Integre o ThreatConnect com o Umbrella

Contents

Introdução

Este documento descreve como integrar o ThreatConnect ao Cisco Umbrella.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Um painel do ThreatConnect com acesso para atualizar o URL para integrações
- Direitos administrativos do painel do Umbrella
- O painel do Umbrella deve ter a integração do ThreatConnect habilitada.

Componentes Utilizados

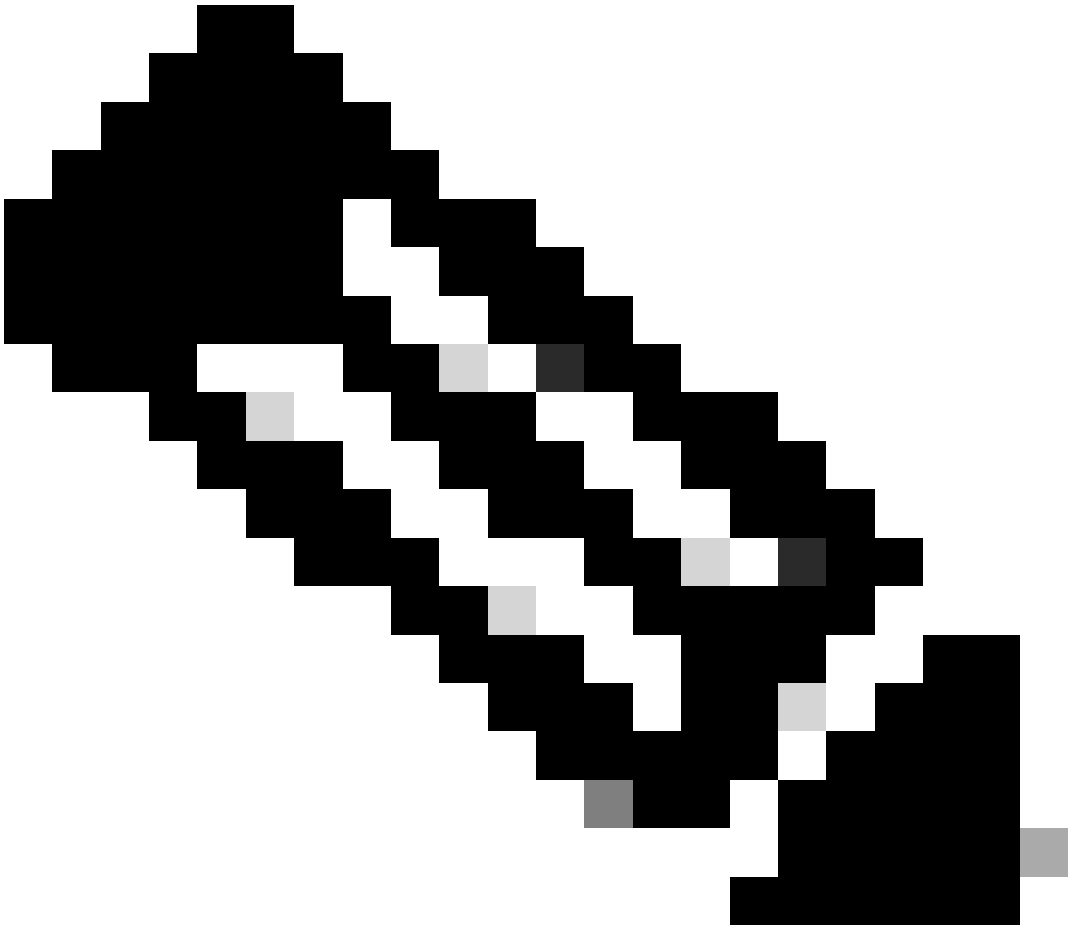
As informações neste documento são baseadas no Cisco Umbrella.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Visão geral da integração do ThreatConnect e do Cisco Umbrella

Com a integração do ThreatConnect com o Cisco Umbrella, os administradores e os responsáveis pela segurança agora podem ampliar a proteção contra ameaças avançadas a laptops, tablets ou telefones móveis, além de fornecer outra camada de aplicação a uma rede corporativa distribuída.

Este guia descreve como configurar o ThreatConnect para se comunicar com o Umbrella para que os eventos de segurança do ThreatConnect TIP sejam integrados em políticas que possam ser aplicadas a clientes protegidos pelo seu Cisco Umbrella.



Note: A integração com o ThreatConnect está incluída apenas em um determinado pacote Cisco Umbrella. Se você não tiver um pacote que inclua essa integração, entre em

