Entender a API de aplicação de guarda-chuva para integrações personalizadas

Contents

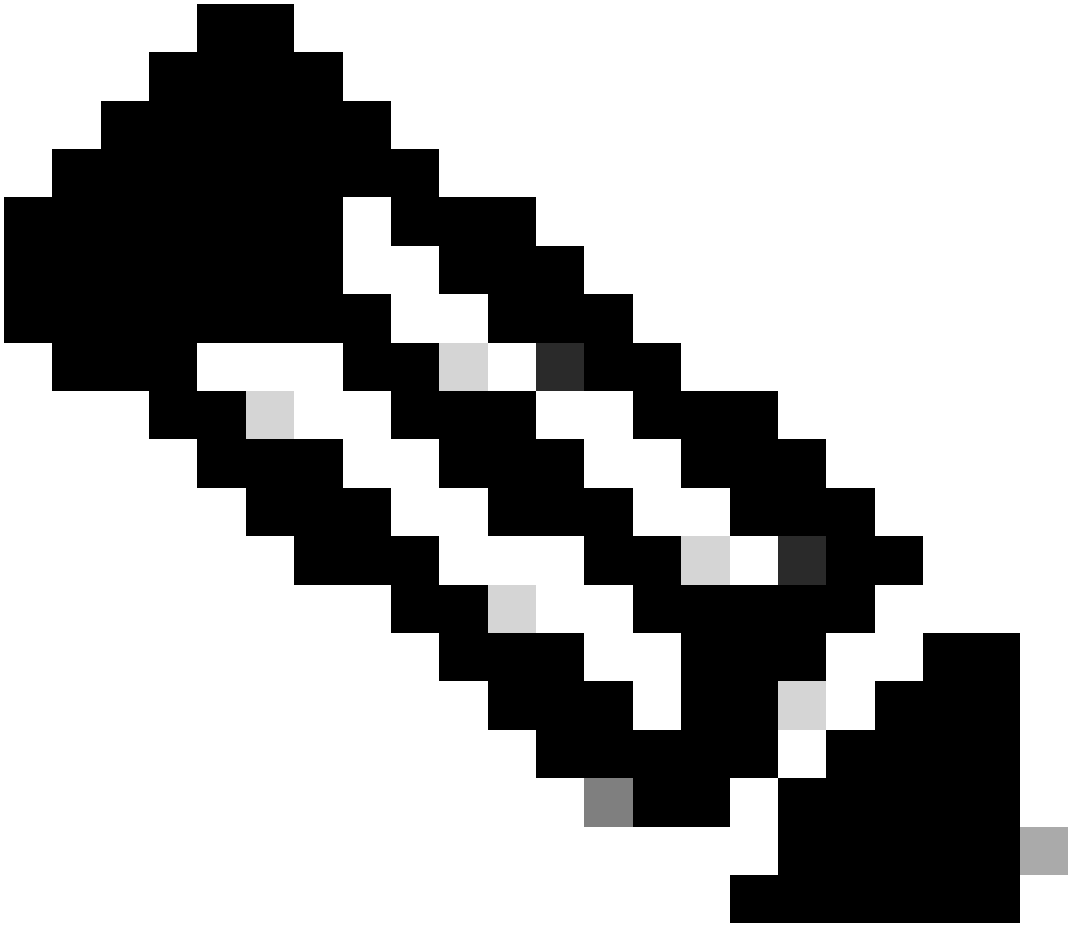
Introdução

Este documento descreve a API de aplicação de guarda-chuva para integrações personalizadas.

O que é a API de aplicação de guarda-chuva?

A API de aplicação do Umbrella permite que parceiros e clientes com seus próprios ambientes SIEM/Plataforma de inteligência de ameaças (TIP) internos injetem eventos e/ou inteligência de ameaças em seu ambiente Umbrella. Esses eventos são convertidos instantaneamente em visibilidade e aplicação que podem se estender além do perímetro e, assim, o alcance dos sistemas que podem ter gerado esses eventos ou inteligência de ameaças.

A API de imposição pode incluir eventos no formato de evento genérico descrito nesta documentação da API e pode suportar as funções ADD, DELETE ou LIST.



