De integratie van beveiligde malware-analyse (voorheen Threat Grid) configureren met Umbrella

Inhoud

Inleiding

In dit document wordt beschreven hoe u Secure Malware Analytics (voorheen Threat Grid) kunt integreren met Umbrella.

Cisco Secure Malware Analytics (Threat Grid) Integration for Cisco Overzicht

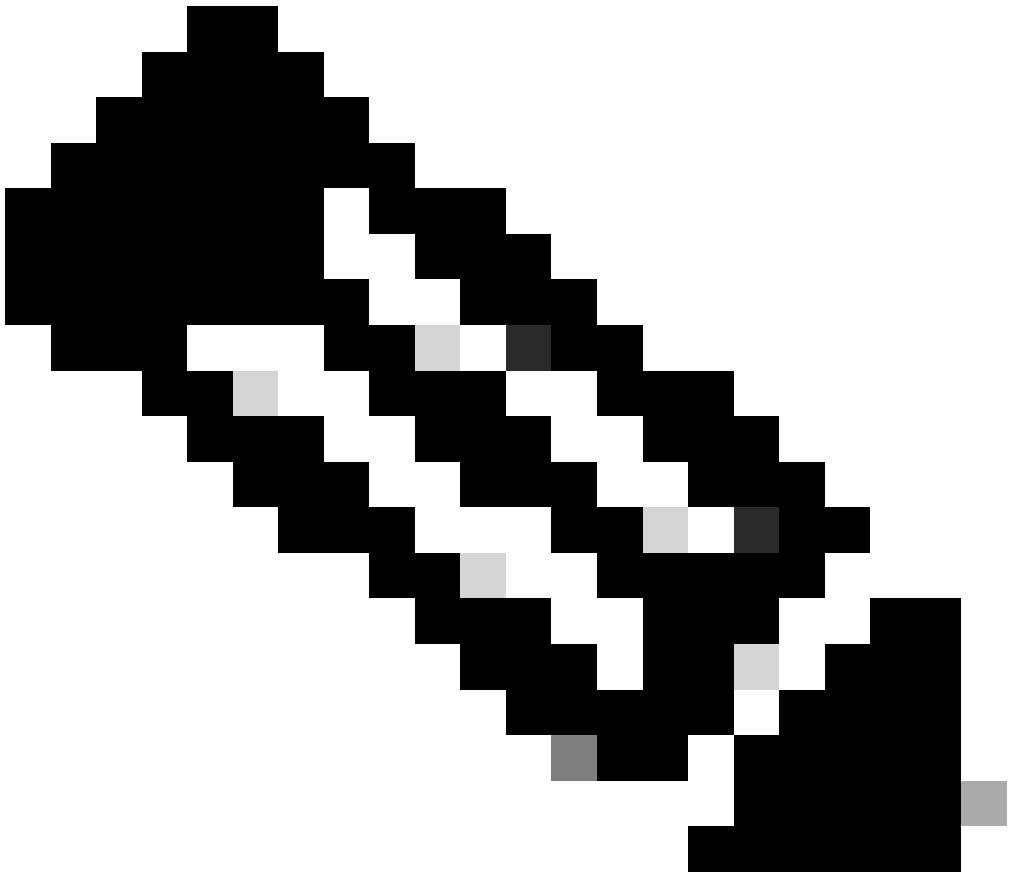
Met de integratie tussen Cisco Secure Malware Analytics (voorheen Threat Grid) en Cisco Umbrella zijn beveiligingsteams nu in staat om hun zichtbaarheid te vergroten en bescherming af te dwingen tegen de geavanceerde bedreigingen van vandaag voor roaming laptops, tablets of telefoons, terwijl ze ook een andere laag van handhaving bieden aan een gedistribueerd bedrijfsnetwerk.

In deze handleiding wordt beschreven hoe u Cisco Secure Malware Analytics (Threat Grid)

configureert om te communiceren met Cisco Umbrella, zodat bedreigingsinformatie die wordt gegenereerd door Cisco Secure Malware Analytics (Threat Grid) automatisch kan worden geïntegreerd in beleidsregels die clients kunnen beschermen onder uw Cisco Umbrella.