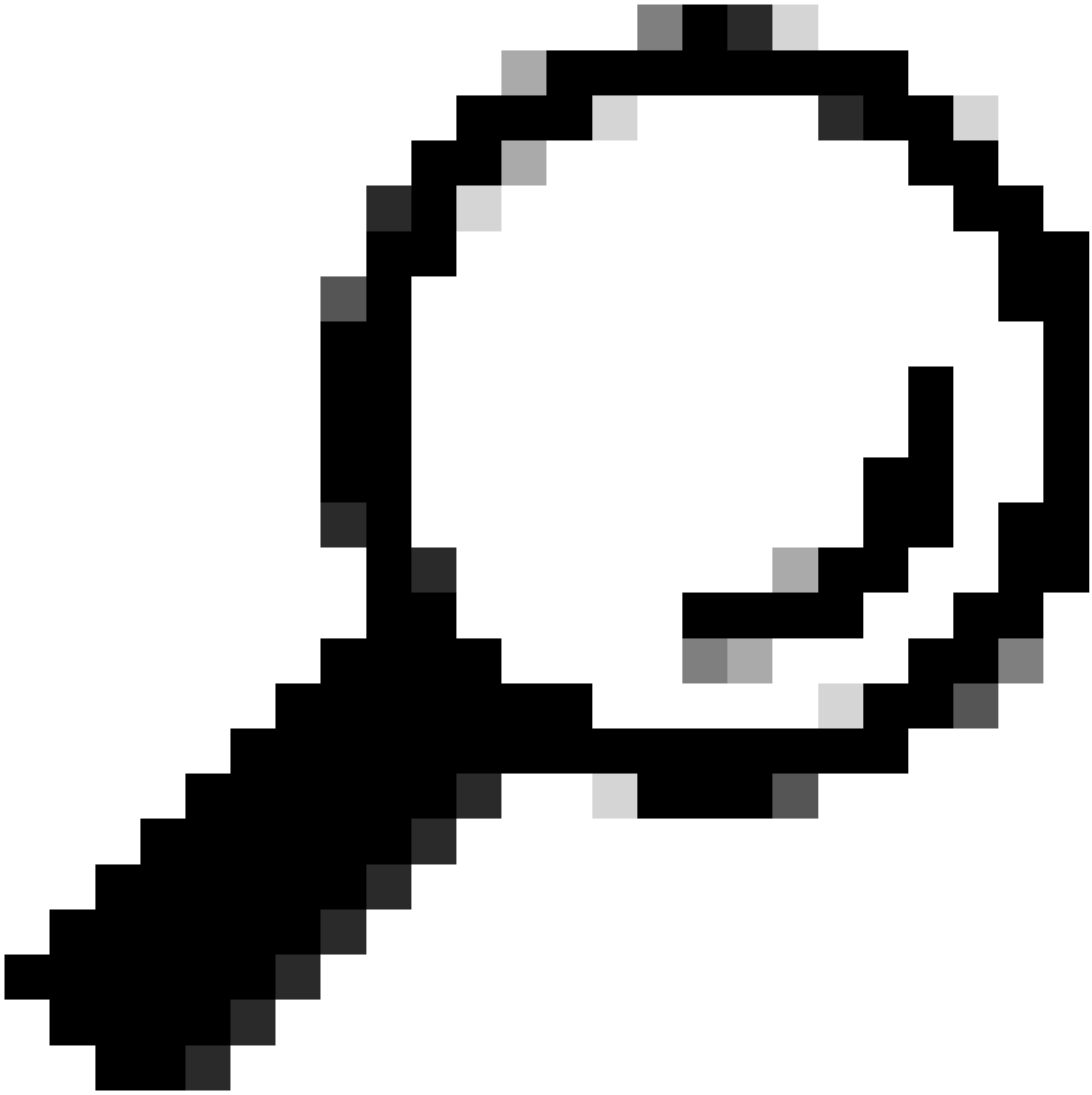
---

contato com seu representante Cisco Umbrella para obtê-lo. Se você tiver o pacote correto, mas não vir o ThreatConnect como uma integração para seu painel, entre em contato com o Suporte do Cisco Umbrella.

A plataforma ThreatConnect primeiro envia a inteligência de ameaças cibernéticas que encontrou, como domínios que hospedam malware, comandos e controle para sites de botnet ou phishing, para a Umbrella.

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

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



Tip: 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 qualquer interrupção indesejada, o Umbrella sugere adicionar quaisquer domínios que você não deseja que sejam bloqueados para a Lista de Permissões Global ou outras listas de destino de acordo com 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.
- Aplicativos em nuvem menos conhecidos dos quais você depende muito, mas que a Umbrella não reconhece ou não inclui em sua validação automática de domínio. Por exemplo, localcloudservice.com.

A Lista de permissões global encontra-se em Policies > Destination Lists no Umbrella.

Consulte a documentação do para obter mais informações: Gerenciar listas de destino

Configure o painel Umbrella para receber eventos do ThreatConnect

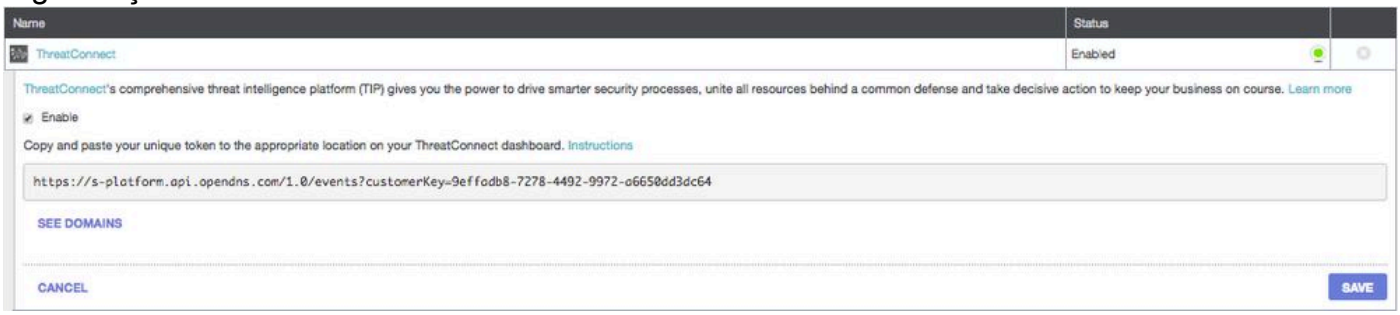
Comece localizando sua URL exclusiva no Umbrella para que o dispositivo ThreatQ se comunique com:

1. Faça login no painel do Umbrella.

2. Navegue até Policies > Integrations.

3. Na tabela, selecione ThreatConnect para expandi-la.

4. Selecione Ativar e, em seguida, Salvar. Isso gera um URL exclusivo e específico para sua organização no Umbrella.



Você precisará do URL posteriormente neste artigo quando estiver configurando o ThreatConnect para enviar dados ao Umbrella.

Configurar o ThreatConnect para se comunicar com o Umbrella

Para começar a enviar tráfego do ThreatConnect para o Umbrella, você precisa configurar o ThreatConnect com as informações de URL geradas na primeira seção deste artigo:

1. Faça login no painel do ThreatConnect.

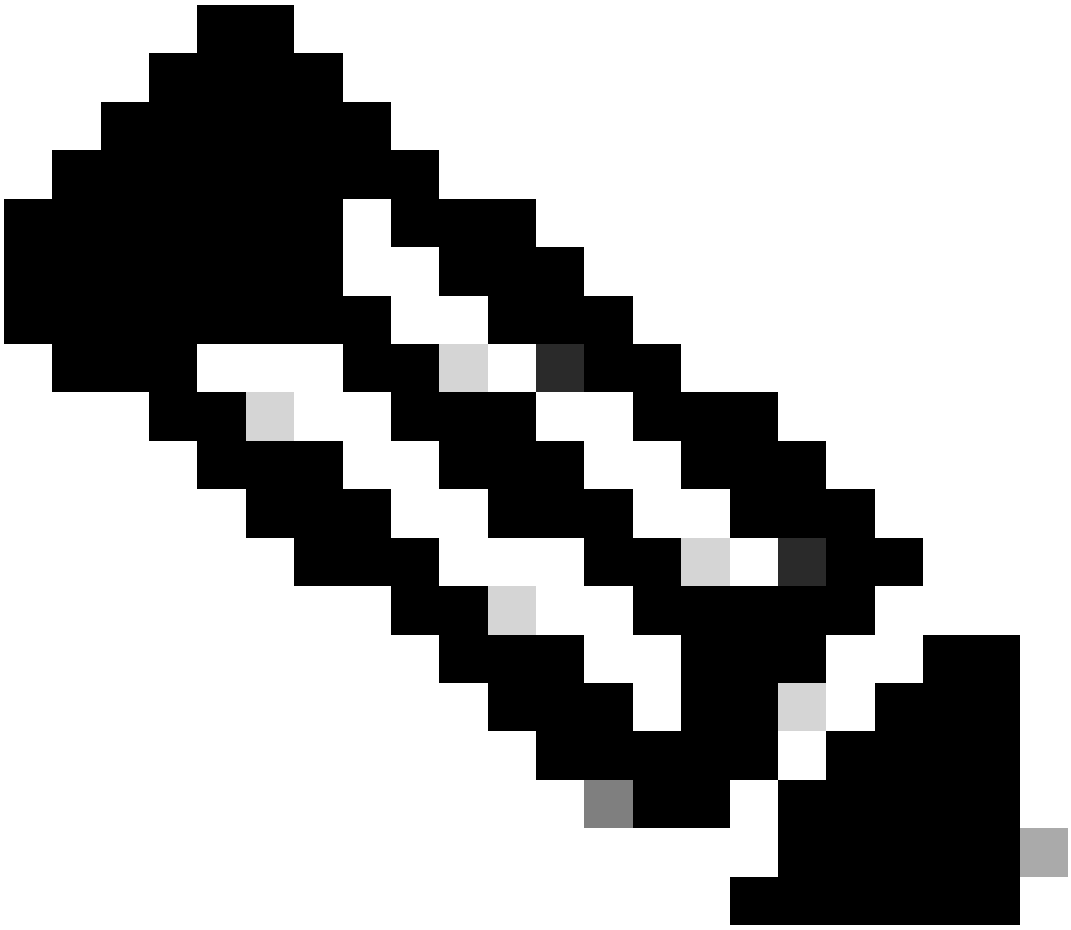
2. Adicione o URL na área apropriada para conectar-se ao Umbrella.

Instruções exatas variam e a Umbrella sugere entrar em contato com o suporte do ThreatConnect se você não souber como ou onde configurar integrações de API no ThreatConnect.