Note: Se você não tiver a API de aplicação do Umbrella para integrações personalizadas em seu painel do Umbrella e quiser ter acesso, entre em contato com seu representante da Cisco Umbrella.

Por que eu o usaria?

Você já pode processar, gerenciar e organizar seu próprio sistema de inteligência de ameaças e processos que resultem no desejo de tomar medidas em domínios identificados como mal-intencionados ou suspeitos. Nesse caso, uma vez tomada a decisão de que um evento precisa ser acionado (por exemplo, convertido em proteção), em vez de adicionar manualmente a proteção ao Umbrella para fins de aplicação, você pode usar a API de Aplicação para automatizar esse processo e aplicar instantaneamente a proteção com base nos domínios associados ao evento.

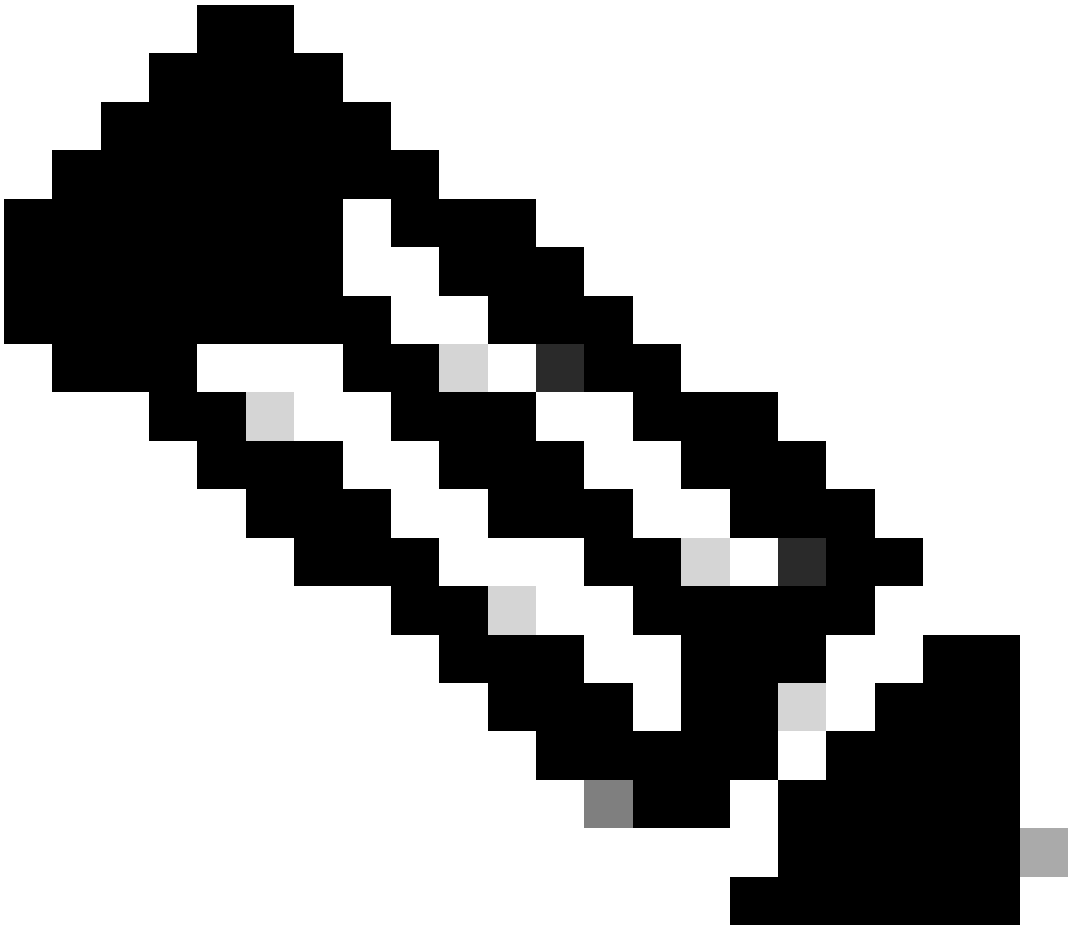
Isso permite que sua equipe de segurança concentre seu tempo e esforço na investigação, em vez da configuração contínua do Umbrella. Ele permite que sua equipe de segurança fique dentro

de suas ferramentas e processos, em vez de ter que ir para o painel do Umbrella para atualizar as listas de destino. Em essência, você é capaz de criar uma lista de destinos no Umbrella a partir de uma fonte externa que você gerencia diretamente através da API, em seguida, escolher bloquear esses destinos para identidades dentro do Umbrella.

