Conozca la API Umbrella Enforcement para integraciones personalizadas

Contenido

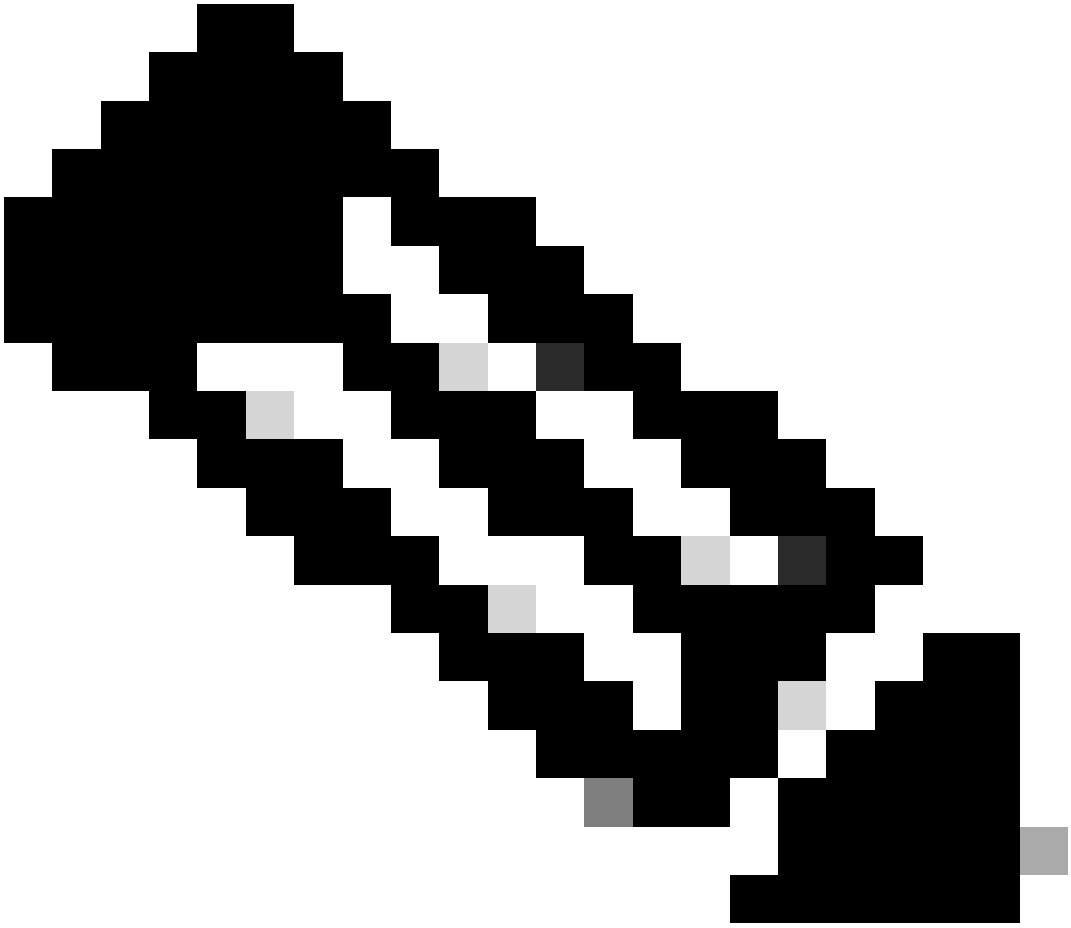
Introducción

Este documento describe la API de Umbrella Enforcement para las integraciones personalizadas.

¿Qué es la API de aplicación de Umbrella?

La API Umbrella Enforcement permite a los partners y clientes con sus propios entornos SIEM/Threat Intelligence Platform (TIP) internos introducir eventos o inteligencia de amenazas en su entorno Umbrella. Estos eventos se convierten instantáneamente en visibilidad y aplicación que puede extenderse más allá del perímetro y, por tanto, en el alcance de los sistemas que podrían haber generado dichos eventos o inteligencia de amenazas.

