Integre o ThreatQ com o Umbrella

Contents

Introdução

Este documento descreve como integrar o ThreatQ ao Cisco Umbrella.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

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

Componentes Utilizados

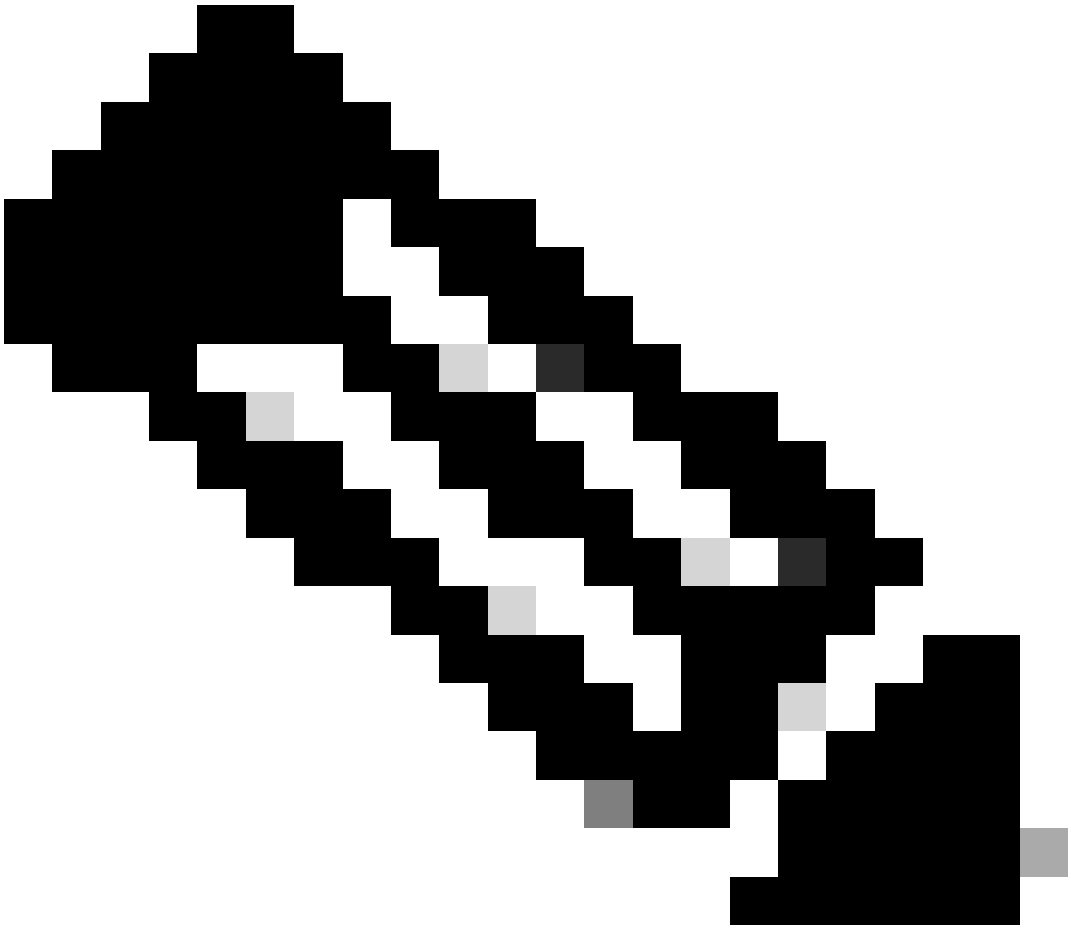
As informações neste documento são baseadas no Cisco Umbrella.

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 ThreatQ e Cisco Umbrella

Ao integrar o ThreatQ ao 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 ThreatQ para se comunicar com o Umbrella para que os eventos de segurança do ThreatQ TIP sejam integrados em políticas que possam ser aplicadas a clientes protegidos pelo Cisco Umbrella.



