Configurar a integração do Secure Malware Analytics (antigo Threat Grid) com o Umbrella

Contents

Introdução

Este documento descreve como integrar o Secure Malware Analytics (antigo Threat Grid) ao Umbrella.

Visão geral da integração do Cisco Secure Malware Analytics (Threat Grid) com o Cisco Umbrella

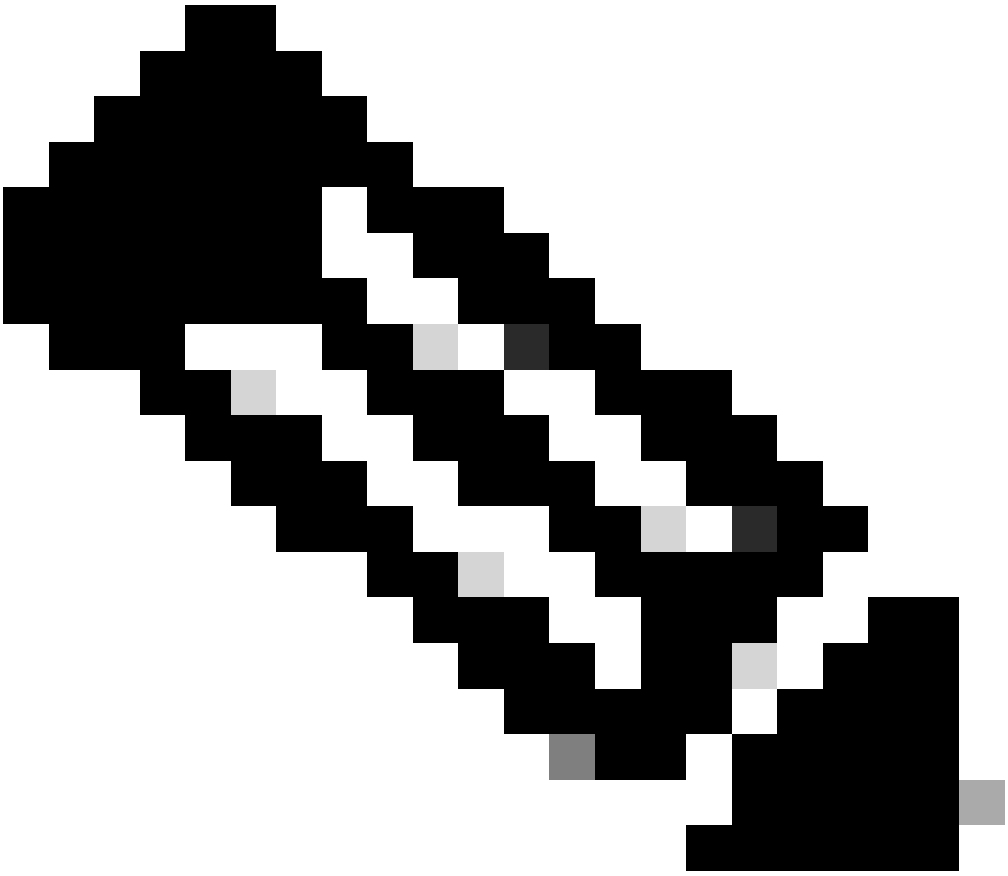
Com a integração entre o Cisco Secure Malware Analytics (antigo Threat Grid) e o Cisco Umbrella, as equipes de segurança agora podem ampliar sua visibilidade e aplicar a proteção contra as ameaças avançadas atuais a laptops, tablets ou telefones móveis, ao mesmo tempo em que fornecem outra camada de aplicação a uma rede corporativa distribuída.

Este guia descreve como configurar o Cisco Secure Malware Analytics (Threat Grid) para se comunicar com o Cisco Umbrella para que a inteligência de ameaças gerada pelo Cisco Secure Malware Analytics (Threat Grid) possa ser automaticamente integrada às políticas que podem

proteger os clientes sob o seu Cisco Umbrella.