La API de aplicación puede incorporar eventos en el formato de evento genérico descrito en esta documentación de la API y admite las funciones ADD, DELETE o LIST.



Nota: Si no dispone de la API de Umbrella Enforcement para las integraciones personalizadas en su panel de Umbrella y le gustaría tener acceso, [póngase en contacto con su representante de Cisco Umbrella.]

¿Por qué lo usaría?

Es posible que ya procese, gestione y conserve su propio sistema de inteligencia de amenazas y procesos que se traduzcan en el deseo de realizar acciones en dominios identificados como maliciosos o sospechosos. En ese caso, una vez que se ha tomado la decisión de que es necesario actuar sobre un evento (por ejemplo, convertirlo en protección), en lugar de agregar manualmente protección a Umbrella para fines de aplicación, puede utilizar la API de aplicación para automatizar este proceso y aplicar de forma instantánea la protección basada en los dominios asociados con el evento.

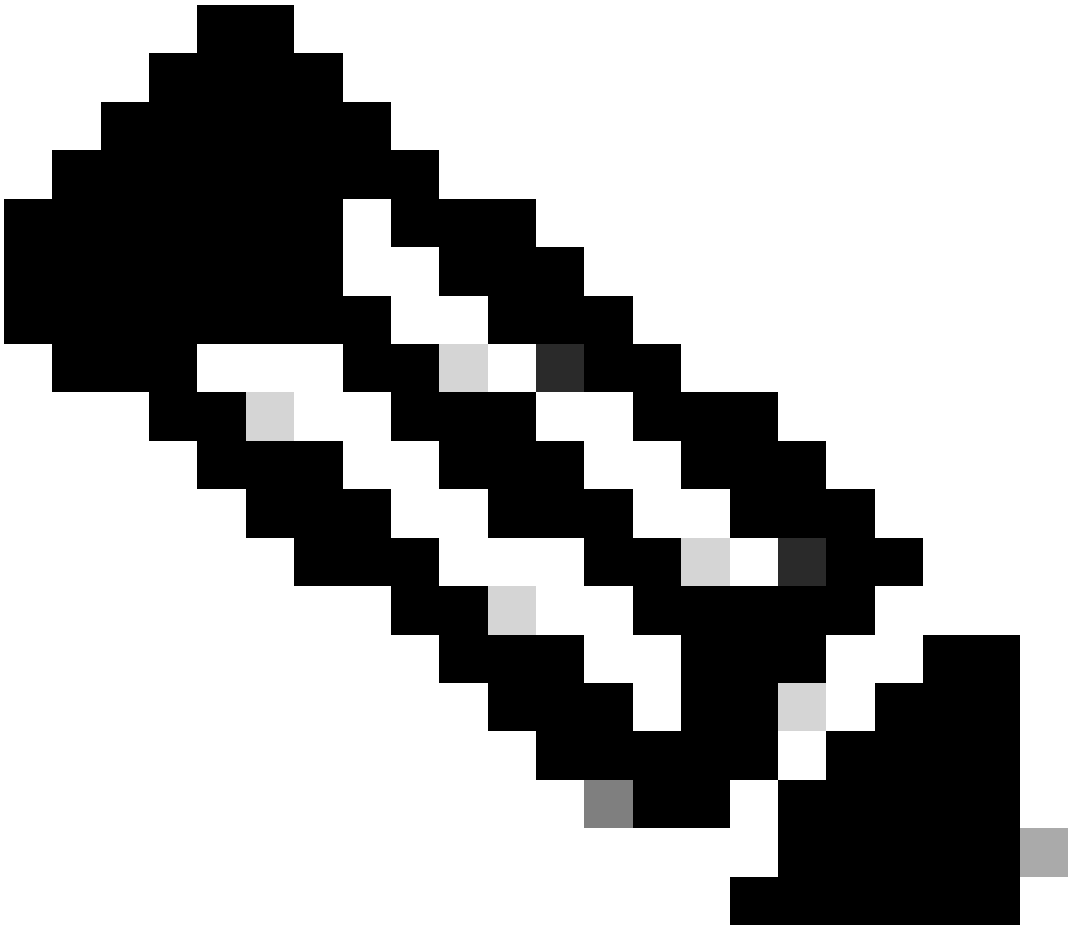
Esto permite a su equipo de seguridad dedicar su tiempo y esfuerzo a la investigación en lugar de a la configuración en curso de Umbrella. Permite que su equipo de seguridad permanezca dentro