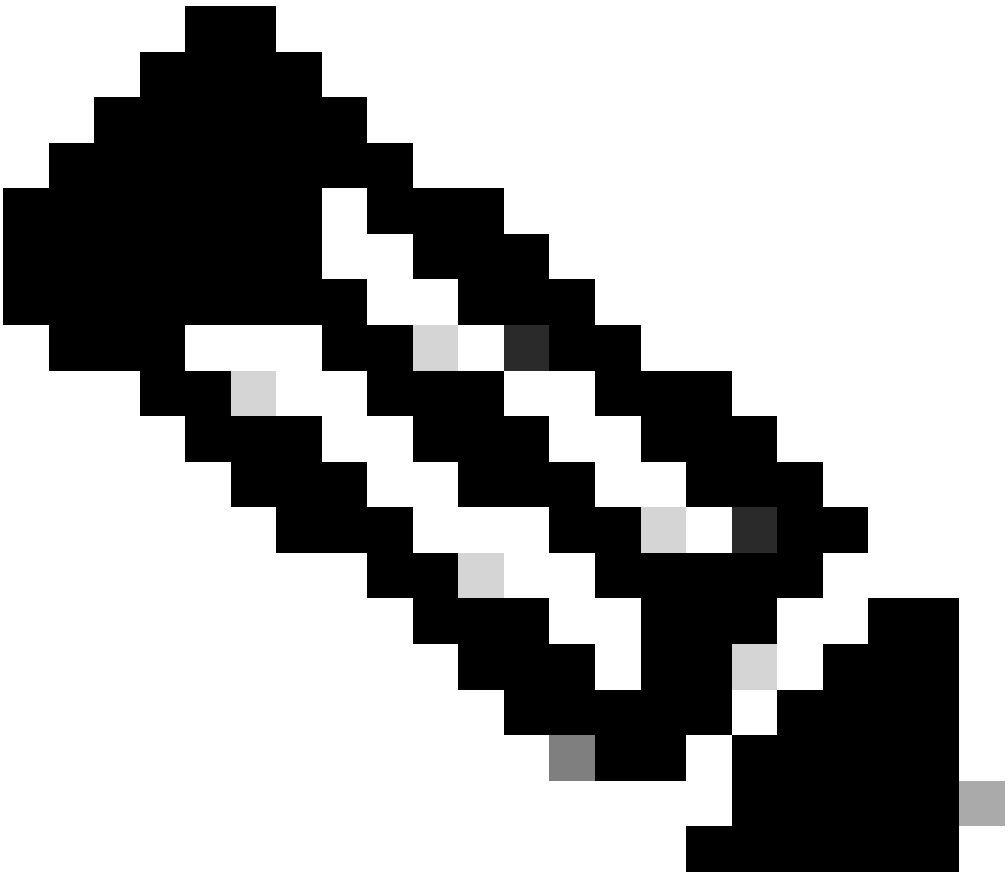
Voorwaarden

- Een functioneel Cisco Secure Malware Analytics (Threat Grid)-dashboard met toegang tot de API-sleutel van uw account.



Opmerking: Cisco Secure Malware Analytics (Threat Grid)-apparaten en -eindpunten worden momenteel niet ondersteund.

- Administratieve rechten Cisco Umbrella Dashboard.
- Het Cisco Umbrella-dashboard moet de integratie van Cisco Secure Malware Analytics (Threat Grid) hebben ingeschakeld.



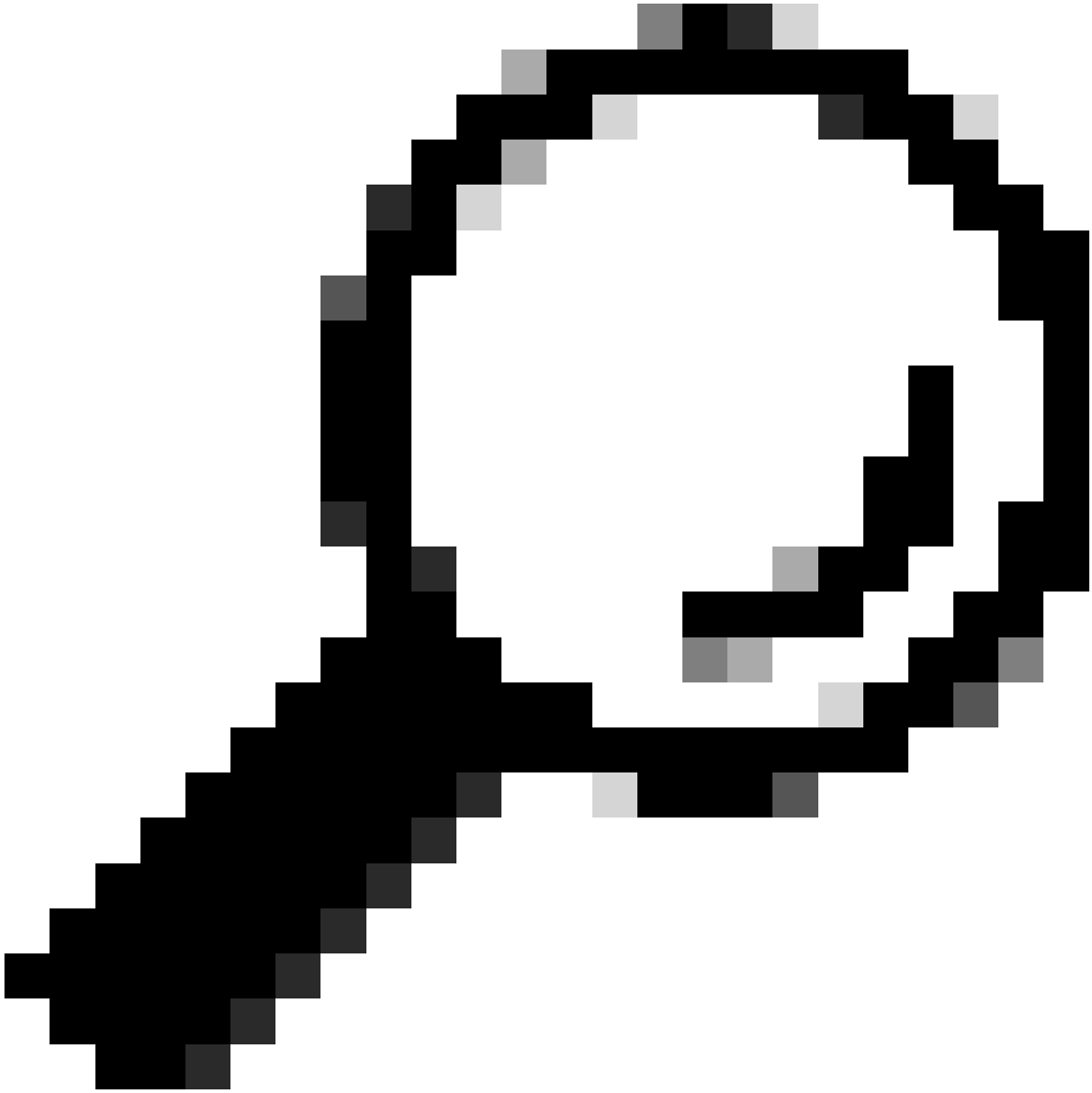
Opmerking: De integratie van Cisco Secure Malware Analytics (Threat Grid) is alleen opgenomen in Cisco-overkoepelende pakketten zoals DNS Essentials, DNS Advantage, SIG Essentials of SIG Advantage. Als u geen Cisco Umbrella-pakket hebt en deze integratie wilt hebben, neemt u contact op met uw Cisco Umbrella-accountmanager. Als u een Cisco Umbrella-pakket hebt, maar Cisco Secure Malware Analytics (Threat Grid) niet ziet als een integratie voor uw Dashboard, neemt u contact op met Cisco Umbrella Support.

