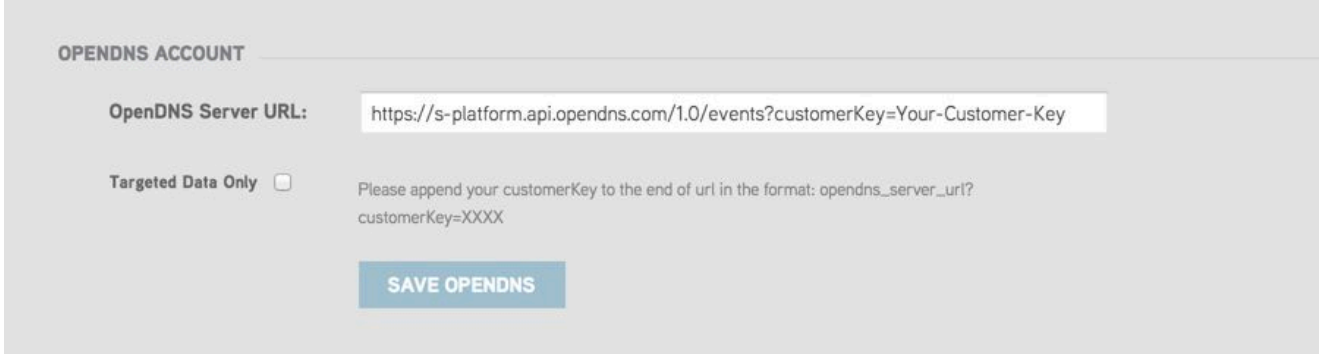


Necesitará la URL más adelante cuando esté configurando ZeroFOX, así que copie la URL y vaya a su panel de ThreatQ.

Paso 2: Configure su panel de ZeroFOX Enterprise para enviar información a Umbrella

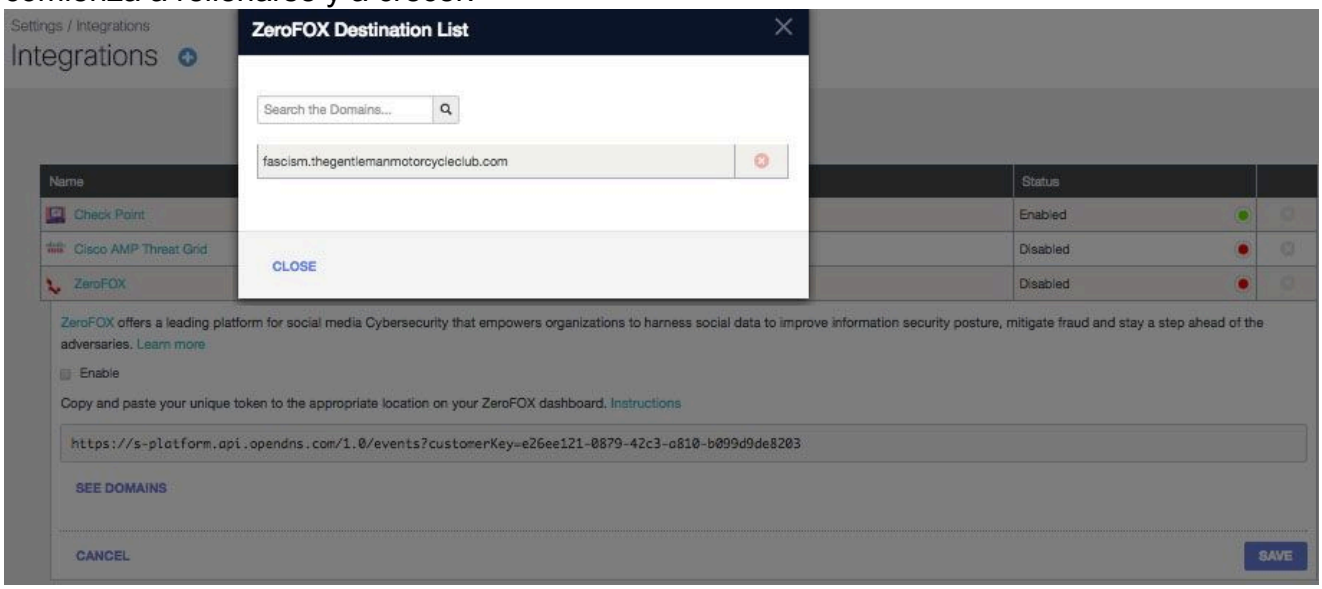
El siguiente paso es agregar la URL que copió en el paso uno al panel de ZeroFOX.