Note: A integração com o ThreatQ está incluída apenas em determinados pacotes do Cisco Umbrella. Se você não tiver o pacote necessário e quiser a integração com o

---

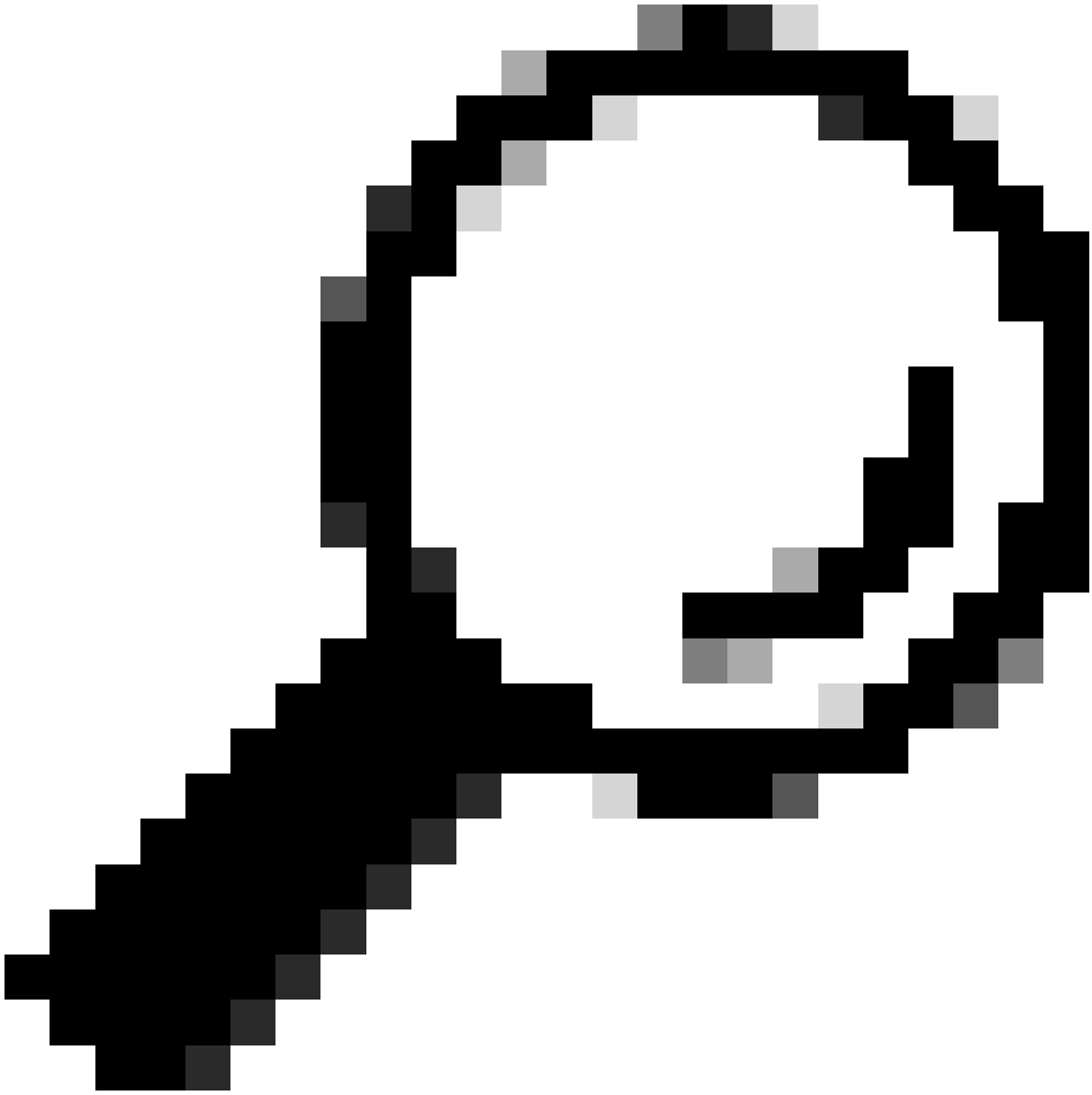
ThreatQ, entre em contato com seu representante Cisco Umbrella. Se você tiver o pacote Cisco Umbrella correto, mas não vir o ThreatQ como uma integração para seu painel, entre em contato com o Suporte do Cisco Umbrella.

Funcionalidade de integração

A plataforma ThreatQ 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 ThreatQ forem confirmadas como uma ameaça, o endereço de domínio será adicionado à lista de destino do ThreatQ 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 ThreatQ.

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



Tip: Embora o Cisco Umbrella faça o possível para validar e permitir domínios que são conhecidos como seguros em geral (por exemplo, Google e Salesforce), para evitar interrupções indesejadas, sugerimos adicionar domínios que você nunca deseja bloquear à Lista de Permissões Global ou a outras listas de destino de acordo com sua política. Por exemplo:

- A página inicial da sua organização
- 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 menos conhecidos baseados em nuvem dos quais você depende não fazem parte da validação automática de domínio do Cisco Umbrella. Por exemplo, "localcloudservice.com".