Hoe werkt deze integratie?

Cisco Umbrella reikt uit naar de Cisco Secure Malware Analytics (Threat Grid) API en haalt lijsten op van domeinen die zijn gegenereerd uit de analyse van kwaadaardige monsters. Cisco Umbrella importeert deze lijst vervolgens via de Cisco Umbrella Enforcement API. Deze aanpak is anders dan hoe andere integraties werken in die Cisco Umbrella trekt de dreiging intelligentie in door het maken van API queries naar de Cisco Secure Malware Analytics (Threat Grid) API, in plaats van het accepteren van incidenten van andere systemen die duwen threat intelligence in de Cisco Umbrella service.

Cisco Umbrella valideert vervolgens de dreiging om ervoor te zorgen dat deze aan uw beleid kan worden toegevoegd. Als wordt bevestigd dat de informatie van Cisco Secure Malware Analytics (Threat Grid) een bedreiging vormt of geen bekend goed domein is, wordt het domeinadres toegevoegd aan de bestemmingslijst van Cisco Secure Malware Analytics (Threat Grid) als onderdeel van een beveiligingsinstelling die kan worden toegepast op elk Cisco Umbrella-beleid. Dat beleid wordt onmiddellijk toegepast op alle verzoeken die worden ingediend vanaf apparaten die gebruikmaken van het beleid dat gebruikmaakt van de integratie van Cisco Secure Malware Analytics (Threat Grid).

Cisco Umbrella haalt twee afzonderlijke feeds uit Cisco Secure Malware Analytics (Threat Grid): een publieke (wereldwijde) feed en een Customer Only (privé, specifiek voor één klant) feed.



Tip: Terwijl Cisco Umbrella zijn best doet om domeinen waarvan bekend is dat ze over het algemeen veilig zijn (bijvoorbeeld Google en Salesforce) te valideren en toe te staan, om

---

ongewenste onderbrekingen te voorkomen, raden we aan om domeinen die u nooit wilt hebben geblokkeerd toe te voegen aan de Global Allow List of andere bestemmingslijsten volgens uw beleid.

Voorbeelden zijn:

- De homepage voor uw organisatie.
- Domeinen die diensten vertegenwoordigen die u levert en die zowel interne als externe records kunnen hebben. Bijvoorbeeld "mail.myservicedomain.com" en "portal.myotherservicedomain.com".
- Minder bekende cloudtoepassingen waar u sterk afhankelijk van bent, zijn mogelijk niet bekend met Cisco Umbrella of zijn niet opgenomen in hun automatische domeinvalidatie. Bijvoorbeeld "localcloudservice.com".

Deze domeinen moeten worden toegevoegd aan de Global Allow List, die te vinden is onder Beleid > Bestemmingslijsten in Cisco Umbrella.

Uw Cisco Umbrella Dashboard configureren om informatie te verkrijgen van Cisco Secure Malware Analytics (Threat Grid)

De eerste stap is het vinden of genereren van de API-sleutel in uw Cisco Secure Malware Analytics (Threat Grid) dashboard:

1. Meld u aan bij uw Cisco Secure Malware Analytics (Threat Grid)-dashboard en selecteer uw accountgegevens.
2. Onder uw accountgegevens is mogelijk al een API-sleutel zichtbaar als u er al een hebt gemaakt. Als dat niet het geval is, selecteert u "Genereer nieuwe API-sleutel".

   Uw API-sleutel is dan zichtbaar onder Gebruikersgegevens > API-sleutel.

Voeg vervolgens de API-sleutel toe aan het Cisco Umbrella Dashboard zodat deze gegevens kan ophalen uit Cisco Secure Malware Analytics (Threat Grid):

1. Meld u aan bij uw Cisco Umbrella-dashboard als beheerder.
2. Ga naar Beleid > Beleidscomponenten > Integraties en selecteer "Cisco AMP Threat Grid" (Cisco Secure Malware Analytics (Threat Grid)) in de tabel om deze uit te breiden.
3. Selecteer Inschakelen, plak uw API-sleutel in het vak API-sleutel en selecteer vervolgens Opslaan.

Op dit moment, als u een fout ontvangt, is er waarschijnlijk een probleem met uw API-sleutel of communicatie tussen de services. Controleer uw API-sleutel en probeer het opnieuw en neem contact op met Cisco Umbrella Support als dit nog steeds mislukt.

Als u een succesbericht ontvangt, geeft dit aan dat de Cisco Umbrella-service de API-sleutel kon gebruiken om een eerste verbinding te maken met de Cisco Secure Malware Analytics (Threat Grid) API. De Cisco Umbrella-service gebruikt een polling-interval van vijf minuten om gegevens op te halen uit Cisco Secure Malware Analytics (Threat Grid).

Zelfs na het interval van vijf minuten, als er geen geldige gegevens of geldige bedreigingsgebeurtenissen beschikbaar zijn om door het Cisco Umbrella Dashboard te worden getrokken, wordt informatie mogelijk niet weergegeven. Wanneer de integratie voor het eerst is ingeschakeld, begint deze gewoon door vijf minuten terug te gaan voor zowel de globale als alleen-org-feeds en de eerste keer dat gegevens worden opgehaald, is met het volgende interval van vijf minuten, dus gegevens worden mogelijk niet onmiddellijk weergegeven.

Als de API-sleutel aan de kant van Cisco Secure Malware Analytics (Threat Grid) is gedeactiveerd of verwijderd, wordt de integratie uitgeschakeld. Om de integratie te herstellen, moet een nieuwe API-sleutel worden verstrekt in het Cisco Umbrella Dashboard. Als er een time-out of interne servicefout optreedt tussen Cisco Umbrella en Cisco Secure Malware Analytics (Threat Grid), wordt een ander soort uitzondering gemaakt en wordt de integratie niet uitgeschakeld, maar worden verbindingen elke vijf minuten geprobeerd, zoals in normale omstandigheden.