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

Com o tempo, os eventos do painel do ThreatConnect podem começar a preencher uma lista de destinos específica que pode ser aplicada às políticas como uma categoria de segurança do ThreatConnect. Por padrão, a lista de destino e a categoria de segurança estão no modo de

Auditoria, o que significa que elas não são aplicadas a políticas e não resultam em qualquer alteração nas políticas do Umbrella existentes.



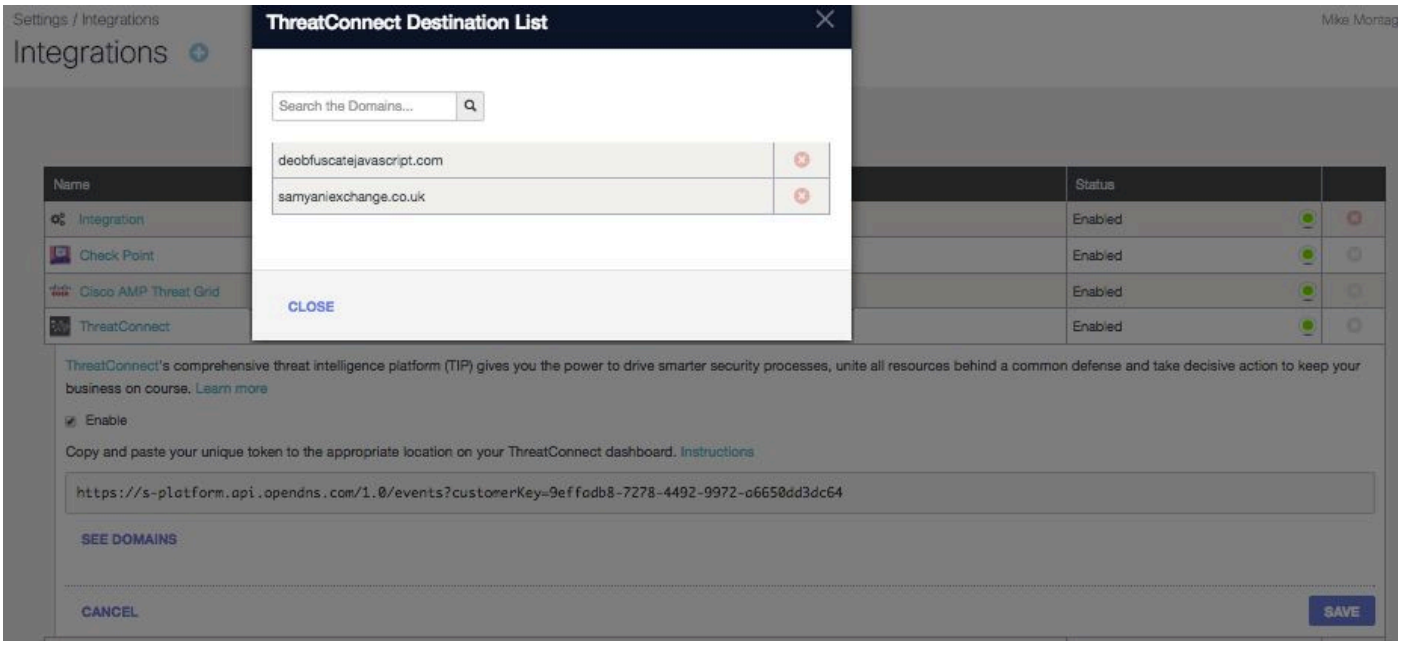
Note: O modo de auditoria pode ser ativado por quanto tempo for necessário, com base no perfil de implantação e na configuração da rede.

Revisar lista de destinos

Você pode rever a lista de destinos do ThreatConnect no Umbrella a qualquer momento:

1. No painel Umbrella, navegue para Policies > Integrations.

2. Na tabela, expanda ThreatConnect e selecione Ver domínios.



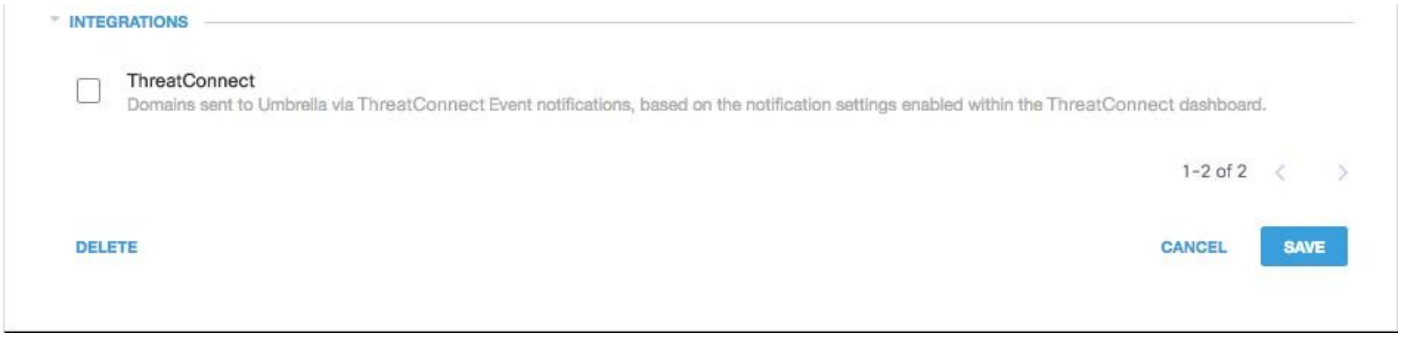
Revisar Configurações de Segurança para uma Política