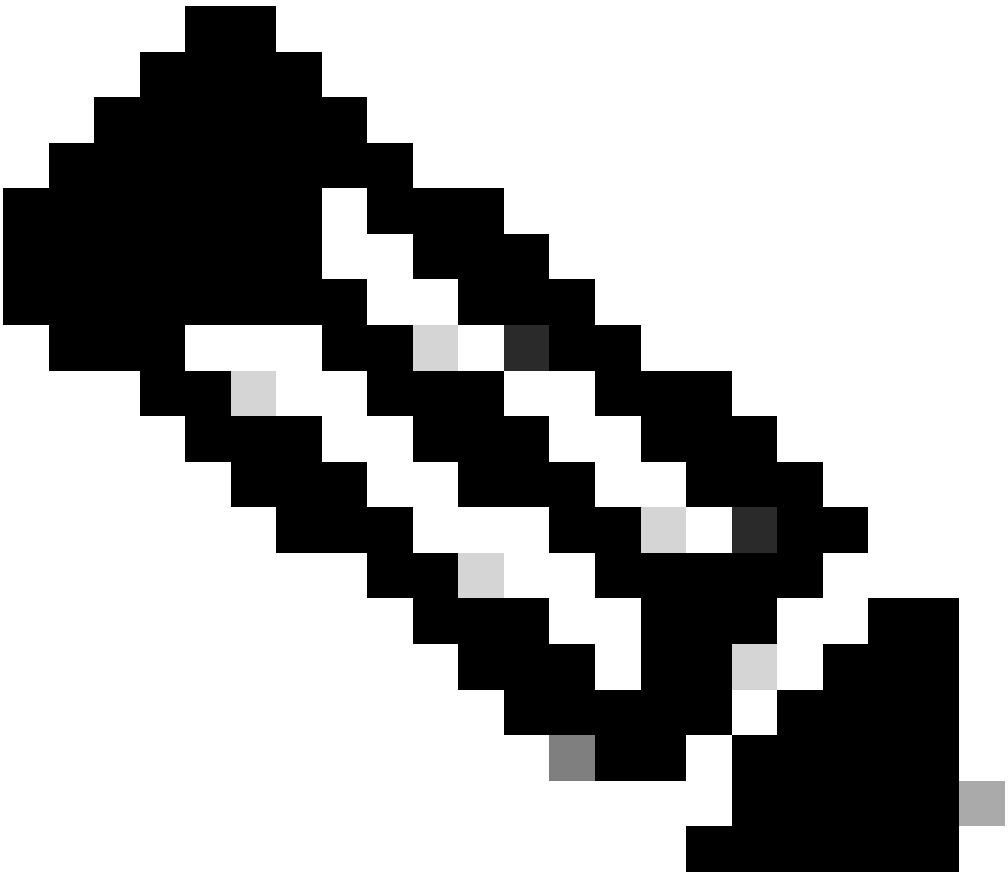
Pré-requisitos

- Um painel funcional do Cisco Secure Malware Analytics (Threat Grid) com acesso à chave de API da sua conta.



Note: Os dispositivos e endpoints do Cisco Secure Malware Analytics (Threat Grid) não são compatíveis no momento.

- Direitos administrativos do Cisco Umbrella Dashboard.
- O painel do Cisco Umbrella deve ter a integração do Cisco Secure Malware Analytics (Threat Grid) habilitada.



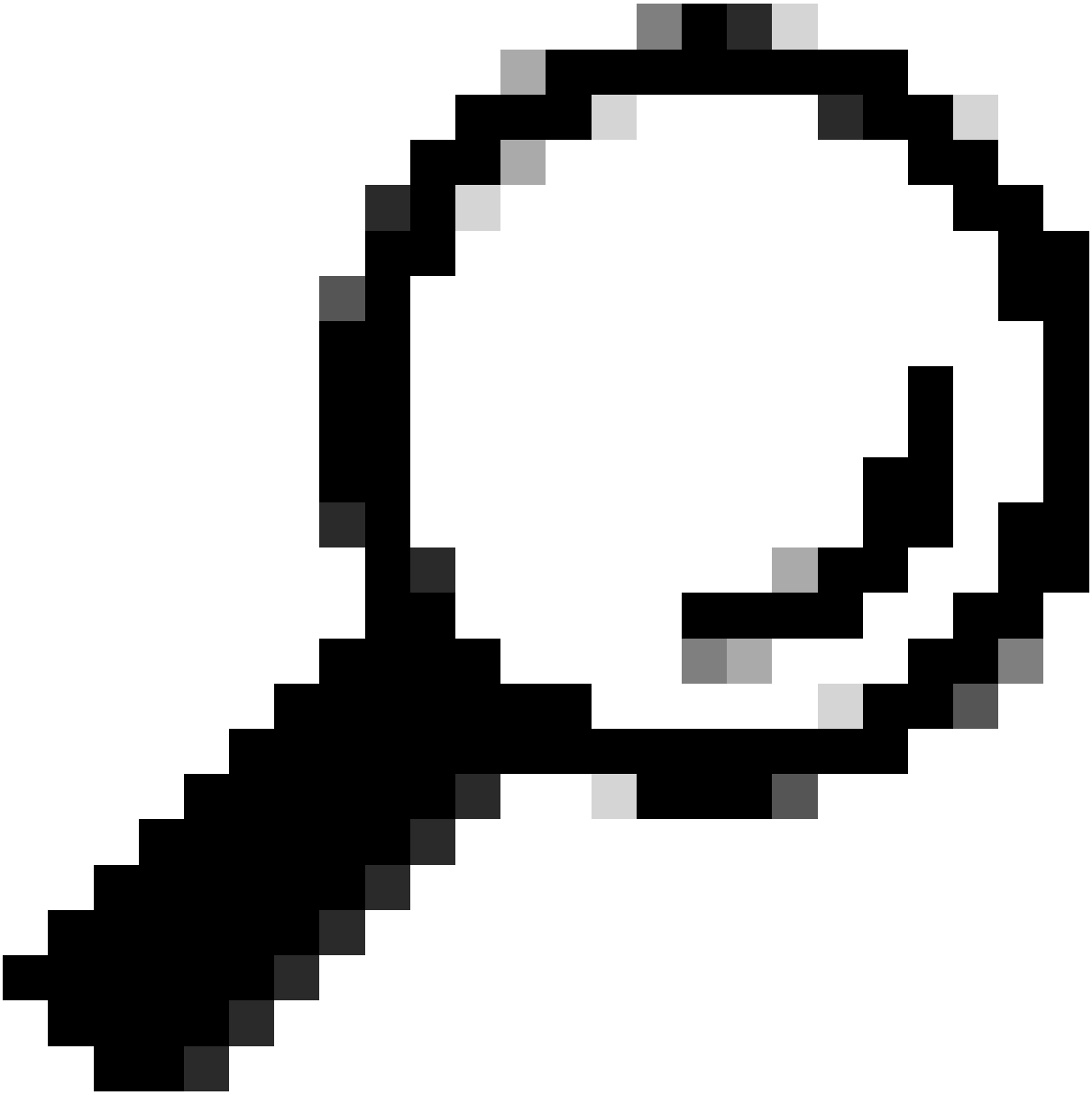
Note: A integração do Cisco Secure Malware Analytics (Threat Grid) está incluída apenas nos pacotes do Cisco Umbrella como DNS Essentials, DNS Advantage, SIG Essentials ou SIG Advantage. Se você não tiver um pacote Cisco Umbrella e quiser ter essa integração, entre em contato com seu Gerente de Conta Cisco Umbrella. Se você tiver um pacote Cisco Umbrella, mas não vir o Cisco Secure Malware Analytics (Threat Grid) como uma integração para o seu Painel, entre em contato com o Suporte do Cisco Umbrella.

