ThreatQ integreren met paraplu

Inhoud

Inleiding

Voorwaarden

- Vereisten
- Gebruikte componenten

ThreatQ en Cisco Umbrella Integration Overzicht

Integratiefunctionaliteit

Umbrella Script en API Token Generation

Hoe ThreatQ te configureren om te communiceren met een paraplu

- Gebeurtenissen observeren die in de beveiligingscategorie ThreatQ zijn toegevoegd in de controlemodus
- Bestemmingslijst bekijken
- Beveiligingsinstellingen voor een beleid bekijken

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

Rapportage in Paraplu voor ThreatQ-gebeurtenissen

- Rapporteren over ThreatQ-beveiligingsgebeurtenissen
- Rapporteren wanneer domeinen zijn toegevoegd aan de ThreatQ-bestemmingslijst

Omgaan met ongewenste detecties of valse positieven

- Lijsten toestaan
- Domeinen verwijderen uit de bestemmingslijst van ThreatQ

Inleiding

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

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Een ThreatQ-dashboard met toegang om de URL voor integraties bij te werken
- Administratieve rechten overkoepelend dashboard
- Het dashboard van de paraplu moet ThreatQ-integratie hebben ingeschakeld.

Gebruikte componenten

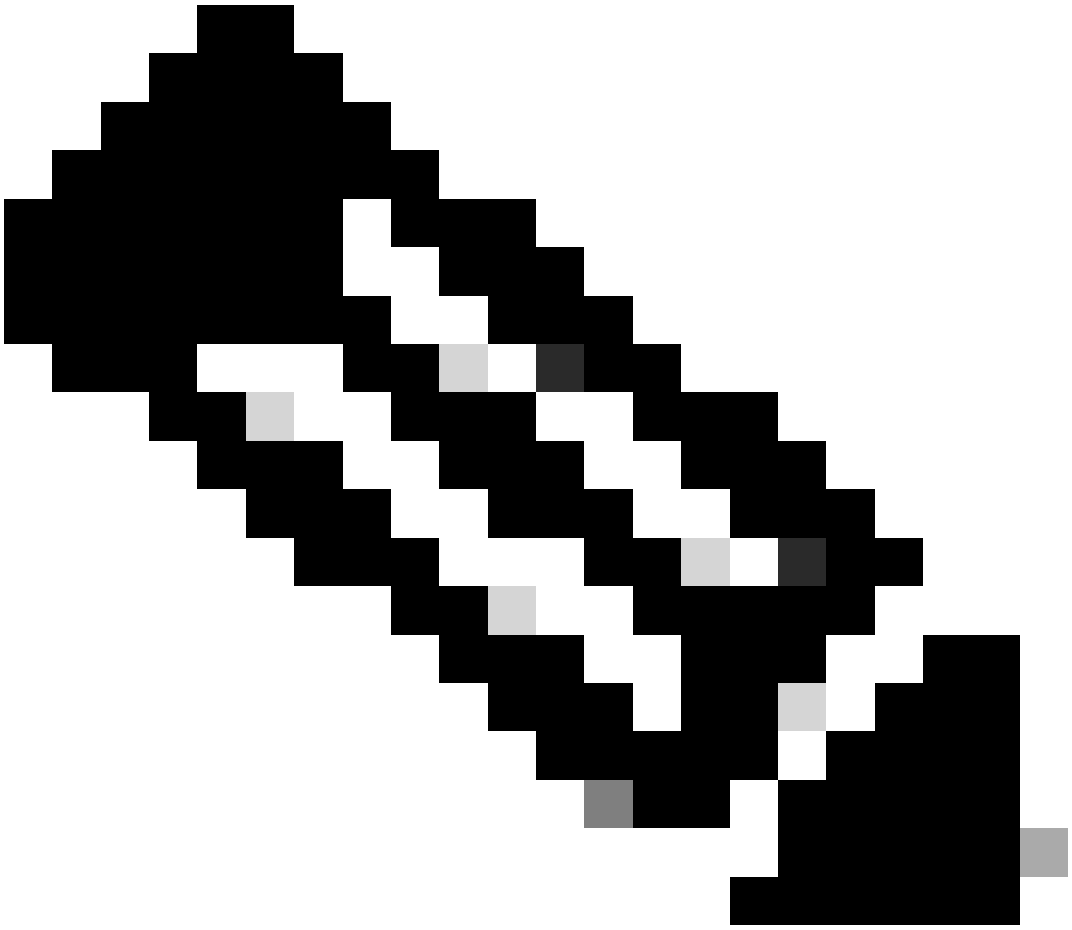
De informatie in dit document is gebaseerd op Cisco Umbrella.

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.

