Integre o ZeroFOX ao Umbrella

Contents

Introdução

Este documento descreve como integrar o ZeroFOX Enterprise ao Umbrella para que os eventos de segurança possam ser aplicados aos clientes protegidos pelo Umbrella.

Visão geral da integração do ZeroFOX Enterprise e do Cisco Umbrella

Ao integrar o ZeroFOX Enterprise com o Cisco Umbrella, os administradores e oficiais de segurança podem ampliar a proteção contra as ameaças atuais baseadas em mídias sociais a laptops, tablets ou telefones móveis, ao mesmo tempo em que fornecem outra camada de aplicação a uma rede corporativa distribuída.

Integração do Cisco Umbrella e do ZeroFox: Como funciona?

A ZeroFOX Enterprise envia todas as ameaças encontradas, como ameaças cibernéticas baseadas em mídias sociais, incluindo malware direcionado, phishing, engenharia social, personificações e outras atividades fraudulentas ou mal-intencionadas, para o Cisco Umbrella

para aplicação global.

Em seguida, o Umbrella valida a ameaça para garantir que ela possa ser adicionada a uma política. Se as informações do ZeroFOX forem confirmadas como uma ameaça, o endereço de domínio será adicionado à lista de destino do ZeroFOX como parte de uma configuração de segurança que pode ser aplicada a qualquer política do Umbrella. Essa política é aplicada imediatamente a todas as solicitações feitas de dispositivos atribuídos a essa política.

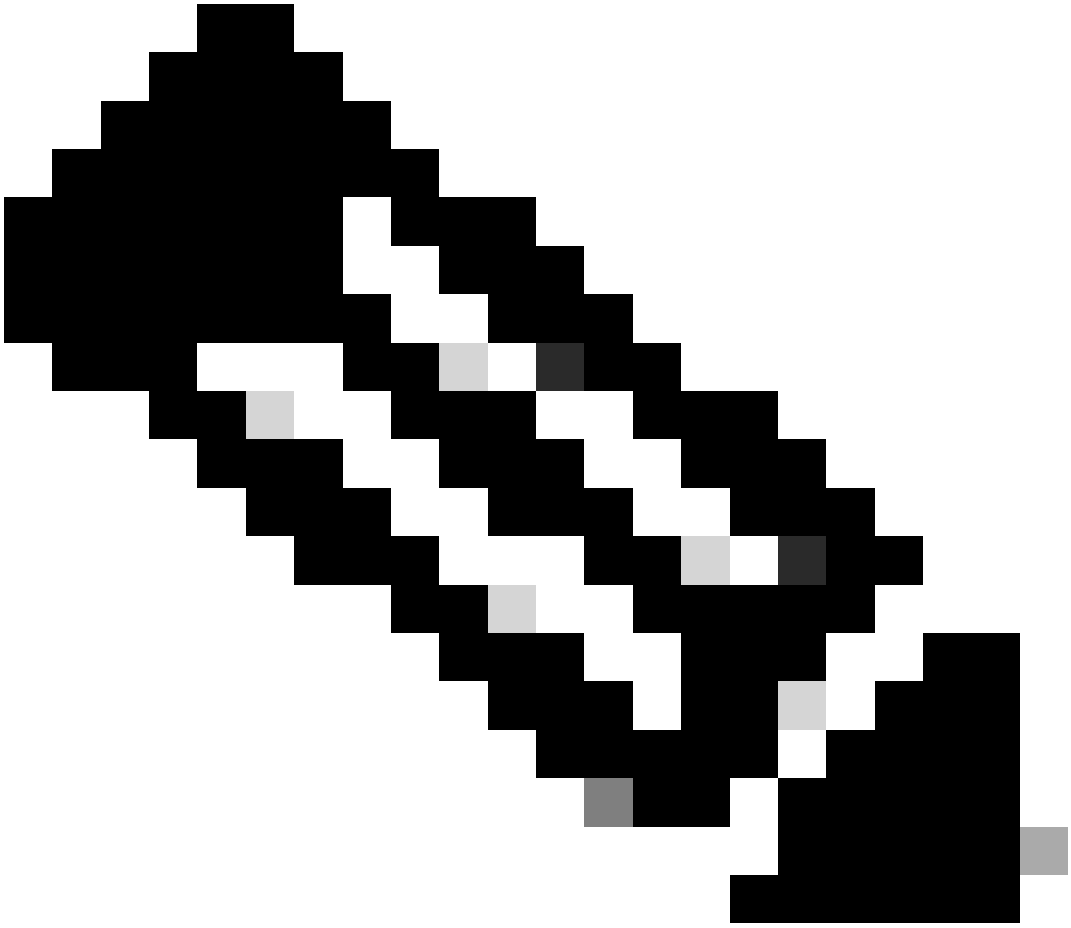
No futuro, o Cisco Umbrella analisa automaticamente os alertas do ZeroFOX e adiciona sites mal-intencionados à lista de destino do ZeroFOX, estendendo a inteligência do ZeroFOX a todos os usuários e dispositivos remotos e fornecendo outra camada de aplicação à sua rede corporativa.