Como essa integração funciona?

O Cisco Umbrella acessa a API do Cisco Secure Malware Analytics (Threat Grid) e recupera listas de domínios gerados a partir da análise de amostras mal-intencionadas. Em seguida, o Cisco Umbrella importa essa lista por meio da API de aplicação do Cisco Umbrella. Essa abordagem é diferente de como outras integrações funcionam, pois o Cisco Umbrella extrai a inteligência de ameaças fazendo consultas de API à API do Cisco Secure Malware Analytics (Threat Grid), em vez de aceitar incidentes de outros sistemas que enviam a inteligência de ameaças para o serviço Cisco Umbrella.

O Cisco Umbrella valida a ameaça para garantir que ela possa ser adicionada à sua política. Se as informações do Cisco Secure Malware Analytics (Threat Grid) forem confirmadas como uma ameaça ou não forem um domínio em boas condições, o endereço de domínio será adicionado à lista de destino do Cisco Secure Malware Analytics (Threat Grid) como parte de uma configuração de segurança que pode ser aplicada a qualquer política do Cisco Umbrella. Essa política é aplicada imediatamente a todas as solicitações feitas de dispositivos que usam políticas que aproveitam a integração do Cisco Secure Malware Analytics (Threat Grid).

O Cisco Umbrella recebe dois feeds separados do Cisco Secure Malware Analytics (Threat Grid): um feed Público (global) e um feed Apenas para cliente (particular, específico para um único cliente).



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 à Lista de Permissões Global ou a outras listas de destino, de acordo com sua política, os domínios que você nunca deseja bloquear.

Por exemplo:

- A página inicial da sua organização.
- Domínios que representam os serviços que você fornece que podem ter registros internos e externos. Por exemplo, "mail.myservicedomain.com" e "portal.myotherservicedomain.com".
- Você depende muito de aplicativos em nuvem menos conhecidos dos quais o Cisco Umbrella talvez não conheça ou não os inclua na validação automática de domínio. Por exemplo, "localcloudservice.com".

Esses domínios devem ser adicionados à Lista de permissões global, que se encontra em Políticas > Listas de destino no Cisco Umbrella.

Configurando seu painel do Cisco Umbrella para obter informações do Cisco Secure Malware Analytics (Threat Grid)

A primeira etapa é localizar ou gerar a chave de API no painel do Cisco Secure Malware Analytics (Threat Grid):

1. Faça login no painel do Cisco Secure Malware Analytics (Threat Grid) e selecione os detalhes da sua conta.
2. Em Detalhes da conta, uma chave de API pode já estar visível se você já tiver criado uma. Caso não tenha feito isso, selecione "Gerar nova chave de API".

   Sua chave de API estará visível em Detalhes do usuário > Chave de API.

Em seguida, adicione a chave de API ao Cisco Umbrella Dashboard para que ele obtenha dados do Cisco Secure Malware Analytics (Threat Grid):

1. Efetue login no painel do Cisco Umbrella como um administrador.
2. navegue até Policies > Policy Components > Integrations e selecione "Cisco AMP Threat Grid" (Cisco Secure Malware Analytics (Threat Grid)) na tabela para expandi-la.
3. Selecione Enable, cole sua chave de API na caixa API Key e selecione Save.

Neste ponto, se você receber um erro, provavelmente há um problema com a chave de API ou com as comunicações entre os serviços. Verifique sua chave de API e tente novamente e, se ainda falhar, entre em contato com o Suporte do Cisco Umbrella.

Se você receber uma mensagem de êxito, isso indica que o serviço Cisco Umbrella pôde usar a chave de API para fazer uma conexão inicial à API do Cisco Secure Malware Analytics (Threat Grid). O serviço Cisco Umbrella usa um intervalo de pesquisa de cinco minutos para recuperar dados do Cisco Secure Malware Analytics (Threat Grid).

Mesmo após o intervalo de cinco minutos, se não houver dados válidos ou eventos de ameaça válidos disponíveis para serem extraídos pelo Cisco Umbrella Dashboard, as informações podem não aparecer. Quando a integração é habilitada pela primeira vez, ela apenas começa voltando cinco minutos para os feeds global e somente organização e a primeira vez que obtém dados é no próximo intervalo de cinco minutos, portanto, os dados podem não aparecer imediatamente.

Se a chave de API no lado do Cisco Secure Malware Analytics (Threat Grid) fosse desativada ou removida, a integração seria desativada. Para restaurar a integração, uma nova chave de API deve ser fornecida no Cisco Umbrella Dashboard. Se houver um tempo limite ou um erro de serviço interno entre o Cisco Umbrella e o Cisco Secure Malware Analytics (Threat Grid), um tipo diferente de exceção será gerado e a integração não será desabilitada, mas, em vez disso, as conexões continuarão a ser tentadas a cada cinco minutos, como em condições normais.