de sus herramientas y procesos en lugar de tener que saltar al panel de Umbrella para actualizar las listas de destinos. Básicamente, puede crear una lista de destinos en Umbrella a partir de un origen externo que administre directamente a través de la API y, a continuación, bloquear esos destinos para las identidades dentro de Umbrella.

¿Cómo Lo Utilizaría?

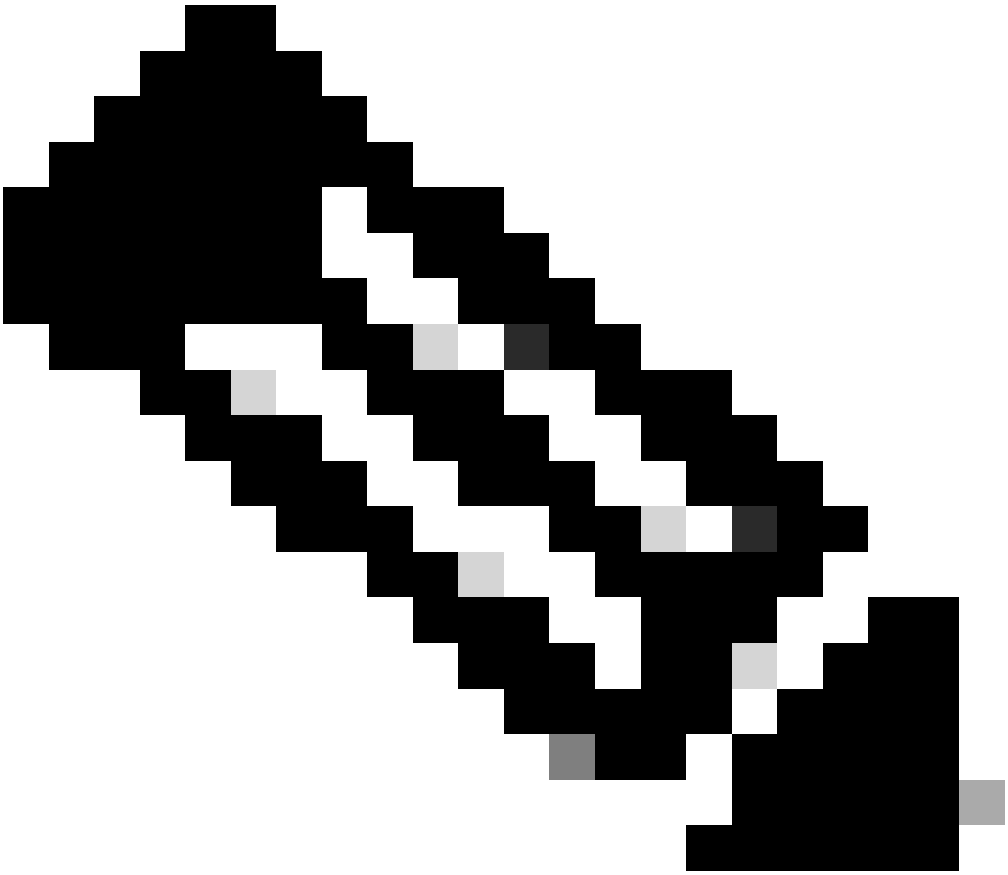
AGREGAR un evento a la API de aplicación

Una vez agregado un evento, el Servicio de aplicación intenta extraer dominios del evento.