Technische details

De exacte API-query's die worden gebruikt om informatie uit de Cisco Secure Malware Analytics (Threat Grid) te halen, worden hieronder vermeld. Merk op dat alleen gebeurtenissen met een ernst groter dan 90, een betrouwbaarheid groter dan 90 en van het type Domeinen worden verzameld. De tijd in dit voorbeeld is een bereik van vijf minuten dat wordt verhoogd voor de volgende query. De `api_key` in Cisco Umbrella wordt gebruikt in plaats van de variabele `<key>`:

- Openbaar (wereldwijde feed):

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

- Alleen voor klanten (privéfeed):

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

of:

- Openbaar (wereldwijde feed):

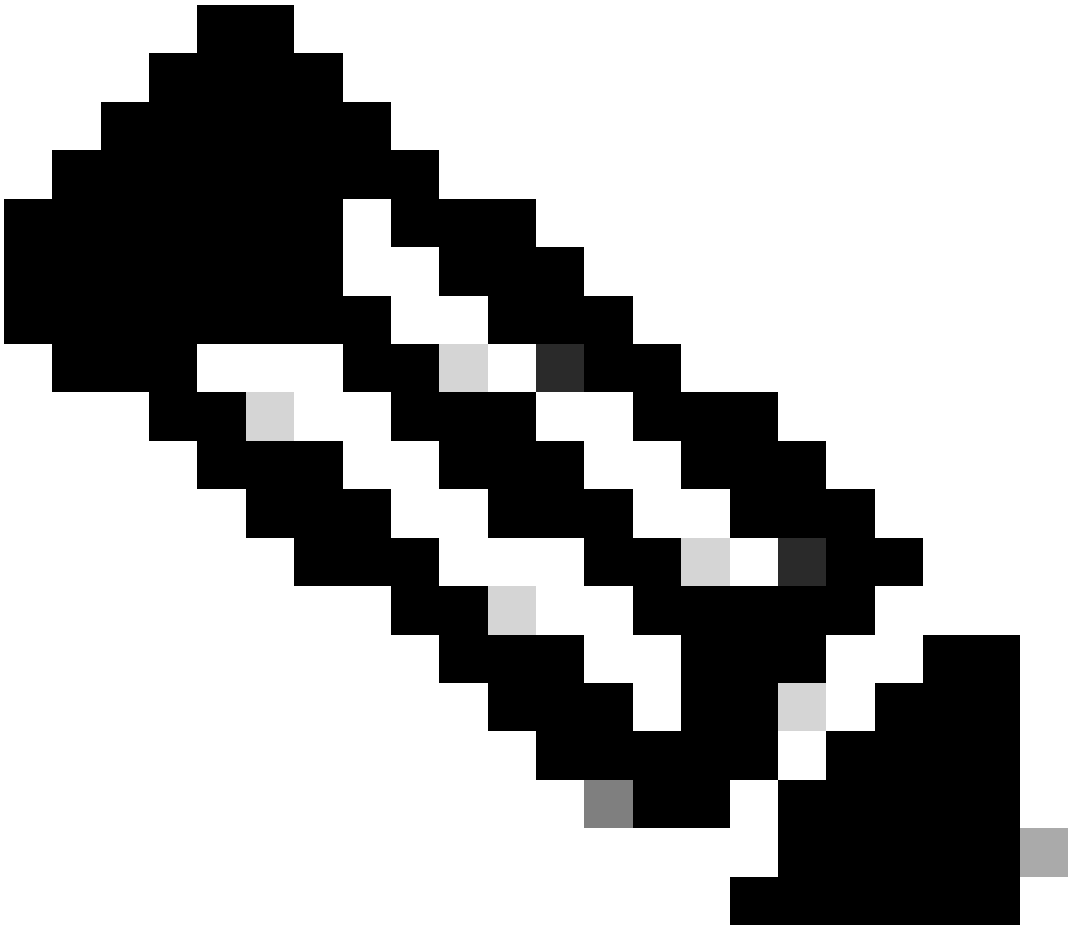
```
hxxps://panacea.threatgrid.eu/api/v2/iocs/feeds/domains?limit=100&offset=0&severity=90&confidence
```

- Alleen voor klanten (privéfeed):

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

Gebeurtenissen observeren die zijn toegevoegd aan de Cisco Secure Malware Analytics (Threat Grid) in "auditmodus"

Na verloop van tijd beginnen de gebeurtenissen uit Cisco Secure Malware Analytics (Threat Grid) een specifieke lijst met bestemmingen te vullen die kunnen worden toegepast op beleid als de Cisco Secure Malware Analytics (Threat Grid) -categorie. De doellijst en de beveiligingscategorie bevinden zich standaard in de "controlemodus" en worden niet toegepast op beleidsregels, waardoor verzoeken niet worden geblokkeerd. U kunt echter zien welke verzoeken zijn gekoppeld (en mogelijk zijn geblokkeerd) door de beveiligingscategorie Cisco AMP Threat Grid.



Opmerking: "Controlemodus" kan worden ingeschakeld zolang als nodig is, of zelfs voor onbepaalde tijd, afhankelijk van uw implementatieprofiel en netwerkconfiguratie.

Bestemmingslijst bekijken

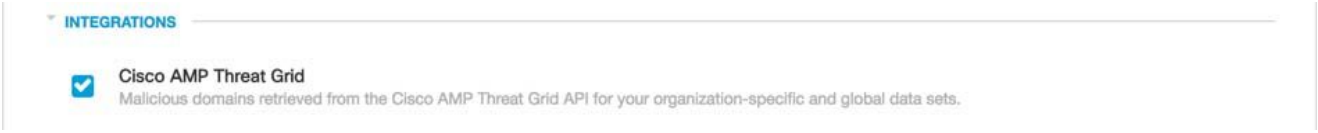
U kunt de Cisco Secure Malware Analytics (Threat Grid) bestemmingslijst op elk gewenst moment bekijken.