Detalhes técnicos

As consultas de API exatas que estão sendo usadas para extrair informações do Cisco Secure Malware Analytics (Threat Grid) estão listadas abaixo. Observe que apenas eventos com severidade maior que 90, confiança maior que 90 e do tipo Domínios estão sendo reunidos. O tempo neste exemplo é um intervalo de cinco minutos que é incrementado para a próxima consulta. A `api_key` fornecida no Cisco Umbrella é usada no lugar da variável `<key>`:

- Público (feed global):

```
hxxps://panacea.threatgrid.com/api/v2/iocs/feeds/domains?limit=100&offset=0&severity=90&confidence
```

- Somente cliente (feed particular):

```
hxxps://panacea.threatgrid.com/api/v2/iocs/feeds/domains?limit=100&offset=0&severity=90&confidence
```

or:

- Público (feed global):

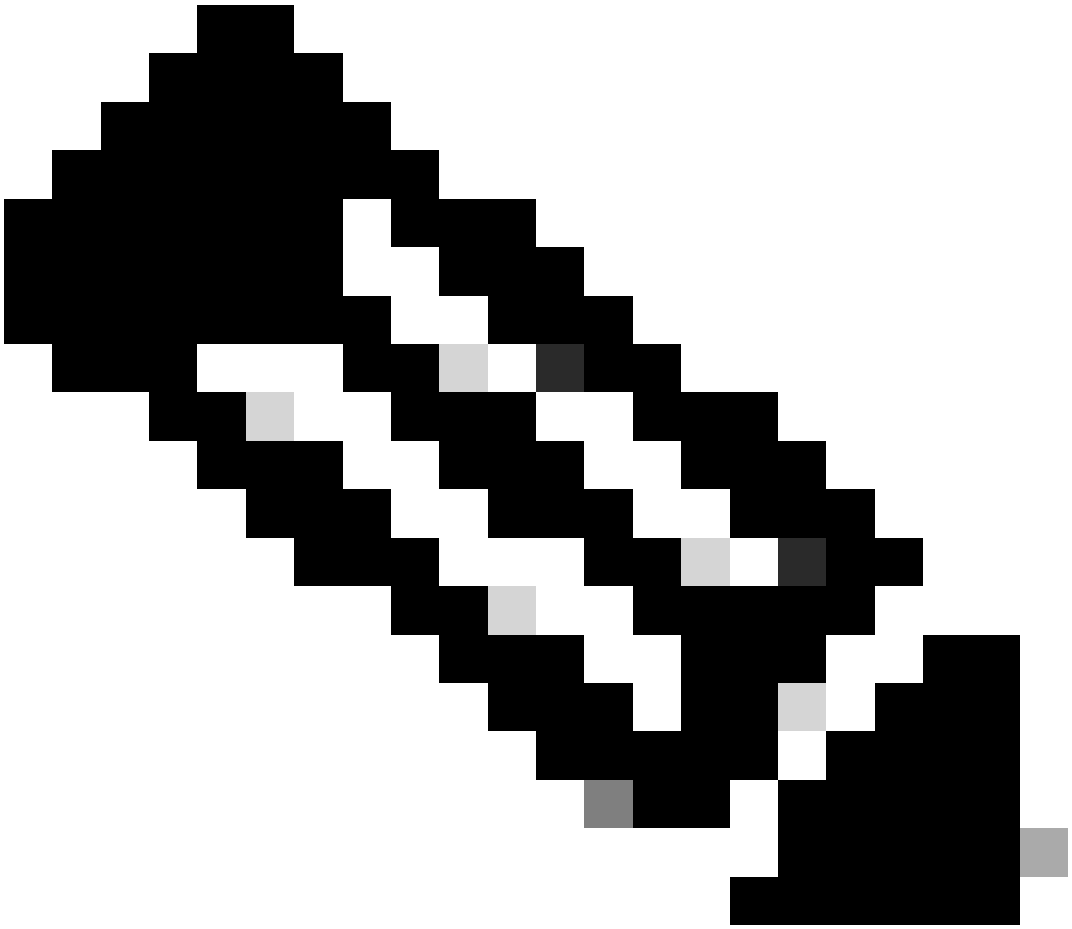
```
hxxps://panacea.threatgrid.eu/api/v2/iocs/feeds/domains?limit=100&offset=0&severity=90&confidence
```

- Somente cliente (feed particular):

```
hxxps://panacea.threatgrid.eu/api/v2/iocs/feeds/domains?limit=100&offset=0&severity=90&confidence=
```

Observação de eventos adicionados ao Cisco Secure Malware Analytics (Threat Grid) no "modo de auditoria"

Com o tempo, os eventos do Cisco Secure Malware Analytics (Threat Grid) começam a preencher uma lista de destinos específicos que pode ser aplicada a políticas como a categoria Cisco Secure Malware Analytics (Threat Grid). Por padrão, a lista de destino e a categoria de segurança estão no "modo de auditoria" e não são aplicadas a nenhuma política e, portanto, não resultam no bloqueio de nenhuma solicitação. No entanto, você pode ver quais solicitações estão associadas (e poderiam ter sido bloqueadas) pela categoria de segurança do Thread Grid de AMP da Cisco.



Note: O "modo de auditoria" pode ser ativado enquanto for necessário, ou até mesmo indefinidamente, dependendo do seu perfil de implantação e da configuração da rede.

