# ThreatConnect integreren met paraplu

## Inhoud



## Inleiding

In dit document wordt beschreven hoe ThreatConnect kan worden geïntegreerd met Cisco Umbrella.

## Voorwaarden

### Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Een ThreatConnect-dashboard met toegang om de URL voor integraties bij te werken
- Administratieve rechten overkoepelend dashboard
- De integratie van ThreatConnect moet zijn ingeschakeld op het Umbrella-dashboard.

### Gebruikte componenten

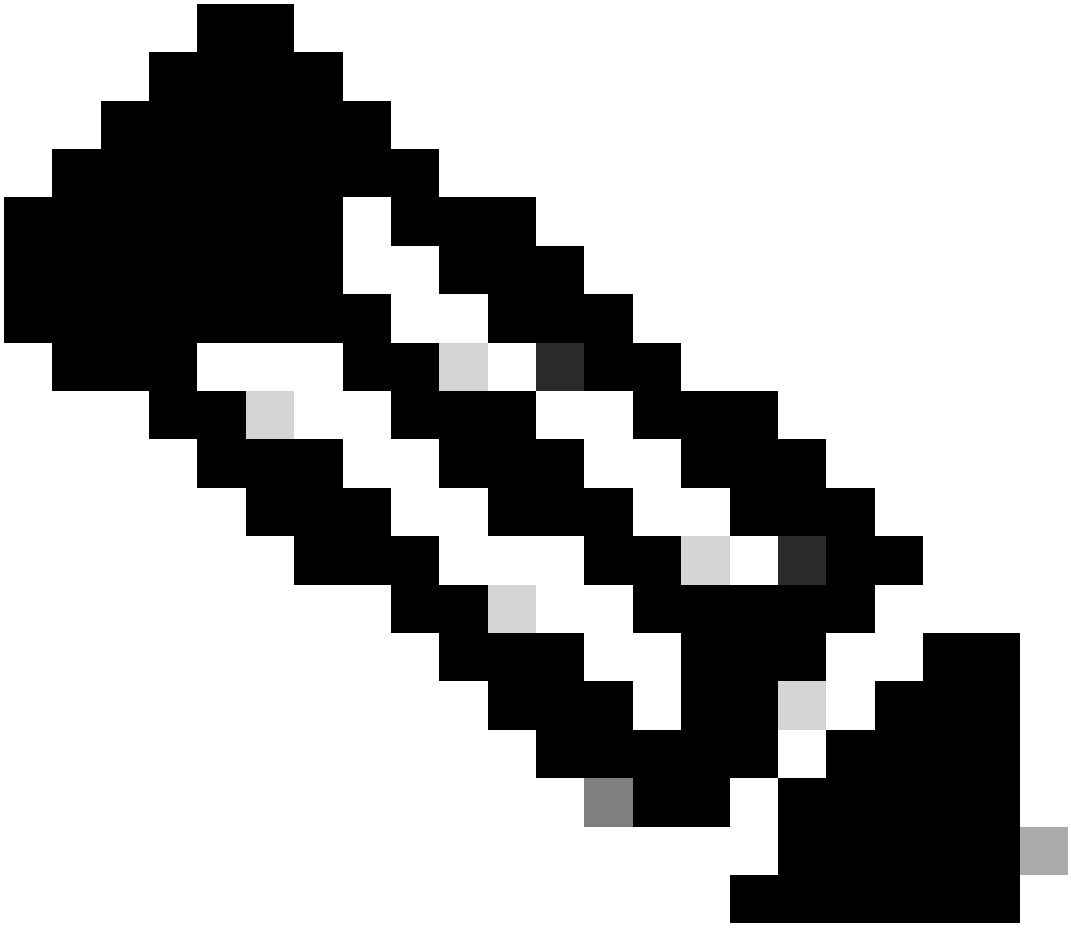
De informatie in dit document is gebaseerd op Cisco Umbrella.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

# Overzicht van de integratie van ThreatConnect en Cisco Umbrella

Door ThreatConnect te integreren met Cisco Umbrella, kunnen beveiligingsmedewerkers en -beheerders nu bescherming tegen geavanceerde bedreigingen uitbreiden naar roaming-laptops, tablets of telefoons, terwijl ze ook een andere handhavingslaag bieden aan een gedistribueerd bedrijfsnetwerk.

In deze handleiding wordt beschreven hoe ThreatConnect kan worden geconfigureerd om te communiceren met Umbrella, zodat beveiligingsgebeurtenissen uit de ThreatConnect-tip worden geïntegreerd in beleid dat kan worden toegepast op clients die worden beschermd door uw Cisco-paraplu.