1. Navigeer naar Beleid > Beleidscomponenten > Integraties.
2. Vouw "Cisco AMP Threat Grid" (Cisco Secure Malware Analytics (Threat Grid)) uit in de tabel en selecteer "Zie domeinen".

Beveiligingsinstellingen voor een beleid bekijken

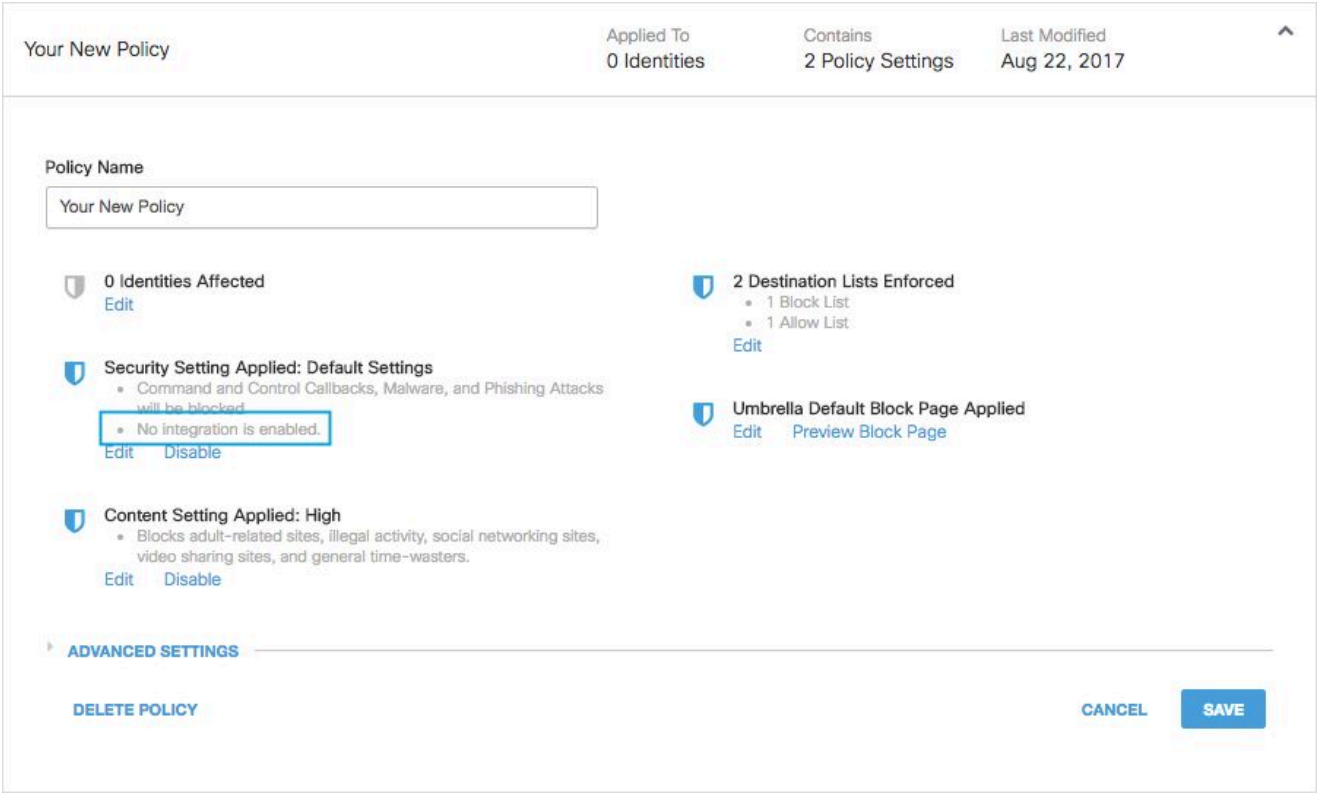
U kunt de beveiligingsinstellingen bekijken die op elk gewenst moment voor een beleid kunnen worden ingeschakeld in Cisco Umbrella:

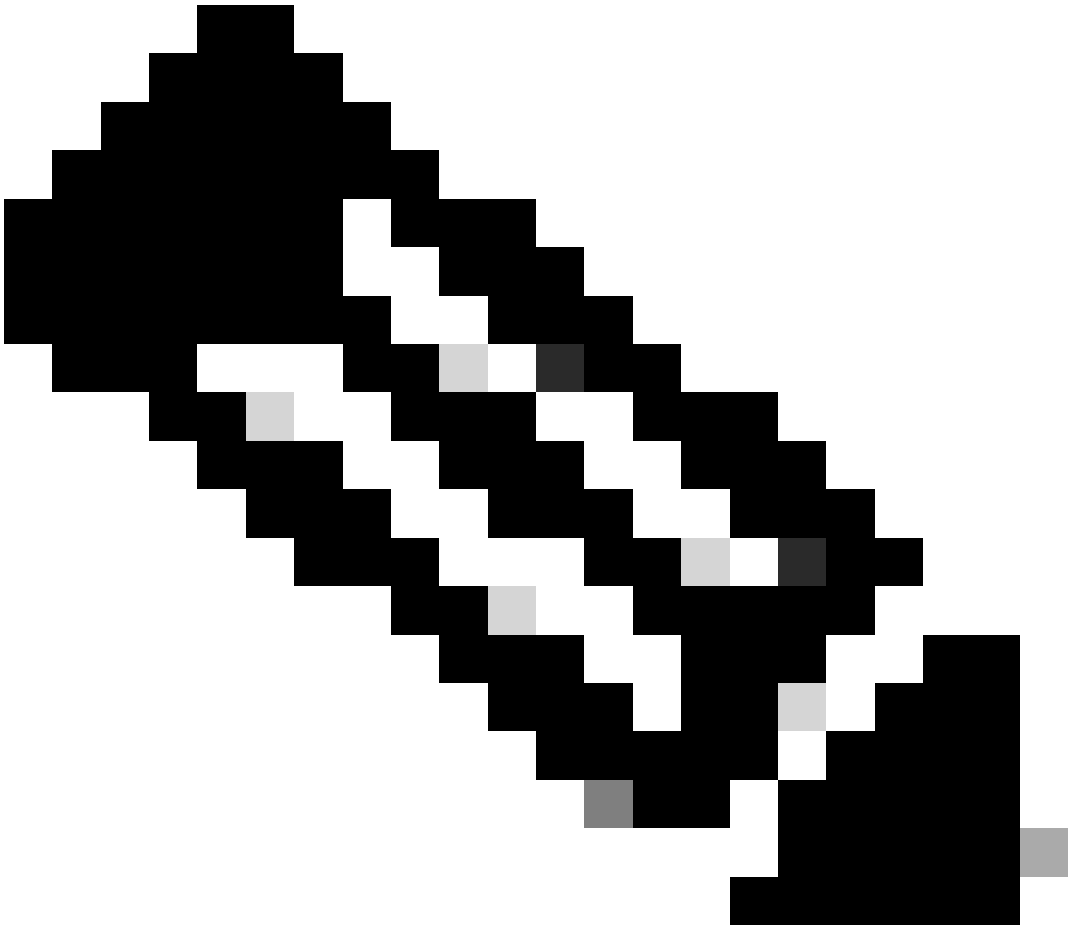
1. Navigeer naar Beleid > Beleidscomponenten > Beveiligingsinstellingen.
2. Klik op een beveiligingsinstelling in de tabel om deze uit te vouwen.
3. Blader naar de sectie Integraties en vouw de sectie uit om de integratie van Cisco AMP Threat Grid (Cisco Secure Malware Analytics (Threat Grid)) weer te geven.
4. Selecteer het vakje voor de integratie van het Cisco AMP Threat Grid (Cisco Secure Malware Analytics (Threat Grid)) en selecteer vervolgens Opslaan.