ThreatQ en Cisco Umbrella Integration Overzicht

Door ThreatQ 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 ThreatQ kan worden geconfigureerd om te communiceren met Umbrella, zodat beveiligingsgebeurtenissen uit de ThreatQ TIP worden geïntegreerd in beleid dat kan worden toegepast op clients die worden beschermd door Cisco Umbrella.



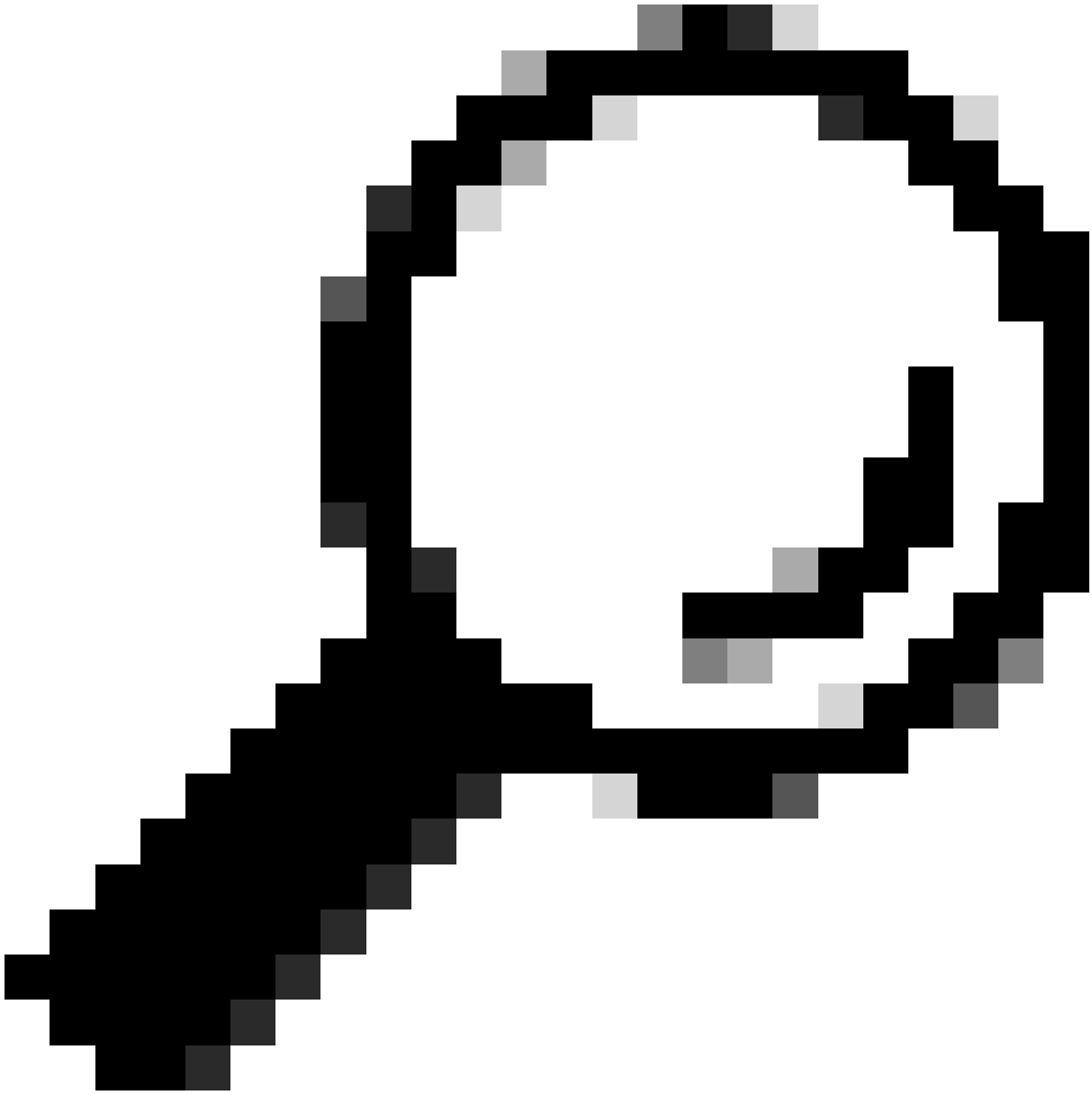
Opmerking: de ThreatQ-integratie is alleen opgenomen in bepaalde Cisco Umbrella-pakketten. Als u niet over het vereiste pakket beschikt en de ThreatQ-integratie wilt, neemt u contact op met uw Cisco Umbrella-vertegenwoordiger. Als u het juiste Cisco Umbrella-pakket hebt, maar ThreatQ niet ziet als een integratie voor uw dashboard, kunt u contact opnemen met Cisco Umbrella Support.

