Begrijp de Umbrella Enforcement API voor aangepaste integraties

Inhoud

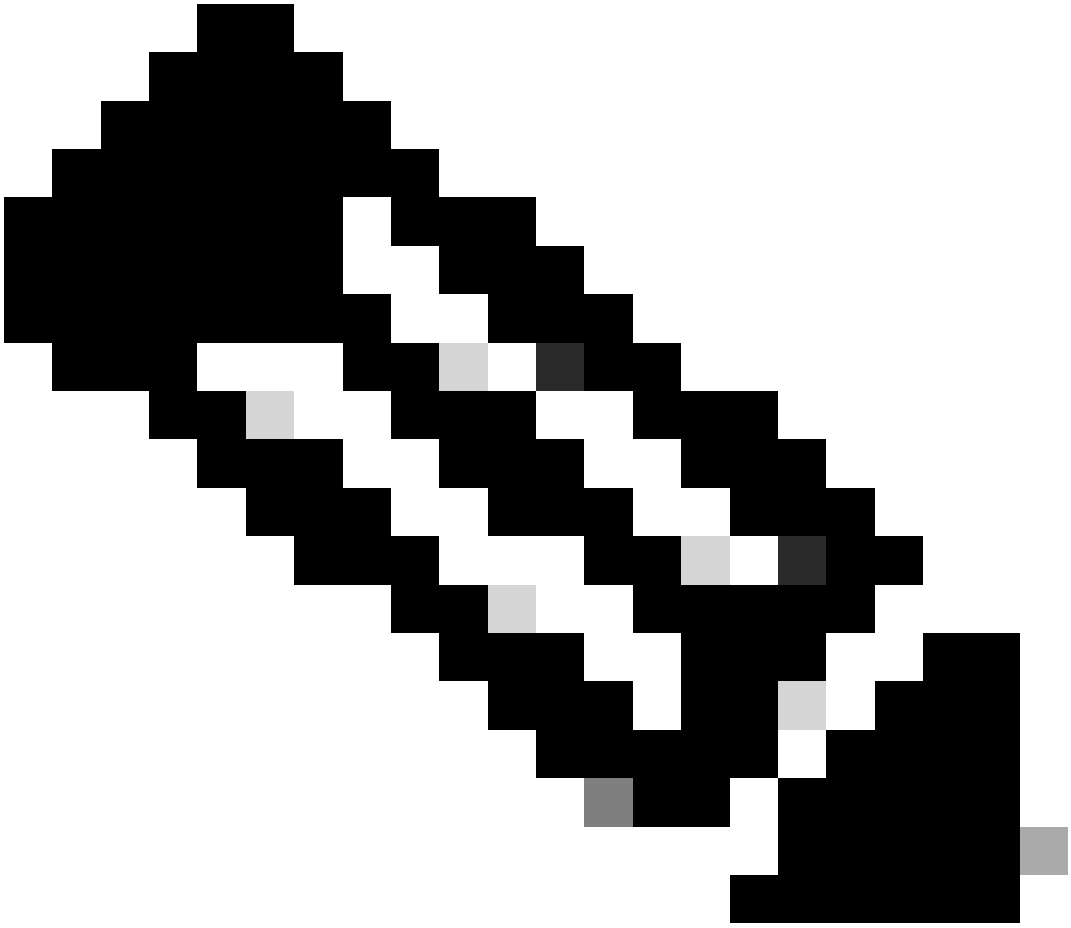
Inleiding

Dit document beschrijft de Umbrella Enforcement API voor aangepaste integraties.

Wat is de Umbrella Enforcement API?

Met de Umbrella Enforcement API kunnen partners en klanten met hun eigen SIEM/Threat Intelligence Platform (TIP)-omgevingen gebeurtenissen en/of bedreigingsinformatie injecteren in hun Umbrella-omgeving. Deze gebeurtenissen worden vervolgens onmiddellijk omgezet in zichtbaarheid en handhaving die zich buiten de perimeter en dus het bereik van de systemen die deze gebeurtenissen of bedreigingsinformatie hebben gegenereerd, kunnen uitstrekken.