Revisar lista de destinos

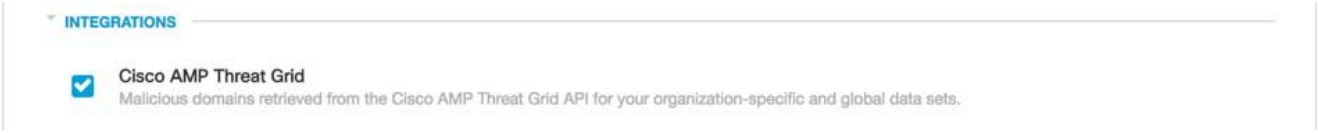
Você pode rever a lista de destinos do Cisco Secure Malware Analytics (Threat Grid)a qualquer momento.

1. Navegue até Policies > Policy Components > Integrations.
2. Expanda "Cisco AMP Threat Grid" (Cisco Secure Malware Analytics (Threat Grid)) na tabela e selecione "Ver domínios".

Revisar Configurações de Segurança para uma Política

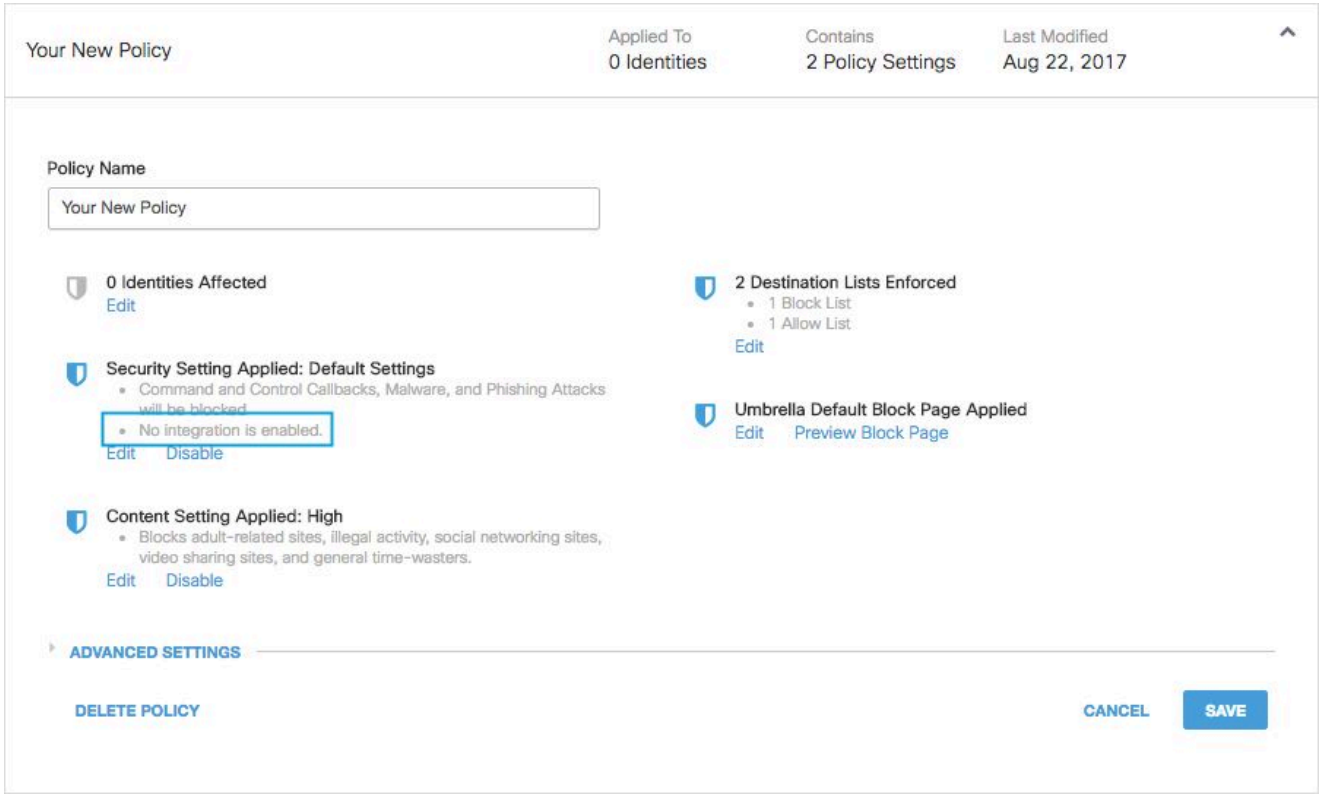
Você pode revisar as configurações de segurança que podem ser ativadas para uma política a qualquer momento no Cisco Umbrella:

1. Navegue até Policies > Policy Components > Security Settings.
2. Clique em uma configuração de segurança na tabela para expandi-la.
3. Role até a seção Integrações e expanda a seção para exibir a integração do Cisco AMP Threat Grid (Cisco Secure Malware Analytics (Threat Grid)).
4. Selecione a caixa para a integração do Cisco AMP Threat Grid (Cisco Secure Malware Analytics (Threat Grid)) e selecione Save.

