Cisco SecureX-software integreren met Cisco Umbrella

Inhoud

Inleiding

Dit document beschrijft het proces om de Umbrella-integratie te configureren en te verifiëren met SecureX met de 3 beschikbare API's.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Cisco-paraplu
- Cisco Secure-X
- Cisco Threat Response

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Umbrella-account met DNS-voordeellicentie
- Secure X

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 de potentiële impact van elke opdracht begrijpen.

Achtergrondinformatie

Om deze integratie volledig te kunnen configureren met al zijn functionaliteiten, hebt u toegang nodig tot deze 3 API's

- Rapportage API (inbegrepen in alle licenties)
- Enforcement API
- API onderzoeken

Om de Umbrella integratie te configureren moet u eerst wat informatie verzamelen van uw Umbrella instanties en vervolgens het formulier Nieuwe Umbrella Module toevoegen invullen.

Configureren

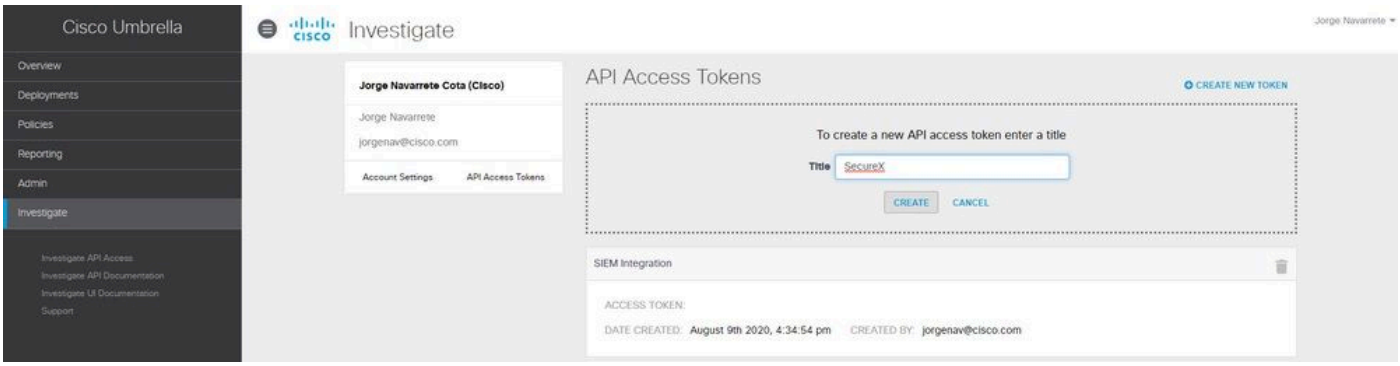
Module maken

1. Meld u aan bij uw Secure X-account. Als u nog geen account hebt, kunt u een account maken met Cisco Secure-aanmelding.
2. Ga naar Integraties > Nieuwe module toevoegen. In de pagina Beschikbare integraties scrolt u omlaag naar de optie Umbrella en klikt u op Nieuwe module toevoegen.

Gebruik deze stappen om de benodigde informatie van uw Umbrella-account te verzamelen om in te dienen in het formulier Nieuwe Umbrella Module toevoegen.