Como Eu O Usaria?

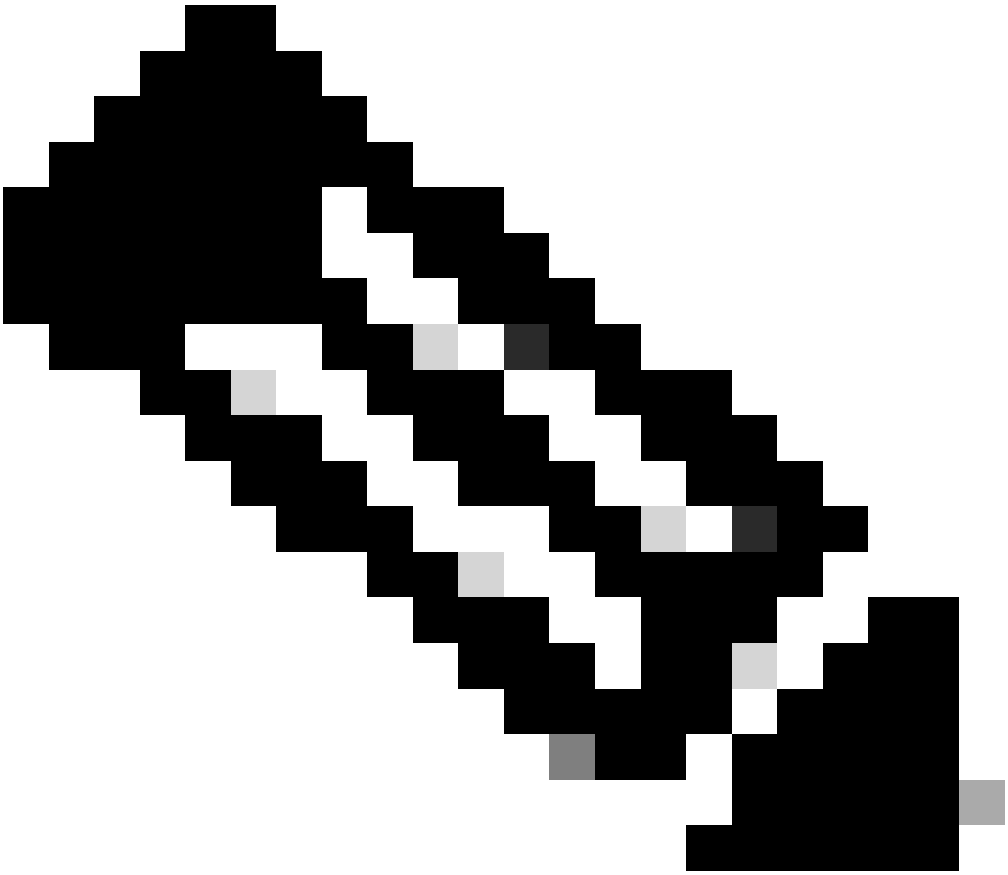
ADICIONAR um evento à API de imposição

Depois que um evento é adicionado, a Imposição tenta extrair domínios do evento.



Note: O suporte para endereços IP e URLs será adicionado no futuro.

- Um evento pode conter qualquer quantidade dos detalhes originais do evento que você gostaria, mas precisa seguir as especificações descritas na documentação da API.



Note: O suporte para detalhes de eventos de superfície no painel Umbrella poderá ser adicionado no futuro.