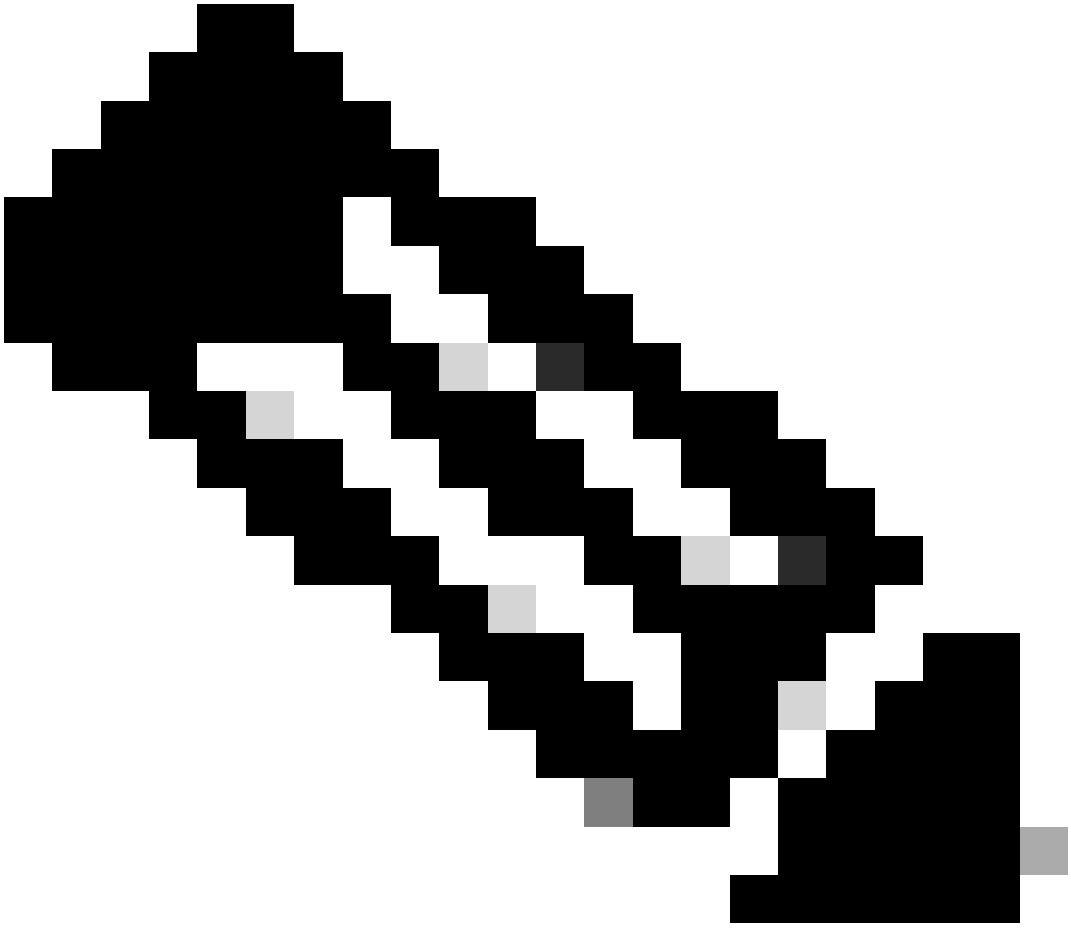


115014151543

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



20993269073556

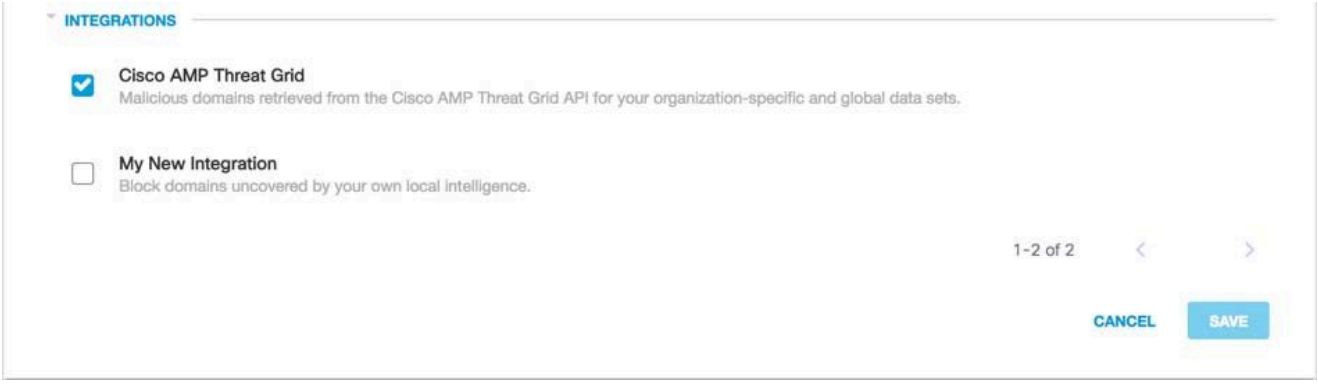


Note: Pode levar até cinco minutos para aplicar as configurações e, se novos eventos não estiverem sendo injetados no sistema Cisco Secure Malware Analytics (Threat Grid), talvez você não veja novos domínios sendo adicionados à sua integração.

Aplicação da configuração de segurança do Cisco Secure Malware Analytics (Threat Grid) no "modo de bloqueio" a uma política para clientes gerenciados

Quando estiver pronto para ter esses domínios bloqueados para clientes gerenciados pelo Cisco Umbrella, altere a configuração de segurança em uma política existente ou crie uma nova política que fique acima da sua política padrão para garantir que ela seja aplicada primeiro.