Isso é obtido por meio destas etapas simples de configuração:

1. Habilite a integração no Umbrella para gerar um token de API.
2. Cole esse token de API na sua conta do ZeroFOX.
3. Configure o ZeroFOX para ser bloqueado nas configurações de segurança da(s) política(s) desejada(s)

Pré-requisitos

- Direitos administrativos do ZeroFOX Enterprise
- Direitos administrativos do painel do Umbrella
- O painel Umbrella deve ter a integração com o ZeroFOX habilitada



Note: A integração com o ZeroFOX está incluída somente no pacote da Plataforma Umbrella. Se você não tiver o pacote de plataforma e quiser ter a integração com o ZeroFOX, entre em contato com seu representante Cisco Umbrella. Se você tiver o pacote de plataforma, mas não vir o ZeroFOX como uma integração para o seu painel, entre em contato com o suporte Umbrella.

Importante: Enquanto o Umbrella tenta o seu melhor para validar e permitir domínios que são conhecidos por serem geralmente seguros (por exemplo, Google e Salesforce), para evitar interrupções indesejadas, sugerimos adicionar quaisquer domínios que você não deseja bloquear à Lista de Permissões Global ou outras listas de destino, de acordo com a sua política.

Por exemplo:

- A página inicial da sua organização. Por exemplo, mydomain.com.
- Domínios que representam os serviços que você fornece e que podem ter registros internos e externos. Por exemplo, mail.myservicedomain.com e portal.myotherservicedomain.com.
- Os aplicativos em nuvem menos conhecidos dos quais você depende muito não podem ser

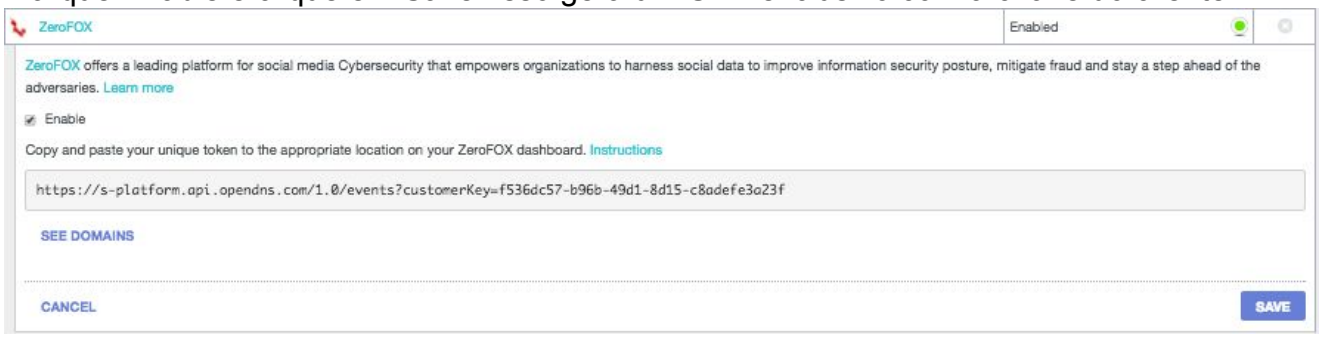
reconhecidos ou incluídos na validação automática de domínio. Por exemplo, localcloudservice.com.

A Lista de permissões global encontra-se em Policies > Destination Lists no Umbrella. Consulte nossa documentação para obter mais informações: Gerenciar listas de destino

Passo 1: Geração de script Umbrella e token API

Comece descobrindo sua URL exclusiva no Umbrella para que o dispositivo ThreatQ se comunique.

1. Faça login no painel do Umbrella como um administrador, navegue para Configurações > Integrações e clique em "ZeroFOX" na tabela para expandi-la.
2. Marque Enable e clique em Save. Isso gera um URL exclusivo com a chave do cliente.

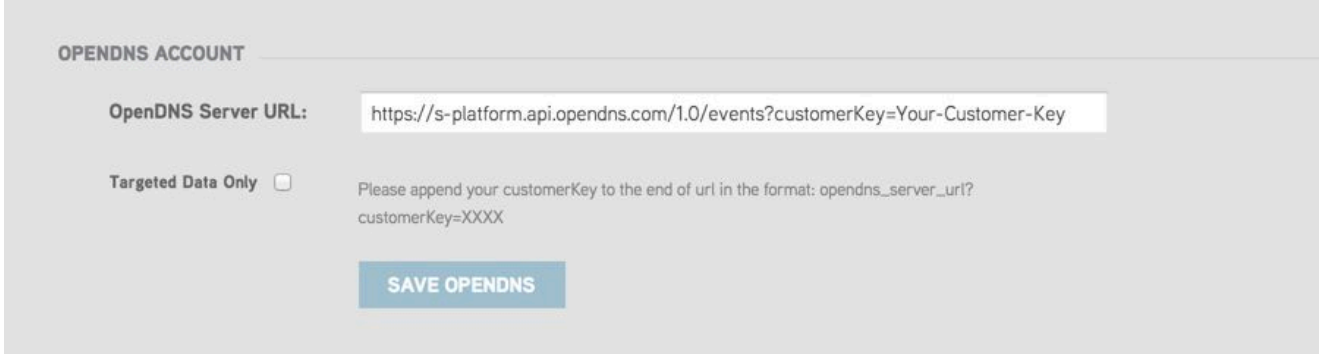


Você precisará do URL mais tarde, quando estiver configurando o ZeroFOX; portanto, copie o URL e vá para o painel do ThreatQ.