Esses domínios podem ser adicionados à Lista de permissões global, que é encontrada

em Políticas > Listas de destino no Cisco Umbrella.

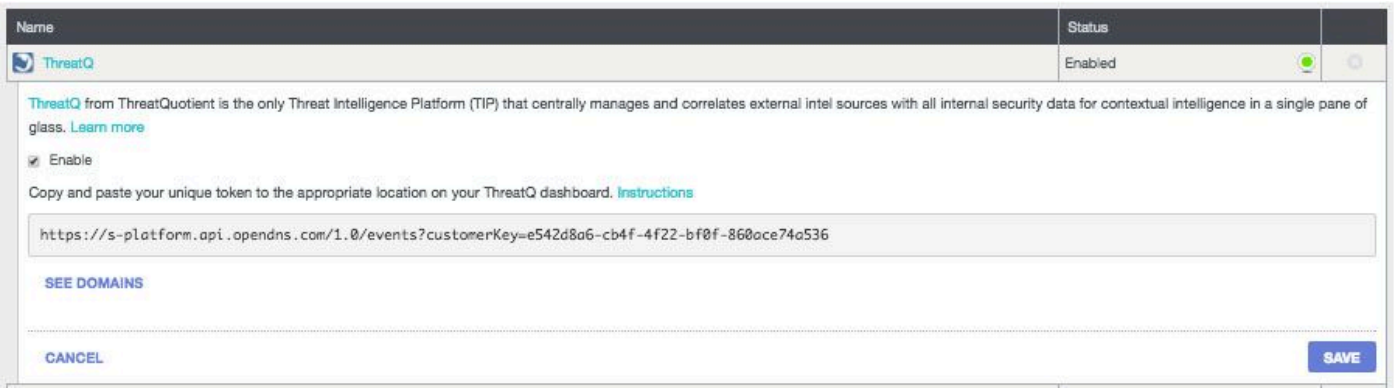
Geração de script Umbrella e token API

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 Settings > Integrations e selecione ThreatQ na tabela para expandi-la.

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



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

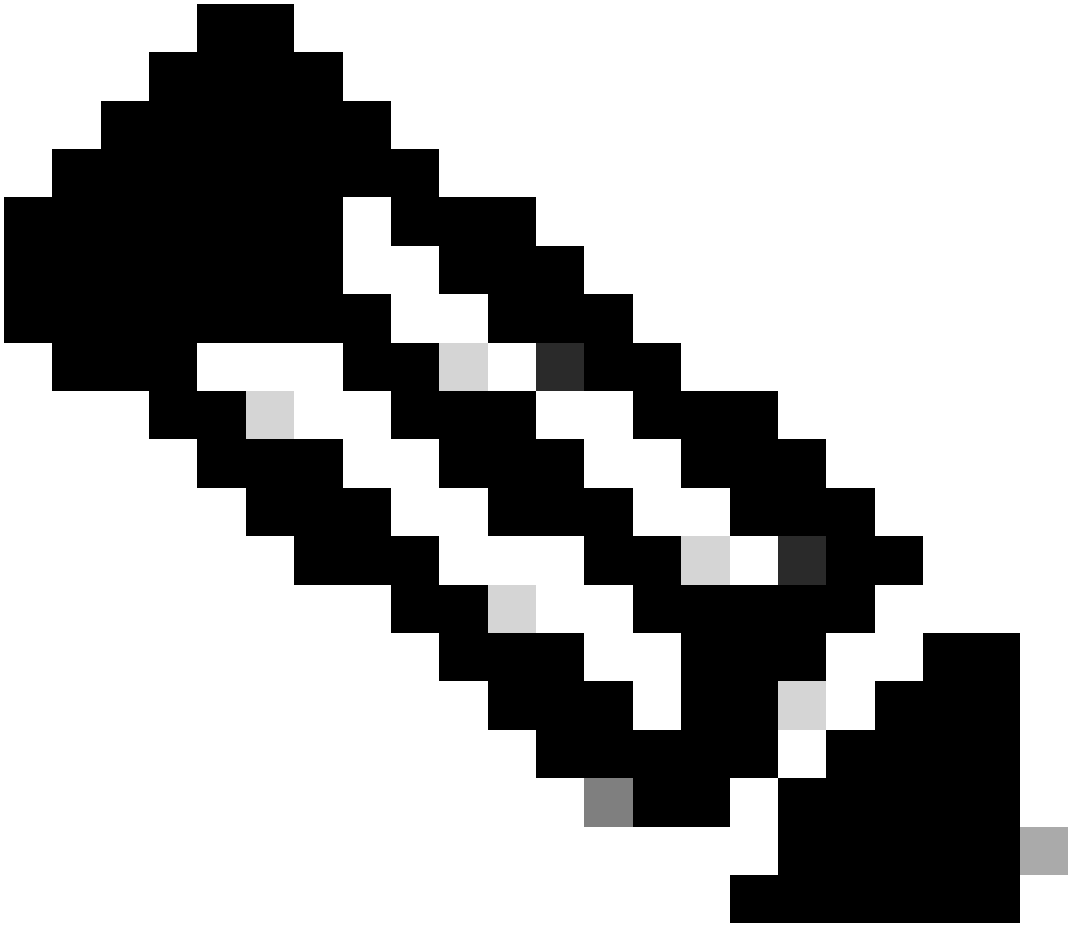
Como configurar o ThreatQ para se comunicar com o Umbrella