115014151543

U kunt ook integratiegegevens bekijken via de overzichtspagina Beveiligingsinstellingen.



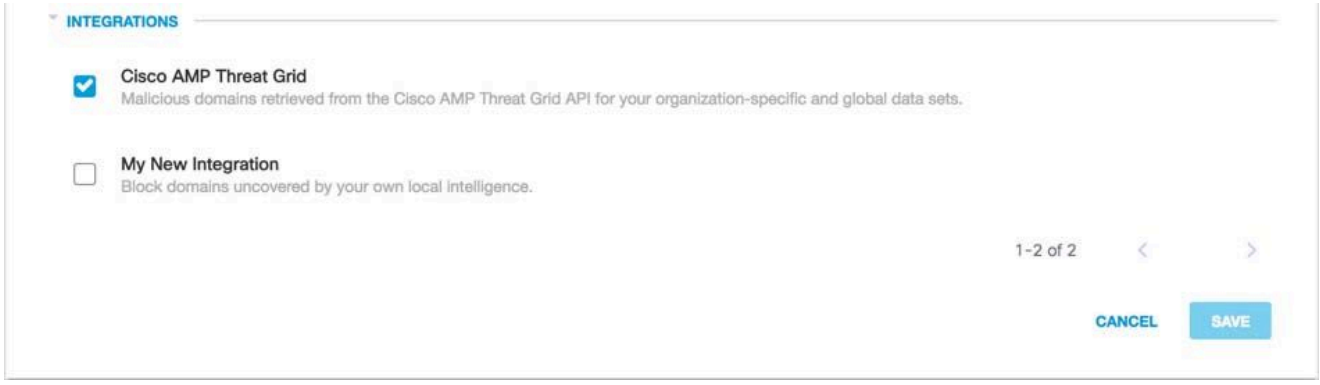


Opmerking: het kan tot vijf minuten duren om instellingen toe te passen en als er geen nieuwe gebeurtenissen worden geïnjecteerd in het Cisco Secure Malware Analytics (Threat Grid) -systeem, ziet u mogelijk geen nieuwe domeinen worden toegevoegd aan uw integratie.

De beveiligingsinstelling Cisco Secure Malware Analytics (Threat Grid) toepassen in de "blokmodus" op een beleid voor beheerde clients

Zodra u klaar bent om deze domeinen te laten blokkeren voor clients die worden beheerd door Cisco Umbrella, wijzigt u de beveiligingsinstelling voor een bestaand beleid of maakt u een nieuw beleid dat boven uw standaardbeleid staat om ervoor te zorgen dat het eerst wordt gehandhaafd.

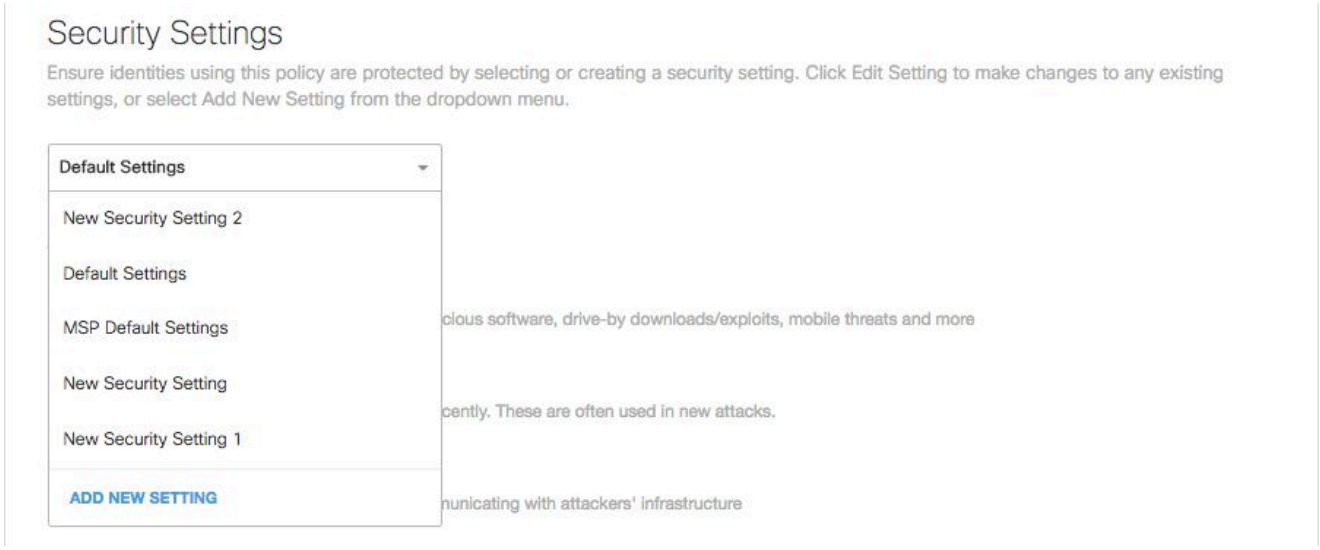
1. Navigeer naar Beleid > Beleidscomponenten > Beveiligingsinstellingen.
2. Controleer onder Integraties of het vak "Cisco AMP Threat Grid" is geselecteerd. Als dit niet het geval is, selecteert u het selectievakje en selecteert u Opslaan.