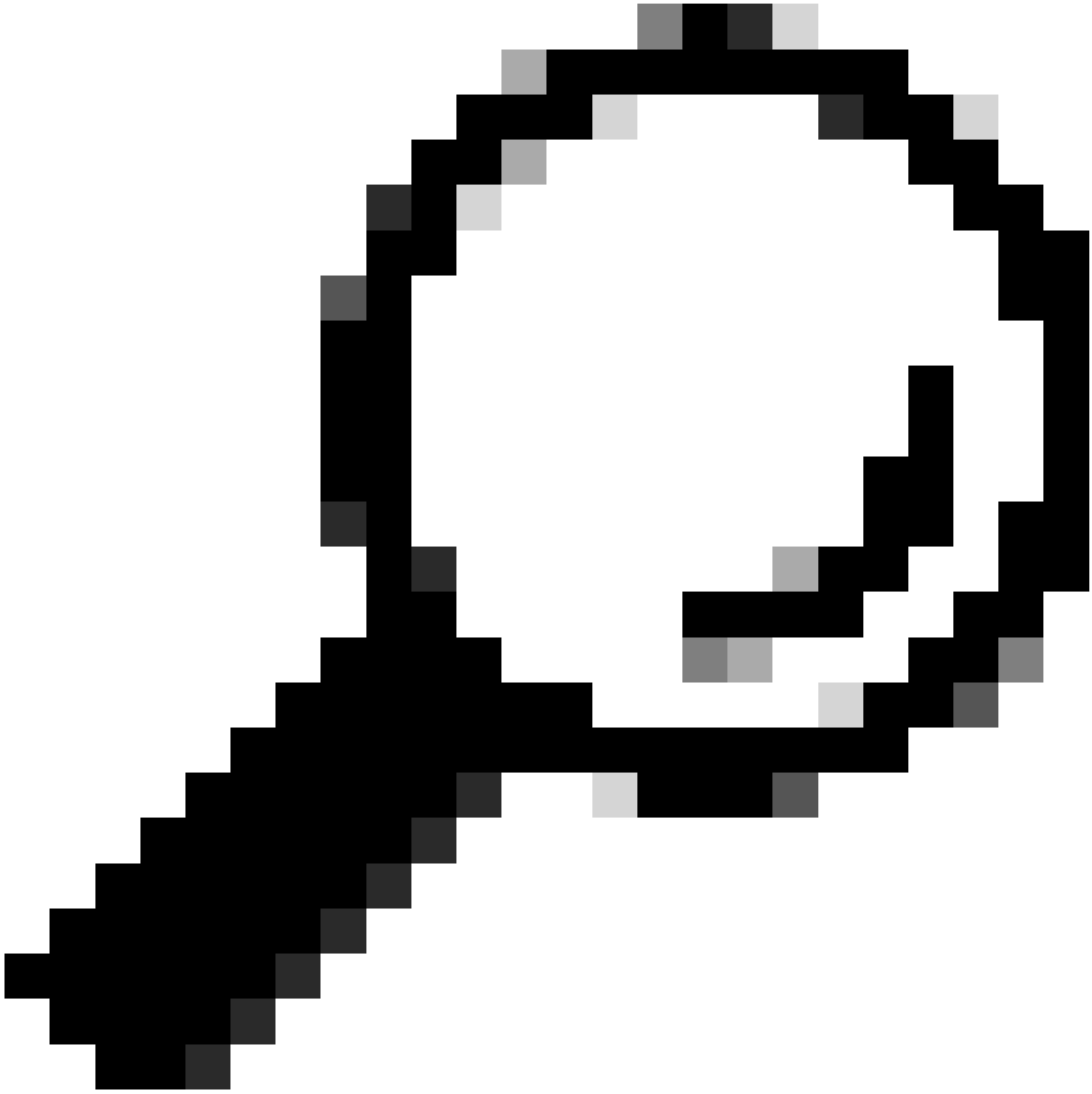
Opmerking: de ThreatConnect-integratie is alleen opgenomen in een bepaald Cisco Umbrella-pakket. Als u geen pakket hebt dat deze integratie bevat, neemt u contact op met uw Cisco Umbrella-vertegenwoordiger om het te verkrijgen. Als u het juiste pakket hebt, maar ThreatConnect niet ziet als een integratie voor uw dashboard, neemt u contact op met Cisco Umbrella Support.

Het ThreatConnect-platform stuurt eerst de Cyber Threat Intelligence die het heeft gevonden, zoals domeinen die malware hosten, commando en controle voor botnet- of phishingsites, naar Umbrella.

Umbrella valideert vervolgens de dreiging om ervoor te zorgen dat deze kan worden toegevoegd aan een beleid. Als wordt bevestigd dat de informatie van ThreatConnect een bedreiging vormt, wordt het domeinadres toegevoegd aan de bestemmingslijst van ThreatConnect als onderdeel van een beveiligingsinstelling die kan worden toegepast op elk overkoepelend beleid. Dat beleid wordt onmiddellijk toegepast op alle verzoeken die worden ingediend vanaf apparaten die gebruikmaken van beleid met de bestemmingslijst van ThreatConnect.

In de toekomst parseert Umbrella automatisch ThreatConnect-waarschuwingen en voegt schadelijke sites toe aan de ThreatConnect-bestemmingslijst, waardoor ThreatConnect-bescherming wordt uitgebreid naar alle externe gebruikers en apparaten en een andere laag van handhaving wordt geboden aan uw bedrijfsnetwerk.

---



Tip: terwijl 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, stelt Umbrella voor om domeinen toe te voegen die u niet wilt worden geblokkeerd in de Global Allow List of andere bestemmingslijsten volgens uw beleid. Voorbeelden zijn:

- De homepage voor uw organisatie. Bijvoorbeeld mydomain.com.
- 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 cloudapplicaties waarvan u sterk afhankelijk bent, maar waarvan Umbrella niet op de hoogte is of die deel uitmaken van de automatische domeinvalidatie. Bijvoorbeeld localcloudservice.com.