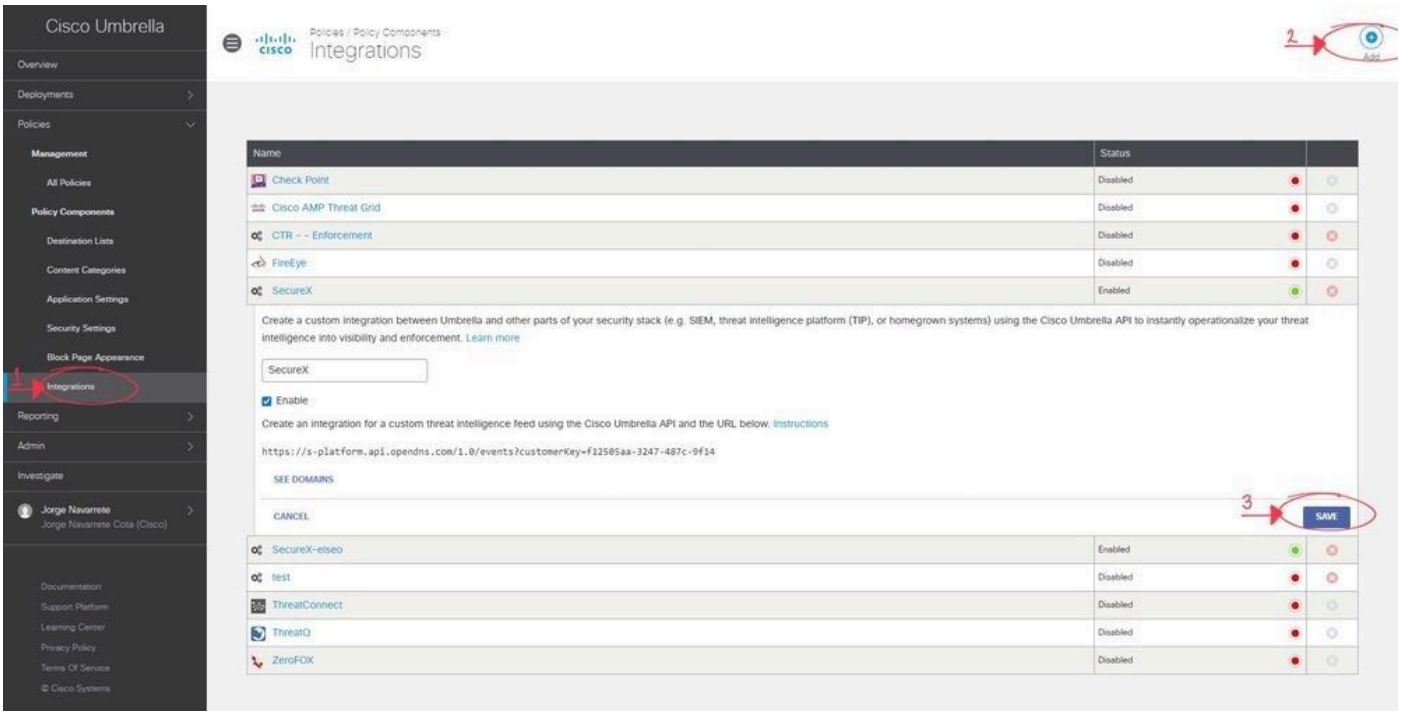
API onderzoeken

1. In Umbrella, navigeer om te onderzoeken > Onderzoek API Toegang, klik creëren Nieuw Token en ingaan een titel voor het token, en klik dan opnieuw creëren Nieuw Token.
2. Kopieert de waarde van Access Token naar het veld API Token op het formulier Nieuwe Umbrella Module.



Enforcement API

1. In Umbrella, navigeer naar Beleid > Beleidscomponenten > Integraties, klik op Toevoegen en voer een naam in en klik op Maken.
2. Klik op de nieuwe integratienaam-link, controleer het selectievakje Inschakelen enOpslaan.
3. Klik op de integratienaam om de integratie-URL weer te geven. Kopieer de integratie-URL naar het veld Aangepaste Umbrella Integratie-URL op het formulier Nieuwe Umbrella-module toevoegen.