Você pode revisar a configuração de segurança que pode ser ativada para uma política a qualquer momento:

1. No painel Umbrella, navegue para Policies > Security Settings.

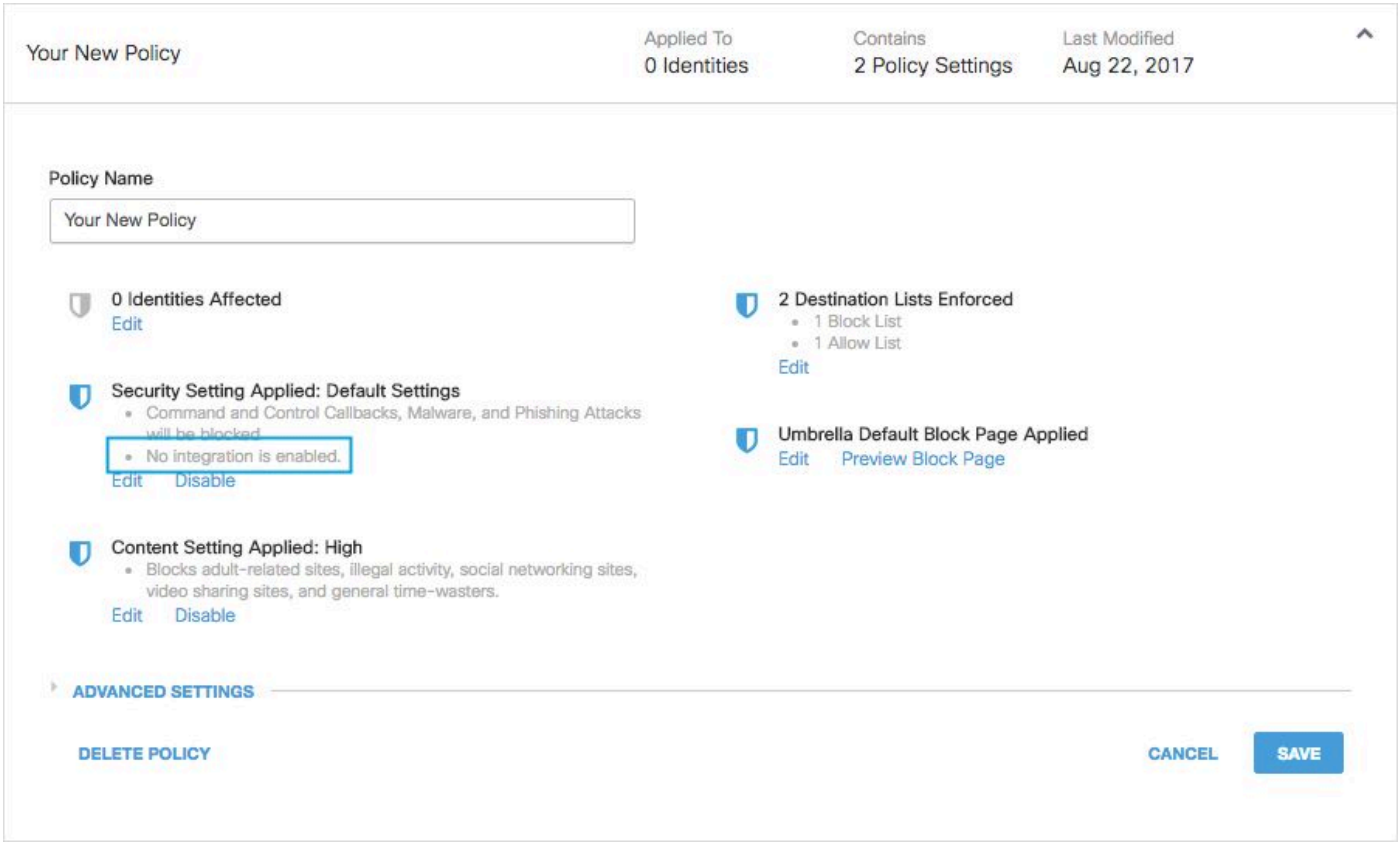
2. Selecione uma configuração de segurança na tabela para expandi-la.