Passo 2: Configure o painel do ZeroFOX Enterprise para enviar informações ao Umbrella

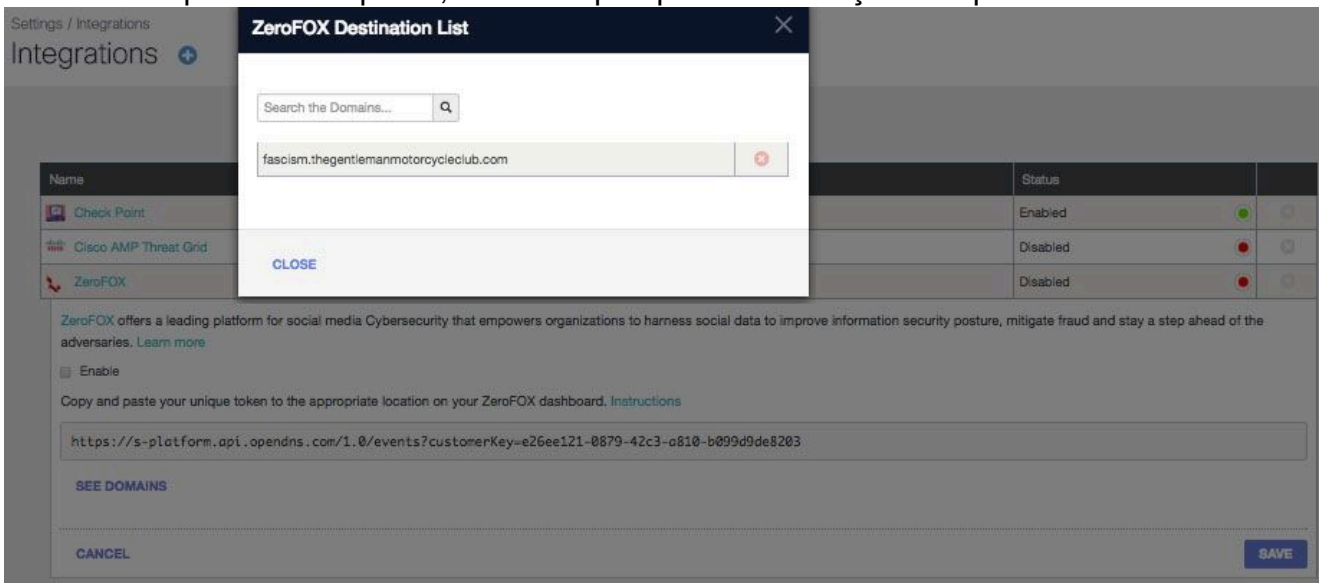
A próxima etapa é adicionar o URL que você copiou na etapa um ao painel do ZeroFOX.

1. Clique no ícone de engrenagem no painel do Zerofox e selecione Configurações da conta.
2. Role a lista de integração para baixo até ver as informações da conta OpenDNS e cole a URL do Umbrella no campo OpenDNS Server URL.
3. Após a primeira habilitação da integração, recomendamos que você marque Somente dados de destino.