De Enforcement API kan gebeurtenissen opnemen in het generieke gebeurtenisformaat dat in deze API-documentatie wordt beschreven en kan functies TOEVOEGEN, VERWIJDEREN of LIJST ondersteunen.



Opmerking: als u geen Umbrella Enforcement API hebt voor aangepaste integraties in uw Umbrella-dashboard en toegang wilt hebben, neemt u contact op met uw Cisco Umbrella-vertegenwoordiger.

Waarom zou ik het gebruiken?

U kunt uw eigen bedreigingsinformatiesysteem en processen al verwerken, beheren en beheren die resulteren in de wens om acties te ondernemen op domeinen die als kwaadaardig of verdacht zijn geïdentificeerd. In dat geval kunt u, zodra een beslissing is genomen dat een gebeurtenis moet worden uitgevoerd (bijvoorbeeld omgezet in bescherming), in plaats van handmatig bescherming toe te voegen aan Umbrella voor handhavingsdoeleinden, de Handhaving-API gebruiken om dit proces te automatiseren en onmiddellijk bescherming af te dwingen op basis van domeinen die verband houden met het evenement.

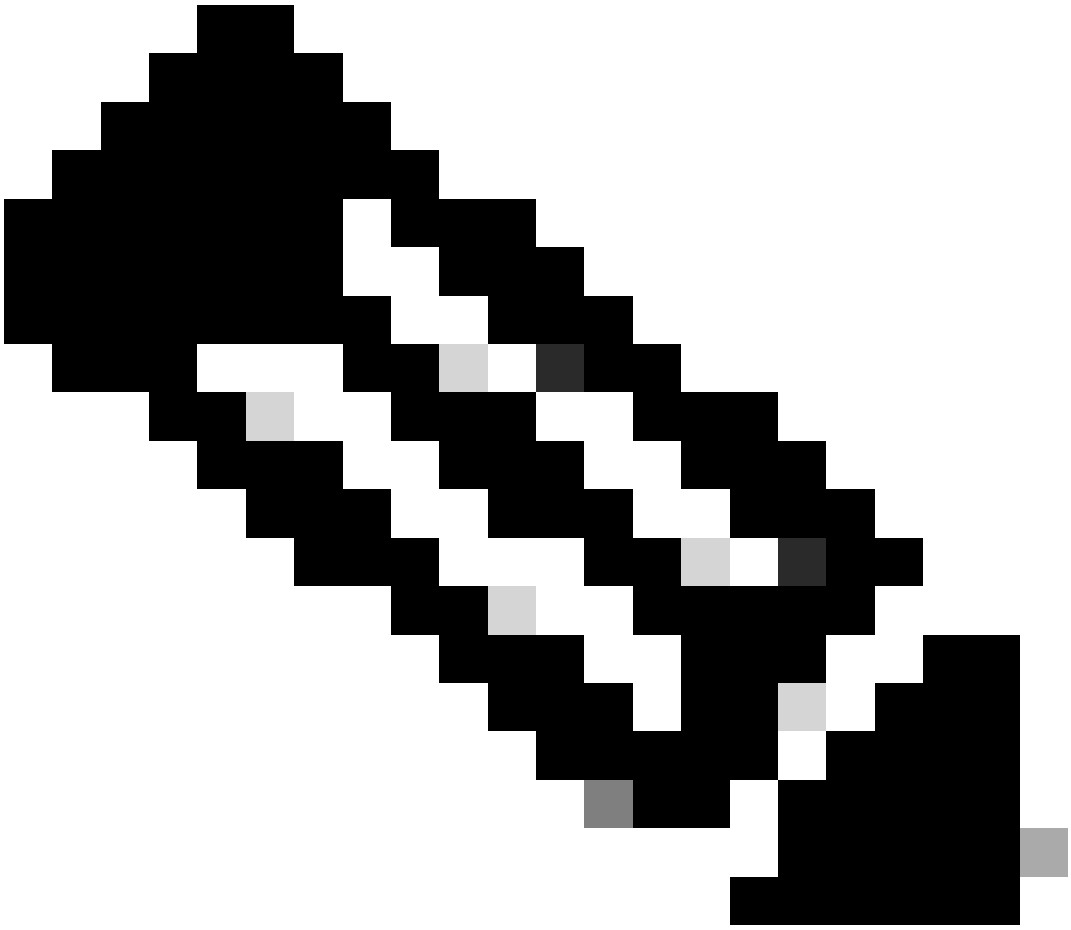
Dit stelt uw beveiligingsteam in staat om hun tijd en moeite te richten op onderzoek in plaats van de voortdurende configuratie van Umbrella. Het stelt uw beveiligingsteam in staat om binnen hun