Nota: En el futuro, se añadirá compatibilidad con direcciones IP y URL.

- Un evento puede contener cualquier cantidad de los detalles originales del evento que desee, pero debe cumplir las especificaciones descritas en la documentación de la API.



Nota: Es posible que en el futuro se añada compatibilidad con los detalles de eventos de superficie en el tablero de mandos de Umbrella.

- Si se extrae un dominio, el gráfico de seguridad de Cisco Umbrella lo valida para garantizar que no se trata de un dominio conocido que puede dar lugar a falsos positivos o que, de otro modo, ya se considera malicioso en el gráfico de seguridad de Cisco Umbrella.
- Si pasa la validación (por ejemplo, si el bloqueo es desconocido y seguro), se agrega a una lista de destinos asociada a esa integración personalizada y aparece en el panel de Umbrella como una categoría de seguridad personalizada.
- La categoría de seguridad personalizada se puede bloquear o permitir según la política, para permitir tanto la aplicación activa como la "auditoría" pasiva de las solicitudes sospechosas.

LISTA de dominios para una lista de API de aplicación

- Si el flujo de trabajo incluye el desbloqueo de dominios que se bloquearon debido a eventos insertados anteriormente, una solicitud LIST proporciona todos los dominios incluidos

actualmente en la lista de destino asociada a esa integración.

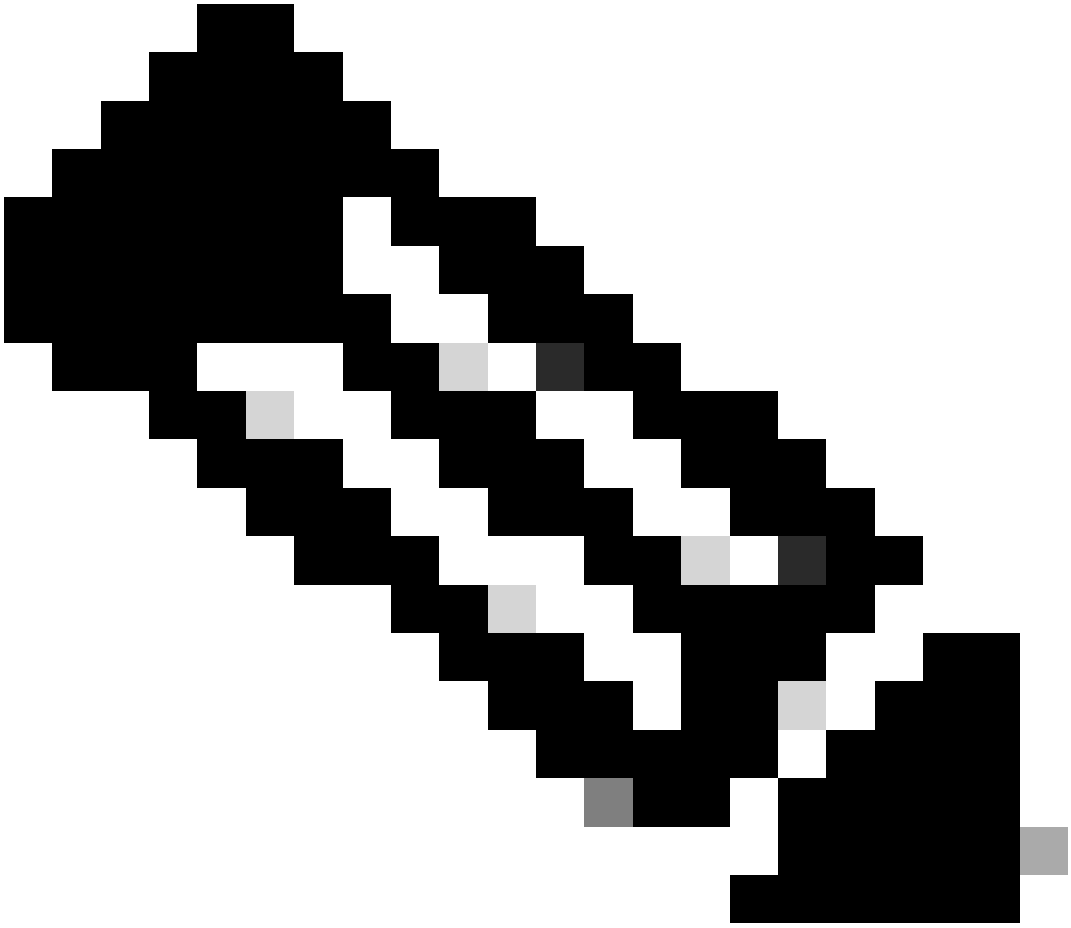
ELIMINAR dominio de la lista API de aplicación