1. Haga clic en el icono de engranaje en el panel de Zerofox, luego seleccione Configuración de la cuenta.
2. Desplácese hacia abajo por la lista de integración hasta que vea la información de cuenta de OpenDNS y pegue la URL de Umbrella en el campo URL del servidor OpenDNS.
3. Tras la primera habilitación de la integración, le recomendamos que marque Solo datos objetivo.



Paso 3: Configuración de los eventos ZeroFOX que se bloquearán dentro de Umbrella

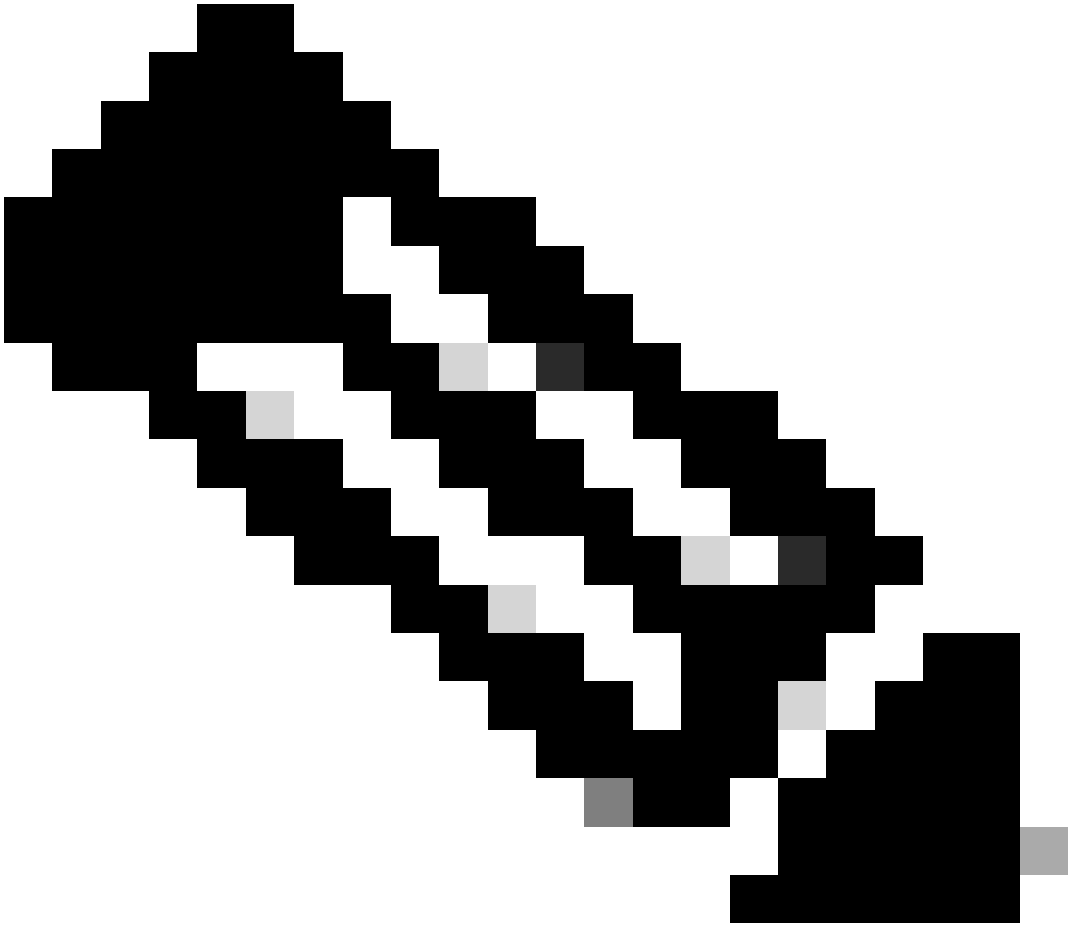
1. Vuelva a iniciar sesión en el panel de Umbrella como administrador.
2. Navegue hasta Configuraciones > Integraciones y haga clic en "ZeroFOX" en la tabla para expandirla.
3. Haga clic en Ver dominios.
   Esto expande una lista de dominios que incluye las últimas horas de eventos de su cuenta ZeroFOX. A partir de ese momento, una lista en la que se pueden realizar búsquedas comienza a rellenarse y a crecer.