3. Role até Integrations para localizar a configuração ThreatConnect.



115014036566

4. Você também pode revisar as informações de integração através da página Resumo das Configurações de Segurança.



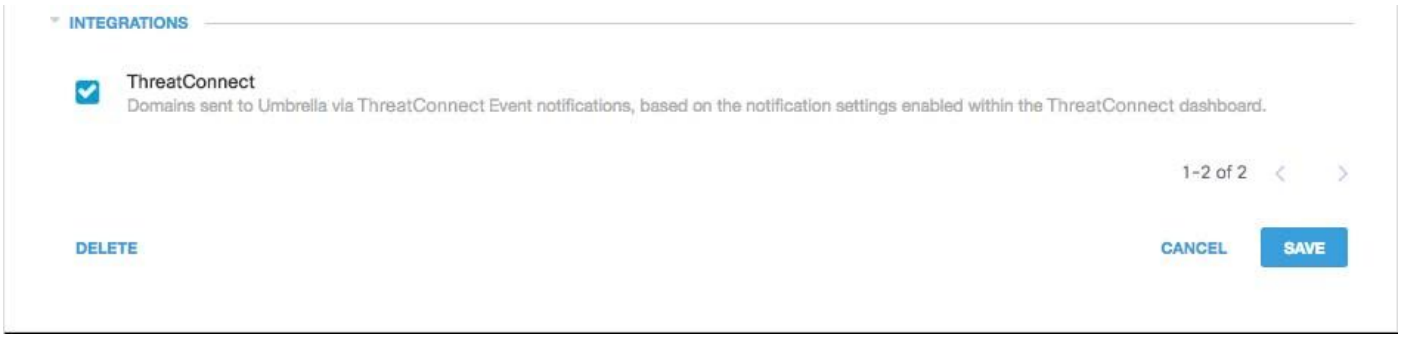
25464103885972

Aplicando as configurações de segurança do ThreatConnect 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 acima da sua política padrão para garantir que ela seja aplicada primeiro:

1. Navegue até Policies > Security Settings.

2. Em Integrações, selecione ThreatConnect e Salvar.



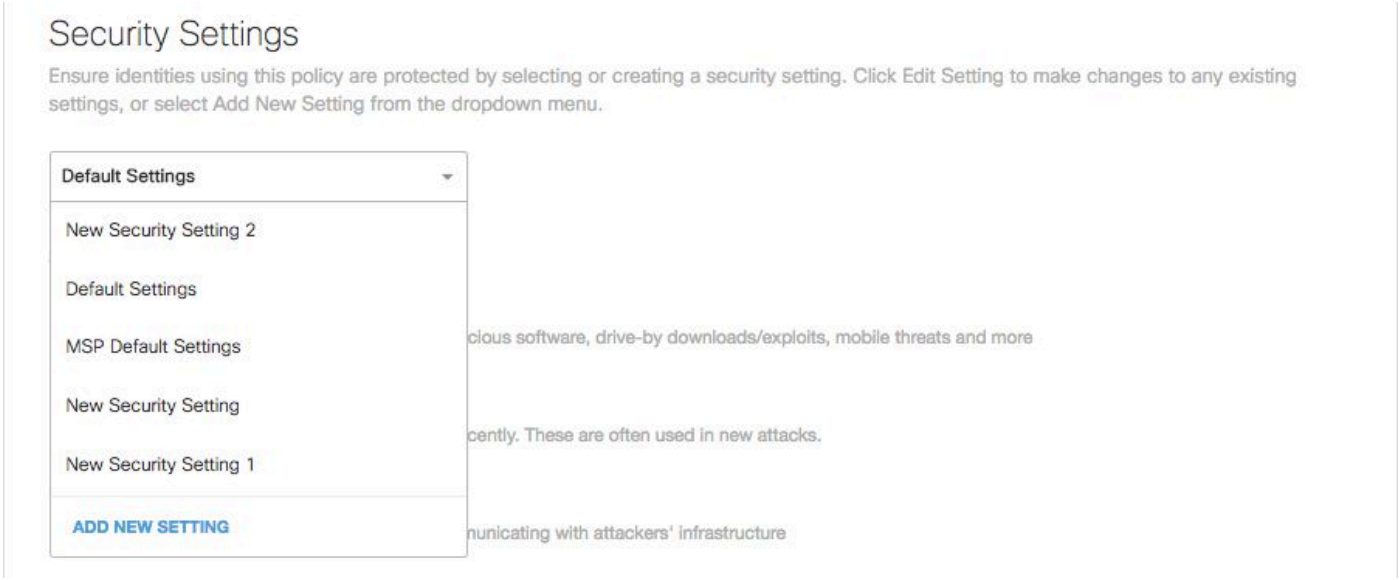
115014203703

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

1. Navegue até Policies > Policy List.

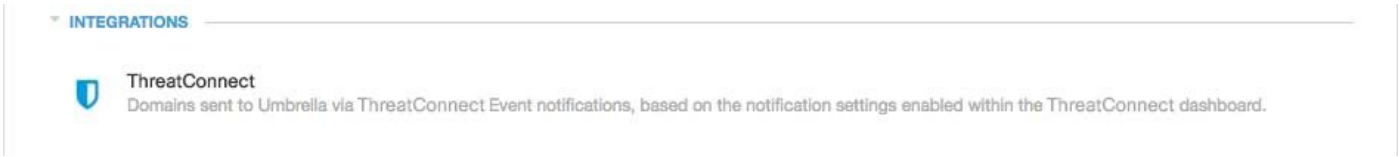
2. Expanda uma política. Em Configuração de segurança aplicada, selecione Editar.

3. No menu suspenso Configurações de segurança, selecione uma configuração de segurança que inclua a configuração ThreatConnect.



25464103908884

O ícone de escudo em Integrações é atualizado para azul.



115014037666

4. Selecione Set & Return.

Os domínios do ThreatConnect contidos na configuração de segurança do ThreatConnect são bloqueados para identidades que usam a política.