- Si el flujo de trabajo incluye el desbloqueo de dominios que se bloquearon debido a eventos insertados anteriormente, una solicitud DELETE (Eliminar) le permite quitar un dominio de la lista de destino asociada a esa integración.
- Si una solicitud DNS entrante de una de las identidades de Umbrella está destinada a un dominio de la lista de destinos de integración personalizada, se bloqueará o se permitirá en función de la configuración de seguridad de la integración personalizada asociada a la directiva que la activó.
- Los resultados se registran junto con todos los demás eventos de Umbrella, a los que se puede acceder a través de la búsqueda de actividad o a través de Amazon S3 mediante la integración de S3. Por lo tanto, el tráfico asociado con la integración personalizada se puede volver a incorporar opcionalmente en el SIEM/TIP y el bucle de retroalimentación se cerrará.

Tutorial sobre el uso de la API de aplicación

Paso 1: Cree su integración personalizada

Puede tener hasta 10 integraciones personalizadas a la vez.



Nota: Si la organización es una organización secundaria de un MSP, MSSP o MOC de Umbrella, las integraciones personalizadas compartidas desde el nivel de consola aparecen antes que las integraciones creadas en el nivel de organización secundaria.

1. En Umbrella, navegue hasta Policies > Policy Components > Integrations y haga clic en Add.
2. Agregue un nombre para la integración personalizada y haga clic en Create.
3. Amplíe su nueva integración personalizada, marque Enable, copie la URL de integración y luego haga clic en Save.

Paso 2: Cree sus scripts personalizados.

1. Vea las secuencias de comandos de ejemplo generate_event y delete_domain en el apéndice de este documento o utilice la documentación de API para crear sus propias secuencias de comandos para generar las solicitudes con el formato correcto para generar eventos o eliminar o enumerar dominios. En el futuro, querrá utilizar la URL de integración

personalizada en estas secuencias de comandos.

Paso 3: Insertar un evento de ejemplo

1. Utilice la secuencia de comandos que ha creado para insertar un evento en la integración personalizada. En nuestro ejemplo, hemos insertado un evento que contiene el dominio "creditcards.com".

Paso 4: Compruebe la lista de destinos en el panel de Umbrella

1. Vuelva a Configuración > Integraciones y en la tabla expanda su integración personalizada.
2. Haga clic en Ver dominios. Aparecerá una lista de los dominios agregados en la que se pueden realizar búsquedas y su evento de muestra del paso 4 estará ahora en la lista.

Paso 5: Compruebe el registro de auditoría de administración.

1. Otra forma de verificar la actividad asociada a su integración personalizada es revisar el registro de auditoría de administración.
2. Vaya a Reporting > Admin Audit Log.
3. En Filtros, introduzca el nombre de la integración personalizada en Filtrar por identidades y configuración y, a continuación, haga clic en Ejecutar filtro.

Cuando expanda la entrada, verá el evento que dio lugar a que su evento de ejemplo (creditcards.com) se agregara a su integración personalizada.