- Se um domínio for extraído, ele será validado pelo gráfico de segurança do Cisco Umbrella para garantir que não seja um domínio em boas condições que provavelmente resulte em falsos positivos ou que já tenha sido considerado mal-intencionado pelo gráfico de segurança do Cisco Umbrella.
- Se for aprovado na validação (por exemplo, é desconhecido e seguro bloquear), ele será adicionado a uma lista de destinos associada a essa integração personalizada e aparecerá no painel do Umbrella como uma categoria de segurança personalizada.
- A categoria de segurança personalizada pode ser bloqueada ou permitida em uma base por política, para permitir a aplicação ativa ou a "auditoria" passiva de solicitações suspeitas.

LISTAR domínios para uma Lista de API de Imposição

- Se o seu fluxo de trabalho incluir o desbloqueio de domínios que foram bloqueados devido a eventos injetados anteriormente, uma solicitação LIST fornecerá todos os domínios

atualmente incluídos na lista de destino associada a essa integração.

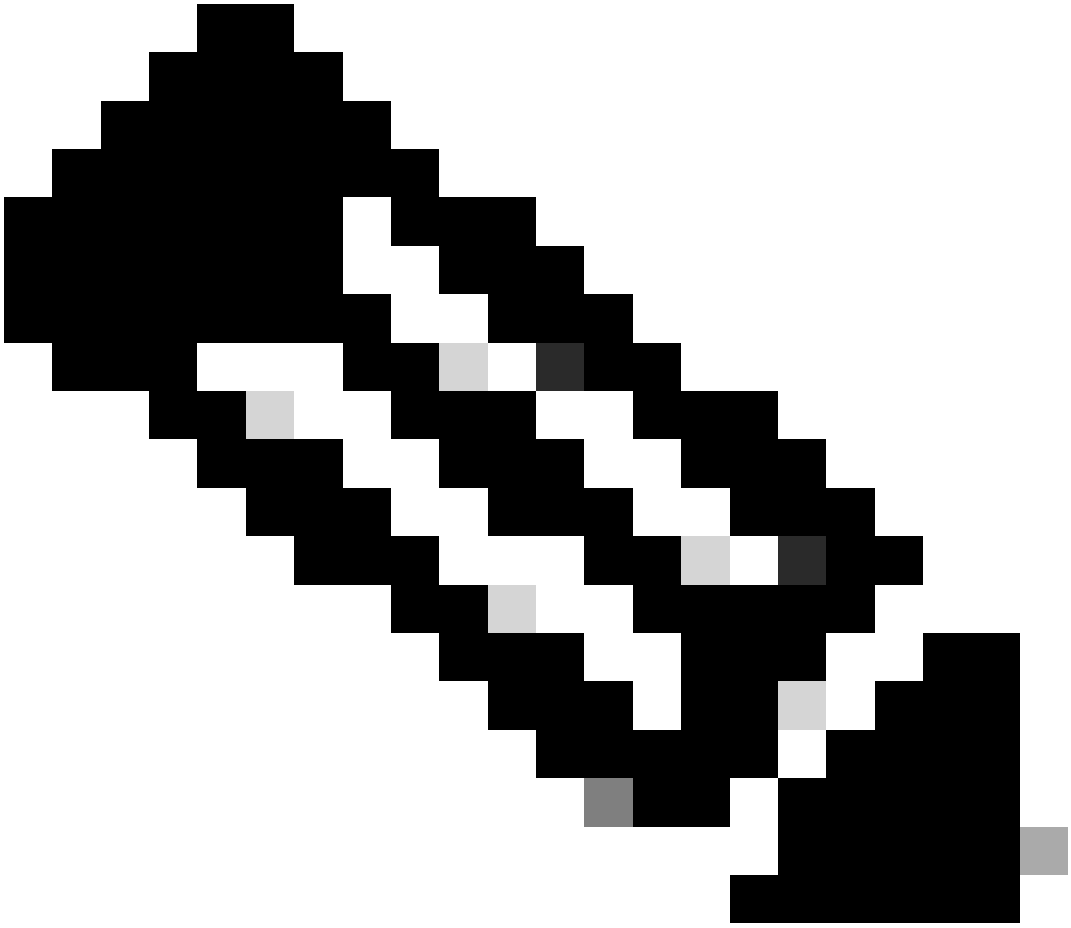
EXCLUIR Domínio da Lista de API de Imposição