Faça login no painel do ThreatQ e adicione o URL na área apropriada para conectar-se ao Umbrella.

As instruções exatas variam e a Umbrella sugere que você entre em contato com o suporte do ThreatQ se não tiver certeza de como ou onde configurar integrações de API no ThreatQ.

Observação de eventos adicionados à categoria de segurança ThreatQ no modo de auditoria

Com o tempo, os eventos do painel do ThreatQ começam a preencher uma lista de destinos específica que pode ser aplicada às políticas como uma categoria de segurança do ThreatQ. 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 nenhuma política e não podem resultar em nenhuma alteração nas políticas do Umbrella existentes.



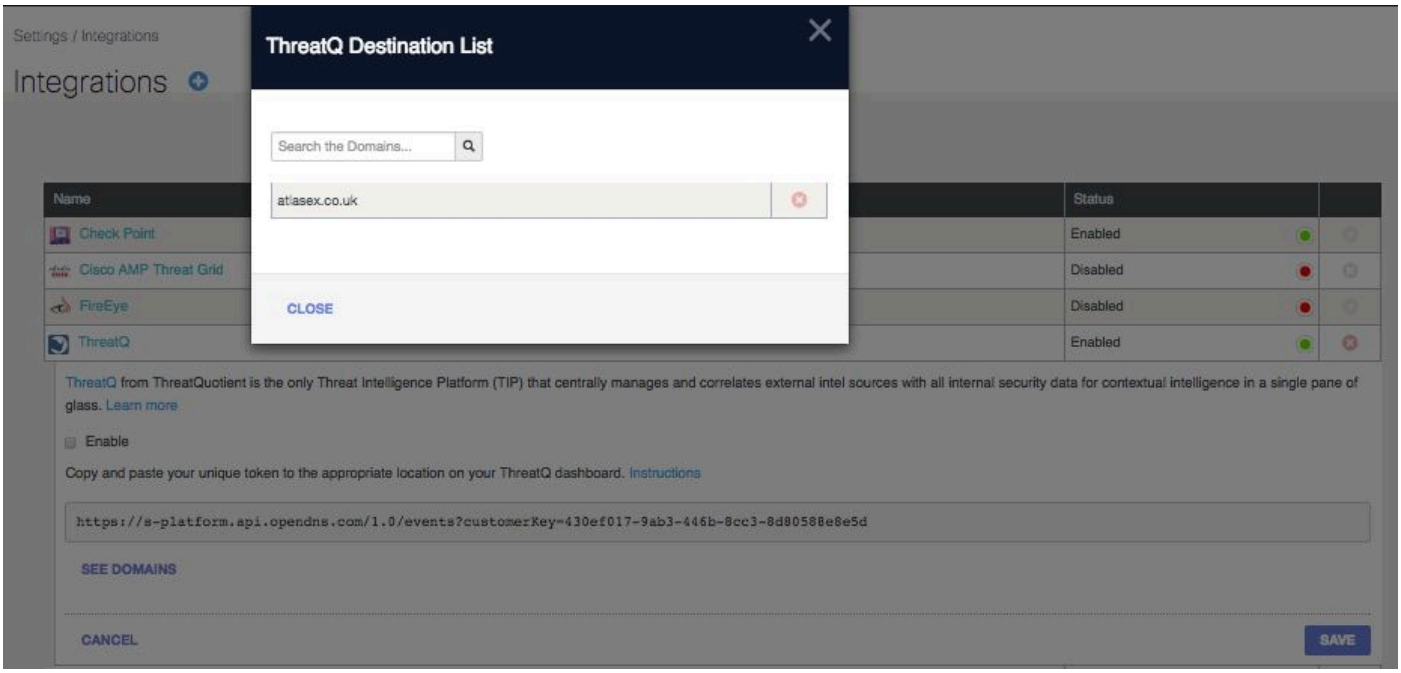
Note: O modo de auditoria pode ser ativado por quanto tempo for necessário, com base no perfil de implantação e na configuração da rede.