tools en processen te blijven in plaats van in het Umbrella-dashboard te hoeven springen om bestemmingslijsten bij te werken. In wezen kunt u een bestemmingslijst in Umbrella maken van een externe bron die u rechtstreeks beheert via de API en vervolgens ervoor kiezen om die bestemmingen te blokkeren voor identiteiten binnen Umbrella.

Hoe zou ik het gebruiken?

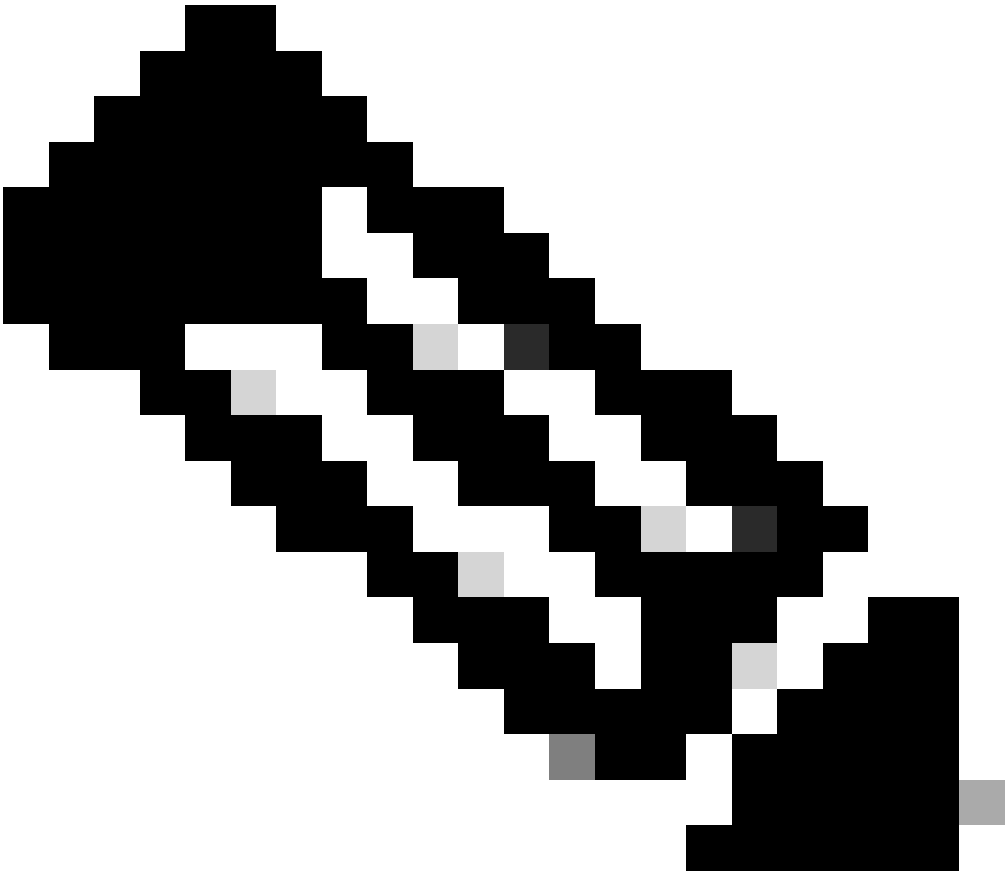
Een gebeurtenis toevoegen aan de API voor handhaving

Zodra een gebeurtenis is toegevoegd, probeert de Handhaving domeinen uit het evenement te halen.



Opmerking: in de toekomst wordt ondersteuning voor IP-adressen en URL's toegevoegd.

- Een evenement kan elke hoeveelheid van de originele gebeurtenisdetails bevatten die u wilt, maar moet zich houden aan de specificaties die zijn beschreven in de API-documentatie.