- Se o seu fluxo de trabalho incluir o desbloqueio de domínios que foram bloqueados devido a eventos injetados anteriormente, uma solicitação DELETE permitirá que você remova um domínio da lista de destino associada a essa integração.
- Se uma solicitação DNS de entrada de uma de suas identidades do Umbrella for destinada a um domínio na lista de destino de integração personalizada, ela será bloqueada ou permitida, dependendo da configuração de segurança da integração personalizada associada à política que a disparou.
- Os resultados são registrados junto com todos os outros eventos Umbrella, acessíveis através da Pesquisa de Atividade, ou através da Amazon S3 usando a integração S3. Assim, o tráfego associado à integração personalizada pode, opcionalmente, ser incluído de volta em seu SIEM/TIP e o loop de feedback fechado.

Acompanhamento do uso da API de imposição

Passo 1: Crie sua integração personalizada

Você pode ter até 10 integrações personalizadas de uma só vez.



Note: Se a organização for uma org. filha de um MSP, MSSP ou MOC do Umbrella, as integrações personalizadas compartilhadas no nível do console serão exibidas antes das integrações criadas no nível da org. filha.

1. No Umbrella, navegue para Policies > Policy Components > Integrations e clique em Add.
2. Adicione um nome para a integração personalizada e clique em Criar.
3. Expanda sua nova integração personalizada, marque Habilitar, copie o URL de integração e clique em Salvar.

Passo 2: Crie seu(s) script(s) personalizado(s).

1. Consulte os scripts de exemplo generate_event e delete_domain no apêndice deste documento ou use a documentação da API para criar seus próprios scripts para gerar as solicitações formatadas corretamente para gerar eventos ou excluir ou listar domínios. Você vai querer usar a URL de integração personalizada nesses scripts daqui para frente.

Passo 3: Injetar um evento de exemplo

1. Use o script que você criou para injetar um evento em sua integração personalizada. Em nosso exemplo, injetamos um evento que contém o domínio "creditcards.com".

Passo 4: Verifique a lista de destinos no painel do Umbrella

1. Retorne a Settings > Integrations e, na tabela, expanda a integração personalizada.
2. Clique em Ver domínios. Uma lista pesquisável dos domínios adicionados é exibida e seu evento de exemplo da Etapa 4 agora está na lista.

Passo 5: Verifique o Log de auditoria do administrador.

1. Outra maneira de verificar a atividade associada à sua integração personalizada é revisando o Log de Auditoria de Admin.
2. Navegue até Relatórios > Log de auditoria do administrador.
3. Em Filtros, insira o nome de sua integração personalizada em Filtrar por identidades e configurações e clique em Executar filtro.

Ao expandir a entrada, você verá o evento que resultou na adição do seu evento de exemplo (creditcards.com) à sua integração personalizada.

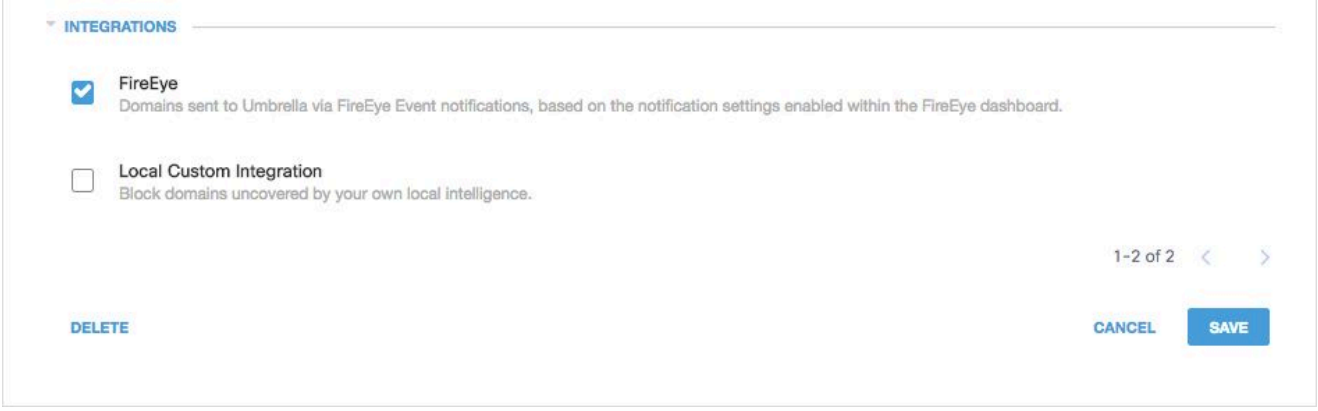
Etapa opcional: Listar ou excluir domínios