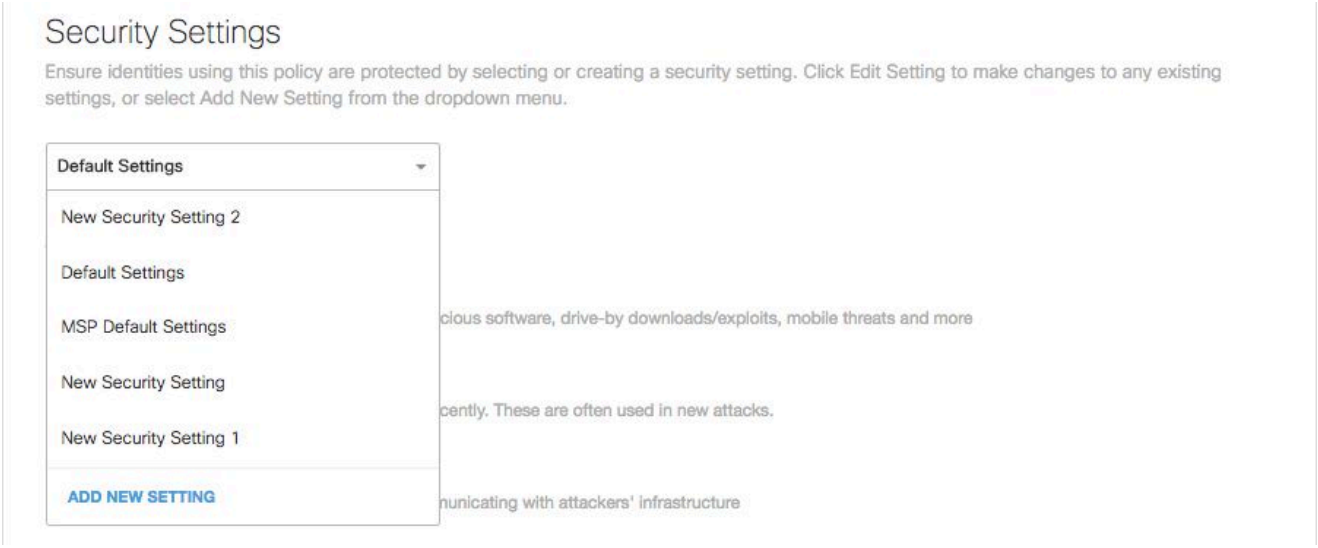
1. Navegue até Policies > Policy Components > Security Settings.
2. Em Integrations, verifique se a caixa "Cisco AMP Threat Grid" está selecionada. Caso contrário, marque a caixa e selecione Salvar.



115013987086

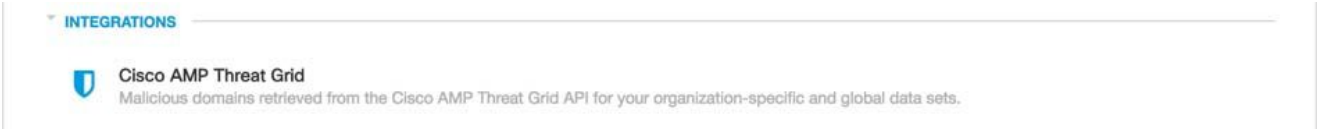
Em seguida, no assistente Cisco Umbrella Policy, adicione uma configuração de segurança à política que você está editando:

1. Navegue até Policies > Management > All Policies.
2. Expanda uma diretiva e em Configuração de segurança aplicada e selecione Editar.
3. No menu suspenso Security Settings, selecione uma configuração de segurança que inclua a configuração "Cisco AMP Threat Grid".



20993282642708

O ícone de escudo em Integrações é atualizado para azul.



115013987446

4. Selecione Set & Return.

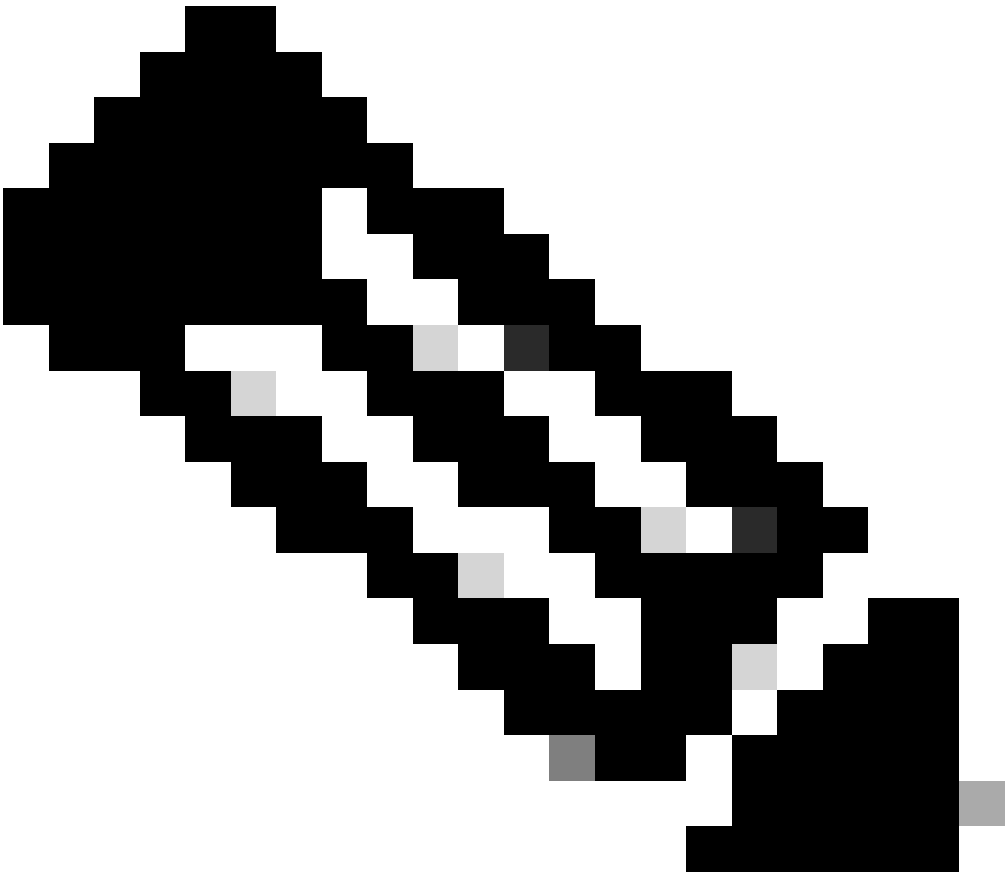
   Os domínios do Cisco Secure Malware Analytics (Threat Grid) contidos na configuração de segurança do Cisco Secure Malware Analytics (Threat Grid) são bloqueados para essas identidades usando a política.