Opmerking: in de toekomst kan ondersteuning worden toegevoegd voor details van oppervlakkige gebeurtenissen in het dashboard van de paraplu.

- Als een domein wordt geëxtraheerd, wordt het gevalideerd door de Cisco Umbrella-beveiligingsgrafiek om ervoor te zorgen dat het geen bekend goed domein is dat waarschijnlijk resulteert in false positives of al op andere wijze als schadelijk wordt beschouwd door de Cisco Umbrella-beveiligingsgrafiek.
- Als het de validatie doorstaat (het is bijvoorbeeld onbekend en veilig om te blokkeren), wordt het toegevoegd aan een bestemmingslijst die is gekoppeld aan die aangepaste integratie en opgedoken in het Umbrella-dashboard als een aangepaste beveiligingscategorie.
- De aangepaste beveiligingscategorie kan worden geblokkeerd of toegestaan op basis van beleid, om zowel actieve handhaving als passieve "auditing" van verdachte verzoeken mogelijk te maken.

LIJST met domeinen voor een API-lijst voor handhaving

- Als uw werkstroom de deblokkering bevat van domeinen die zijn geblokkeerd vanwege

eerder geïnjecteerde gebeurtenissen, biedt een LIST-verzoek alle domeinen die momenteel zijn opgenomen in de bestemmingslijst die is gekoppeld aan die integratie.

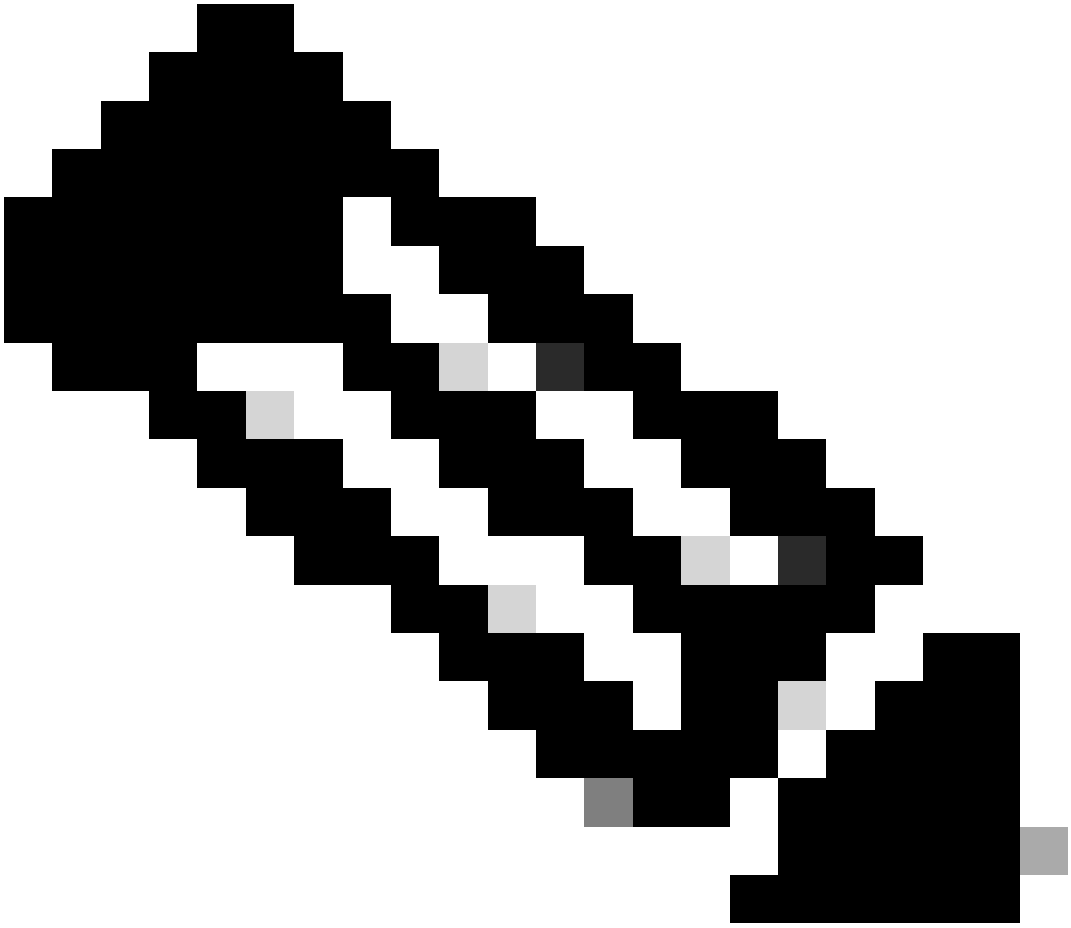
Domein verwijderen uit API-lijst voor handhaving