Passo 3: Configurar eventos ZeroFOX a serem bloqueados no Umbrella

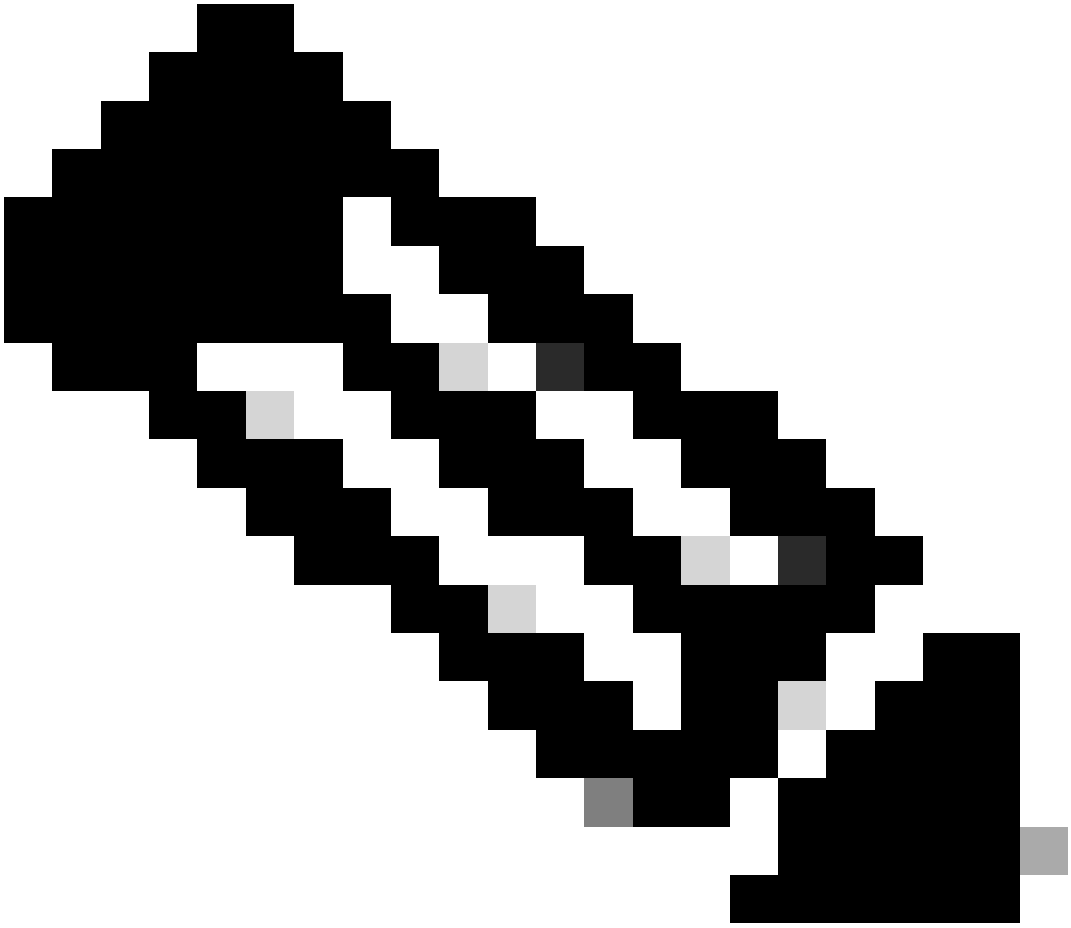
1. Faça login novamente no painel do Umbrella como Administrador.
2. Navegue até Settings > Integrations e clique em "ZeroFOX" na tabela para expandi-la.
3. Clique em Ver domínios.
   Isso expande uma lista de domínios que inclui as últimas horas de eventos da sua conta ZeroFOX. A partir desse ponto, uma lista pesquisável começa a ser preenchida e a crescer.



A próxima etapa é observar e auditar os eventos adicionados à sua nova Categoria de segurança ZeroFOX.

Observação de eventos adicionados à categoria de segurança do ZeroFOX no modo de auditoria

Os eventos do ZeroFOX Enterprise começam a preencher uma lista de destinos específica que pode ser aplicada a políticas como uma categoria de segurança do ZeroFOX. Por padrão, a lista de destino e a categoria de segurança estão no modo de Auditoria e não são aplicadas a nenhuma política e não resultam em nenhuma alteração nas políticas do Umbrella existentes.



Note: O modo de auditoria pode ser ativado por quanto tempo for necessário, com base no perfil de implantação e na configuração da rede.

Revisar lista de destinos

Você pode revisar a Lista de Destinos ZeroFox a qualquer momento.

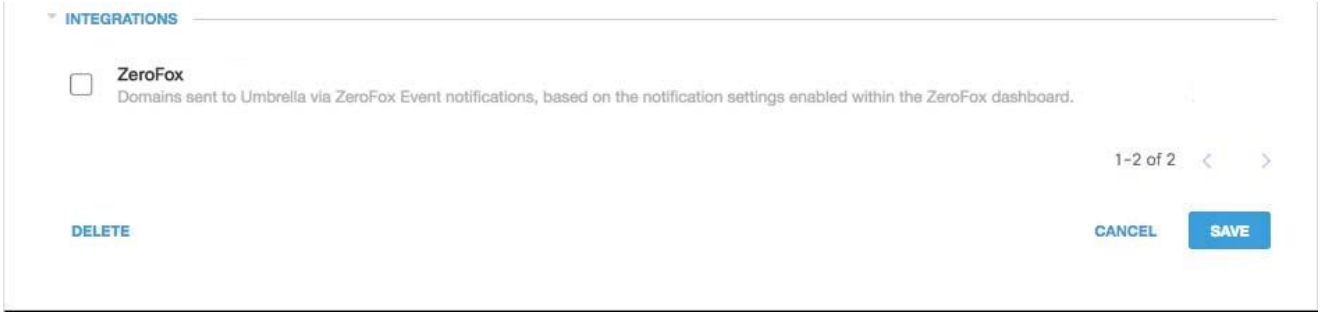
1. Navegue até Configurações > Integrações.
2. Expanda "ZeroFOX" na tabela e clique em Ver domínios.

Revisar Configurações de Segurança para uma Política

Você pode revisar a configuração de segurança que pode ser habilitada para uma política a qualquer momento.