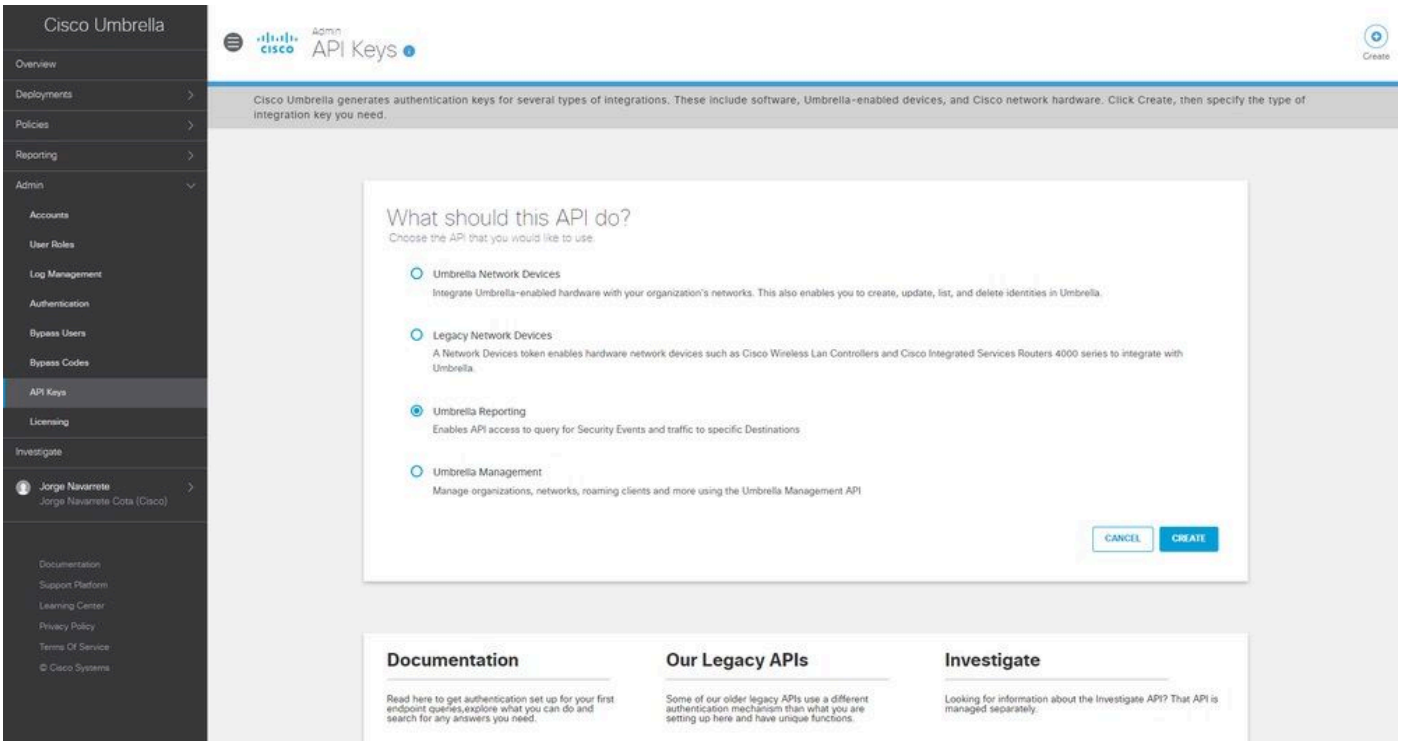
Opmerking: om de Umbrella Enforcement API te integreren, moet u een admin zijn in een Umbrella standalone org of child org in plaats van een admin van een Umbrella console.

API voor rapportage

1. In Umbrella, navigeer aan Admin > API Sleutels en klik creëren.
2. Onder Wat moet deze API doen?, klik op de radioknop Umbrella Reporting en klik vervolgens op Maken.