- Als uw werkstroom de deblokkering bevat van domeinen die zijn geblokkeerd vanwege eerder geïnjecteerde gebeurtenissen, kunt u met een verzoek om te verwijderen een domein verwijderen uit de bestemmingslijst die is gekoppeld aan die integratie.
- Als een binnenkomend DNS-verzoek van een van uw Umbrella-identiteiten is bestemd voor een domein in de lijst met aangepaste integratiebestemmingen, wordt het geblokkeerd of toegestaan, afhankelijk van de beveiligingsinstelling van de aangepaste integratie die is gekoppeld aan het beleid dat het heeft geactiveerd.
- De resultaten worden samen met alle andere Umbrella-evenementen geregistreerd, toegankelijk via de Activity Search of via Amazon S3 met behulp van de S3-integratie. Zo kan het verkeer in verband met de aangepaste integratie optioneel weer worden opgenomen in uw SIEM / TIP en de feedback lus gesloten.

Walkthrough van het gebruik van de Enforcement API

Stap 1: Creëer uw aangepaste integratie

U kunt maximaal 10 aangepaste integraties tegelijk uitvoeren.



Opmerking: Als de organisatie een onderliggend orgaan is van een overkoepelende MSP, MSSP of MOC, worden aangepaste integraties die worden gedeeld vanaf het consoleniveau weergegeven voordat integraties worden gemaakt op het niveau van het onderliggend orgaan.

---

1. Navigeer in Umbrella naar Beleid > Beleidscomponenten > Integraties en klik op Toevoegen.
2. Voeg een naam toe voor de aangepaste integratie en klik op Maken.
3. Vouw uw nieuwe aangepaste integratie uit, vink Inschakelen aan, kopieer de integratie-URL en klik vervolgens op Opslaan.

Stap 2: Maak je eigen script(s) aan.

1. Zie de voorbeeldscripts generate_event en delete_domain in de bijlage van dit document of gebruik de API-documentatie om uw eigen scripts te maken om de correct geformatteerde verzoeken voor het genereren van gebeurtenissen of het verwijderen of vermelden van domeinen te genereren. U wilt de aangepaste integratie-URL in deze scripts gebruiken.

Stap 3: Injecteer een voorval

1. Gebruik het script dat u hebt gemaakt om een gebeurtenis in uw aangepaste integratie te injecteren. In ons voorbeeld hebben we een gebeurtenis geïnjecteerd met het domein "creditcards.com".

Stap 4: Controleer de bestemmingslijst in het Umbrella dashboard

1. Ga terug naar Instellingen > Integraties en vouw in de tabel uw aangepaste integratie uit.
2. Klik op Zie domeinen. Er verschijnt een doorzoekbare lijst met de toegevoegde domeinen en uw voorbeeldevenement van stap 4 staat nu in de lijst.

Stap 5: Controleer het auditlogboek van de beheerder.

1. Een andere manier om activiteiten te controleren die zijn gekoppeld aan uw aangepaste integratie, is door het auditlogboek van de beheerder te bekijken.
2. Navigeer naar Rapportage > Controlelogboek beheren.
3. Voer onder Filters de naam van uw aangepaste integratie in Filter op identiteit en instellingen in en klik vervolgens op Filter uitvoeren.

Wanneer u het item uitbreidt, ziet u nu het evenement dat ertoe heeft geleid dat uw voorbeeldevenement (creditcards.com) aan uw aangepaste integratie is toegevoegd.