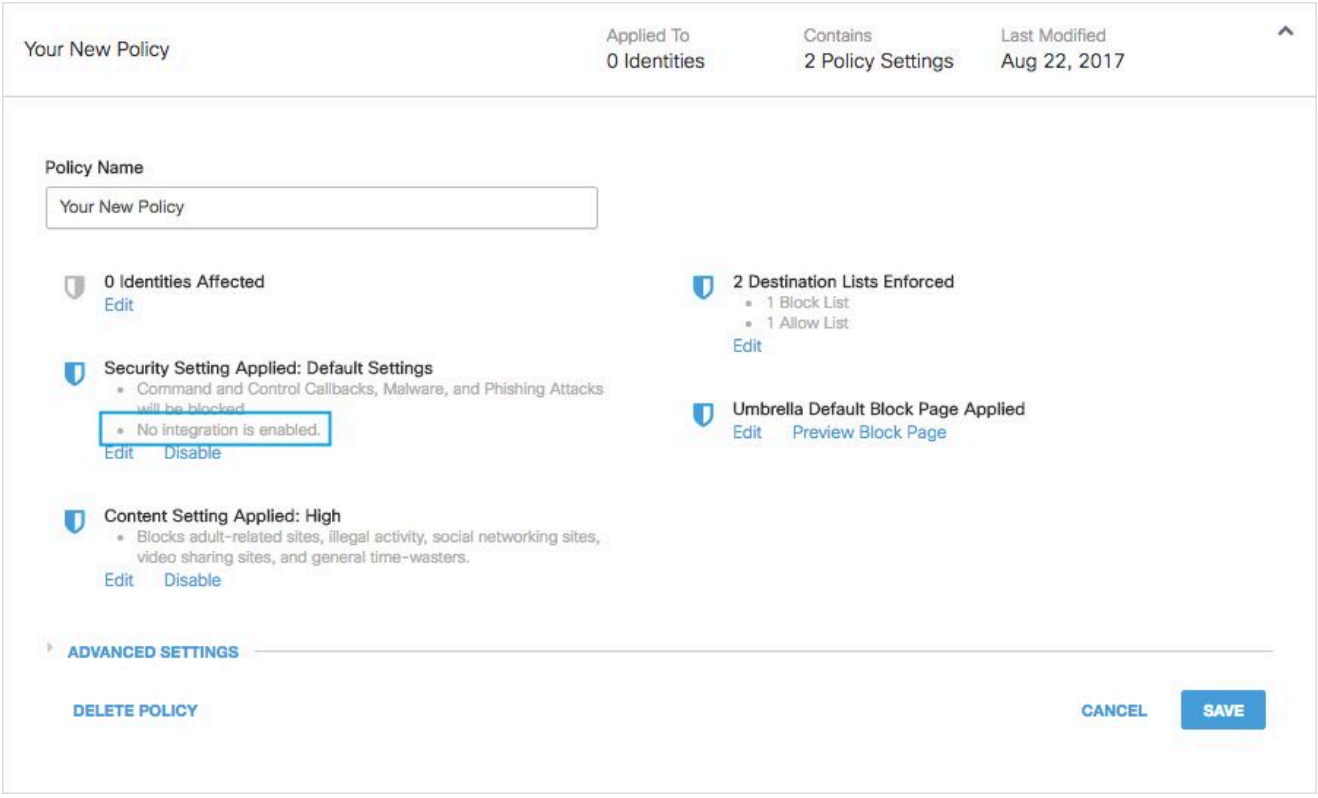
1. Navegue até Policies > Security Settings.
2. Clique em uma configuração de segurança na tabela para expandi-la e role até Integrations

para localizar a configuração ZeroFOX.



115014041606

Você também pode revisar as informações de integração através da página Resumo das configurações de segurança.

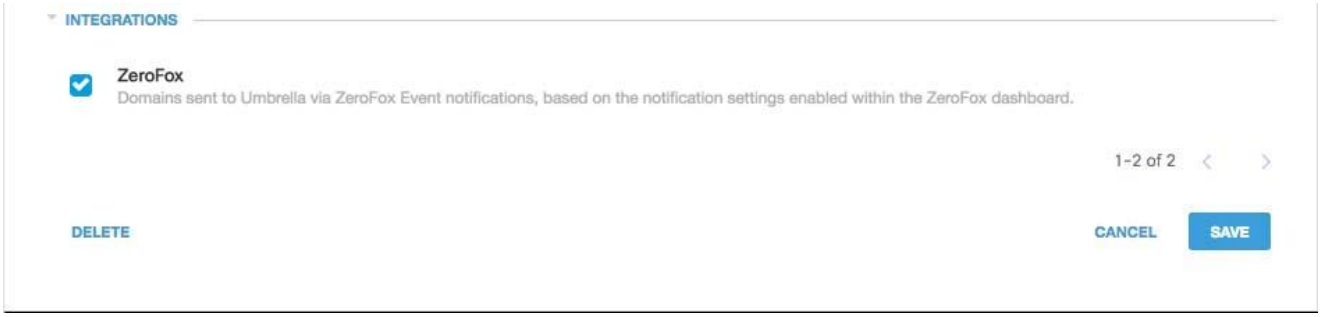


25464154913556

Aplicando as configurações de segurança do ZeroFOX no modo de bloqueio a uma política para clientes gerenciados

Quando estiver pronto para fazer com que essas ameaças de segurança adicionais sejam aplicadas pelos clientes gerenciados pelo Umbrella, basta alterar a configuração de segurança em uma política existente ou criar uma nova política que fique mais alta que a sua política padrão para garantir que ela seja aplicada primeiro.