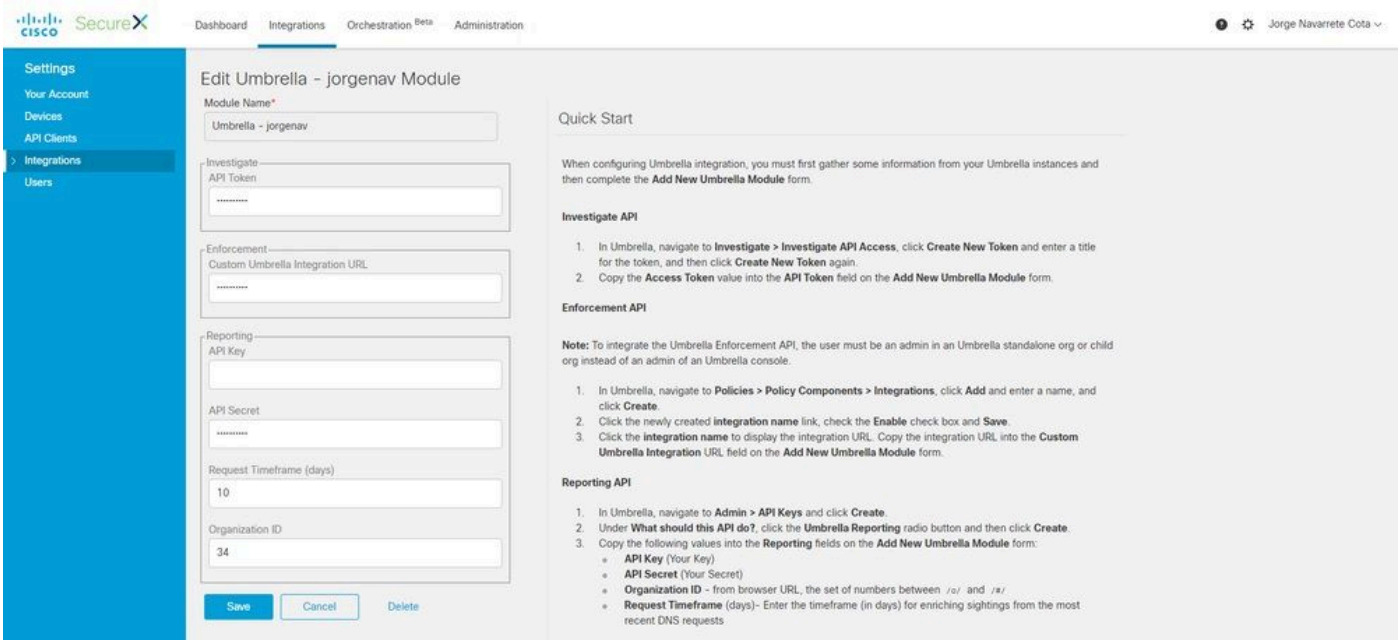
3. Kopieert de volgende waarden naar de velden Rapportage op het formulier Nieuwe Umbrella-module toevoegen:

    - API-sleutel (uw sleutel)
    - API Secret (uw geheim)
    - Organisatie-ID - van browser URL, de reeks getallen tussen`/o/`en`/#/`
    - Tijdlijn aanvragen (dagen) - Voer het tijdpad (in dagen) in voor het verrijken van waarnemingen uit de meest recente DNS-verzoeken