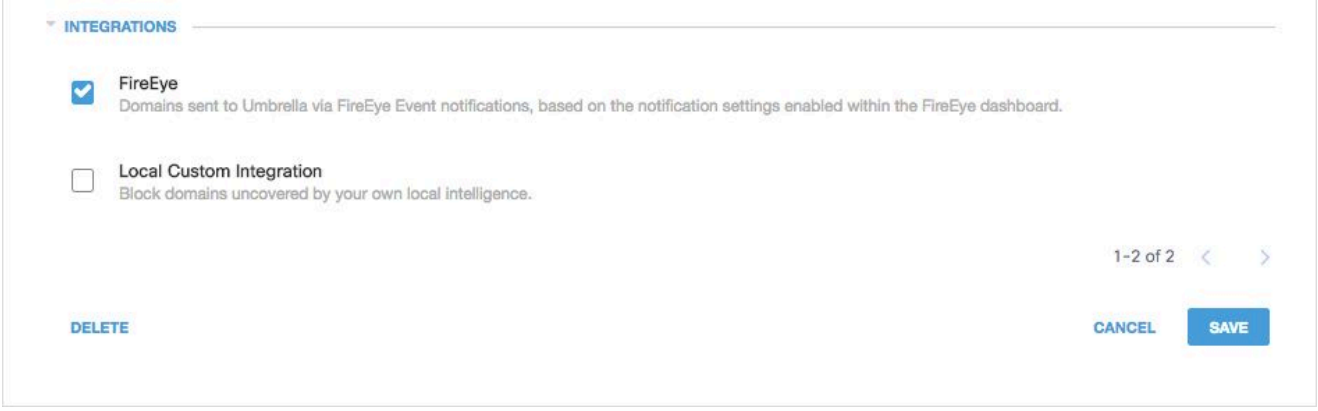
Optionele stap: domeinen aanbieden of verwijderen

U kunt ook testen om ervoor te zorgen dat u domeinen kunt opnemen in uw aangepaste integratie en domeinen kunt verwijderen als u het domein niet langer wilt afdwingen of in uw integratie wilt hebben. Gebruik de stappen in de API-documentatie om domeinen weer te geven en te verwijderen.

Beveiligingsinstellingen configureren

Nu u hebt gevalideerd dat u gebeurtenissen kunt injecteren (en desgewenst domeinen kunt weergeven en verwijderen), kunt u configureren wat u wilt dat er gebeurt met DNS-verzoeken van uw identiteiten die zijn bestemd voor domeinen in de beveiligingscategorie van uw aangepaste integratie.

1. Navigeer naar Beleid > Beveiligingsinstellingen en onder Integraties, controleer uw ingeschakelde integratie (in dit voorbeeld FireEye) en klik op Opslaan.