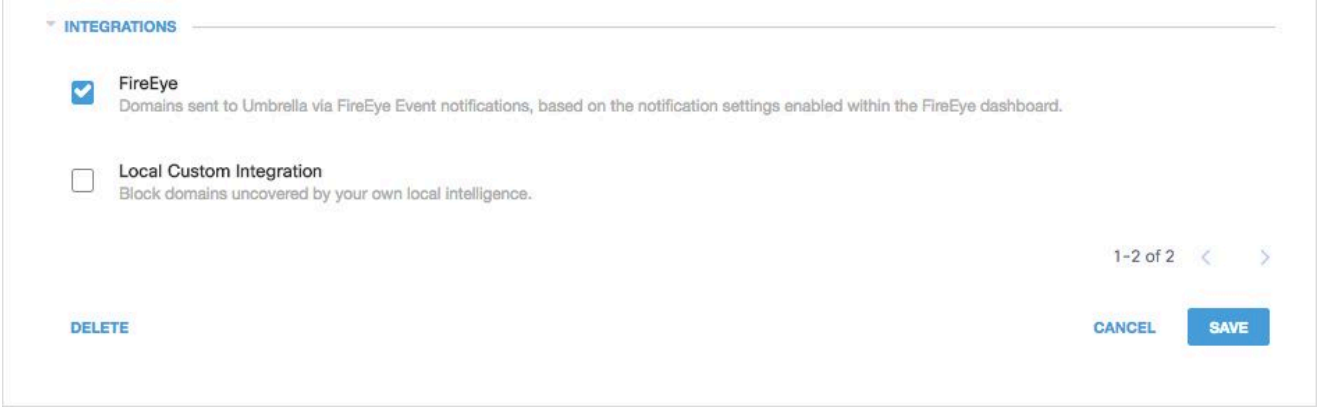
Paso opcional: Lista o eliminación de dominios

También puede realizar pruebas para asegurarse de que puede enumerar los dominios de su integración personalizada y eliminar los dominios en caso de que ya no desee aplicarlos al dominio o incluirlos en su integración. Utilice los pasos descritos en la documentación de la API para enumerar y eliminar dominios.

Configurar los parámetros de seguridad

Ahora que ha validado que puede insertar eventos (y opcionalmente enumerar y eliminar dominios), puede configurar lo que desea que suceda con las solicitudes DNS de sus identidades que están destinadas a dominios de la categoría de seguridad de su integración personalizada.

1. Navegue hasta Políticas > Configuración de seguridad y en Integraciones, verifique su integración habilitada (en este ejemplo, FireEye) y haga clic en Guardar.