Module opslaan

1. Vul de API-informatie in uw Umbrella Module in en klik op Opslaan.

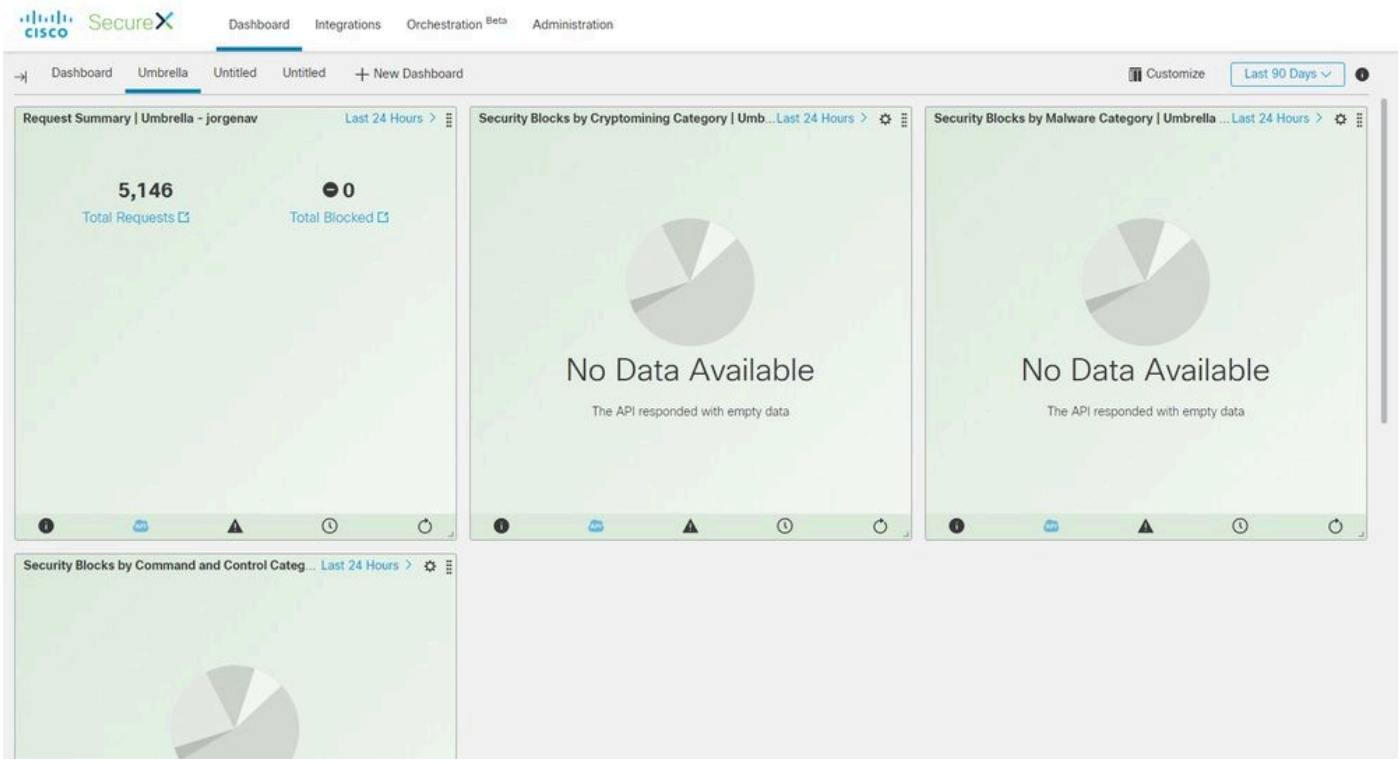


SecureX-dashboard maken

1. Zodra u uw module hebt toegevoegd, kunt u navigeren naar Secure X en een nieuw Dashboard maken.

2. Selecteer onder de beschikbare Dashboards uw Umbrella module en voeg de Categorieën toe die u graag wilt zien.

3. Klik op Opslaan en zie uw informatie ingevuld via de API.



Verifiëren

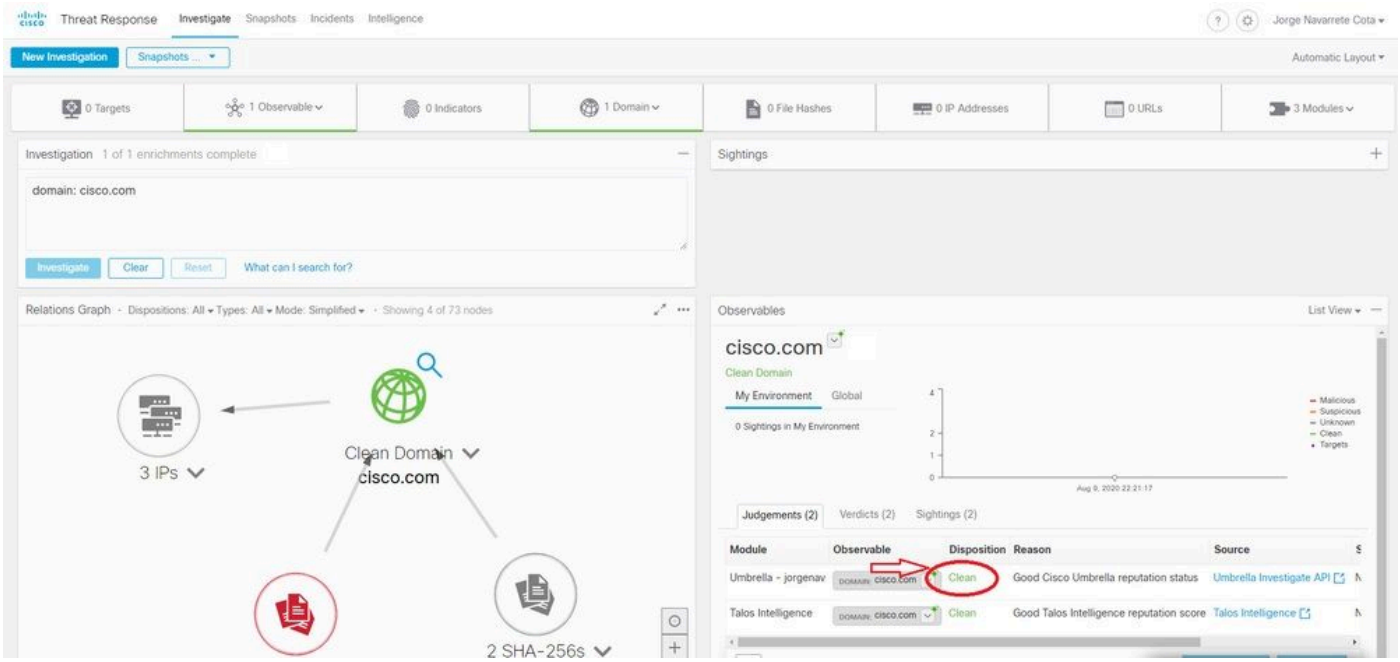
Gebruik deze sectie om te controleren of uw configuratie goed werkt.

onderzoeken

De Investigate API, stelt u in staat om een feed toe te voegen aan een CTR-onderzoek, om de beschikbaarheid van een domein te zien en het onderzoek te verrijken met andere modules.

1. Om deze integratie te verifiëren, stelt u een nieuw onderzoek in naar Cisco Threat Response. Een door Umbrella verstrekte Disposition kan worden gevonden met een zoekopdracht naar een bekend domein, zoals cisco.com.

2. Als u onder het domein in de Relaties Grafiek klikt, kunt u ook draaien van daar naar het Investigate Dashboard in Umbrella.