El siguiente paso es observar y auditar los eventos agregados a su nueva Categoría de Seguridad ZeroFOX.

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

Los eventos de ZeroFOX Enterprise comienzan a llenar una lista de destinos específica que se puede aplicar a políticas como una categoría de seguridad ZeroFOX. De forma predeterminada, la lista de destino y la categoría de seguridad se encuentran en el modo Auditoría y no se aplican a ninguna política, por lo que no se producen cambios en las políticas generales 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 ZeroFox en cualquier momento.

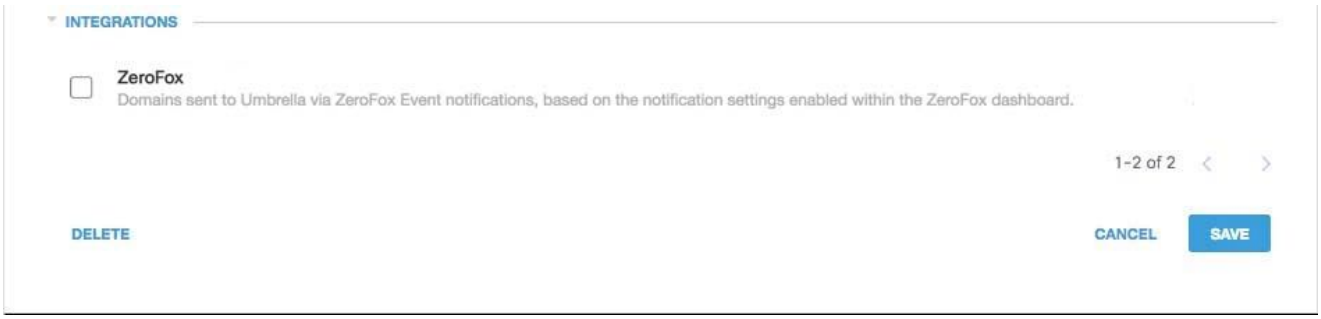
1. Vaya a Configuración > Integraciones.
2. Expanda "ZeroFOX" en la tabla y haga clic en Ver dominios.