Relatórios dentro do Cisco Umbrella para eventos do Cisco Secure Malware Analytics

Relatórios sobre eventos de segurança do Cisco Secure Malware Analytics (Threat Grid)

A lista de destino do Cisco Secure Malware Analytics (Threat Grid) 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 categorias de segurança para mostrar apenas atividades relacionadas ao Cisco Secure Malware Analytics (Threat Grid).

1. Navegue para Relatórios > Relatórios principais > Pesquisa de atividade e, em Categorias de segurança, selecione "Cisco AMP Threat Grid" (Cisco Secure Malware Analytics (Threat Grid)) para filtrar o relatório e mostrar apenas a categoria de segurança para o Cisco Secure Malware Analytics (Threat Grid).



Note: Se a integração do Cisco AMP Threat Grid estiver desabilitada, ela não será exibida no filtro Categorias de segurança.

115014210123

2. Selecione Apply.

Relatórios sobre quando os domínios foram adicionados à lista de destino do Cisco Secure Malware Analytics (Threat Grid)

O log de auditoria do Cisco Umbrella Admin inclui eventos do painel do Cisco Secure Malware Analytics (Threat Grid) à medida que adiciona domínios à lista de destino. Um usuário chamado "Lista de domínios do Thread Grid de AMP da Cisco", que também é marcado com o logotipo da Cisco, gera os eventos. Esses eventos incluem o domínio que foi adicionado e a hora em que ele foi adicionado.

A seleção da entrada Log de auditoria Admin a expande para mostrar detalhes, incluindo o domínio específico que foi adicionado.

Você pode filtrar para incluir apenas as alterações do Cisco Secure Malware Analytics (Threat Grid) aplicando um filtro para o usuário da "Lista de domínios do Cisco AMP Threat Grid".

Lidando com detecções indesejadas ou falsos positivos

Dois tipos de detecções do Cisco Secure Malware Analytics (Threat Grid) e duas resoluções

Atualmente, há dois tipos de blocos do Cisco Secure Malware Analytics (Threat Grid): Um com uma resolução possível e um segundo com uma resolução atual para uma detecção indesejada.

1. Entrada do Threat Grid Global (Pública): No momento, o único método para permitir o domínio é adicioná-lo à sua lista de permissões.
2. Feed somente para clientes (Particular): pode ser endereçado com uma entrada de lista de permissão ou exclusão da lista de integração do AMP Threat Grid.

Listas de permissão

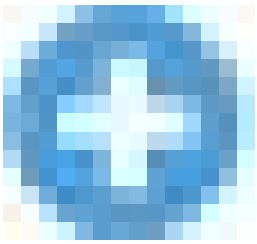
Embora seja improvável, é possível que os domínios adicionados automaticamente pela integração do Cisco Secure Malware Analytics (Threat Grid) possam disparar uma detecção indesejada que bloqueie o acesso de usuários a sites específicos. Em uma situação como essa, recomendamos adicionar o(s) domínio(s) a uma lista de permissão (Políticas > Listas de destino), 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 Cisco Secure Malware Analytics (Threat Grid) fosse readicionar o domínio depois que ele fosse removido, a lista de permissões protegeria contra esse problema que causaria mais problemas. Em segundo lugar, a lista de permissão mostra um registro histórico de domínios problemáticos que podem ser usados para relatórios forenses ou 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 Cisco Secure Malware Analytics (Threat Grid) no modo de bloqueio for aplicada apenas a um subconjunto de suas identidades gerenciadas do Cisco 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 > Policy Components > Destination Lists e selecione 

25463394696852

("Adicionar")
2. Selecione Permitir e adicione seu domínio à lista.
3. Selecione Save.

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

Excluindo domínios da lista de destino do Cisco Secure Malware Analytics (Threat Grid)

Ao lado de cada nome de domínio na lista do Cisco Secure Malware Analytics (Threat Grid) há um ícone ("Excluir"). A exclusão de domínios permite que você limpe a lista de destinos do Cisco Secure Malware Analytics (Threat Grid) no caso de uma detecção indesejada.

A exclusão não será permanente se o painel do Cisco Secure Malware Analytics (Threat Grid) reenviar o domínio para o Cisco Umbrella.

1. Navegue até Policies > Policy Components > Integrations e selecione "Cisco AMP Threat Grid" (Cisco Secure Malware Analytics (Threat Grid)) para expandi-lo.
2. Selecione Ver domínios.
3. Procure o nome de domínio que deseja excluir.
4. Selecione o ícone ("Excluir").
5. Selecione Fechar.
6. Selecione Save.

No caso de uma detecção indesejada ou falso positivo, recomendamos a criação imediata de uma lista de permissões no Cisco Umbrella e, em seguida, a correção do falso positivo no painel do Cisco Secure Malware Analytics (Threat Grid). Posteriormente, você poderá remover o domínio da lista de destinos do Cisco Secure Malware Analytics (Threat Grid).

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.