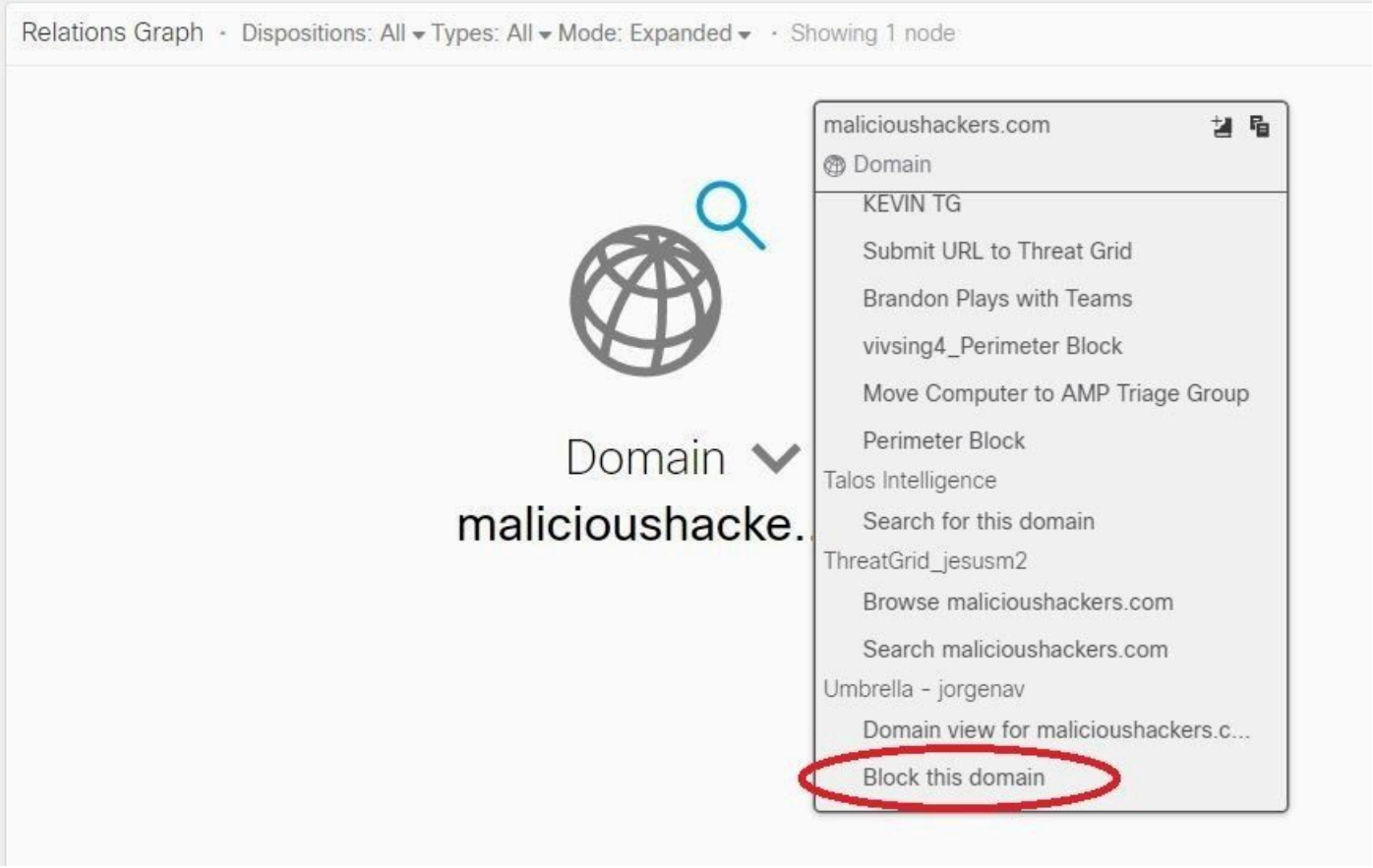


Handhaving

Met de Enforcement API kunt u een domein direct uit een onderzoek blokkeren of deblokkeren.

1. Om te verifiëren dat de API werkt, kunt u een domein blokkeren dat in een onderzoek wordt gezien en dat het domein toevoegt aan de lijst van beleidsblokken in Umbrella.

2. Ga naar Beleid > Beleidscomponenten > Integraties om te controleren of de URL is toegevoegd aan de bloklijst. Selecteer uw SecureX-integratie en klik op Domeinen bekijken. Een venster toont de toegevoegde domeinen van CTR.