Integratiefunctionaliteit

Het ThreatQ-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 de informatie van ThreatQ wordt bevestigd als een bedreiging, wordt het domeinadres toegevoegd aan de ThreatQ-bestemmingslijst 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 ThreatQ.

In de toekomst parseert Umbrella automatisch ThreatQ-waarschuwingen en voegt het kwaadaardige sites toe aan de ThreatQ-bestemmingslijst. Dit breidt ThreatQ-bescherming uit naar alle externe gebruikers en apparaten en biedt een andere afdwingingslaag voor uw bedrijfsnetwerk.



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 domeinen toe te voegen die u nooit wilt hebben geblokkeerd in 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 cloudgebaseerde toepassingen waarvan u afhankelijk bent, zijn niet inbegrepen in automatische domeinvalidatie. Bijvoorbeeld "localcloudservice.com".

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

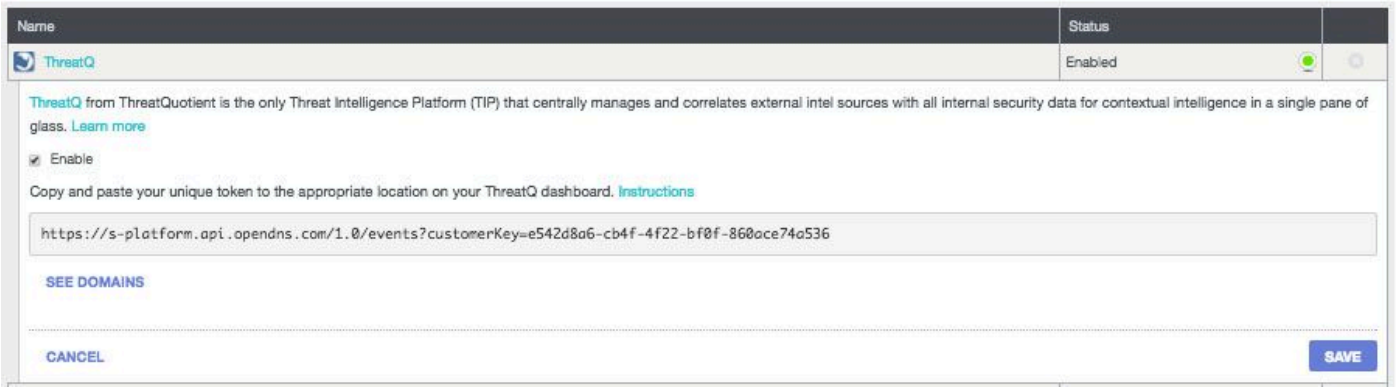
Umbrella Script en API Token Generation

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. Navigeer naar Instellingen > Integraties en selecteer ThreatQ in de tabel om deze uit te vouwen.

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



U hebt de URL later nodig wanneer u de ThreatQ configureert om gegevens naar Umbrella te verzenden, dus kopieer de URL en ga naar uw ThreatQ-dashboard.

