SecureX met Orbital geavanceerde zoekintegratiegids

Inhoud

Inleiding

Dit document beschrijft het proces dat nodig is om Cisco SecureX te integreren en te verifiëren met Cisco Orbital Advanced Search.

Bijgedragen door Yeraldin Sanchez en Uriel Torres, bewerkt door Jorge Navarrete, Cisco TAC Engineers.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Cisco Advanced Malware Protection voor endpoints - essentieel met licentie voor orbitaal, voordeel of premier
- Cisco Orbitaal geavanceerd zoeken
- Basisnavigatie in de SecureX-console
- Optionele virtualisatie van afbeeldingen

Gebruikte componenten

- AMP voor endpoints, versie 5.4.20200804
- AMP voor endpoints - beheerderaccount
- Orbital geavanceerde zoekconsole versie 1.7
- SecureX-console versie 1.54
- SecureX-beheerderaccount

- Microsoft Edge versie 8.0.52.52

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.

Achtergrondinformatie

Orbital is een geavanceerde voorziening in Cisco Advanced Malware Protection voor endpoints, die is ontworpen om veiligheidsonderzoek en de jacht op bedreigingen eenvoudig te maken. Het biedt een implementatie van krachtige Osquery-technologie op elk van uw AMP-endpoints. Orbital stelt u in staat om aangepaste zoekopdrachten te maken om te kijken over uw netwerk voor informatie van belang, maar ook komt met meer dan honderd vooraf ingeblikte vragen, die u in staat stellen om snel complexe vragen te stellen op alle of alle eindpunten.

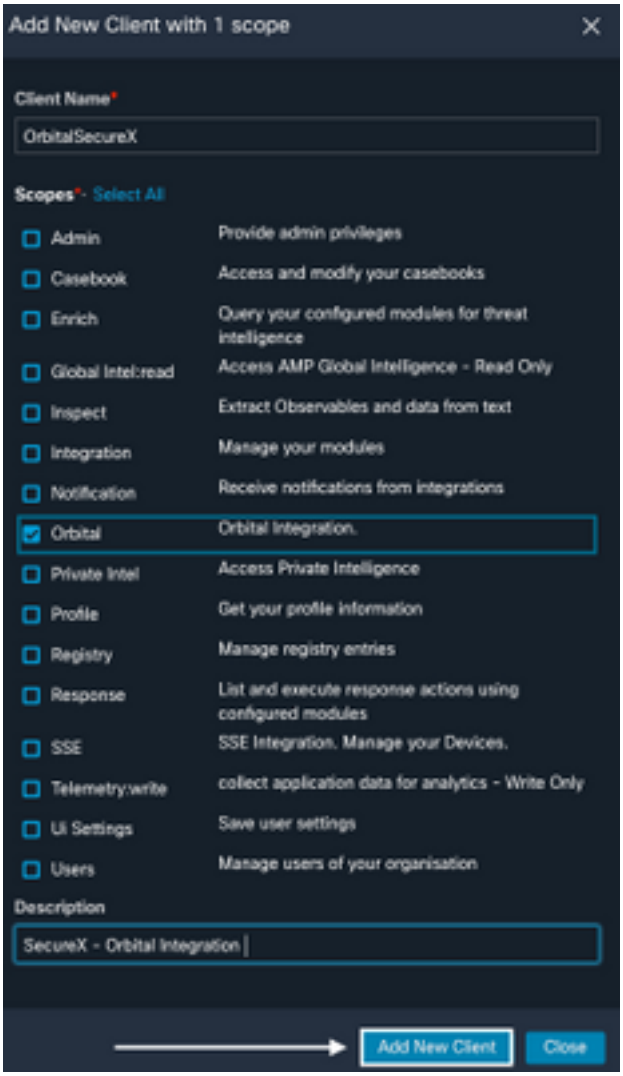
De Orbitummodule heeft 4 tegels die u kunt toevoegen aan een SecureX-dashboard.