115013987086

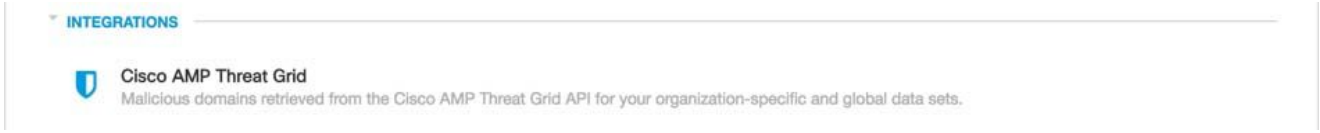
Voeg vervolgens in de wizard Cisco Umbrella Policy een beveiligingsinstelling toe aan het beleid dat u bewerkt:

1. Navigeer naar Beleid > Beheer > Alle Beleid.
2. Vouw een beleid uit onder Beveiligingsinstelling toegepast en selecteer Bewerken.
3. Selecteer in de vervolgkeuzelijst Beveiligingsinstellingen een beveiligingsinstelling die de instelling "Cisco AMP Threat Grid" bevat.



20993282642708

Het schildpictogram onder Integraties wordt bijgewerkt naar blauw.



115013987446

4. Selecteer Instellen en retourneren.

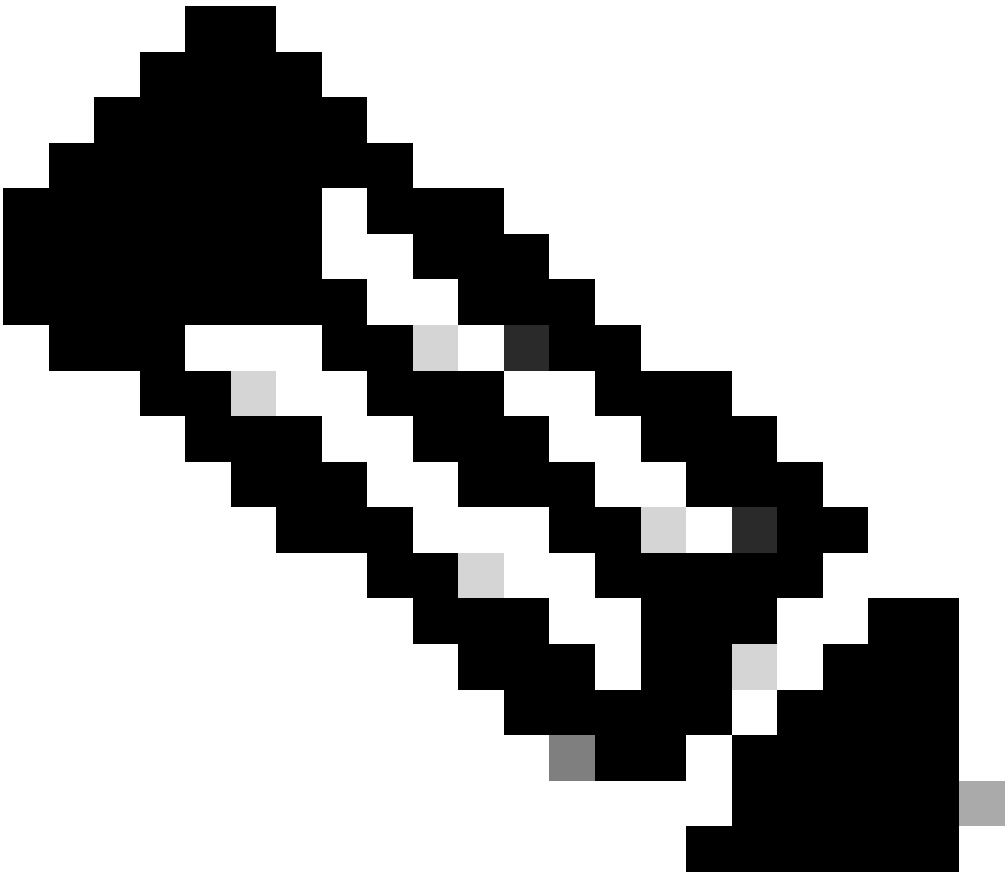
   Cisco Secure Malware Analytics (Threat Grid)-domeinen die zich in de beveiligingsinstelling voor Cisco Secure Malware Analytics (Threat Grid) bevinden, worden geblokkeerd voor die identiteiten die het beleid gebruiken.

Rapportage binnen Cisco Umbrella voor Cisco Secure Malware Analytics-evenementen

Rapportage over beveiligingsgebeurtenissen met Cisco Secure Malware Analytics (Threat Grid)

De Cisco Secure Malware Analytics (Threat Grid) Destination List is een van de lijsten met beveiligingscategorieën waarop u kunt rapporteren. De meeste of alle rapporten gebruiken de beveiligingscategorieën als filter. U kunt bijvoorbeeld beveiligingscategorieën filteren om alleen aan Cisco Secure Malware Analytics (Threat Grid) gerelateerde activiteiten weer te geven.