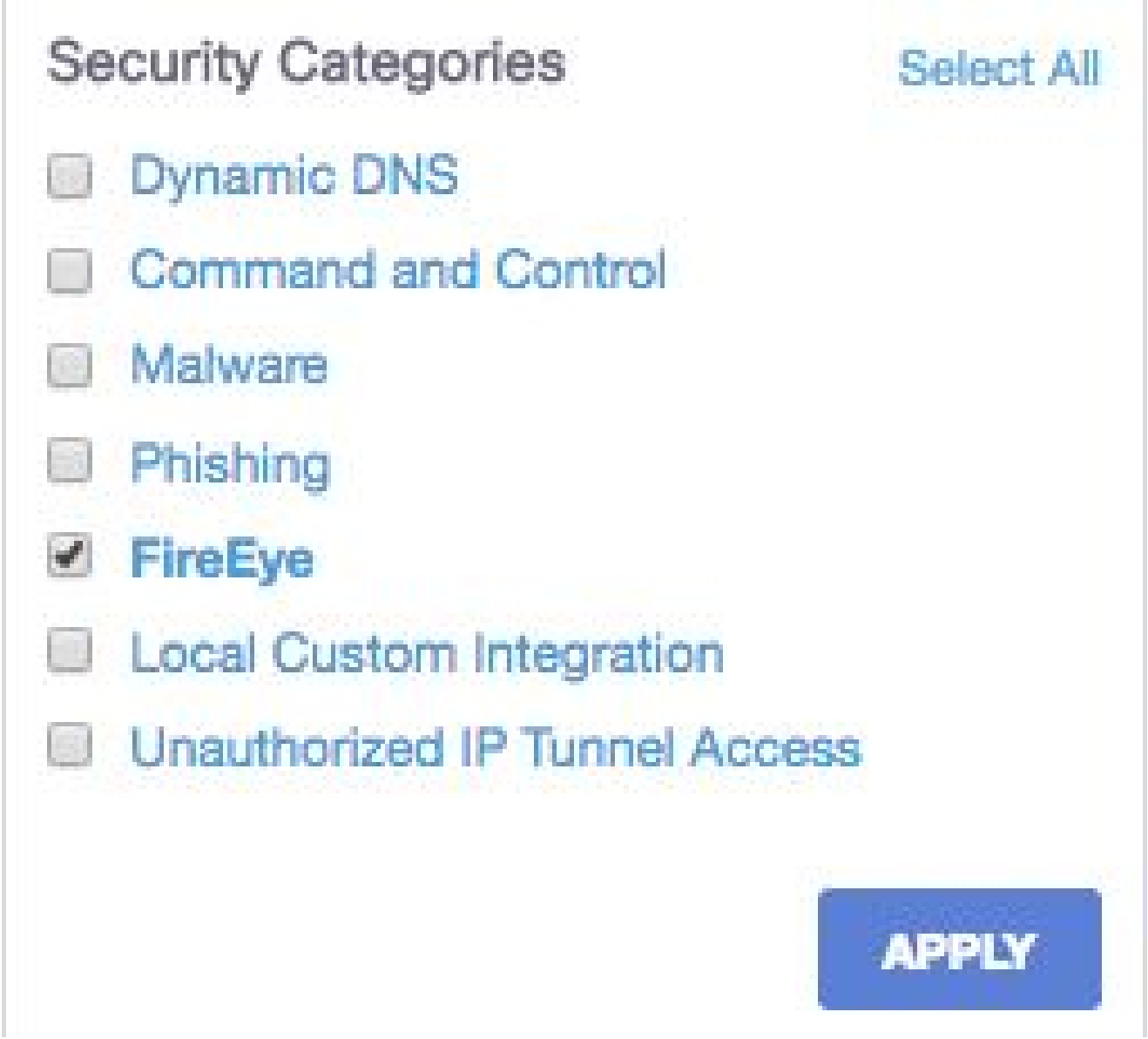


115014145103

Ver informes para la integración personalizada

Genere solicitudes de DNS desde una de sus identidades (por ejemplo, Redes o Equipos en roaming) destinada al dominio en su integración personalizada ("creditcards.com" en nuestro ejemplo). Desde la perspectiva del cliente, ahora puede ver el resultado de bloquear o permitir adecuado en función de cómo haya configurado los parámetros de seguridad.

1. Navegue hasta Reporting > Activity Search y en Security Categories seleccione su integración personalizada (en este ejemplo, FireEye) para filtrar el informe y mostrar solamente la categoría de seguridad para FireEye.