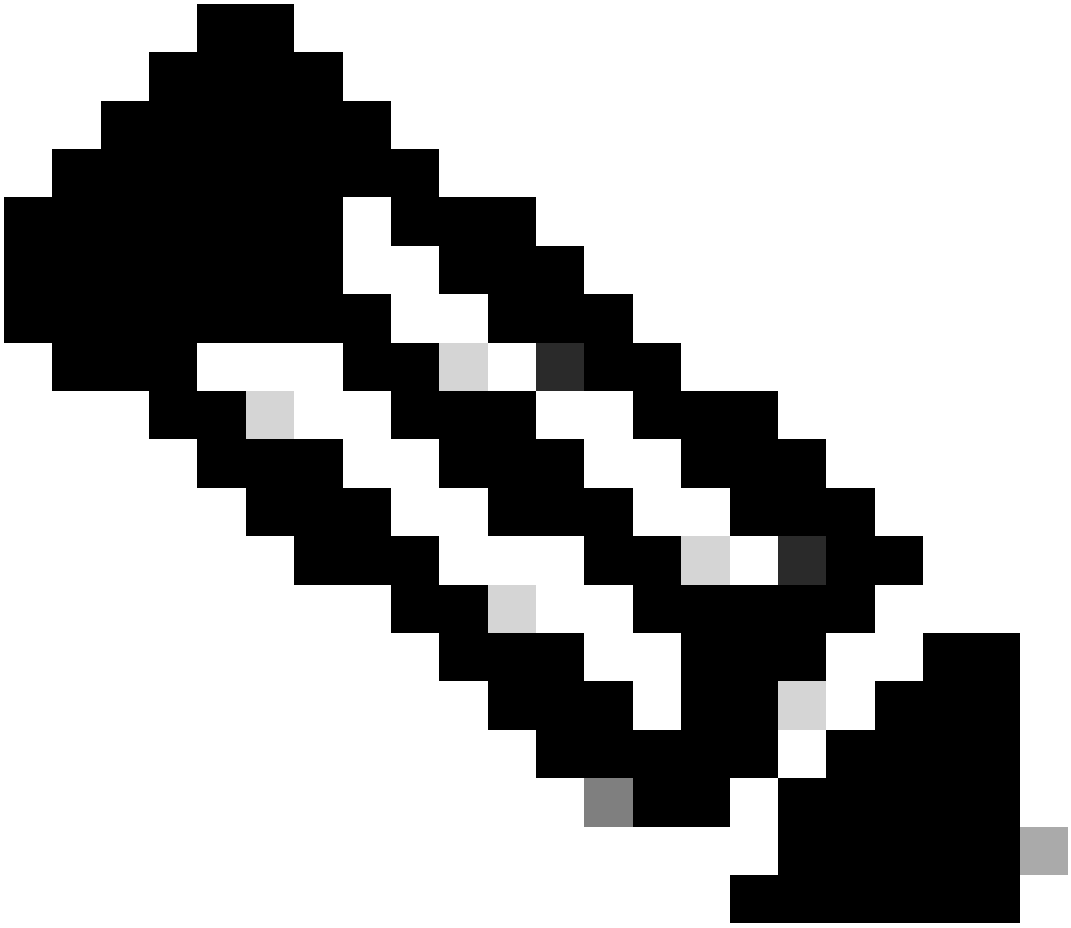
Hoe ThreatQ te configureren om te communiceren met een paraplu

Log in op uw ThreatQ-dashboard en voeg de URL toe aan het juiste gebied om verbinding te maken met Umbrella.

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

Gebeurtenissen observeren die in de beveiligingscategorie ThreatQ zijn toegevoegd in de controlemodus

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



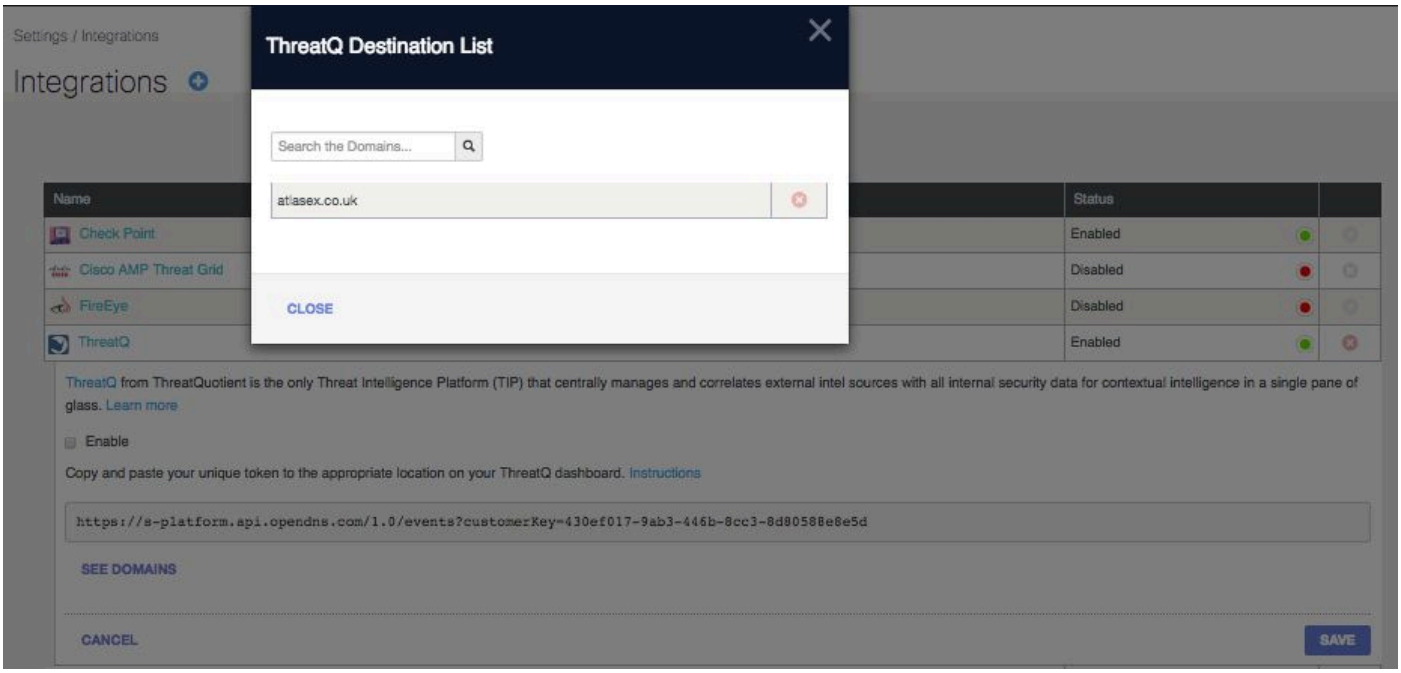
Opmerking: de controlemodus kan worden ingeschakeld zolang dit nodig is op basis van uw implementatieprofiel en netwerkconfiguratie.