Você também pode querer testar para garantir que é capaz de listar domínios em sua integração personalizada e excluir domínios caso não queira mais aplicá-los no domínio ou tê-los em sua integração. Use as etapas descritas na documentação da API para listar e excluir domínios.

Definir configurações de segurança

Agora que você validou que pode injetar eventos (e, opcionalmente, listar e excluir domínios), pode configurar o que deseja que aconteça com as solicitações DNS de suas identidades que são destinadas a domínios na categoria de segurança da sua integração personalizada.

1. Navegue até Policies > Security Settings e, em Integrations, verifique a integração ativada (neste exemplo, FireEye) e clique em Save.

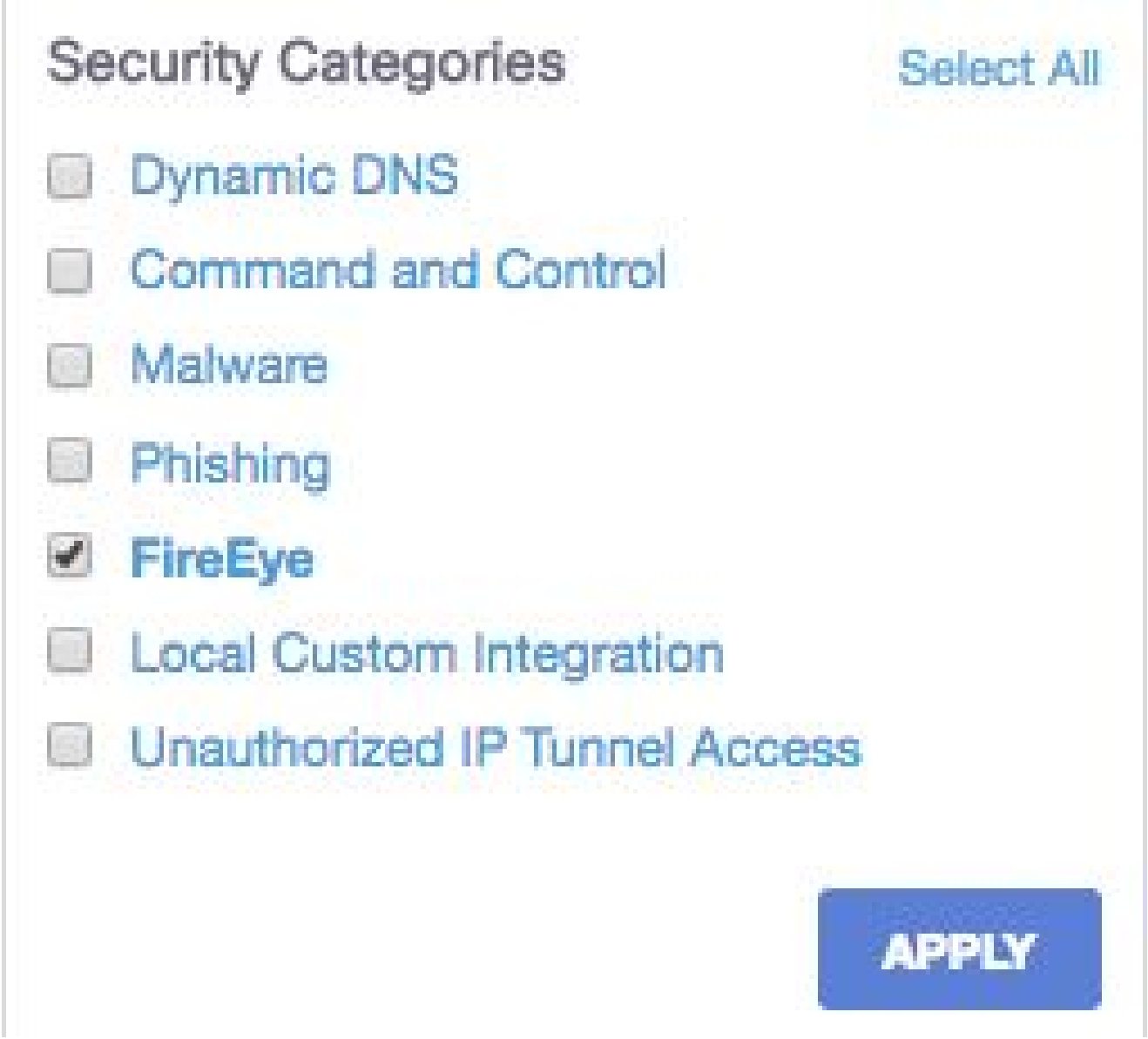


115014145103

Exibir relatórios para sua integração personalizada

Gere solicitações DNS de uma de suas identidades (por exemplo, Redes ou Computadores em Roaming) destinada ao domínio em sua integração personalizada ("creditcards.com" em nosso exemplo). Do ponto de vista do cliente, agora você vê o bloqueio apropriado ou o resultado de permissão, dependendo de como definiu suas configurações de segurança.

1. Navegue para Relatórios > Pesquisa de atividade e, em Categorias de segurança, selecione sua integração personalizada (neste exemplo, FireEye) para filtrar o relatório para mostrar apenas a categoria de segurança para FireEye.