Revisar lista de destinos

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

1. Navegue até Configurações > Integrações.

2. Expanda ThreatQ na tabela e selecione Ver domínios.



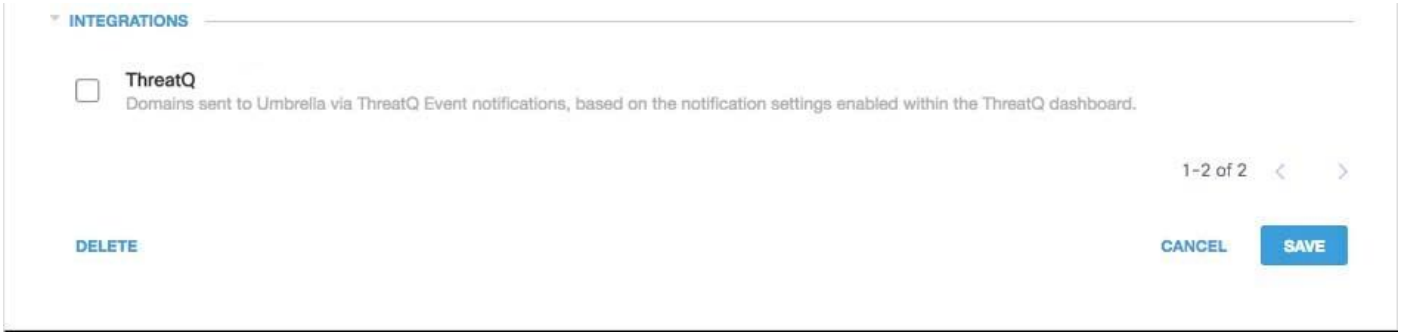
Revisar Configurações de Segurança para uma Política

Você pode revisar a configuração de segurança que pode ser habilitada para uma política no Umbrella a qualquer momento:

1. Navegue até Policies > Security Settings.

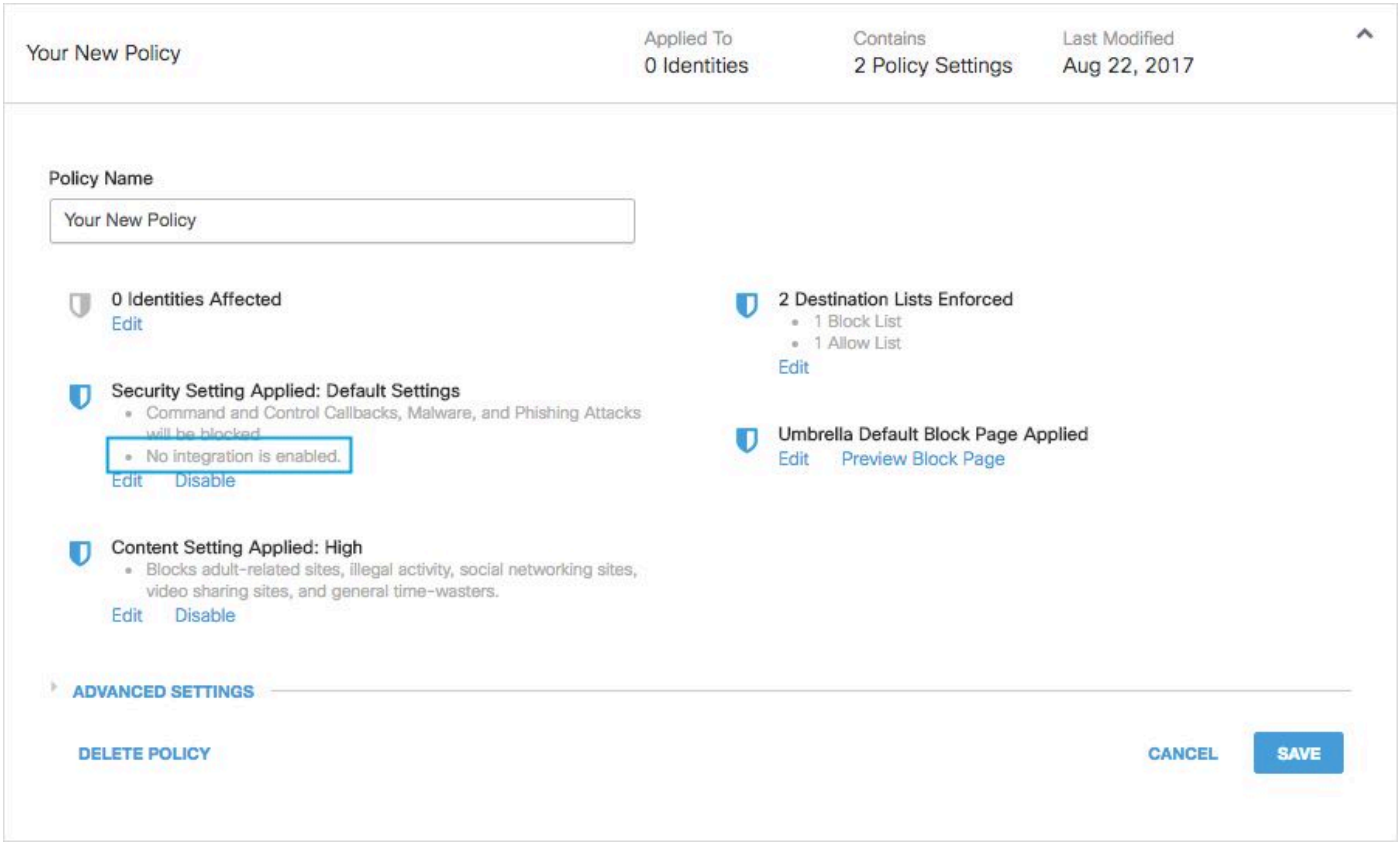
2. Selecione uma configuração de segurança na tabela para expandi-la.

3. Role até Integrations para localizar a configuração ThreatQ.



115014040286

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



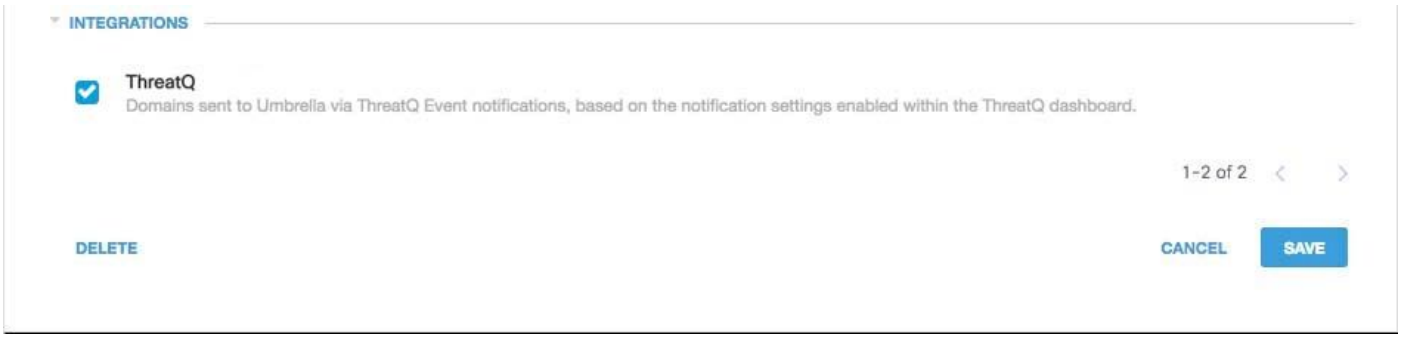
25464141748116

Aplicando as configurações de segurança do ThreatQ 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, você poderá 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.