Bestemmingslijst bekijken

U kunt de ThreatQ-bestemmingslijst in Umbrella op elk gewenst moment bekijken:

1. Ga naar Instellingen > Integraties.

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



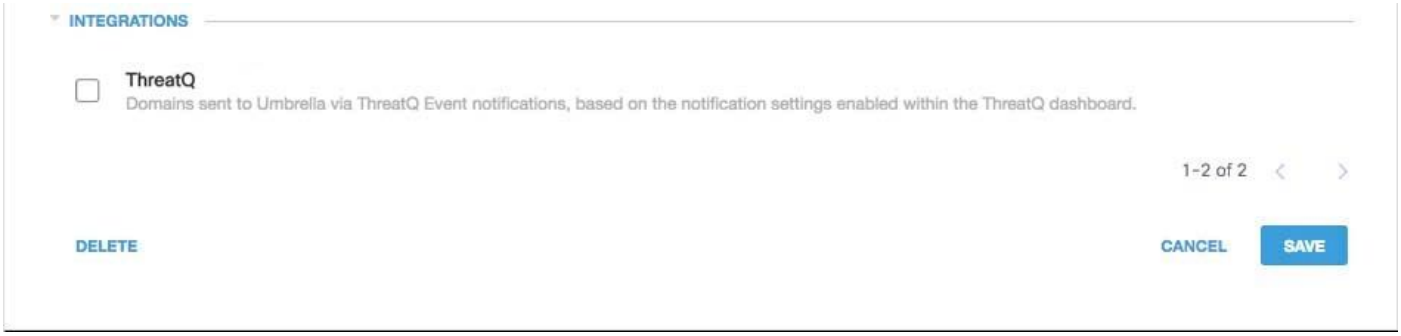
Beveiligingsinstellingen voor een beleid bekijken

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

1. Ga naar Beleid > Beveiligingsinstellingen.

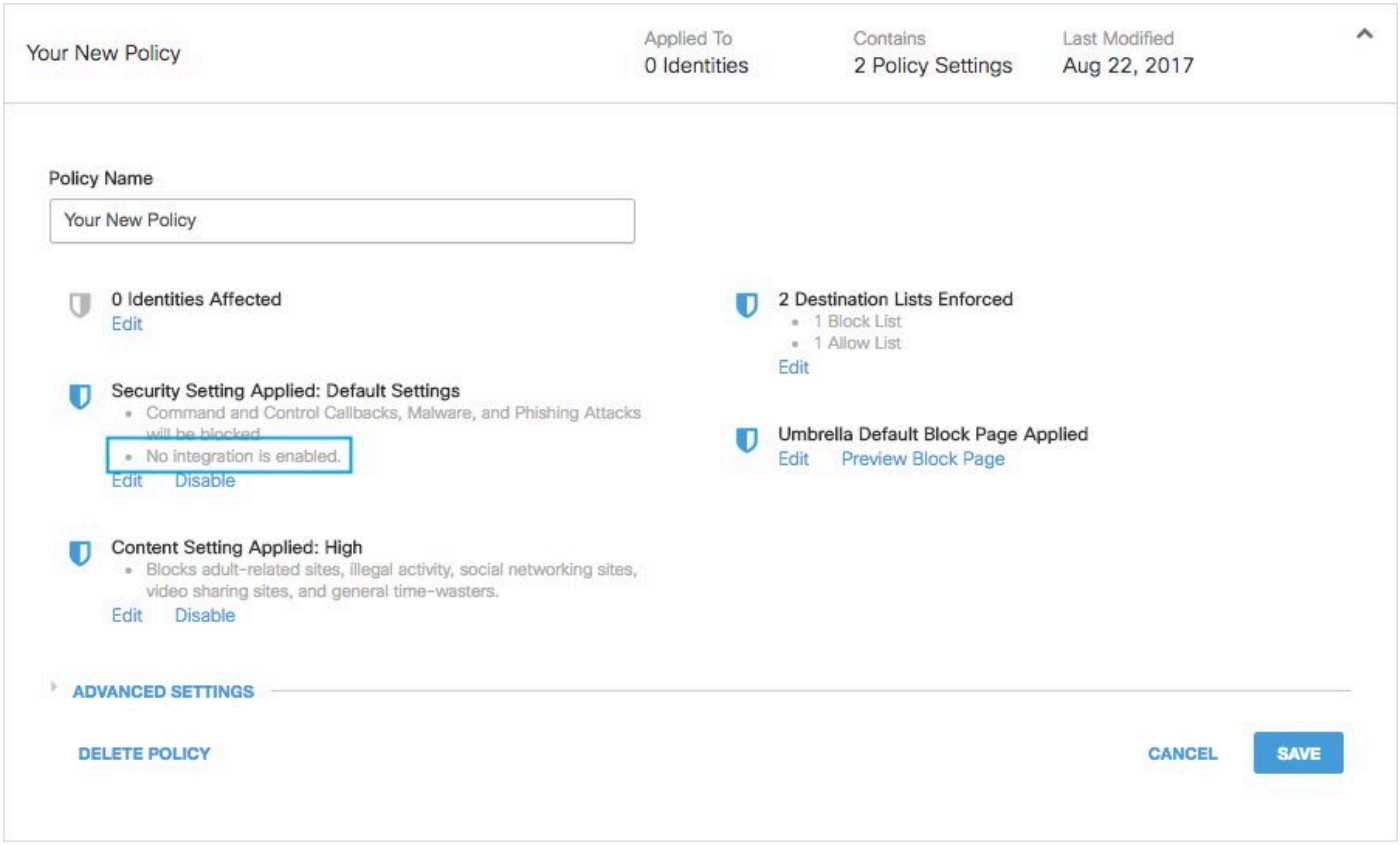
2. Selecteer een beveiligingsinstelling in de tabel om deze uit te vouwen.