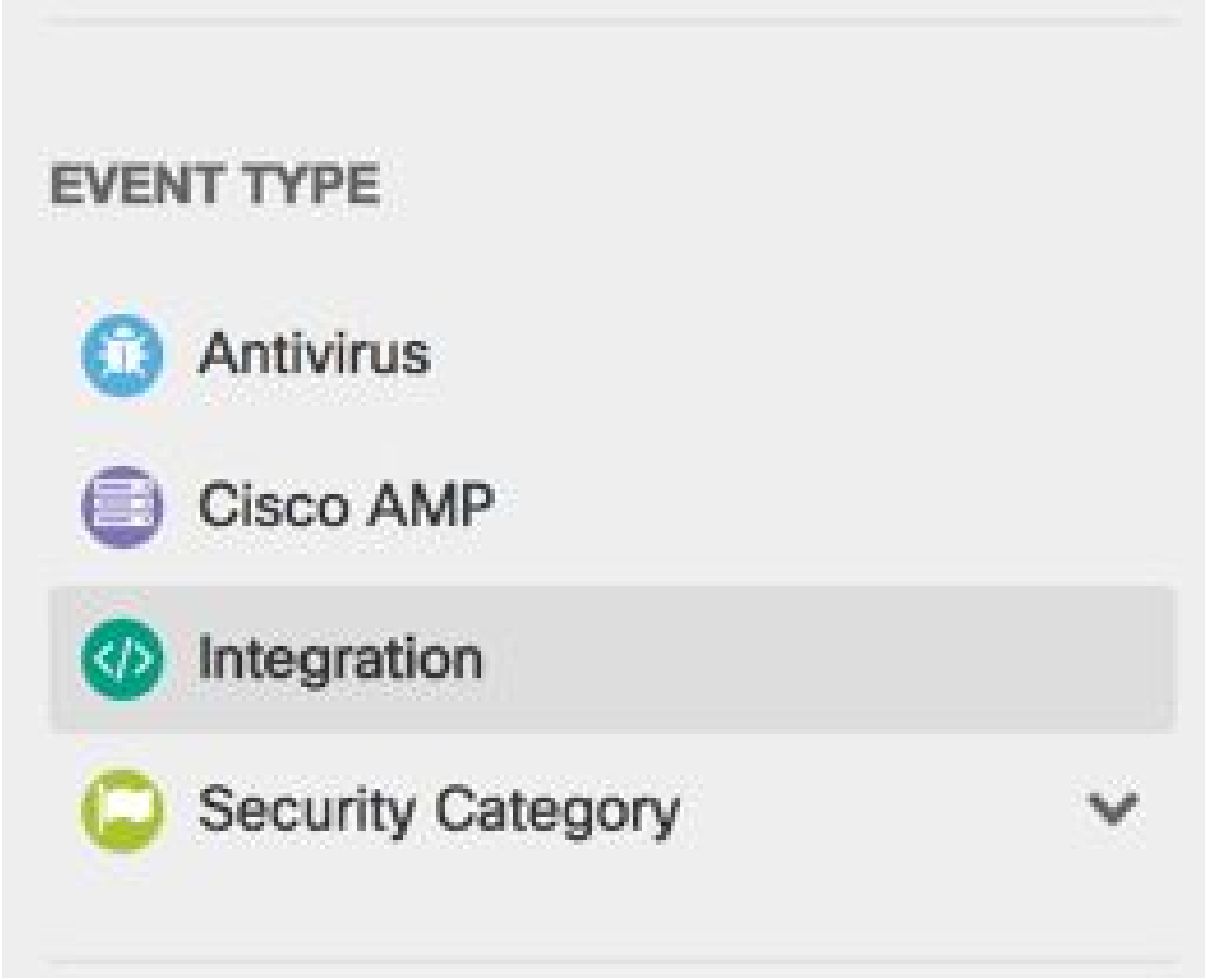


115013981706

2. Clique em Aplicar para ver a atividade para o período selecionado no relatório.

Você também pode exibir o relatório de volume de atividades para ver os relatórios de instantâneos ou tendências ao longo do tempo, incluindo suas integrações personalizadas.

1. Navegue até Relatórios > Volume de atividade de segurança.
2. Em Tipo de evento, selecione Integração.



115013982286

Configure sua integração S3 para armazenamento e consumo de logs (opcional)

Se você quiser alimentar seus logs do Umbrella contendo todas as solicitações para seu ambiente de volta para seu ambiente SIEM/TIP, você pode fazer isso usando nossa integração S3, que permite que você transmita seus eventos de atividade DNS de volta.

Anexo: Scripts de Exemplo

Esses scripts perl fornecem orientação sobre como você pode gerar um evento para sua integração personalizada. Substitua o valor customerKey de sua Integração em ambos os scripts. Observe que esses scripts são fornecidos como exemplos e a personalização ou as atualizações podem ser necessárias.

generate_event.pl:

```
#!/usr/bin/perl -w

