Begrijpen hoe CTR koppelen aan paraplu

Inhoud

Inleiding

In dit document wordt beschreven hoe u de Cisco Threat Response (CTR)-portal kunt verbinden met Cisco Umbrella en alle vereiste vereisten.

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

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

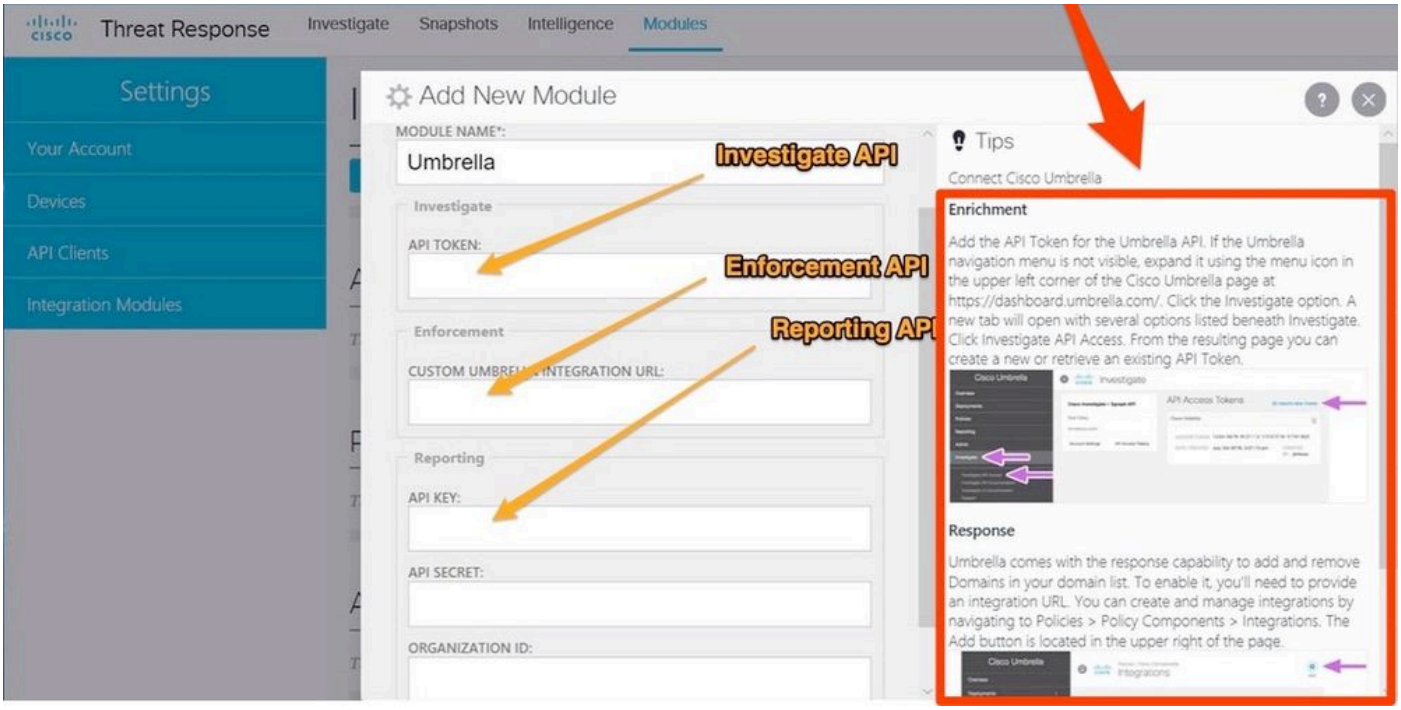
In dit artikel wordt besproken hoe u het CTR-portaal kunt verbinden met Umbrella en alle vereisten die nodig zijn om deze verbinding te maken. De CTR is onderverdeeld in drie paraplu-componenten:

- Onderzoeken (vereist abonnement op Cisco Umbrella)

- Handhaving (Vereist verhoogd Cisco Umbrella-abonnement met toegang tot Enforcement API)
- verslaggeving

De CTR-koppeling naar de paraplu configureren

Het koppelen van CTR aan Umbrella bestaat uit maximaal drie stappen, afhankelijk van uw niveau van Umbrella-abonnement. De link pagina ziet eruit als deze screenshot:



360034168072

Paraplu-rapportage koppelen aan CTR

Alle Umbrella-gebruikers hebben toegang tot de rapportage-API. Om te beginnen, heb je een API-sleutel en geheim nodig. Zie de documentatie van de Umbrella API voor informatie over het vinden van uw API-verificatiegegevens. Voer ten slotte de organisatie-ID van de overkoepelende organisatie in om naar de CTR te linken.