- **Organisation Query and Results Stats:**Een verzameling metriek die organisatievragen en resultaten beschrijft
- **Gebruikerscatalogus Statistieken:** Een reeks metriek die de meest gebruikte catalogusvragen voor deze gebruiker beschrijft
- **Organisatiecatalogus Stats:** Een reeks metriek die de meest gebruikte catalogusvragen voor deze organisatie beschrijft
- **User Query en Results Stats:** Een verzameling metriek die gebruikersvragen en -resultaten beschrijft

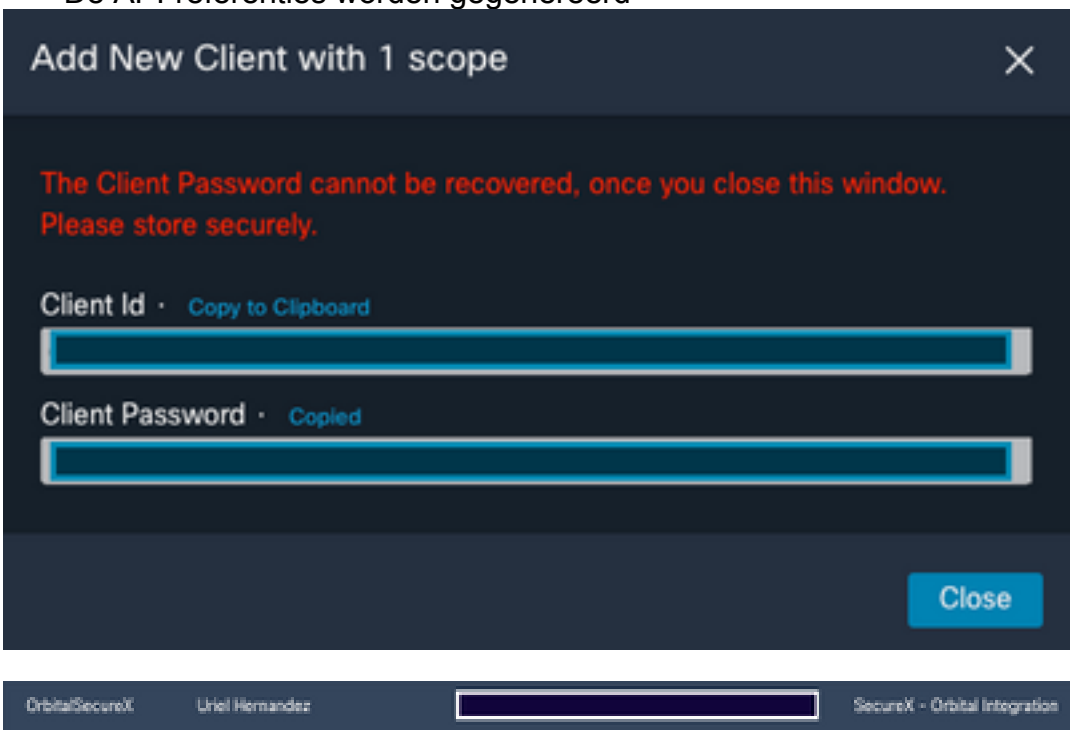
Configureren

De API-referenties genereren in de SecureX-console

- Inloggen op SecureX
- Navigeren naar **integraties** > **Instellingen** > **API-clients**
- Klik op **Generate API-client**
- Geef de client een naam, controleer **Orbital,** beschrijf de API en klik op **Nieuwe client toevoegen**



- De API-referenties worden gegenereerd



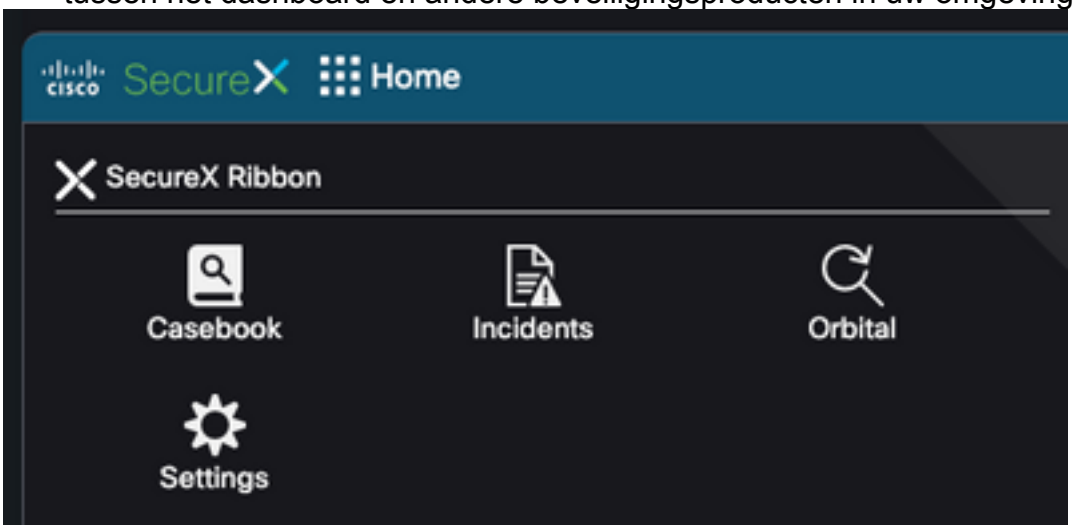
Opmerking: Deze informatie is alleen beschikbaar in dit venster. Sla uw referenties op in een reservebestand.