De globale lijst met toegestane items is te vinden op Beleid > Bestemmingslijsten in Paraplu. Zie de documentatie voor meer informatie: Bestemmingslijsten beheren

---

## Het Umbrella Dashboard configureren om gebeurtenissen van ThreatConnect te ontvangen

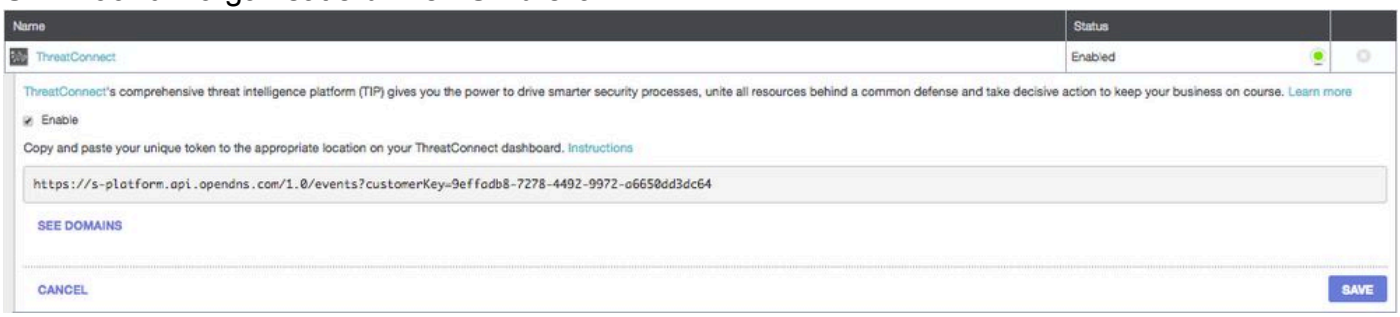
Begin met het vinden van uw unieke URL in Umbrella voor het ThreatQ-apparaat om mee te communiceren:

1. Log in op het dashboard van uw paraplu.

2. Ga naar Beleid > Integraties.

3. Selecteer in de tabel ThreatConnect om deze uit te vouwen.

4. Selecteer Inschakelen en selecteer vervolgens Opslaan. Dit genereert een unieke, specifieke URL voor uw organisatie binnen Umbrella.




U hebt de URL later in dit artikel nodig wanneer u de ThreatConnect configureert om gegevens naar Umbrella te verzenden.

## ThreatConnect configureren voor communicatie met de paraplu

Om te beginnen met het verzenden van verkeer van ThreatConnect naar Umbrella, moet u ThreatConnect configureren met de URL-informatie die is gegenereerd in het eerste deel van dit artikel:

1. Log in op uw ThreatConnect-dashboard.

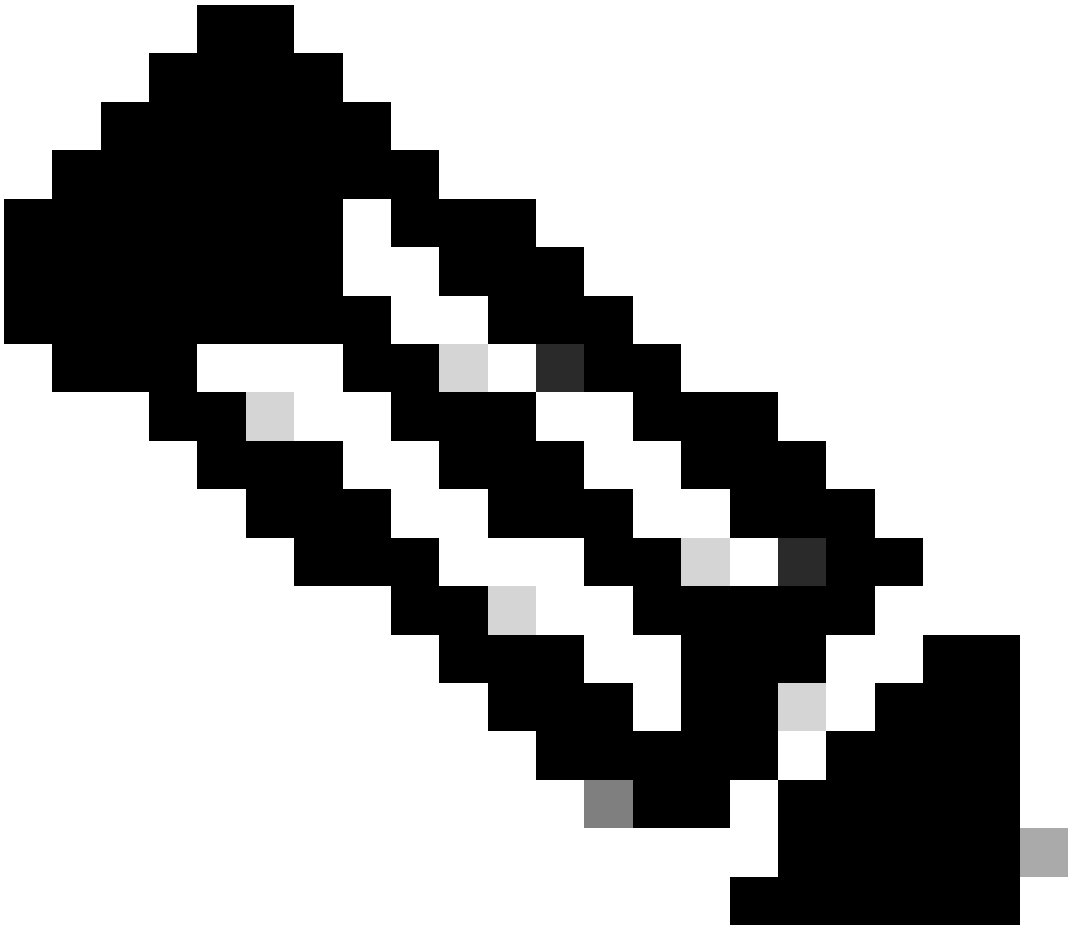
2. Voeg de URL toe in het juiste gebied om verbinding te maken met Umbrella.

Exacte instructies variëren en Umbrella stelt voor contact op te nemen met ThreatConnect-ondersteuning als u niet zeker weet hoe of waar API-integraties binnen ThreatConnect moeten worden geconfigureerd.