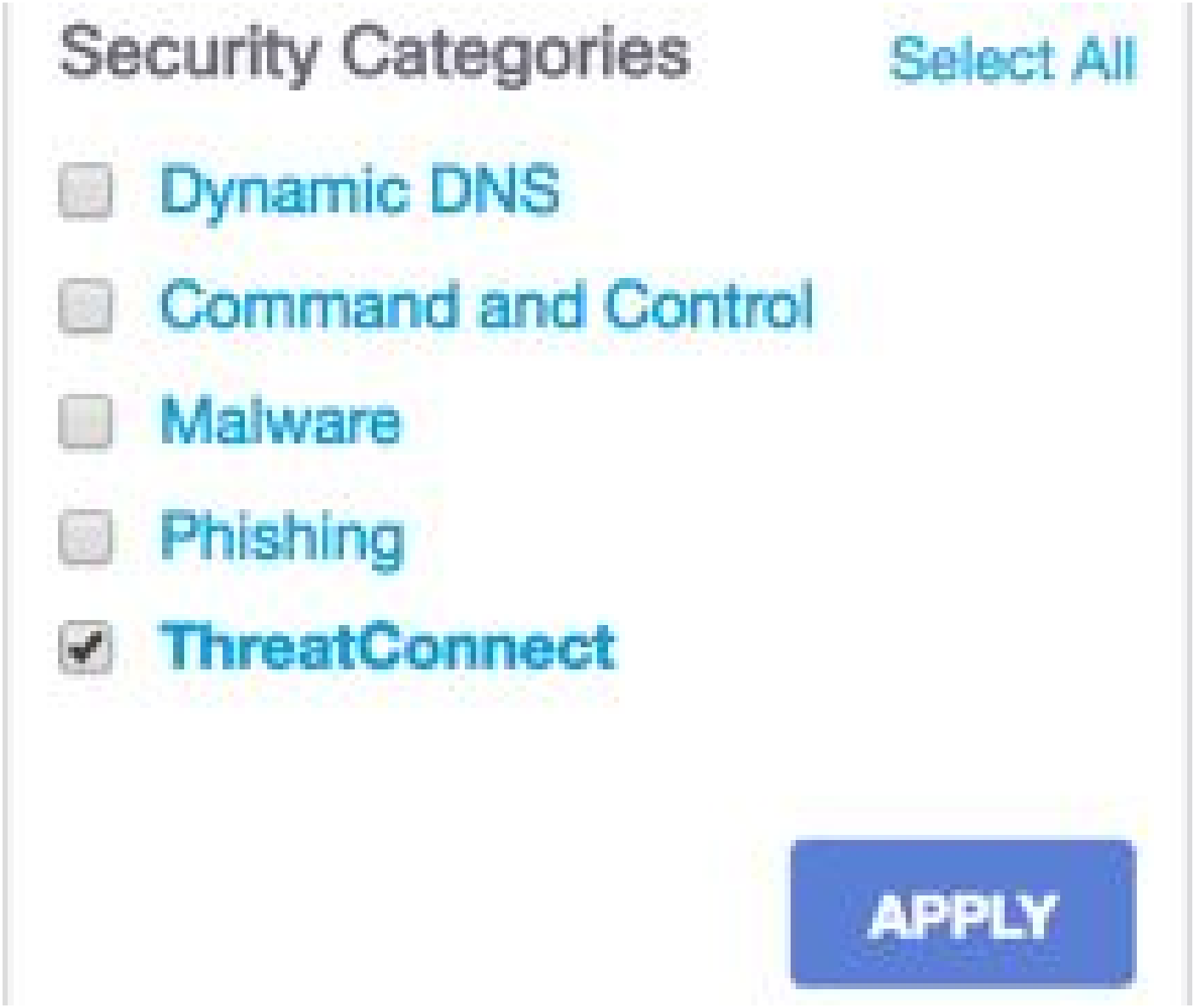
Relatórios no Umbrella para eventos do ThreatConnect