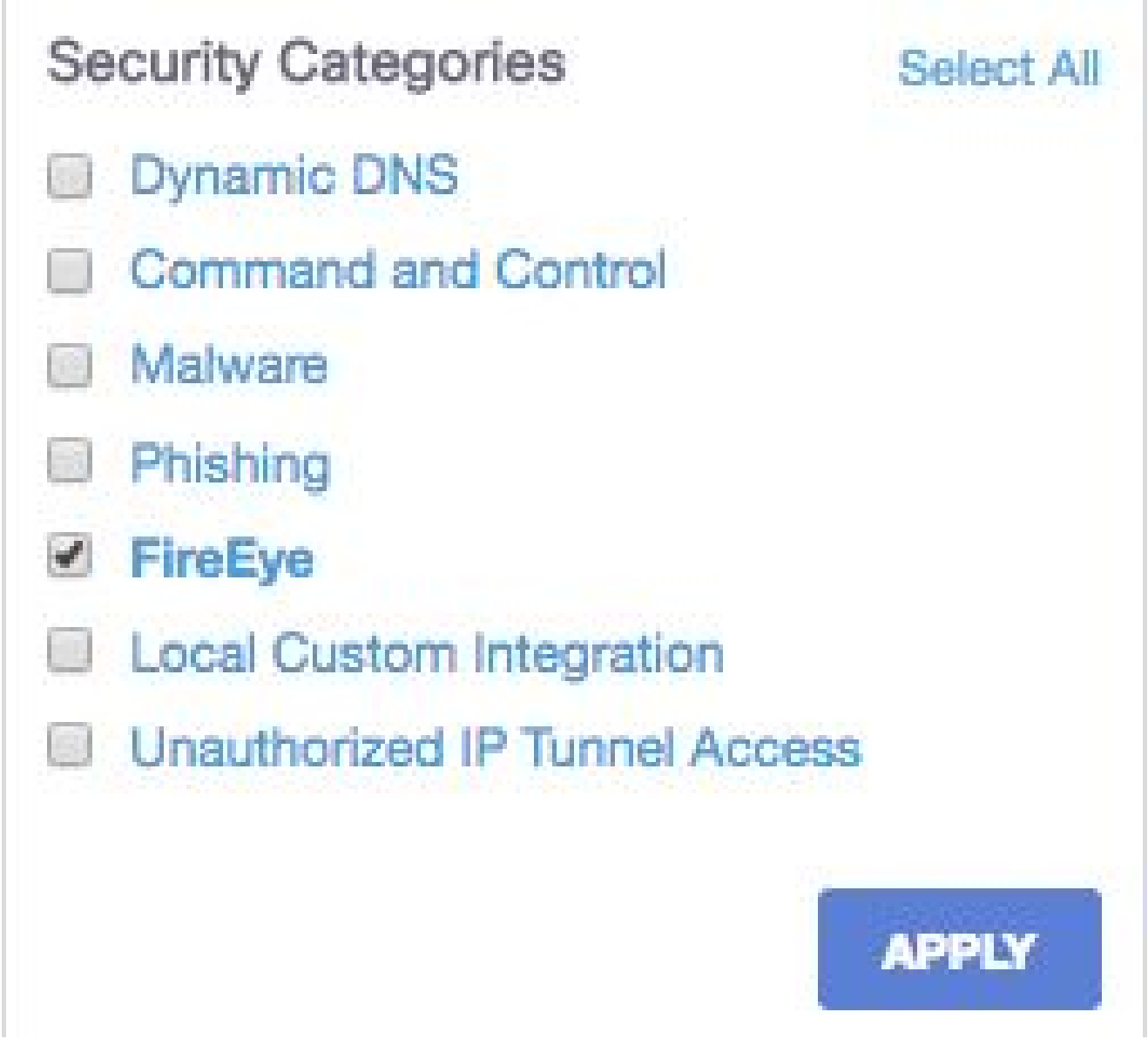


115014145103

Rapportage bekijken voor uw aangepaste integratie

Genereer DNS-verzoeken van een van uw identiteiten (bijvoorbeeld Netwerken of Zwervende Computers) die bestemd zijn voor het domein in uw aangepaste integratie ("creditcards.com" in ons voorbeeld). Vanuit het perspectief van de klant ziet u nu het juiste blok of het juiste resultaat, afhankelijk van hoe u uw beveiligingsinstellingen hebt geconfigureerd.

1. Navigeer naar Rapportage > Activiteit zoeken en selecteer onder Beveiligingscategorieën uw aangepaste integratie (in dit voorbeeld FireEye) om het rapport te filteren zodat alleen de beveiligingscategorie voor FireEye wordt weergegeven.