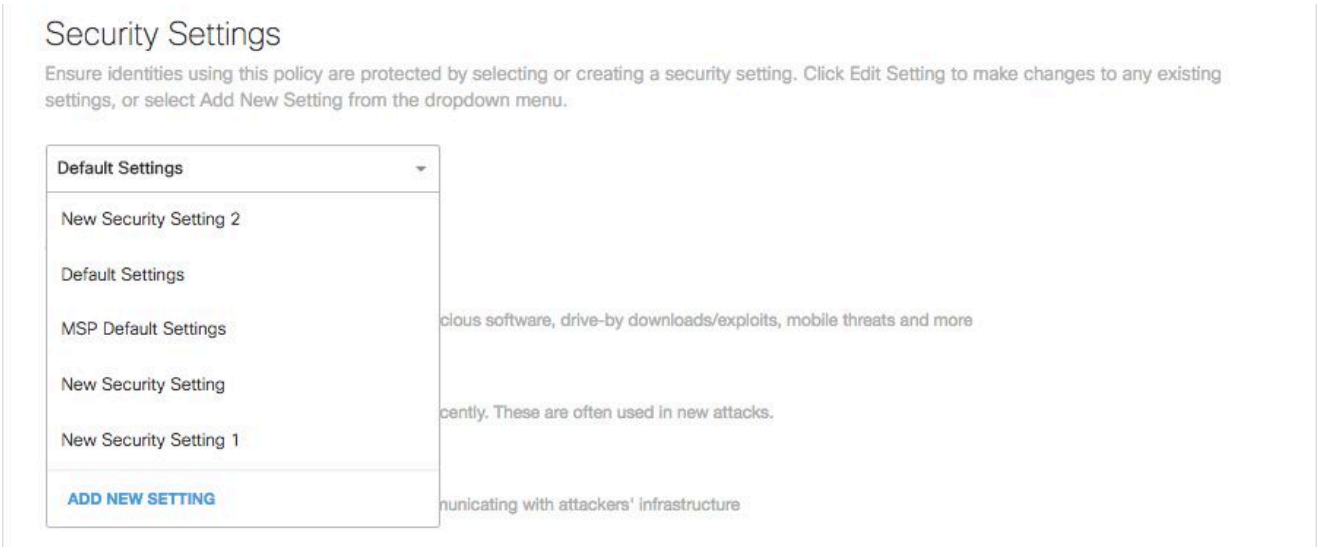
1. Navegue até Policies > Security Settings e, em Integrations, marque ZeroFOX e clique em Save.



115014042806

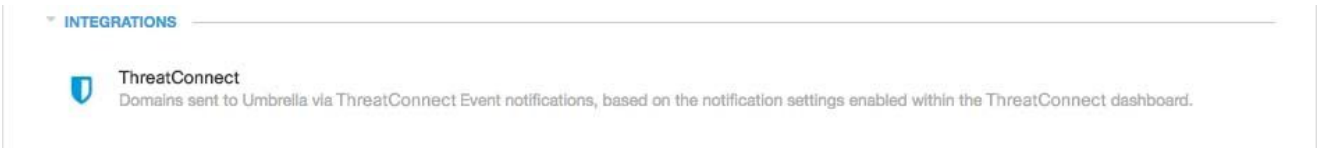
Em seguida, no Assistente de política, adicione uma configuração de segurança à política que você está editando:

1. Navegue até Policies > Policy List.
2. Expanda uma diretiva e clique em Editar em Configuração de segurança aplicada.
3. No menu suspenso Configurações de segurança, selecione uma configuração de segurança que inclua a configuração do ThreatConnect.



25464147943700

O ícone de escudo em Integrações é atualizado para azul.



25464147957652

4. Clique em Set & Return.

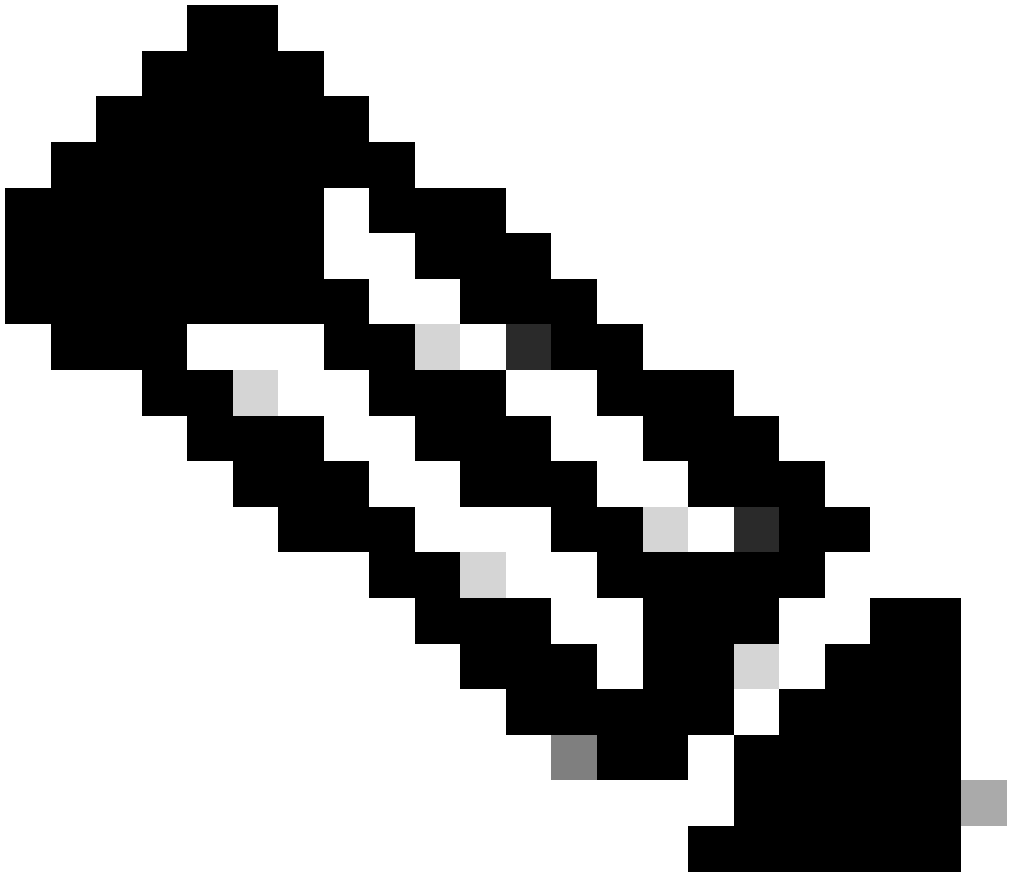
Os domínios ZeroFOX contidos na configuração de segurança do ZeroFOX são bloqueados para essas identidades que usam essa política.