1. Navigeer naar Rapportage > Kernrapporten > Zoeken naar activiteiten en selecteer onder Beveiligingscategorieën "Cisco AMP Threat Grid" (Cisco Secure Malware Analytics (Threat Grid)) om het rapport te filteren zodat alleen de beveiligingscategorie voor Cisco Secure Malware Analytics (Threat Grid) wordt weergegeven.



Opmerking: Als de integratie van het Cisco AMP Threat Grid is uitgeschakeld, wordt deze niet weergegeven in het filter Beveiligingscategorieën.

115014210123

2. Selecteer Toepassen.

Rapporteren over wanneer domeinen zijn toegevoegd aan de bestemmingslijst van Cisco Secure Malware Analytics (Threat Grid)

Het Cisco Umbrella Admin Audit-logboek bevat gebeurtenissen uit het Cisco Secure Malware Analytics (Threat Grid)-dashboard omdat het domeinen aan de bestemmingslijst toevoegt. Een gebruiker met de naam "Cisco AMP Threat Grid Domain List", die ook wordt gebrandmerkt met het Cisco-logo, genereert de gebeurtenissen. Deze gebeurtenissen omvatten het domein dat is toegevoegd en het tijdstip waarop het is toegevoegd.

Als u het item Controlelogboek voor beheerders selecteert, wordt dit uitgebreid om details weer te geven, inclusief het specifieke domein dat is toegevoegd.

U kunt filteren om alleen wijzigingen in Cisco Secure Malware Analytics (Threat Grid) op te nemen door een filter toe te passen voor de gebruiker "Cisco AMP Threat Grid Domain List".

Omgaan met ongewenste detecties of valse positieven

Twee soorten Cisco Secure Malware Analytics (Threat Grid) Detecties en twee resoluties

Momenteel zijn er twee soorten Cisco Secure Malware Analytics (Threat Grid) -blokken: een met een mogelijke resolutie en een tweede met een huidige resolutie voor een ongewenste detectie.

1. Global Threat Grid Entry (openbaar): op dit moment is de enige methode om het domein toe te staan het toevoegen aan uw lijst met machtigingen.
2. Alleen voor klanten bestemde feed (privé): kan worden behandeld met een vermelding in de machtigingslijst of met verwijdering uit de integratielijst van het AMP-bedreigingsraster.

Lijsten toestaan

Hoewel onwaarschijnlijk, is het mogelijk dat domeinen die automatisch worden toegevoegd door uw integratie van Cisco Secure Malware Analytics (Threat Grid) mogelijk een ongewenste detectie veroorzaken die uw gebruikers blokkeert om toegang te krijgen tot bepaalde websites. In een dergelijke situatie raden we aan om de domeinnamen toe te voegen aan een lijst met machtigingen (Beleid > Bestemmingslijsten), die voorrang heeft op alle andere soorten blokkeringslijsten, inclusief beveiligingsinstellingen.

Er zijn twee redenen waarom deze aanpak de voorkeur heeft. Ten eerste, in het geval dat het Cisco Secure Malware Analytics (Threat Grid)-dashboard het domein opnieuw zou toevoegen nadat het was verwijderd, staat de lijst beveiligingen toe tegen dit veroorzaken van verdere problemen. Ten tweede toont de allow-lijst een historisch overzicht van problematische domeinen die kunnen worden gebruikt voor forensische of auditrapporten.

Standaard is er een algemene lijst met toegestane items die wordt toegepast op alle beleidsregels. Als u een domein toevoegt aan de algemene machtigingslijst, wordt het domein toegestaan in alle beleidsregels.

Als de beveiligingsinstelling voor Cisco Secure Malware Analytics (Threat Grid) in de blokmodus alleen wordt toegepast op een subset van uw beheerde Cisco Umbrella-identiteiten (deze wordt bijvoorbeeld alleen toegepast op zwervende computers en mobiele apparaten), kunt u een specifieke lijst met machtigingen voor deze identiteiten of beleidsregels maken.

U maakt als volgt een lijst met machtigingen:

1. Navigeer naar Beleid > Beleidscomponenten > Bestemmingslijsten en selecteer 

("Toevoegen").
2. Selecteer Toestaan en voeg uw domein toe aan de lijst.

3. Selecteer Opslaan.

Zodra de lijst is opgeslagen, kunt u deze toevoegen aan een bestaand beleid voor die clients die zijn getroffen door het ongewenste blok.

Domeinen verwijderen uit de bestemmingslijst van Cisco Secure Malware Analytics (Threat Grid)

Naast elke domeinnaam in de lijst van Cisco Secure Malware Analytics (Threat Grid) staat een pictogram ("Verwijderen"). Als u domeinen verwijdert, kunt u de bestemmingslijst van Cisco Secure Malware Analytics (Threat Grid) opschonen in het geval van een ongewenste detectie.

De verwijdering is niet permanent als het Cisco Secure Malware Analytics (Threat Grid)-dashboard het domein opnieuw naar Cisco Umbrella zou verzenden.

1. Navigeer naar Beleid > Beleidscomponenten > Integraties en selecteer "Cisco AMP Threat Grid" (Cisco Secure Malware Analytics (Threat Grid)) om het uit te breiden.
2. Selecteer Zie domeinen.
3. Zoek naar de domeinnaam die je wilt verwijderen.
4. Selecteer het pictogram ("Verwijderen").
5. Selecteer Sluiten.
6. Selecteer Opslaan.

In het geval van een ongewenste detectie of vals-positief, raden we aan om onmiddellijk een lijst met machtigingen in Cisco Umbrella te maken en vervolgens het vals-positieve te herstellen in het Cisco Secure Malware Analytics (Threat Grid) -dashboard. Later kunt u het domein verwijderen uit de bestemmingslijst van Cisco Secure Malware Analytics (Threat Grid).

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.