2. Em Integrações, selecione ThreatQ e Salvar.



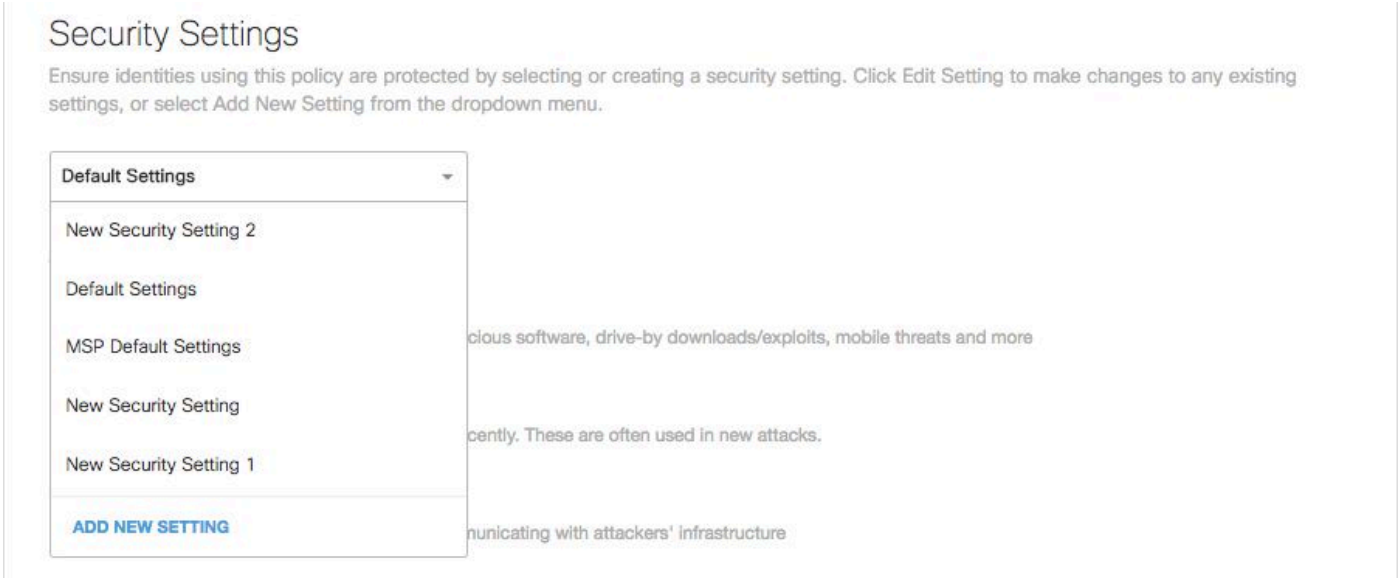
115014207403

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

1. Navegue até Policies > Policy List.

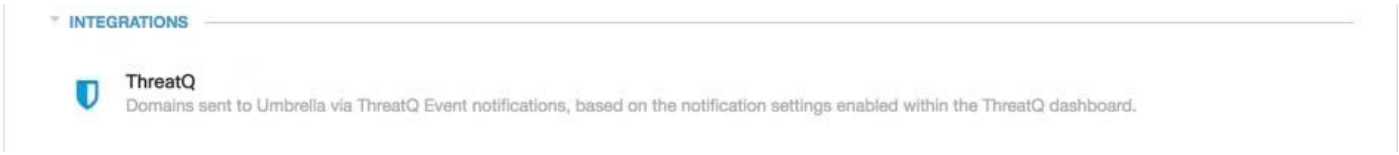
2. Expanda uma política e selecione Editar em Configuração de Segurança Aplicada.

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



25464141787668

O ícone de escudo em Integrações é atualizado para azul.



115014040506

4. Selecione Set & Return.

Os domínios do ThreatQ contidos na configuração de segurança do ThreatQ agora estão bloqueados para identidades que usam a política.