# Gebeurtenissen observeren die zijn toegevoegd aan de beveiligingscategorie ThreatConnect in de controlemodus

Na verloop van tijd kunnen gebeurtenissen uit uw ThreatConnect-dashboard beginnen met het invullen van een specifieke bestemmingslijst die kan worden toegepast op beleid als een ThreatConnect-beveiligingscategorie. Standaard bevinden de doellijst en de beveiligingscategorie zich in de controlemodus, wat betekent dat ze niet worden toegepast op beleidsregels en niet resulteren in wijzigingen in uw bestaande overkoepelende beleidsregels.

---



> Opmerking: de controlemodus kan worden ingeschakeld zolang dit nodig is op basis van uw implementatieprofiel en netwerkconfiguratie.

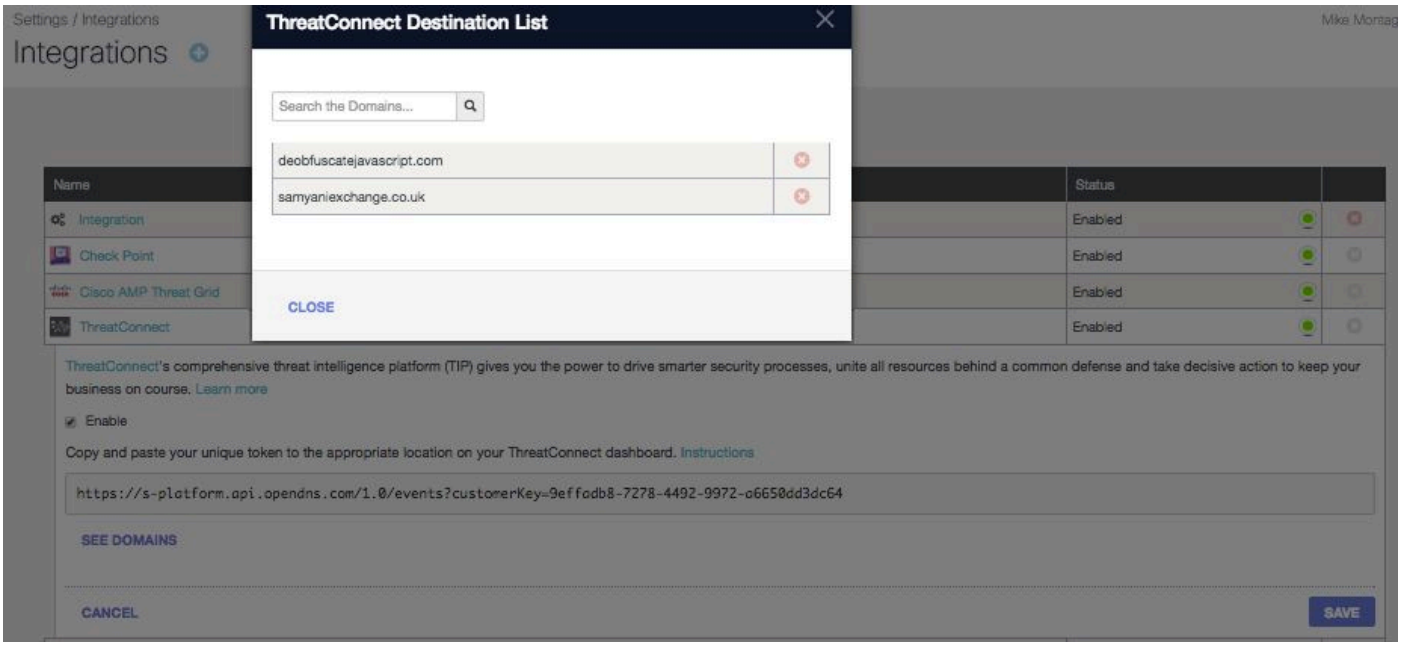
---

## Bestemmingslijst bekijken

U kunt de bestemmingslijst van ThreatConnect op elk gewenst moment bekijken in Umbrella:

1. Navigeer in het dashboard van de paraplu naar Beleid > Integraties.

2. Vouw in de tabel ThreatConnect uit en selecteer Zie domeinen.



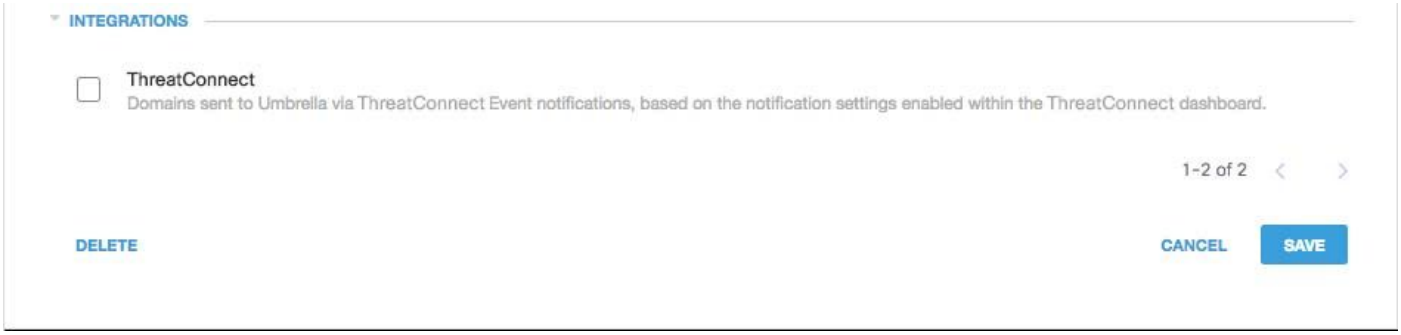

## Beveiligingsinstellingen voor een beleid bekijken

U kunt op elk gewenst moment de beveiligingsinstelling bekijken die voor een beleid kan worden ingeschakeld:

1. Navigeer in het dashboard van de paraplu naar Beleid > Beveiligingsinstellingen.

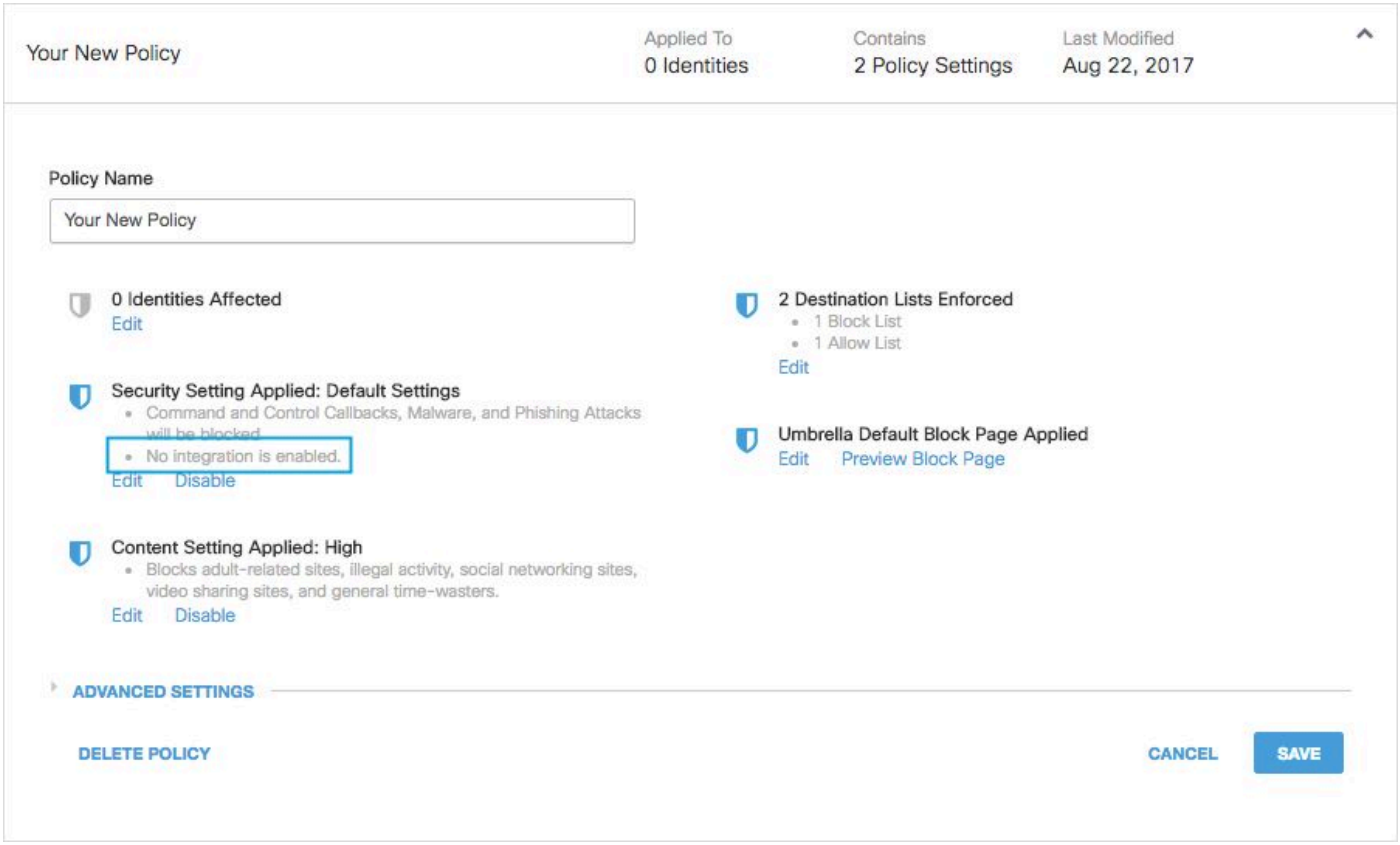
2. Selecteer een beveiligingsinstelling in de tabel om deze uit te vouwen.