Revisar la configuración de seguridad de una directiva

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

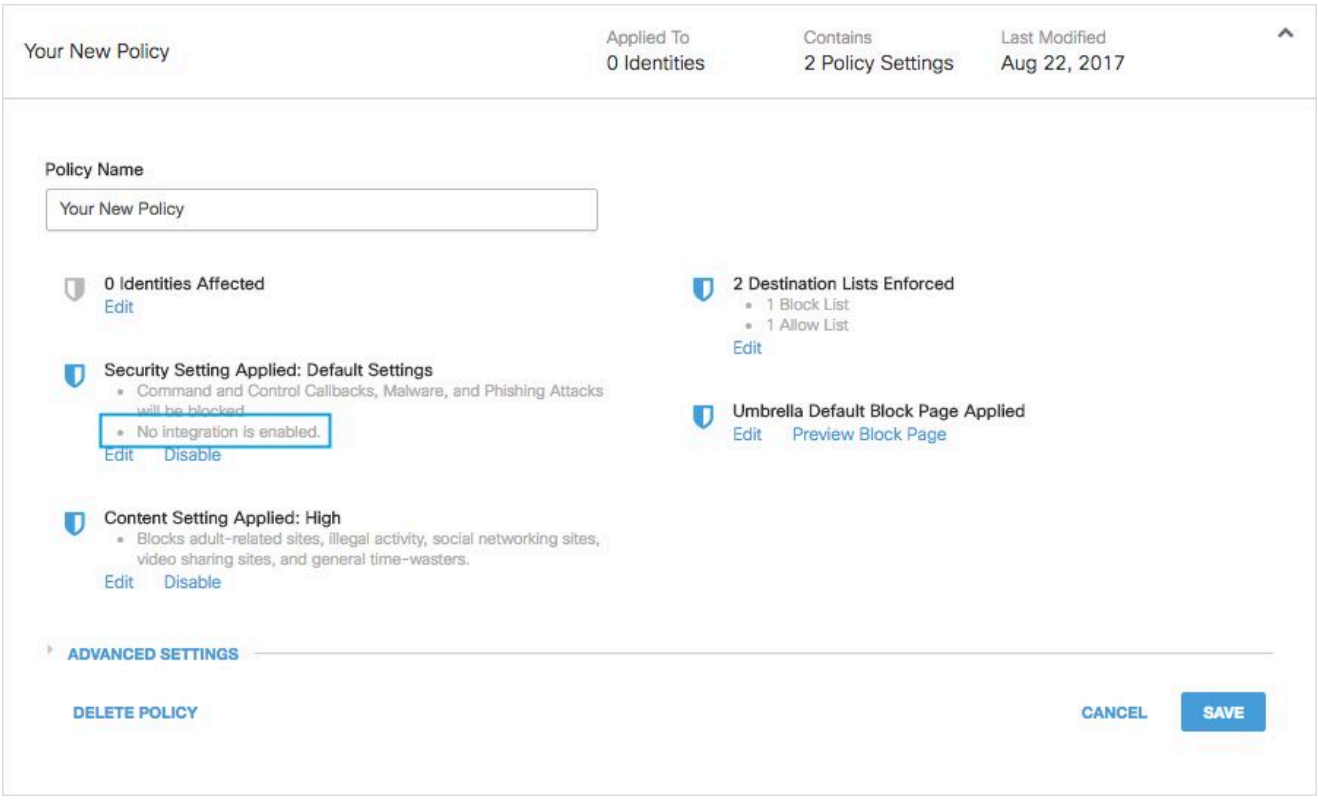
1. Vaya a Políticas > Configuración de seguridad.
2. Haga clic en una configuración de seguridad de la tabla para expandirla y desplácese hasta

Integraciones para localizar la configuración de ZeroFOX.



115014041606

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

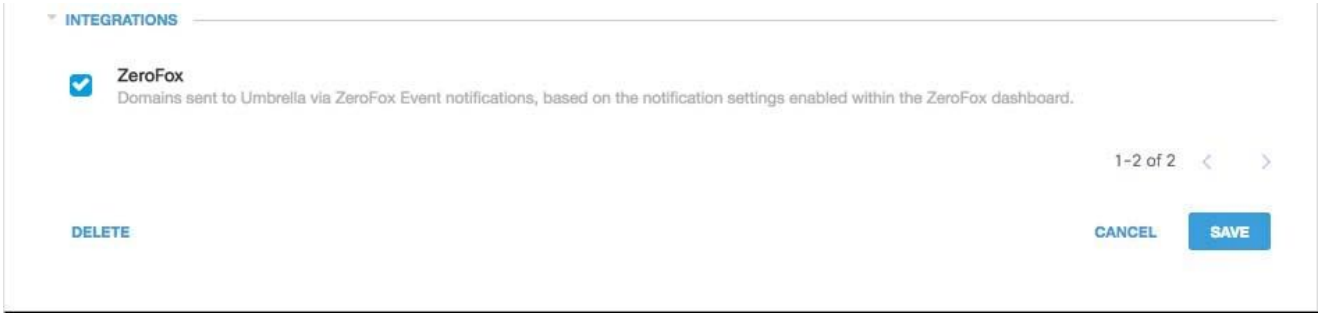


25464154913556

Aplicación de la Configuración de Seguridad ZeroFOX en Modo de Bloqueo a una Política para Clientes Administrados