Relatórios em eventos do Umbrella for ThreatQ

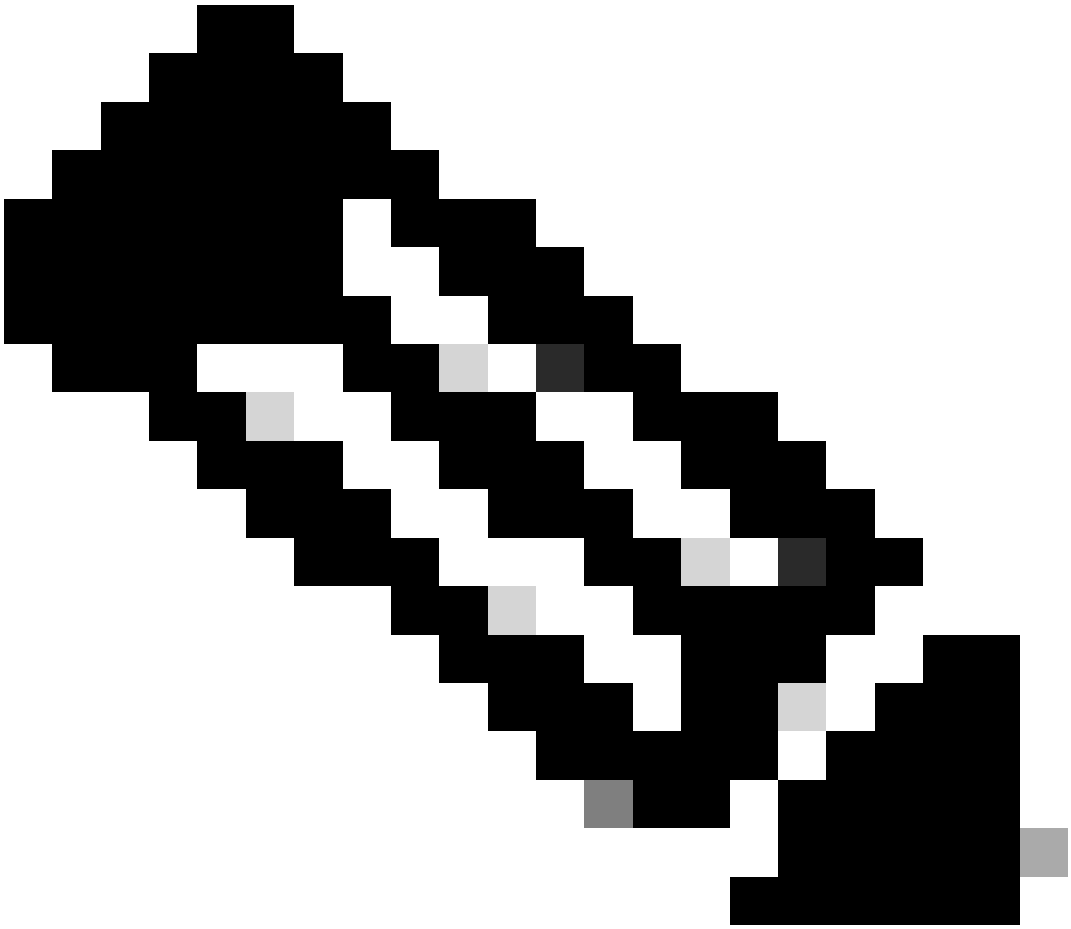
Relatórios sobre eventos de segurança do ThreatQ

A lista de destinos do ThreatQ 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 ThreatQ.

1. Navegue até Relatórios > Pesquisa de Atividade.

2. Em Categorias de Segurança, selecione ThreatQ para filtrar o relatório para mostrar apenas a

categoria de segurança para ThreatQ.



Note: Se a integração com o ThreatQ estiver desativada, ela não será exibida no filtro Categorias de segurança.

115014207603

3. Selecione Aplicar.

Relatórios de quando domínios foram adicionados à lista de destinos do ThreatQ

O log de auditoria do Umbrella Admin inclui eventos do painel do ThreatQ à medida que adiciona domínios à lista de destino. Um usuário chamado "Conta ThreatQ", que também é marcado com o logotipo ThreatQ, gera os eventos. Esses eventos incluem o domínio que foi adicionado e a hora em que ele foi adicionado. O registro de auditoria do Umbrella Admin pode ser encontrado em Relatórios > Log de auditoria do administrador.

Você pode filtrar para incluir apenas alterações de ThreatQ aplicando um filtro para o usuário da conta ThreatQ.

Lidando com detecções indesejadas ou falsos positivos

Listas de permissão

Embora seja improvável, é possível que os domínios adicionados automaticamente pelo ThreatQ possam disparar um bloqueio indesejado que possa impedir que os usuários acessem determinados sites. 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.

Esta abordagem é preferível por duas razões:

- Primeiro, caso o painel do ThreatQ fosse readicionar o domínio depois que ele fosse removido, a lista de permissões protegeria contra esse problema adicional.
- 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 ThreatQ 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 for 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 ThreatQ

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

Para excluir um domínio:

1. Navegue até Configurações > Integrações e selecione ThreatQ para expandi-lo.

2. Selecione Ver Domínios.

3. Procure o nome de domínio que deseja deletar.

4. Selecione o ícone Deletar.

5. Selecione Fechar.

6. Selecione 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 ThreatQ. Posteriormente, você poderá remover o domínio da lista de destinos do ThreatQ.

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.