3. Blader naar Integraties om de instelling ThreatConnect te vinden.




115014036566

4. U kunt integratiegegevens ook bekijken via de pagina Overzicht van beveiligingsinstellingen.



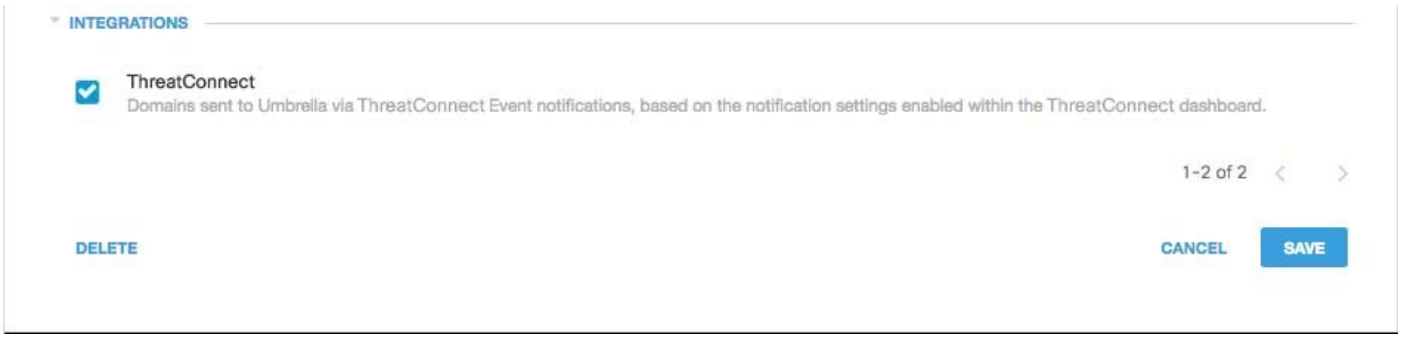

25464103885972

# De beveiligingsinstellingen van ThreatConnect in de blokmodus toepassen op een beleid voor beheerde clients

Zodra u klaar bent om deze extra beveiligingsbedreigingen te laten afdwingen door clients die door Umbrella worden beheerd, wijzigt u eenvoudig de beveiligingsinstelling op een bestaand beleid of maakt u een nieuw beleid dat boven uw standaardbeleid staat om ervoor te zorgen dat het eerst wordt afgedwongen:

1. Ga naar Beleid > Beveiligingsinstellingen.

2. Selecteer onder Integraties de optie ThreatConnect en selecteer vervolgens Opslaan.



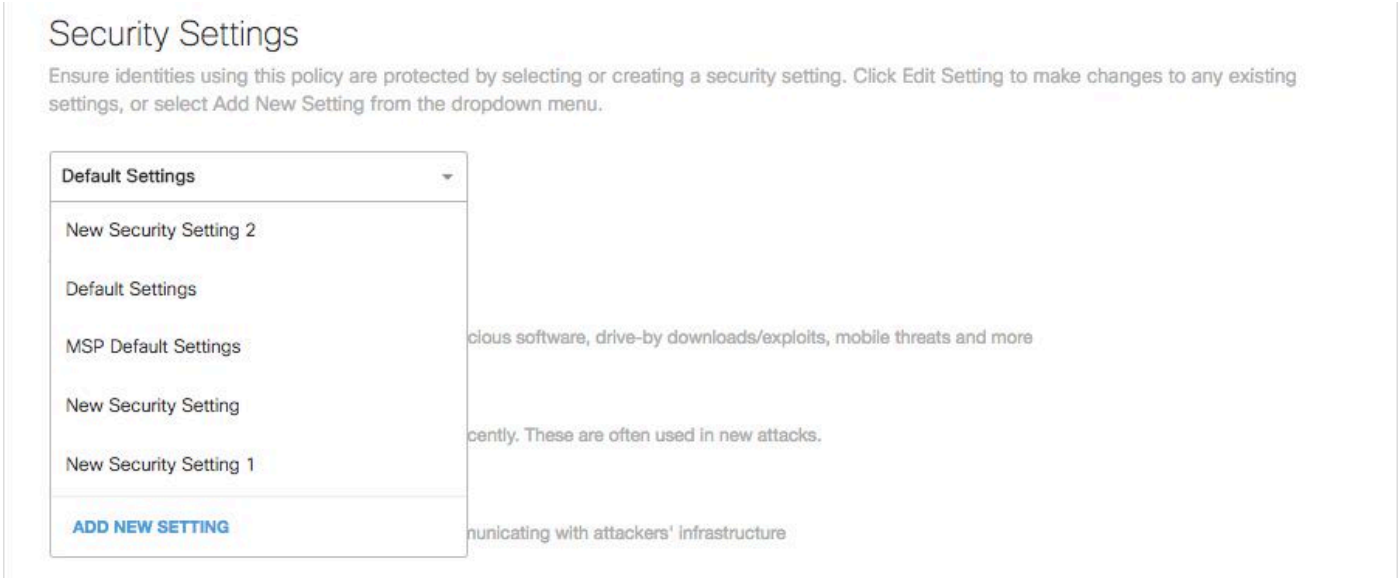

115014203703

Voeg vervolgens in de wizard Beleid een beveiligingsinstelling toe aan het beleid dat u bewerkt:

1. Navigeer naar Beleid > Beleidslijst.

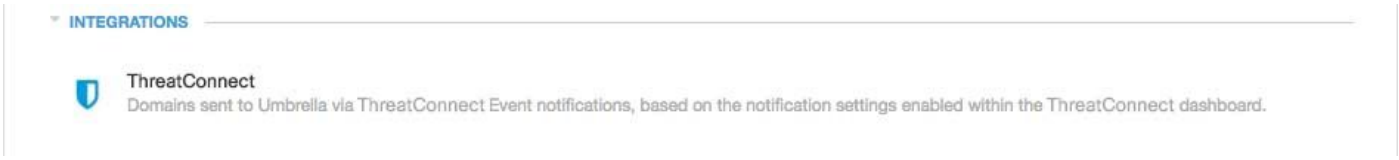
2. Een beleid uitbreiden. Selecteer onder Beveiligingsinstelling toegepast de optie Bewerken.

3. Selecteer in de vervolgkeuzelijst Beveiligingsinstellingen een beveiligingsinstelling die de instelling ThreatConnect bevat.




25464103908884

Het schildpictogram onder Integraties wordt bijgewerkt naar blauw.




115014037666

4. Selecteer Set & Return.

ThreatConnect-domeinen in de beveiligingsinstelling voor ThreatConnect worden vervolgens geblokkeerd voor identiteiten die het beleid gebruiken.