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



115014040286

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



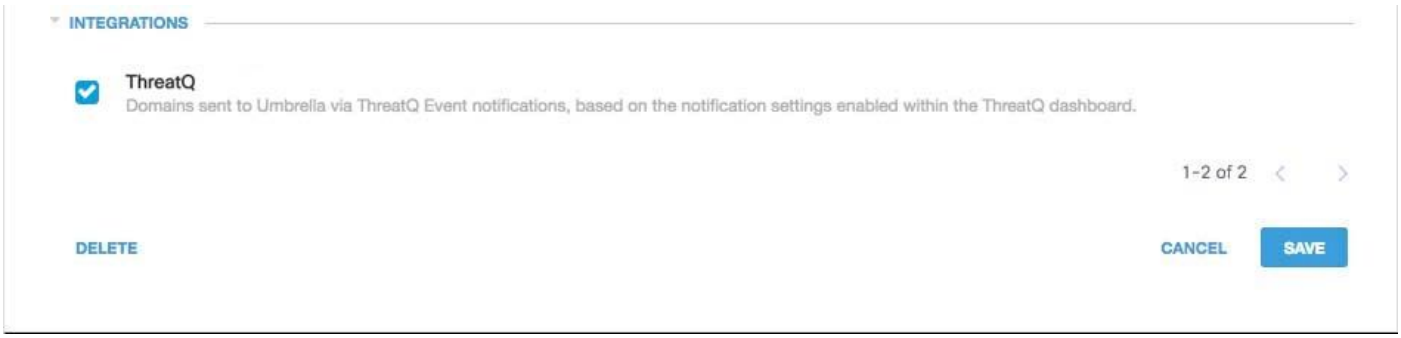
25464141748116

De beveiligingsinstellingen van ThreatQ 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, kunt u de beveiligingsinstelling voor een bestaand beleid wijzigen of een nieuw beleid maken dat hoger ligt dan uw standaardbeleid om ervoor te zorgen dat het eerst wordt gehandhaafd:

1.Navigeer naar Beleid > Beveiligingsinstellingen.