Vereisten

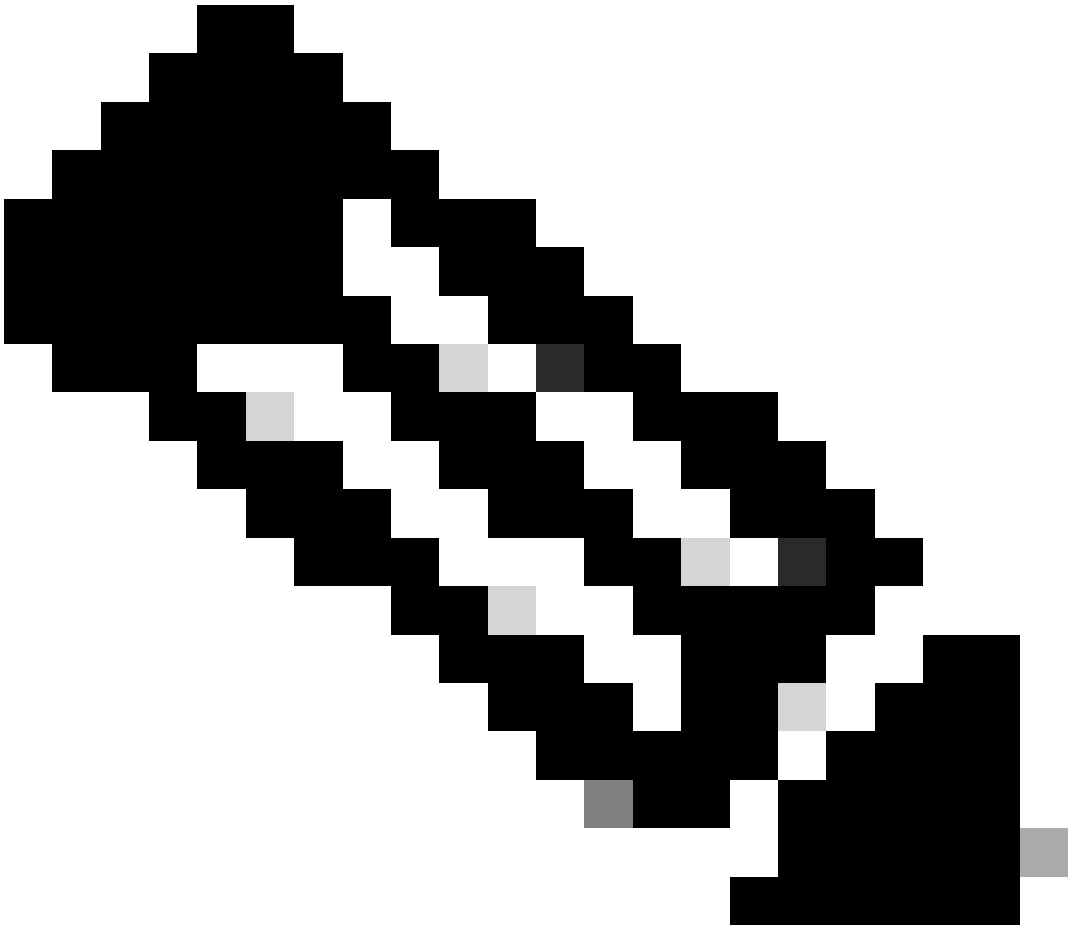
- Abonneer u op de paraplu diensten.

Umbrella Enforcement koppelen aan CTR

De Umbrella Enforcement API is een functie die het mogelijk maakt om automatisch nieuwe domeinen toe te voegen aan een handhavingslijst voor beveiliging. Voor meer informatie, bekijk de Umbrella documentatie.