SecureX-lint in de AMP-console inschakelen

SecureX is zowel een gecentraliseerde console als een gedistribueerde reeks functies die zichtbaarheid verenigen, automatisering mogelijk maken, incidentresponsworkflows versnellen en bedreigingsjacht verbeteren. Deze gedistribueerde mogelijkheden worden gepresenteerd in de vorm van toepassingen (apps) en tools in het SecureX-lint, het SecureX-lint kan worden ingeschakeld in de Orbitale console.

- Inloggen op orbitale console
- Op de orbitale console
- Navigeren naar **<Yout User> > Instellingen**
- Het SecureX-lint inschakelen

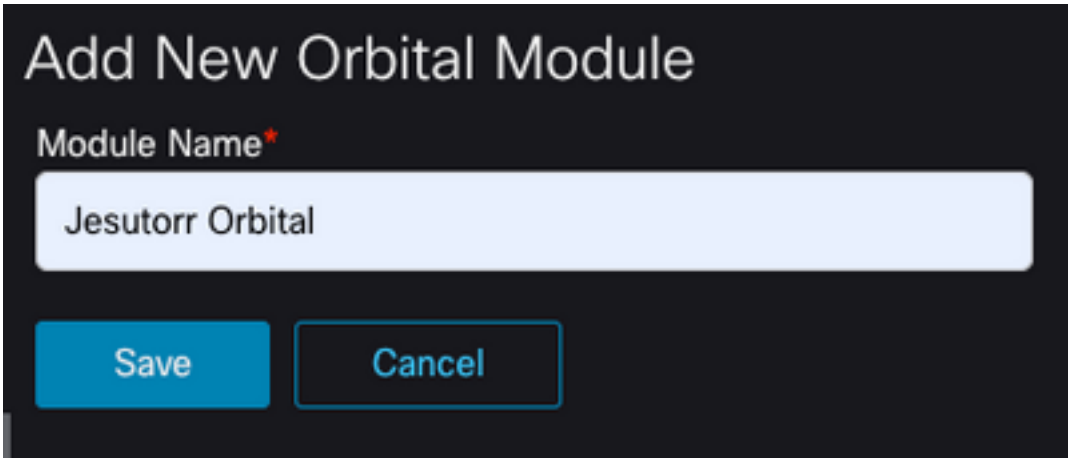
- Het lint bevindt zich in het onderste deel van de pagina en blijft bestaan wanneer u zich tussen het dashboard en andere beveiligingsproducten in uw omgeving beweegt



De orbitummodule integreren in SecureX

Orbital kan informatie verrijken die wordt gepresenteerd in de Threat Response-grafiek door als u in Orbital om aanvullende informatie te vragen en te verzamelen over uw host, IP, IP4, IP6, MAC, en OS, etc. De Orbital-app is beschikbaar op het SecureX-lint en stelt u in staat om een live query uit te voeren. U kunt ook gegevens en recente vragen in het rechter deelvenster weergeven.