Relatórios no Umbrella para eventos ZeroFOX

Relatórios sobre eventos de segurança do ZeroFOX

A Lista de Destinos ZeroFOX é uma das listas de categorias de segurança sobre as quais você pode gerar relatórios. A maioria ou todos os relatórios usam as Categorias de Segurança como um filtro. Por exemplo, você pode filtrar as categorias de segurança para mostrar apenas a atividade relacionada ao ZeroFOX.

1. Navegue para Relatórios > Pesquisa de atividade e, em Categorias de segurança, selecione ZeroFOX para filtrar o relatório para mostrar apenas a categoria de segurança para o ZeroFOX.



Note: Se a integração com o ZeroFOX estiver desativada, ela não aparecerá no

filtro Categorias de segurança.

115014043046

2. Clique em Apply.

Relatando quando os domínios foram adicionados à lista de destino do ZeroFOX

O registro de auditoria do Umbrella Admin inclui eventos da sua conta ZeroFOX à medida que adiciona domínios à lista de destino.

O registro de Auditoria do Umbrella Admin pode ser encontrado em Relatórios > Log de Auditoria do Administrador. Para gerar relatórios sobre quando um domínio foi adicionado, filtre para incluir apenas alterações do ZeroFOX aplicando um filtro a Identidades e Configurações para a Lista de Destino do ZeroFox.

Depois de executar o relatório, você verá uma lista das alterações feitas quando a lista de destino ZeroFOX foi adicionada ao a partir da integração.

Lidando com detecções indesejadas ou falsos positivos

Gerenciando uma lista de permissões para detecção indesejada

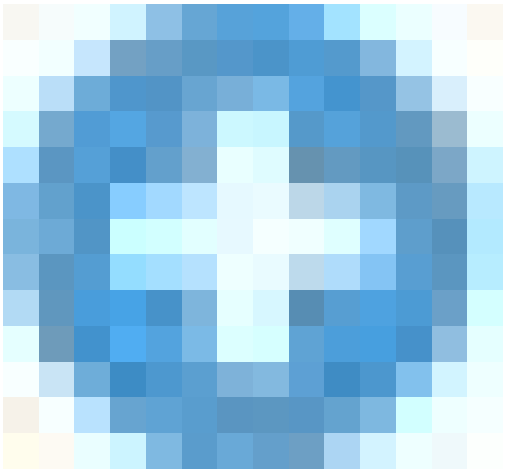
Embora improvável, é possível que os domínios adicionados automaticamente pelo ZeroFOX possam disparar um bloqueio indesejado que impediria os usuários de acessar sites específicos. Em uma situação como essa, recomendamos adicionar o(s) domínio(s) a uma lista de permissão, que tem precedência sobre todos os outros tipos de listas de bloqueio, incluindo as configurações de segurança. Uma lista de permissão tem precedência sobre uma lista de bloqueio quando um domínio está presente em ambos.

Há duas razões para esta abordagem ser preferível. Primeiro, caso o dispositivo ZeroFOX fosse readicionar o domínio novamente após sua remoção, a lista de permissão protege contra isso, causando mais problemas. Em segundo lugar, a lista de permissão mostra um registro histórico de domínios problemáticos que podem ser usados para computação forense ou relatórios de auditoria.

Por padrão, há uma Lista de Permissões Global que é aplicada a todas as políticas. Adicionar um domínio à Lista de Permissões Global resulta na permissão do domínio em todas as políticas.

Se a configuração de segurança do ZeroFOX no modo de bloqueio for aplicada apenas a um subconjunto de suas identidades gerenciadas do Umbrella (por exemplo, ela só é aplicada a computadores móveis e dispositivos móveis em roaming), você poderá criar uma lista de permissões específica para essas identidades ou políticas.