Cuando esté listo para que los clientes que administra Umbrella apliquen estas amenazas de seguridad adicionales, simplemente cambie la configuración de seguridad de una directiva existente o cree una nueva directiva superior a la predeterminada para asegurarse de que se aplica en primer lugar.

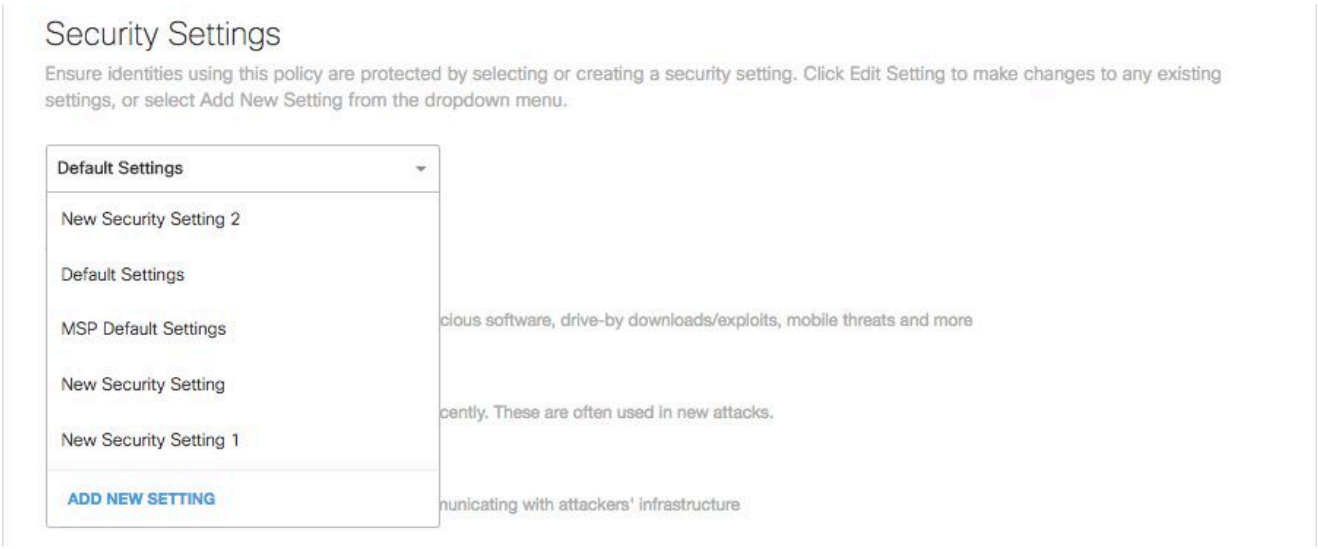
1. Navegue hasta Políticas > Configuración de seguridad y en Integraciones, marque ZeroFOX y haga clic en Guardar.



115014042806

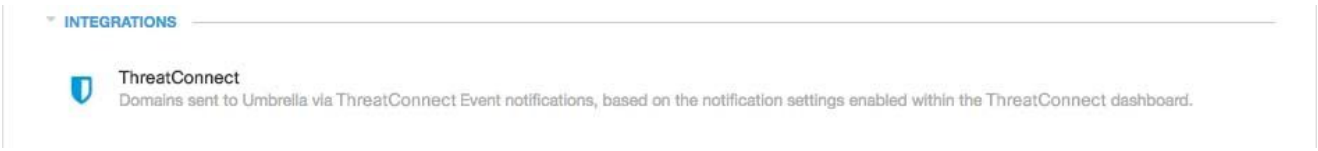
A continuación, en el Asistente para directivas, agregue una configuración de seguridad a la directiva que está editando:

1. Vaya a Políticas > Lista de políticas.
2. Expanda una directiva y haga clic en Editar en Configuración de seguridad aplicada.
3. En el menú desplegable Security Settings, seleccione una configuración de seguridad que incluya la configuración de ThreatConnect.