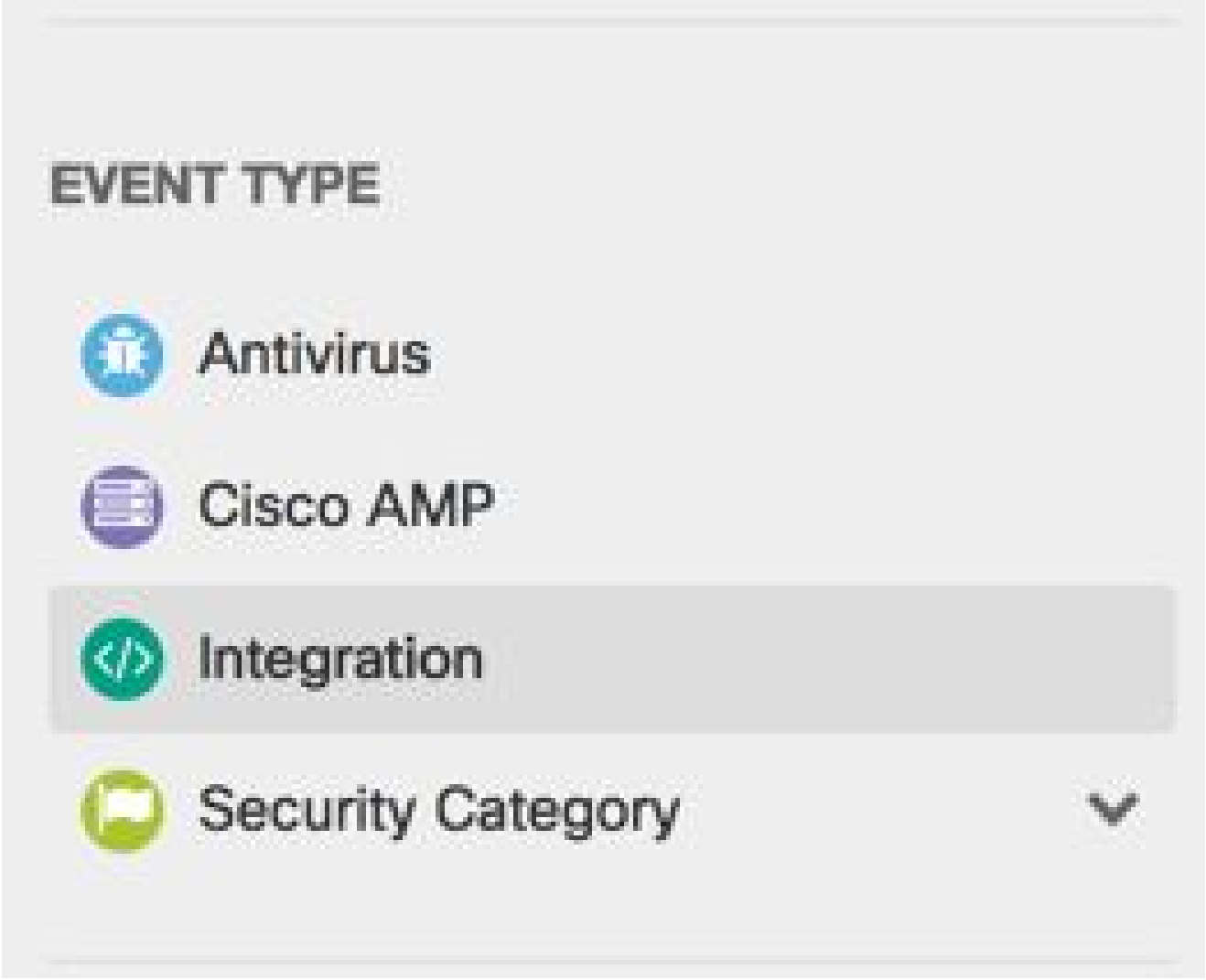


115013981706

2. Haga clic en Aplicar para ver la actividad del período de tiempo seleccionado en el informe.

También puede ver el informe Volumen de actividad para ver los informes de recuento de instantáneas o tendencias a lo largo del tiempo, incluidas las integraciones personalizadas.

1. Vaya a Informes > Volumen de actividad de seguridad.
2. En Tipo de evento, seleccione Integración.



115013982286

Configuración de la integración de S3 para el almacenamiento y el consumo de registros (opcional)

Si desea volver a alimentar los registros de Umbrella, que contienen todas las solicitudes de su entorno, en su entorno SIEM/TIP, puede hacerlo mediante nuestra integración S3, que le permite volver a transmitir los eventos de actividad DNS.

Apéndice: Scripts de ejemplo

Estas secuencias de comandos de perl proporcionan orientación sobre cómo generar un evento para la integración personalizada. Sustituya el valor customerKey de la integración en ambos scripts. Tenga en cuenta que estas secuencias de comandos se proporcionan como ejemplos y que puede ser necesario personalizarlas o actualizarlas.

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);
```

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).