Para criar uma lista de permissões:

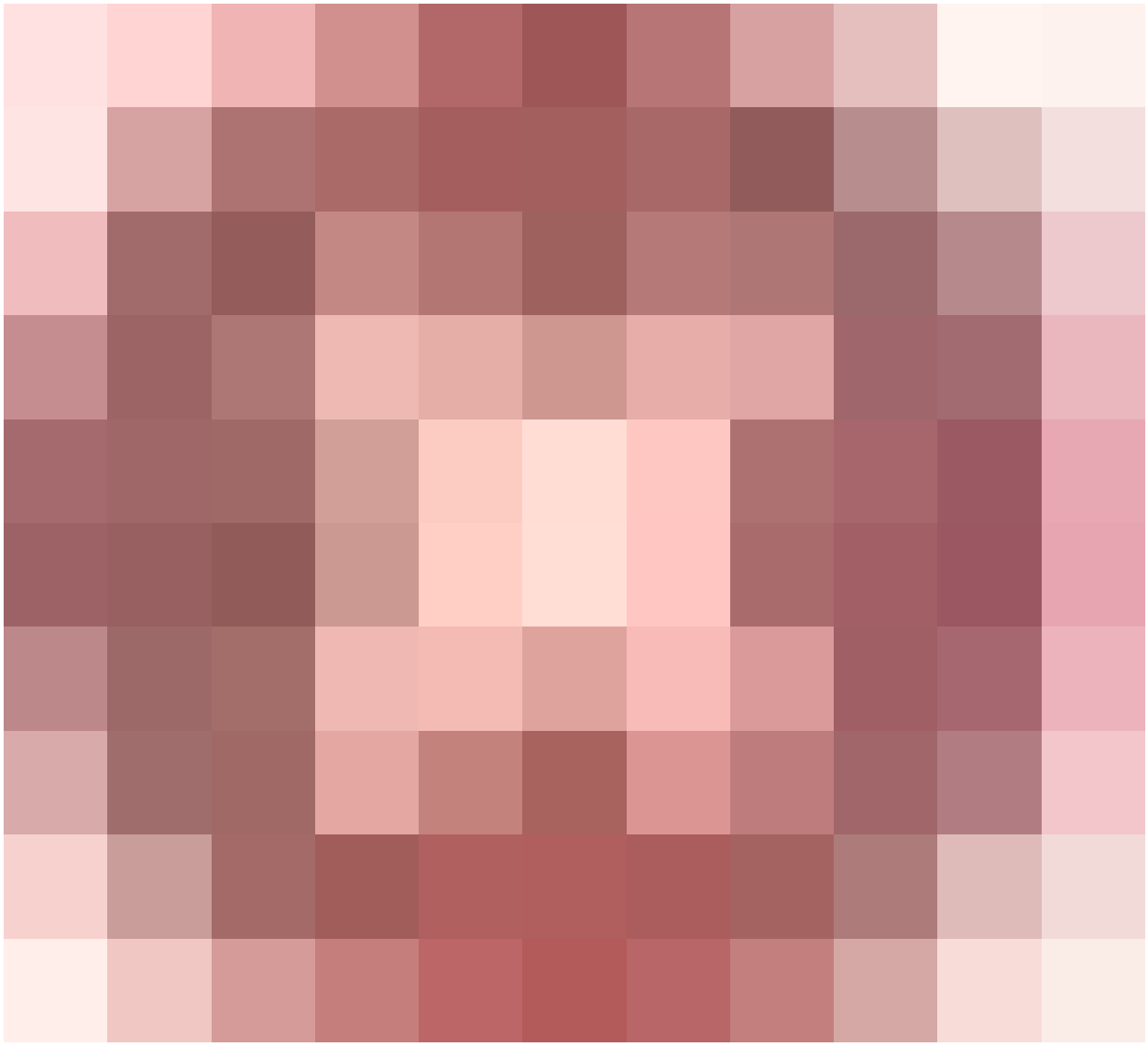
1. Navegue até Policies > Destination Lists, clique no botão 

   25464155856404

   Ícone Adicionar.
2. Selecione Permitir e adicione seu domínio à lista.
3. Click Save.

Depois que a lista de destino tiver sido salva, você poderá adicioná-la a uma política existente que abranja os clientes que foram afetados pelo bloqueio indesejado.

Excluindo domínios da lista de destinos do ZeroFOX



Existe um (Excluir) ao lado de cada nome de domínio na lista de destino do ZeroFOX. A exclusão de domínios permite limpar a lista de destinos do ZeroFOX no caso de uma detecção indesejada.

No entanto, a exclusão não é permanente se o ZeroFOX reenvia o domínio para o Umbrella.

Para excluir um domínio:

1. Navegue até Configurações > Integrações e clique em "ZeroFOX" para expandi-lo.
2. Clique em Ver domínios.
3. Procure o nome de domínio que deseja excluir.
4. Clique no ícone Delete (Excluir).

5. Clique em Close.
6. Click Save.

No caso de uma detecção indesejada ou falso positivo, recomendamos a criação imediata de uma lista de permissões no Umbrella e, em seguida, a correção do falso positivo no ZeroFOX. Mais tarde, você pode remover o domínio da lista de destinos do ZeroFOX.

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.