2. Selecteer onder Integraties ThreatQ en selecteer Opslaan.



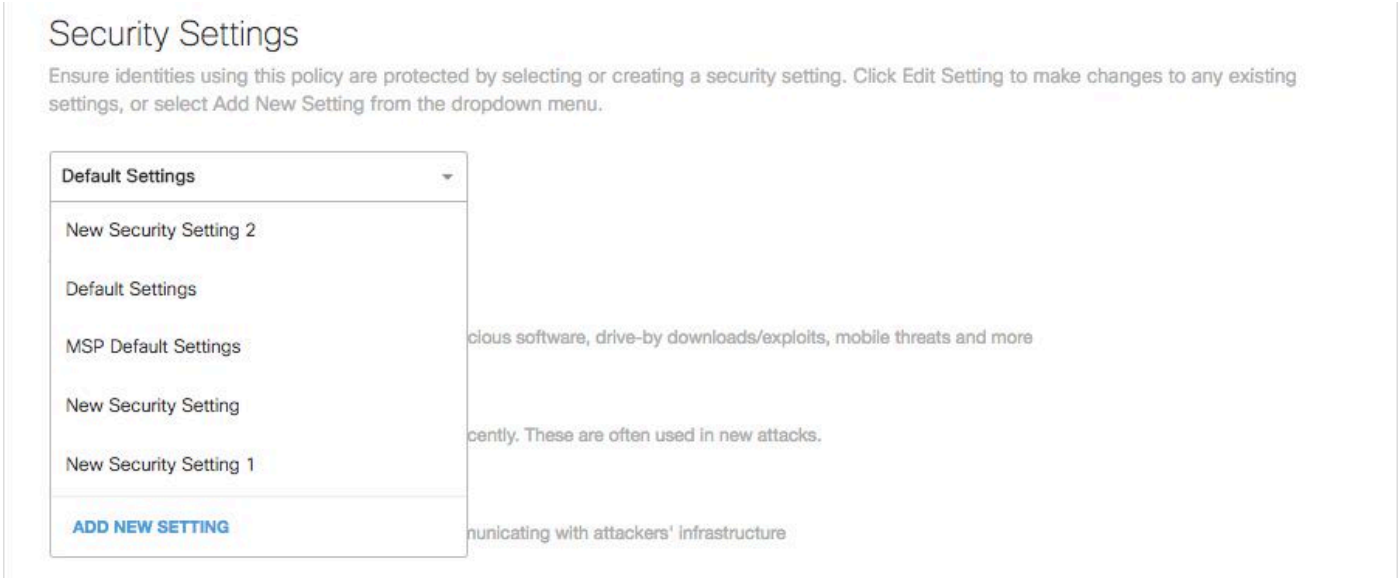
115014207403

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

1. Navigeer naar Beleid > Beleidslijst.

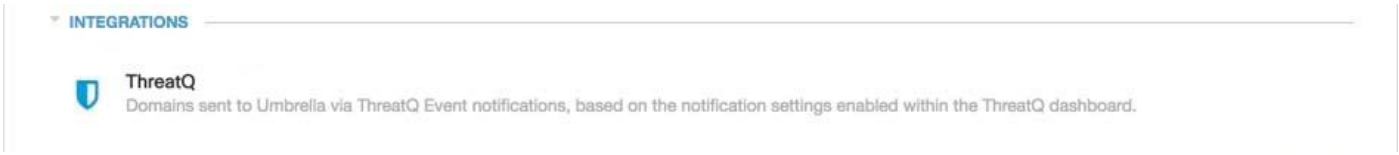
2. Vouw een beleid uit en selecteer Bewerken onder Beveiligingsinstelling toegepast.

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



25464141787668

Het schildpictogram onder Integraties wordt bijgewerkt naar blauw.



115014040506

4. Selecteer Set & Return.

ThreatQ-domeinen in de beveiligingsinstelling voor ThreatQ worden nu geblokkeerd voor identiteiten die het beleid gebruiken.