25464147943700

El icono de escudo en Integraciones se actualiza a azul.



25464147957652

4. Haga clic en Set & Return.

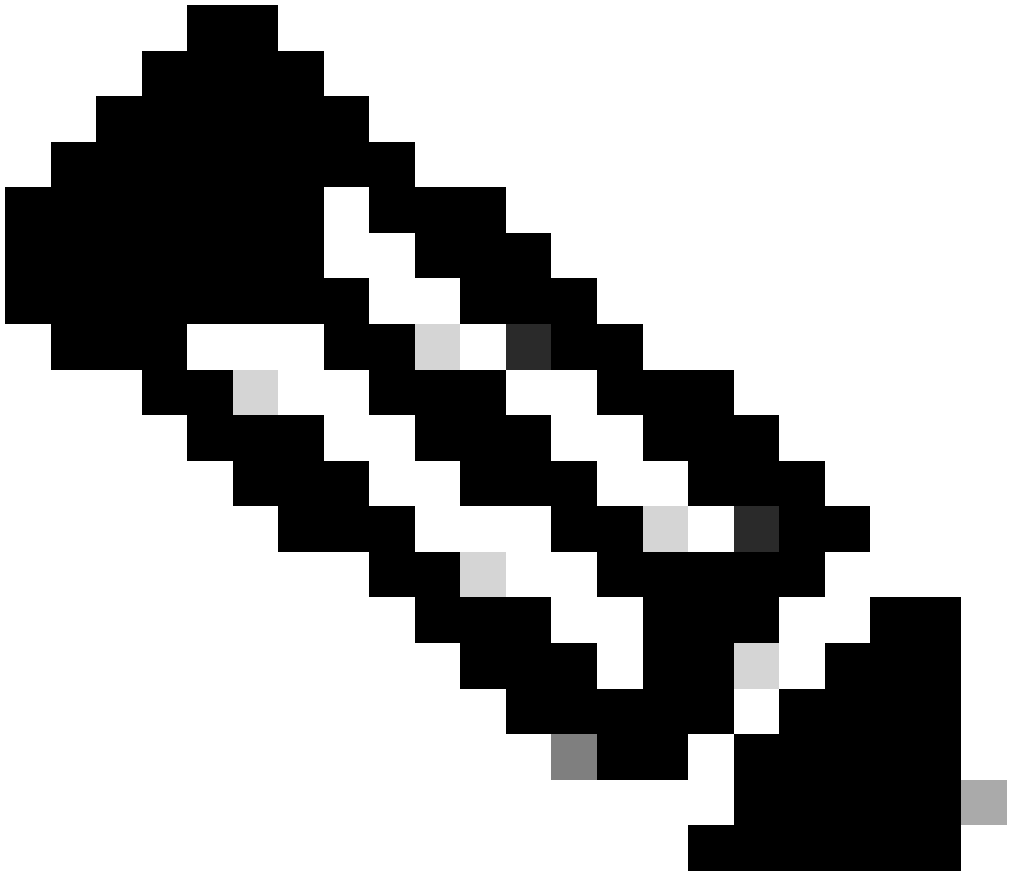
Los dominios ZeroFOX incluidos en la configuración de seguridad de ZeroFOX se bloquean para las identidades que utilizan esa política.

Generación de informes generales para eventos de ZeroFOX

Informes sobre eventos de seguridad de ZeroFOX

La lista de destino de ZeroFOX es una de las listas de categorías de seguridad sobre las que puede informar. La mayoría o la totalidad de los informes utilizan las categorías de seguridad como filtro. Por ejemplo, puede filtrar las categorías de seguridad para mostrar sólo la actividad relacionada con ZeroFOX.