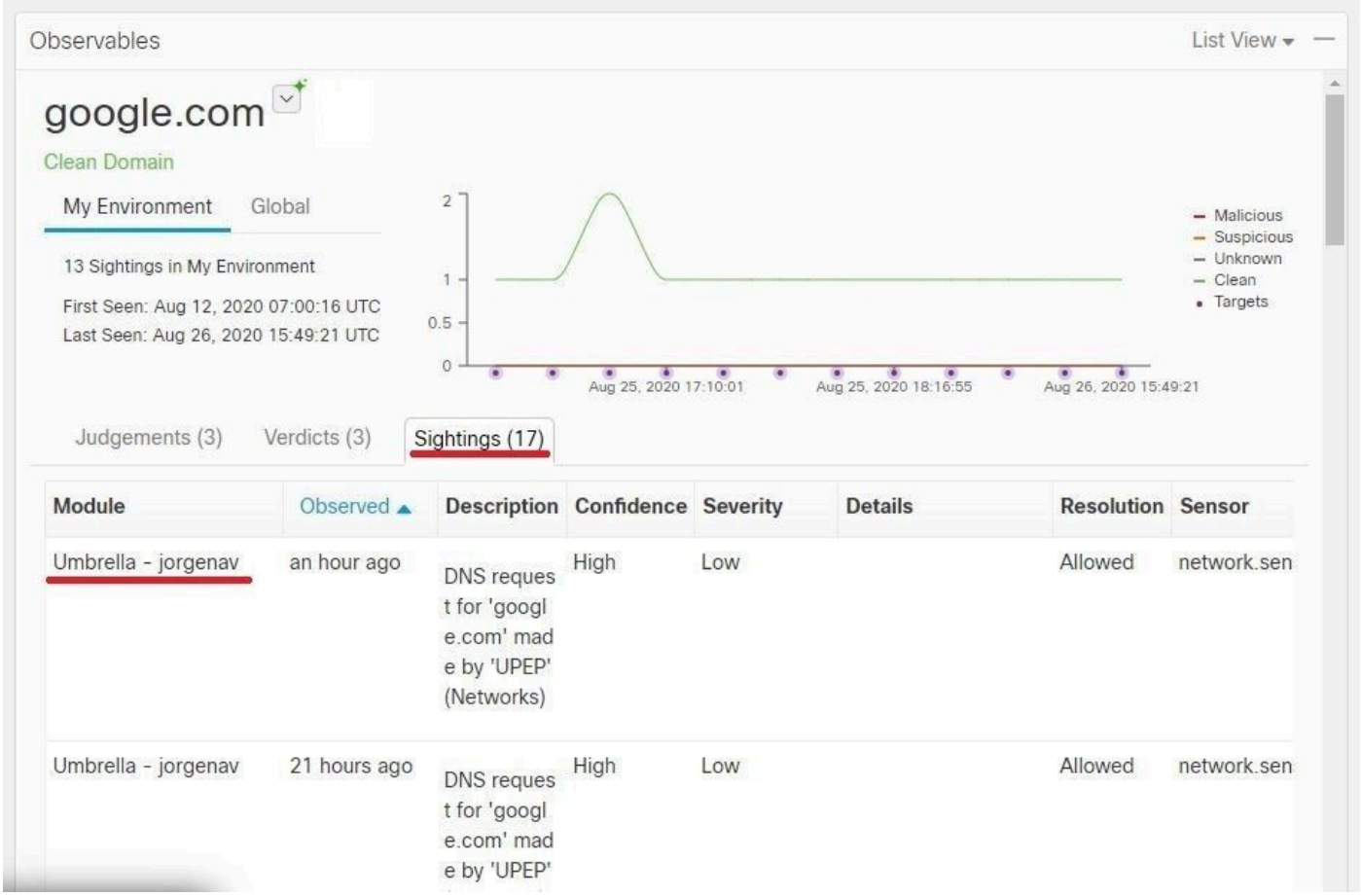
3. Als de domeinen niet worden geblokkeerd, navigeer dan op uw Umbrella dashboard naar Beleid > Beleidscomponenten > Beveiligingsinstellingen. Controleer onder Integraties of u de gewenste lijst hebt toegepast.

Rapportage

Met de API voor rapportage kunt u de informatie van uw Umbrella-implementaties zien binnen SecureX.

U kunt de integratie verifiëren met een onderzoek van een domein waarvan u weet dat het in uw omgeving in CTR is gezien.

In het onderzoek van de CTR, wordt de lijst van computers die een bepaald domein hebben betreden weergegeven onder Sightings.



Video

U vindt de configuratie-informatie in dit artikel in deze video.

Gerelateerde informatie

- [Technische ondersteuning en documentatie – Cisco Systems]

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.