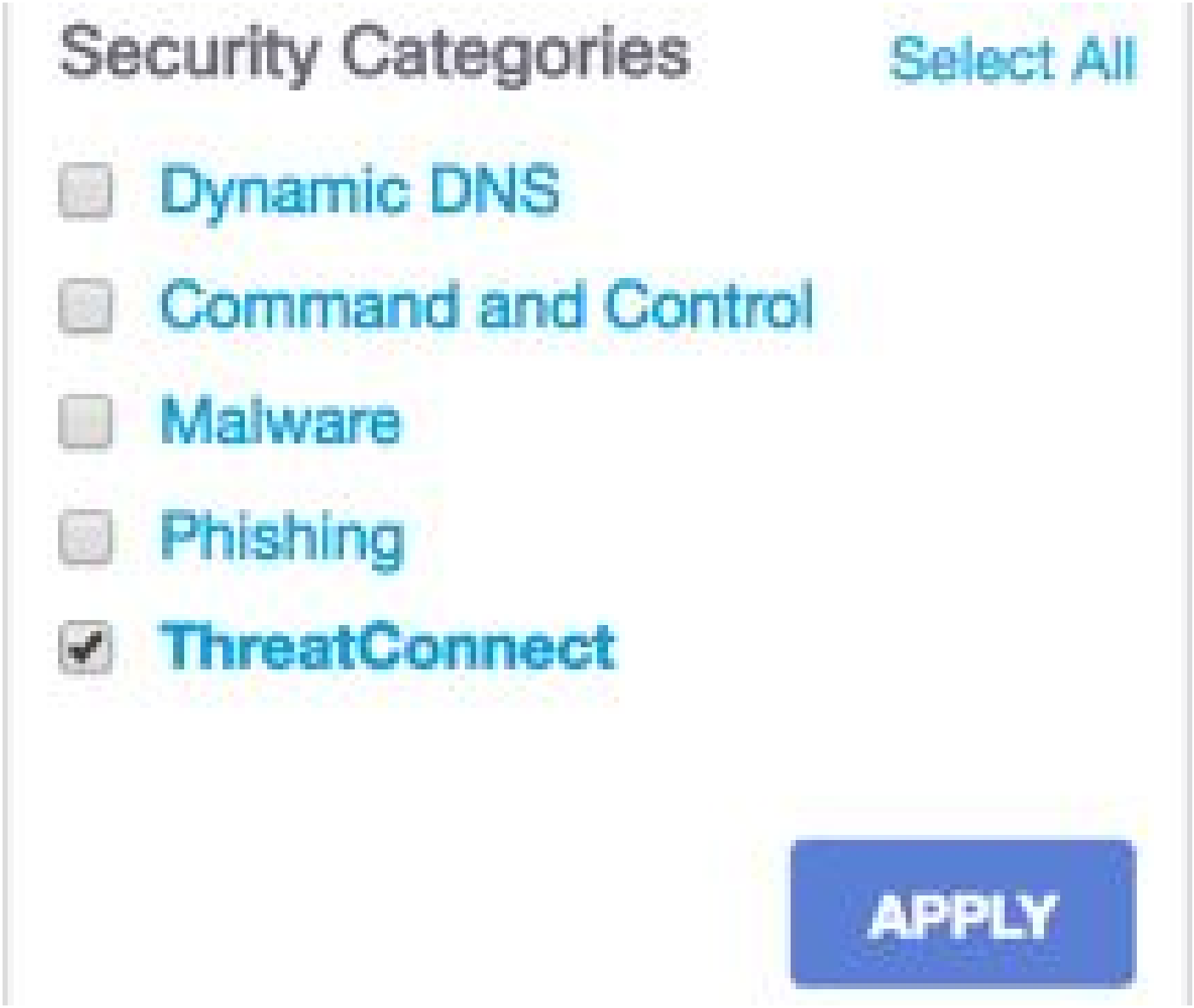
# Rapportage in Paraplu voor ThreatConnect-gebeurtenissen

## Rapporteren over ThreatConnect-beveiligingsgebeurtenissen

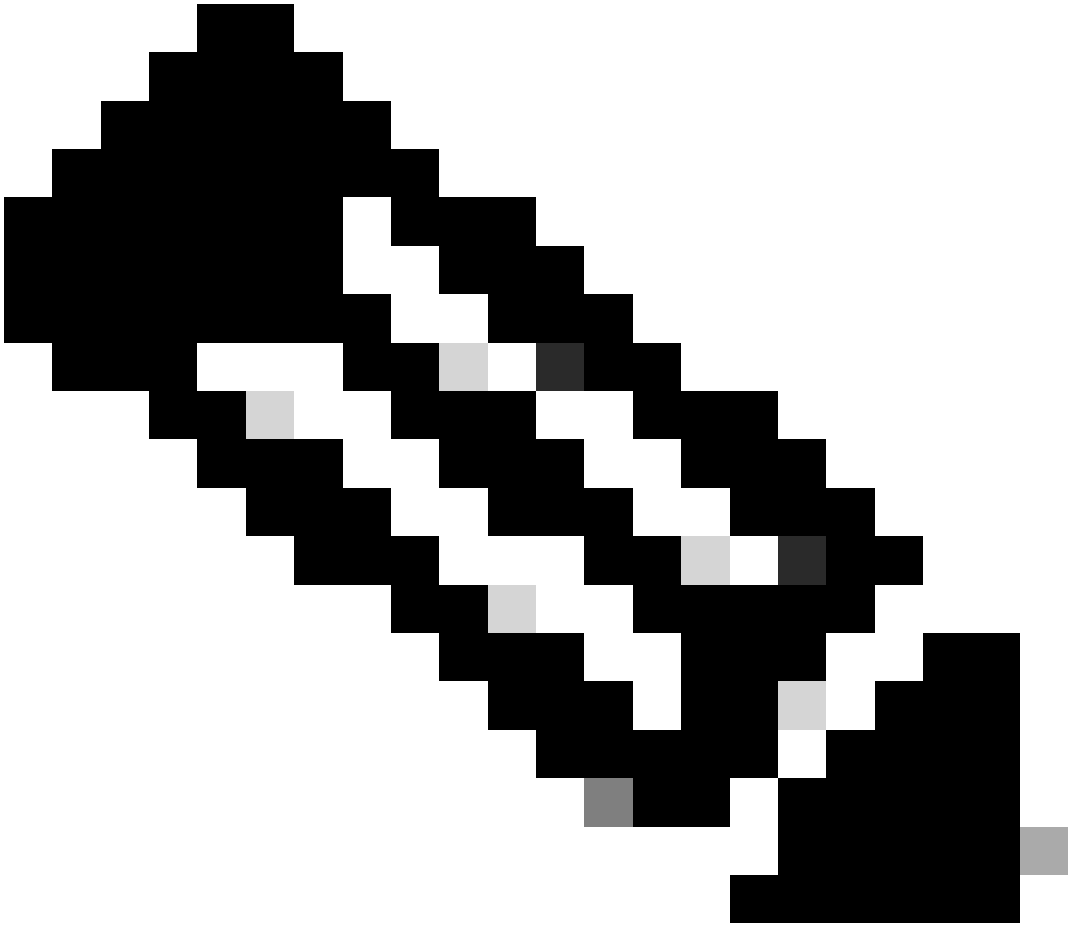
De bestemmingslijst van ThreatConnect is een van de lijsten met beveiligingscategorieën waarover u kunt rapporteren. De meeste of alle rapporten gebruiken de beveiligingscategorieën als filter. U kunt bijvoorbeeld beveiligingscategorieën filteren om alleen ThreatConnect-gerelateerde activiteiten weer te geven:

1. Navigeer naar Rapportage > Zoeken naar activiteiten.

2. Selecteer onder Beveiligingscategorieën de optie ThreatConnect om het rapport te filteren zodat alleen de beveiligingscategorie voor ThreatConnect wordt weergegeven.




115014206603



Opmerking: Als de integratie van ThreatConnect is uitgeschakeld, wordt deze niet weergegeven in het filter Beveiligingscategorieën.

3. Selecteer Toepassen.

## Rapporteren wanneer domeinen zijn toegevoegd aan de bestemmingslijst van ThreatConnect

Het auditlogboek van de beheerder bevat gebeurtenissen uit het ThreatConnect-dashboard, omdat het domeinen aan de bestemmingslijst toevoegt. Een gebruiker met de naam "ThreatConnect-account", die ook wordt gebrandmerkt met het ThreatConnect-logo, genereert de gebeurtenissen. Deze gebeurtenissen omvatten het domein dat is toegevoegd en het moment waarop het is toegevoegd.

U kunt filteren om alleen wijzigingen in ThreatConnect op te nemen door een filter toe te passen voor de gebruiker van "ThreatConnect-account".

# Omgaan met ongewenste detecties of valse positieven

## Lijsten toestaan

Hoewel onwaarschijnlijk, is het mogelijk dat domeinen die automatisch door ThreatConnect worden toegevoegd, een ongewenste blokkering kunnen veroorzaken die gebruikers zou verhinderen toegang te krijgen tot bepaalde websites. In een situatie als deze raadt Umbrella aan om de domeinnamen toe te voegen aan een lijst met machtigingen, die voorrang heeft op alle andere soorten bloklijsten, inclusief beveiligingsinstellingen.

Er zijn twee redenen waarom deze aanpak de voorkeur verdient:

- Ten eerste, in het geval dat het ThreatConnect-dashboard het domein opnieuw heeft toegevoegd nadat het is verwijderd, staat de lijst beveiligingen toe tegen problemen die verdere problemen veroorzaken.
- Bovendien toont de lijst met machtigingen een historisch record van problematische domeinen die kunnen worden gebruikt voor forensisch onderzoek of controleverslagen.

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 ThreatConnect in de blokmodus alleen wordt toegepast op een subset van uw beheerde paraplu-identiteiten (deze wordt bijvoorbeeld alleen toegepast op zwervende computers en mobiele apparaten), kunt u een specifieke lijst met machtigingen voor die identiteiten of beleidsregels maken.

U maakt als volgt een lijst met machtigingen:

1. Navigeer naar Beleid > Doellijsten en selecteer het pictogram Toevoegen (+).

2. Selecteer Toestaan en voeg uw domein toe aan de lijst.

3. Selecteer Opslaan.

Zodra de bestemmingslijst 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 ThreatConnect

Er is een pictogram Verwijderen naast elke domeinnaam in de bestemmingslijst van ThreatConnect. Als u domeinen verwijdert, kunt u de bestemmingslijst van ThreatConnect opschonen in het geval van een ongewenste detectie. Het verwijderen is echter niet permanent als het ThreatConnect-dashboard het domein opnieuw naar Umbrella verzendt.

Een domein verwijderen:

1. Ga naar Beleid > Integraties.

2. Selecteer ThreatConnect om het uit te vouwen.

3. Selecteer Zie domeinen.

4. Zoek naar de domeinnaam die u wilt verwijderen.

5. Selecteer het pictogram Verwijderen.


6. Selecteer Sluiten en selecteer Opslaan.

In het geval van een ongewenste detectie of vals-positief, raadt Umbrella aan om onmiddellijk een allow-lijst in Umbrella te maken en vervolgens het vals-positieve in het ThreatConnect-dashboard te herstellen. Later kunt u het domein verwijderen uit de bestemmingslijst van ThreatConnect.

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.