Vereisten

- Abonneer u op Umbrella Services met toegang tot de Enforcement API in het dashboard.



> 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.

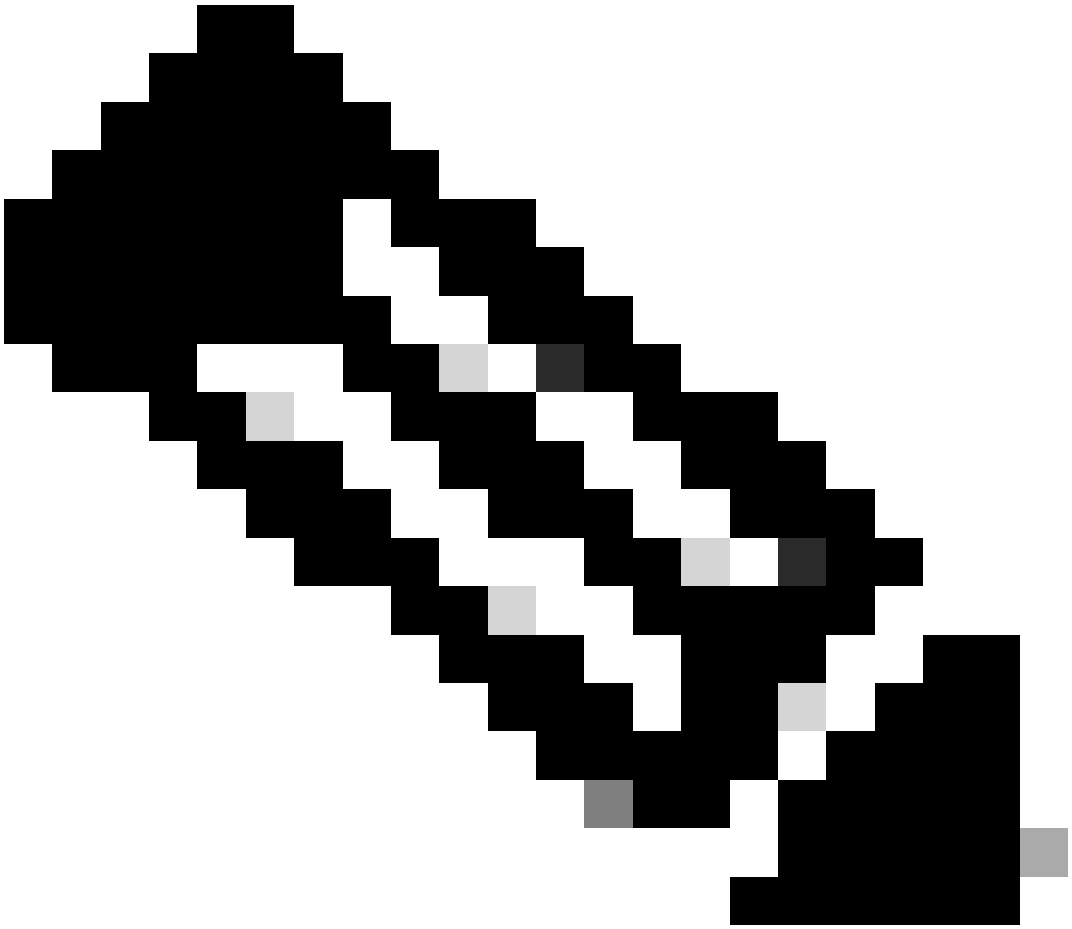
Paraplu koppelen aan CTR

De Umbrella Investigate API is een functie waarmee vragen kunnen worden gesteld aan het Cisco Umbrella Investigate-systeem buiten het webportaal Investigate. De toegang tot de API is beperkt. Voor meer informatie, bekijk de Umbrella documentatie.

Vereisten

- Abonneer u op Cisco Umbrella Investigate (https://investigate.umbrella.com).
  - Het pakket of de add-on voor de Investigate API moet actief zijn.
  - Sommige rechten maken een laag aantal zoekopdrachten mogelijk. CTR kan

functioneren tot de querylimiet is bereikt.



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.

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.