Rapportage in Paraplu voor ThreatQ-gebeurtenissen

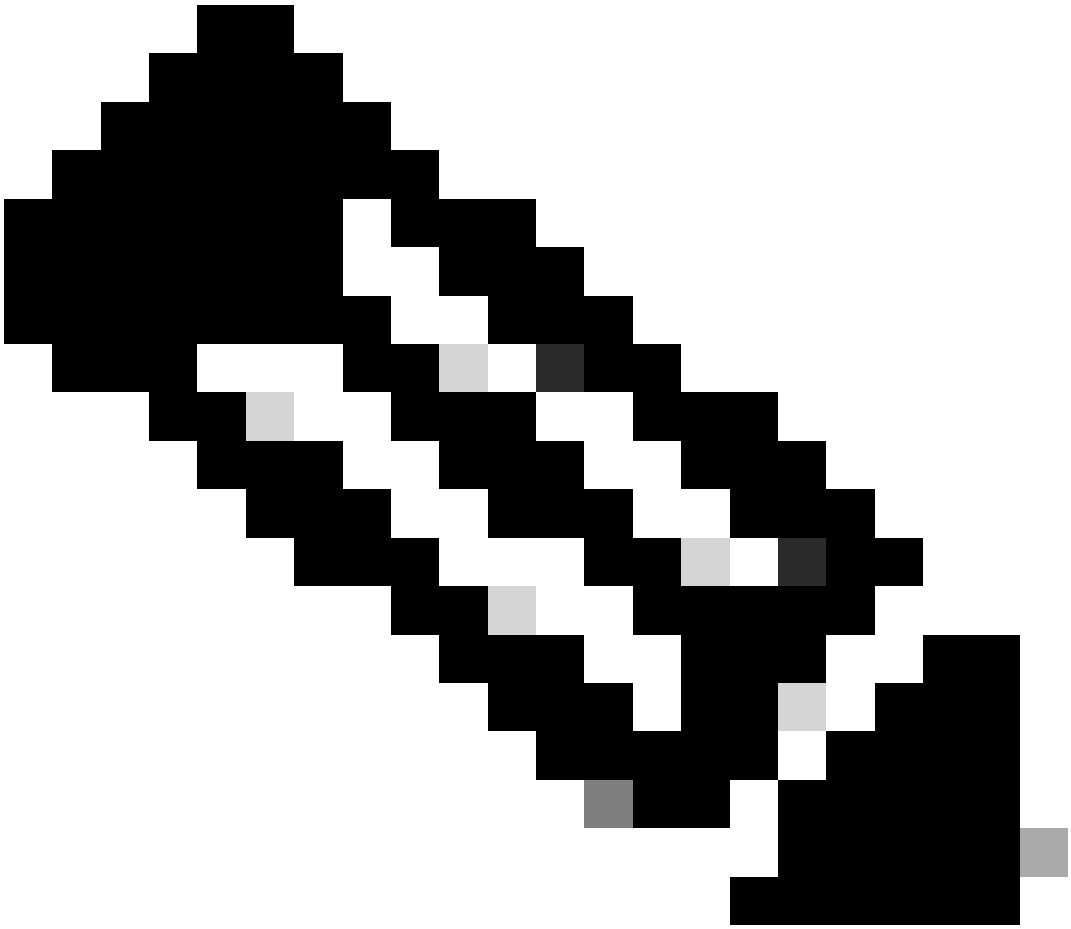
Rapporteren over ThreatQ-beveiligingsgebeurtenissen

De bestemmingslijst van ThreatQ 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 ThreatQ-gerelateerde activiteiten weer te geven.

1. Navigeer naar Rapportage > Zoeken naar activiteiten.

2. Selecteer onder Beveiligingscategorieën de optie ThreatQ om het rapport te filteren zodat

alleen de beveiligingscategorie voor ThreatQ wordt weergegeven.



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

115014207603

3. Selecteer Toepassen.

Rapporteren wanneer domeinen zijn toegevoegd aan de ThreatQ-bestemmingslijst

Het auditlogboek van de Umbrella Admin bevat gebeurtenissen uit het ThreatQ-dashboard, omdat het domeinen aan de bestemmingslijst toevoegt. Een gebruiker met de naam "ThreatQ Account", die ook wordt gebrandmerkt met het ThreatQ-logo, genereert de gebeurtenissen. Deze gebeurtenissen omvatten het domein dat is toegevoegd en het moment waarop het is toegevoegd. Het overkoepelende auditlogboek van de beheerder is te vinden op Rapportage > Controlelogboek van de beheerder.

U kunt filteren om alleen ThreatQ-wijzigingen op te nemen door een filter toe te passen voor de gebruiker van ThreatQ-accounts.

Omgaan met ongewenste detecties of valse positieven

Lijsten toestaan

Hoewel onwaarschijnlijk, is het mogelijk dat domeinen die automatisch door ThreatQ worden toegevoegd, een ongewenste blokkering kunnen veroorzaken die gebruikers kan beletten 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 ThreatQ-dashboard het domein opnieuw zou toevoegen nadat het was verwijderd, staat de lijst beveiligingen toe tegen dat wat verdere problemen veroorzaakt.
- Ten tweede toont de allow-lijst een historisch record van problematische domeinen die kunnen worden gebruikt voor forensisch onderzoek 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 ThreatQ 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 machtigingslijst maken voor die identiteiten of beleidsregels.

U maakt als volgt een lijst met machtigingen:

1. Navigeer naar Beleid > Bestemmingslijsten 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 ThreatQ

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

Een domein verwijderen:

1. Navigeer naar Instellingen > Integraties en selecteer vervolgens ThreatQ om het uit te vouwen.

2. Selecteer Zie domeinen.

3. Zoek naar de domeinnaam die u wilt verwijderen.

4. Selecteer het pictogram Verwijderen.

5. Selecteer Sluiten.

6. 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 fout-positieve in het ThreatQ-dashboard te herstellen. Later kunt u het domein verwijderen uit de ThreatQ-bestemmingslijst.

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.