# Custom integration - ADD EVENT URL

my $cust_key = 'https://s-platform.api.opendns.com/1.0/events?customerKey=XXXXXXXX-XXXX-XXXX-XXXX-XXXXX

die "Usage: $0 - Please supply a domain\n" if @ARGV < 1;
my $domain = $ARGV[0];

my $json_blob = "{
    \"alertTime\" : \"2013-02-08T11:14:26.0Z\",
    \"deviceId\" : \"ba6a59f4-e692-4724-ba36-c28132c761de\",
    \"deviceVersion\" : \"13.7a\",
    \"dstDomain\" : \"$domain\",
    \"dstUrl\" : \"http://$domain/a-bad-url\",
    \"eventTime\" : \"2013-02-08T09:30:26.0Z\",
    \"protocolVersion\" : \"1.0a\",
    \"providerName\" : \"Security Platform\"
}";

my $curl_request = "curl '" . $cust_key . "' -v -X POST -H 'Content-Type: application/json' -d '" . $js

my $results = exec($curl_request);
```

delete_domain.pl:

```
#!/usr/bin/perl -w

# Custom integration - DELETE URL

my $cust_key = 'https://s-platform.api.opendns.com/1.0/domains?customerKey=XXXXXXXX-XXXX-XXXX-XXXX-XXXX

die "Usage: $0 - Please supply a domain\n" if @ARGV < 1;
my $domain = $ARGV[0];

my $curl_request = "curl '" . $cust_key . "&where[name]=" . $domain . "' -v -i -g -X DELETE -H 'Content
my $results = exec($curl_request);
```

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.