1. Navegue hasta Reporting > Activity Search y en Security Categories seleccione ZeroFOX para filtrar el informe y mostrar solamente la categoría de seguridad para ZeroFOX.



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

115014043046

2. Haga clic en Apply (Aplicar).

Notificación de cuándo se agregaron los dominios a la lista de destino de ZeroFOX

El registro Umbrella Admin Audit incluye eventos de su cuenta ZeroFOX cuando agrega dominios a la lista de destino.

El registro de auditoría de administración de Umbrella se puede encontrar en Reporting > Admin Audit Log . Para informar sobre cuándo se agregó un dominio, filtre para incluir solamente los cambios de ZeroFOX aplicando un filtro a Identidades y Configuración para la Lista de Destino de ZeroFox.

Una vez que ejecute el informe, verá una lista de los cambios realizados cuando se agregó la lista de destino de ZeroFOX a desde la integración.

Gestión de detecciones no deseadas o falsos positivos

Administración de una lista de permitidos para la detección no deseada

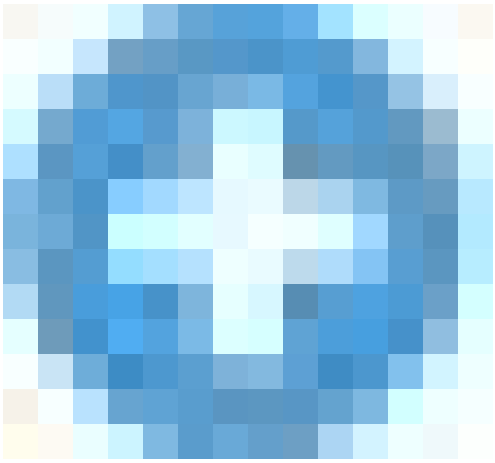
Aunque es poco probable, es posible que los dominios agregados automáticamente por ZeroFOX puedan desencadenar un bloqueo no deseado que evitaría que los usuarios accedan a sitios web particulares. En una situación como esta, se recomienda agregar los dominios a una lista de permitidos, que tiene prioridad sobre todos los demás tipos de listas de bloqueo, incluida la configuración de seguridad. Una lista de permitidos tiene prioridad sobre una lista de bloqueo cuando un dominio está presente en ambos.

Hay dos razones por las que este enfoque es preferible. En primer lugar, en caso de que el dispositivo ZeroFOX tuviera que volver a agregar el dominio después de que se haya eliminado, la lista de permitidos protege contra esto y causa más problemas. 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 ZeroFOX 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 dispositivos móviles móviles), puede crear una lista de permitidos específica para esas identidades o políticas.