Relatórios sobre eventos de segurança do ThreatConnect

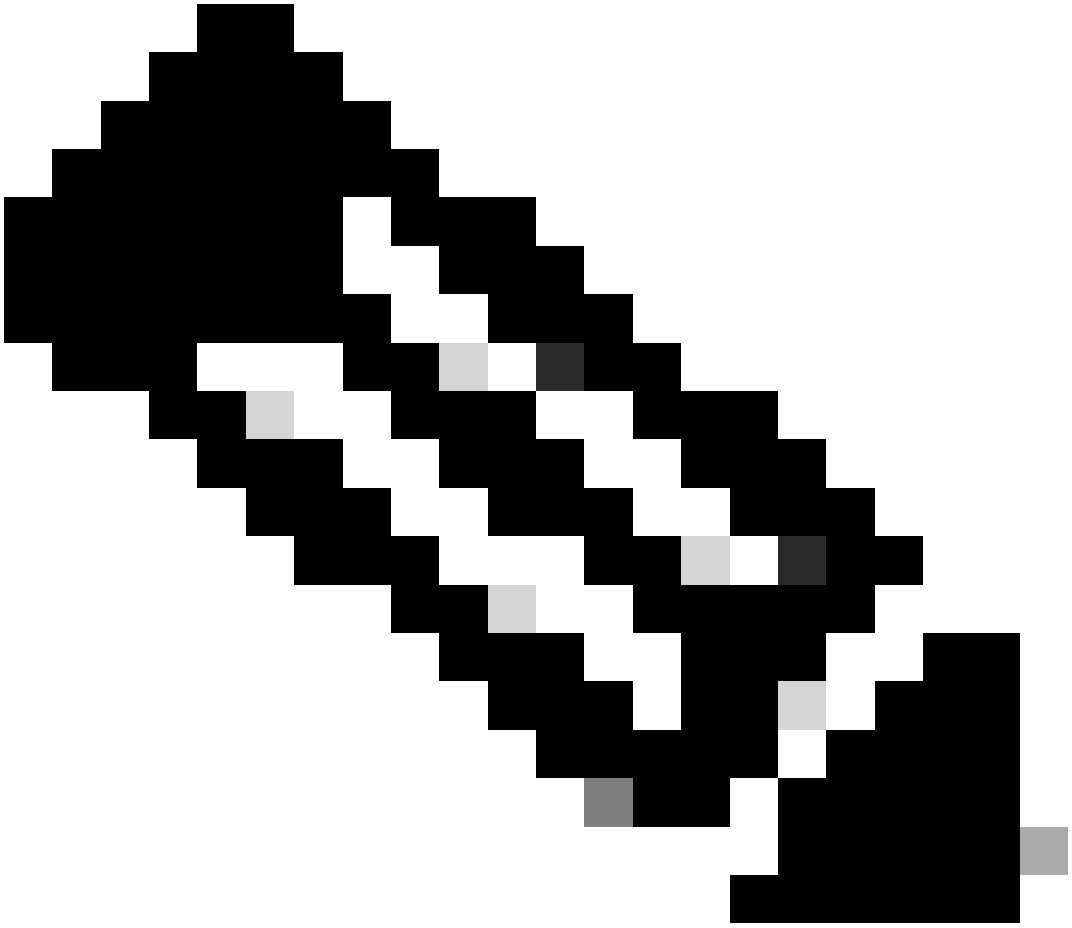
A lista de destinos do ThreatConnect é uma das listas de categorias de segurança sobre as quais você pode gerar relatórios. A maioria ou todos os relatórios usam as Categorias de segurança como um filtro. Por exemplo, você pode filtrar as categorias de segurança para mostrar apenas a atividade relacionada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

1. Navegue até Relatórios > Pesquisa de Atividade.

2. Em Categorias de Segurança, selecione ThreatConnect para filtrar o relatório para mostrar apenas a categoria de segurança do ThreatConnect.



115014206603



Note: Se a integração com o ThreatConnect estiver desativada, ela não aparecerá no filtro Categorias de segurança.

3. Selecione Aplicar.

Relatórios sobre a adição de domínios à lista de destinos do ThreatConnect

O log de auditoria do administrador inclui eventos do painel do ThreatConnect, à medida que adiciona domínios à lista de destino. Um usuário chamado "Conta do ThreatConnect", que também é marcado com o logotipo do ThreatConnect, gera os eventos. Esses eventos incluem o domínio que foi adicionado e a hora em que ele foi adicionado.

Você pode filtrar para incluir apenas as alterações do ThreatConnect aplicando um filtro para o usuário da "Conta do ThreatConnect".

Lidando com detecções indesejadas ou falsos positivos

Listas de permissão

Embora seja improvável, é possível que os domínios adicionados automaticamente pelo ThreatConnect possam disparar um bloqueio indesejado que impediria os usuários de acessar sites específicos. Em uma situação como essa, a Umbrella recomenda 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.

Há duas razões pelas quais esta abordagem é preferível:

- Primeiro, caso o painel do ThreatConnect tenha adicionado novamente o domínio após sua remoção, a lista de permissões protege contra esse problema que está causando mais problemas.
- Além disso, 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 ThreatConnect no modo de bloqueio for aplicada apenas a um subconjunto de suas identidades do Umbrella gerenciado (por exemplo, ela só é aplicada a computadores e dispositivos móveis móveis 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 e selecione o ícone Add (+).

2. Selecione Permitir e adicione seu domínio à lista.

3. Selecione Salvar.

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.

Exclusão de domínios da lista de destinos do ThreatConnect

Há um ícone Excluir ao lado de cada nome de domínio na lista de destinos do ThreatConnect. A exclusão de domínios permite limpar a lista de destinos do ThreatConnect em caso de detecção indesejada. No entanto, a exclusão não será permanente se o painel do ThreatConnect reenviar o domínio para o Umbrella.

Para excluir um domínio:

1. Navegue até Políticas > Integrações.

2. Selecione ThreatConnect para expandi-lo.

3. Selecione Ver Domínios.

4. Procure o nome de domínio que deseja deletar.

5. Selecione o ícone Deletar.

6. Selecione Fechar e, em seguida, Salvar.

No caso de uma detecção indesejada ou falso positivo, a Umbrella recomenda criar imediatamente uma lista de permissões no Umbrella e, em seguida, corrigir o falso positivo no painel do ThreatConnect. Posteriormente, você poderá remover o domínio da lista de destinos do ThreatConnect.

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.