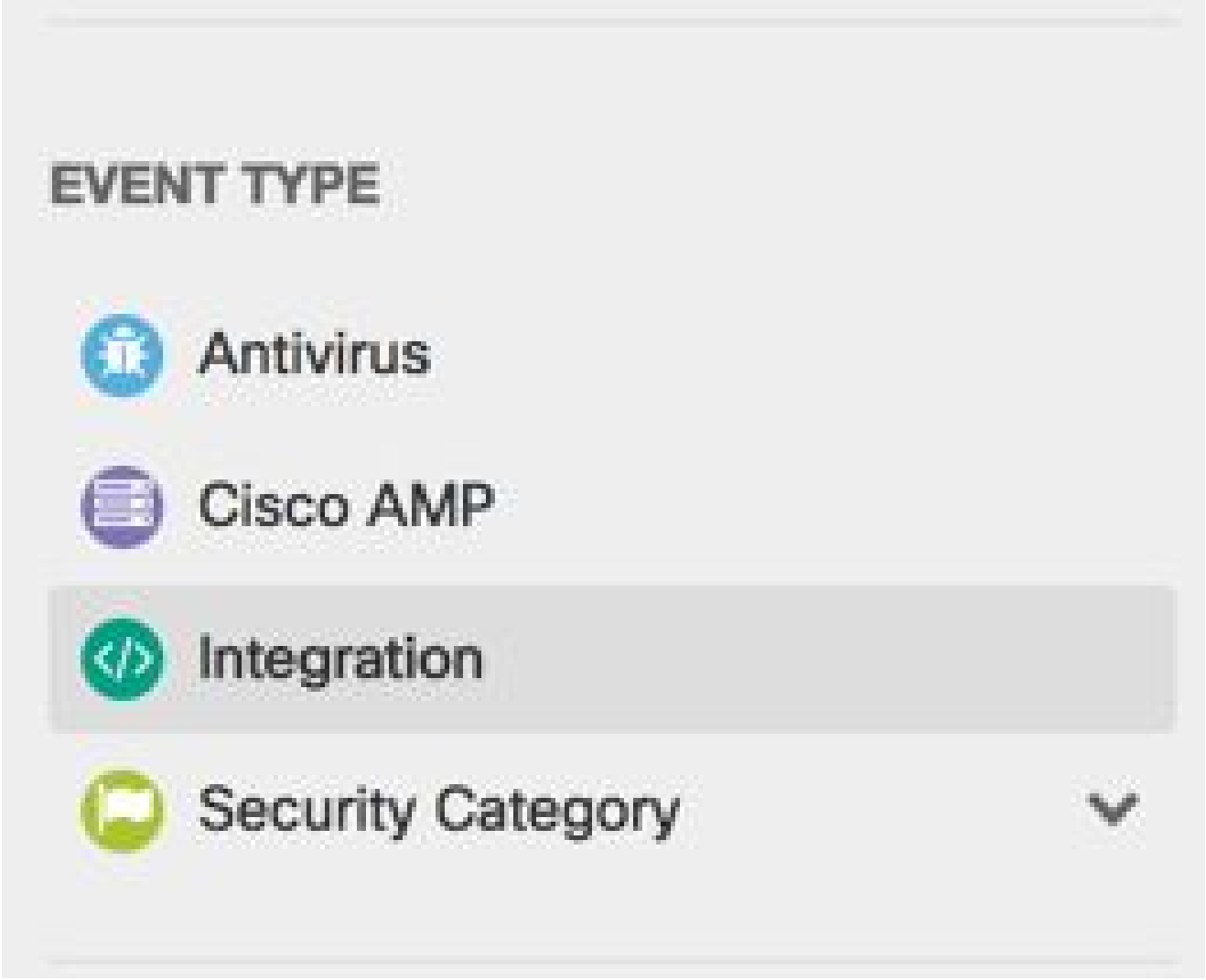


115013981706

2. Klik op Toepassen om de activiteit voor de geselecteerde tijdsperiode in het rapport te bekijken.

U kunt ook het activiteitenvolumerapport bekijken om de snapshot- of trendtellingsrapporten in de loop van de tijd te bekijken, inclusief uw aangepaste integratie(s).

1. Navigeer naar Rapportage > Volume beveiligingsactiviteiten.
2. Selecteer Integratie onder Gebeurtenistype.



115013982286

Configureer uw S3-integratie voor logboekopslag en -verbruik (optioneel)

Als u vervolgens uw Umbrella-logs met alle verzoeken voor uw omgeving terug wilt invoeren in uw SIEM / TIP-omgeving, kunt u dit doen met behulp van onze S3-integratie, waarmee u uw DNS-activiteitsevenementen terug kunt streamen.

Bijlage: Voorbeeldscripts

Deze perl scripts geven richtlijnen over hoe u een evenement kunt genereren voor uw aangepaste integratie. Vervang de CustomerKey-waarde van uw integratie in beide scripts. Deze scripts worden als voorbeeld gegeven en aanpassingen of updates kunnen nodig zijn.

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);
```

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.