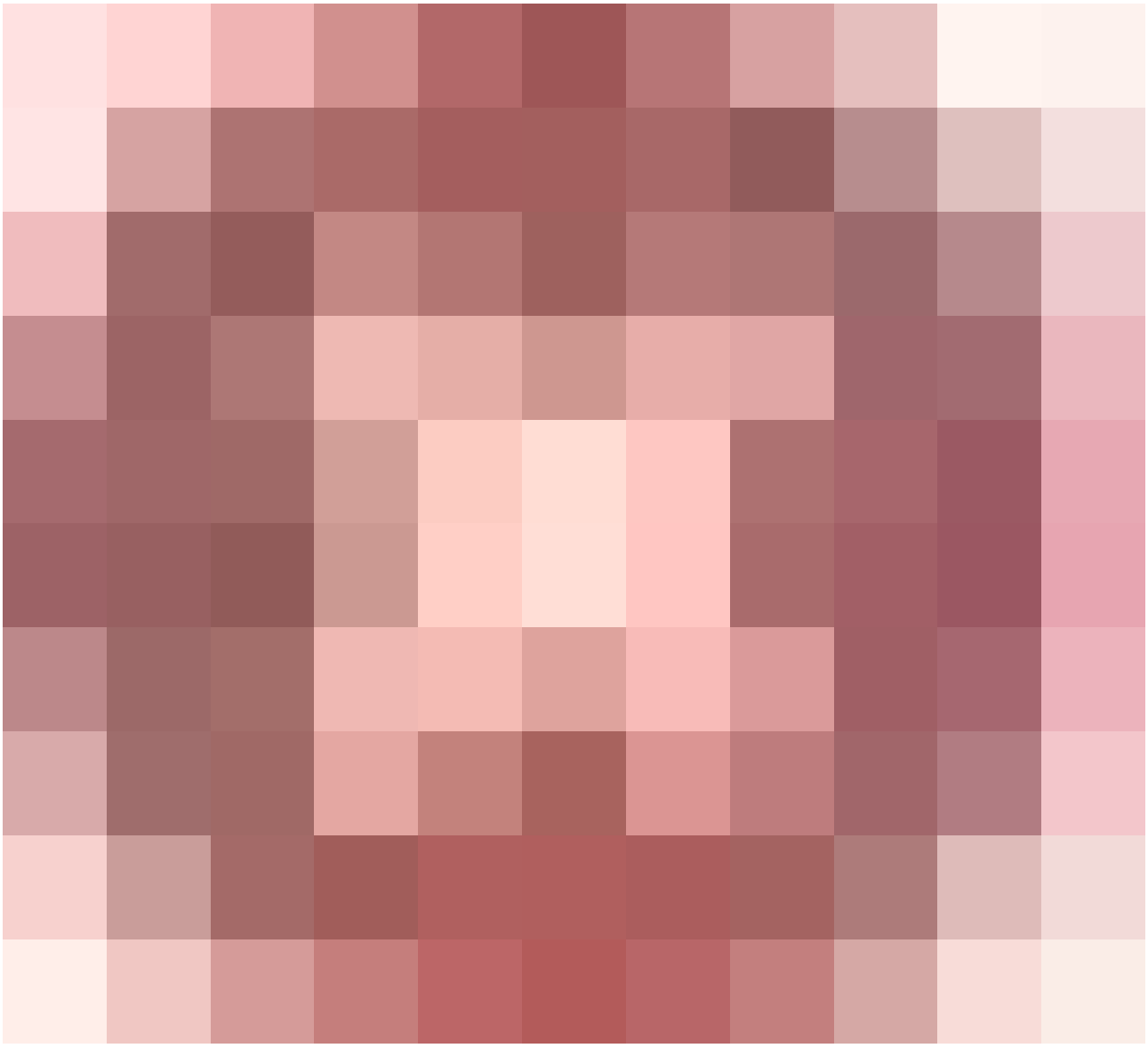
Para crear una lista de permitidos:

1. Vaya a Políticas > Listas de destino, haga clic en el botón 

   Icono Agregar.
2. Seleccione Allow y agregue su dominio a la lista.
3. Click Save.

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 ZeroFOX

Hay un  (Eliminar) junto a cada nombre de dominio de la lista de destino de ZeroFOX. La eliminación de dominios le permite limpiar la lista de destino de ZeroFOX en caso de una detección no deseada.

Sin embargo, la eliminación no es permanente si ZeroFOX vuelve a enviar el dominio a Umbrella.

Para eliminar un dominio:

1. Navegue hasta Configuraciones > Integraciones, luego haga clic en "ZeroFOX" para expandirlo.
2. Haga clic en Ver dominios.
3. Busque el nombre de dominio que desea eliminar.
4. Haga clic en el icono Delete (Eliminar).

5. Haga clic en Close (Cerrar).

6. Click Save.

En el caso de una detección no deseada o falso positivo, recomendamos crear una lista de permitidos en Umbrella inmediatamente y luego remediar el falso positivo dentro de ZeroFOX. Más adelante, puede quitar el dominio de la lista de destino de ZeroFOX.

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).