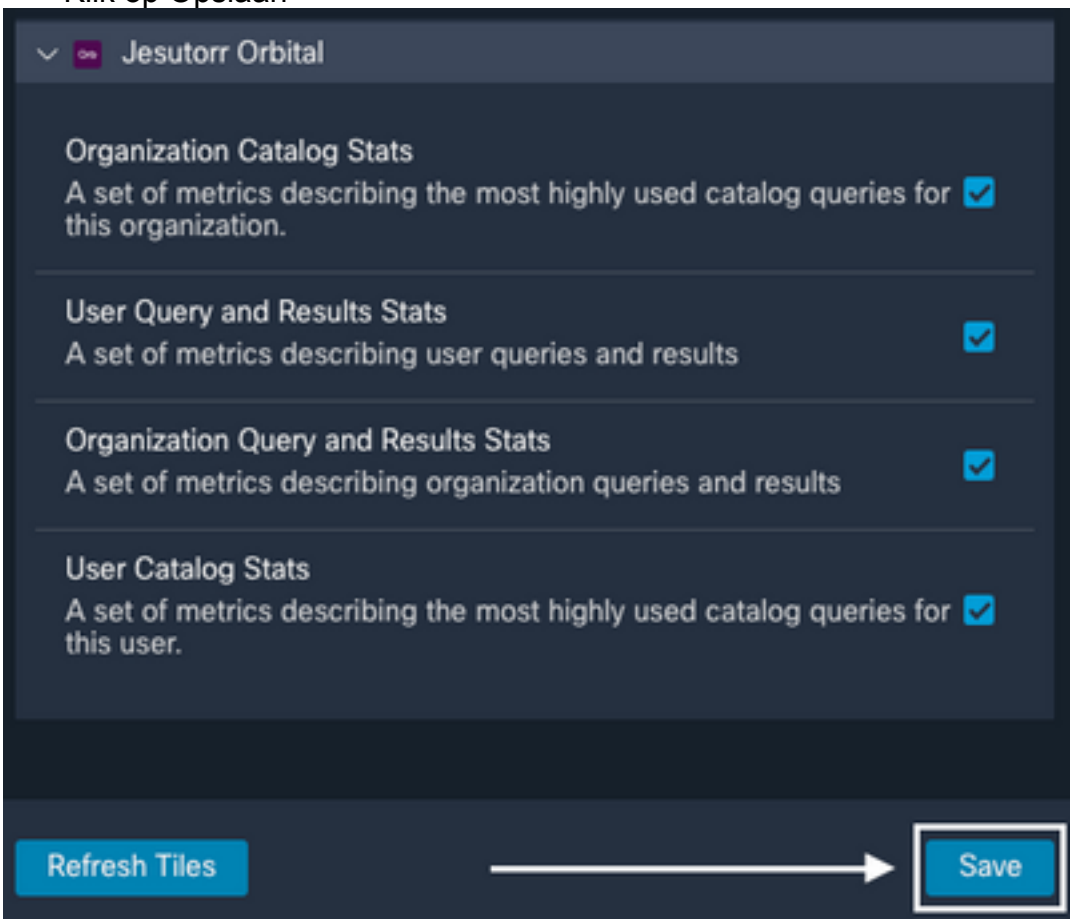
- Op SecureX
- Navigeren naar **integraties > Nieuwe module toevoegen**
- Selecteer Orbital en klik op **Add New Module**
- Geef de module een naam en klik op **Opslaan**



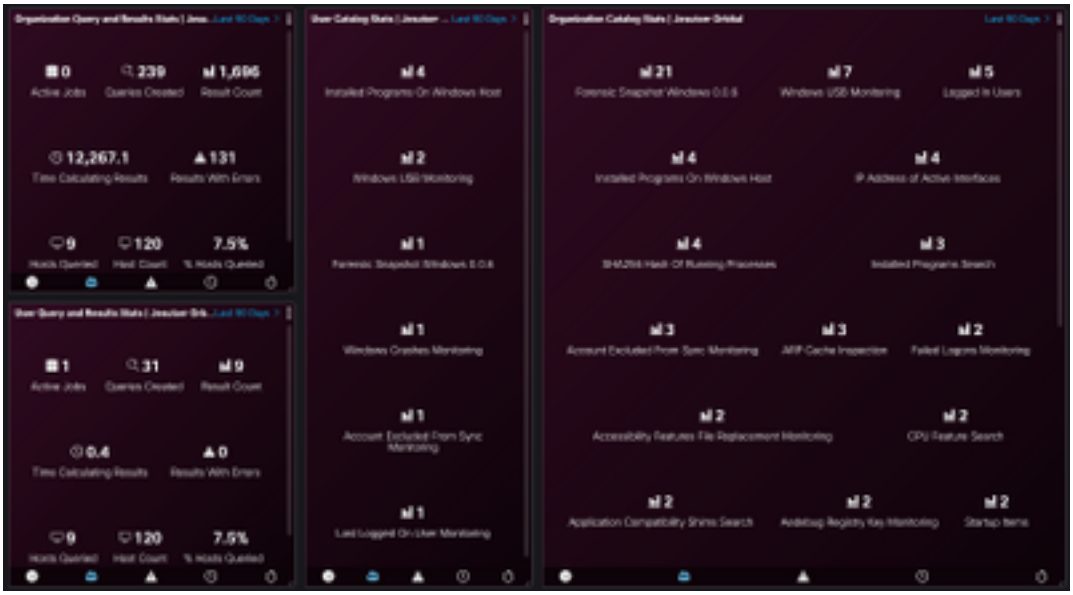
Verifiëren

Controleer of de informatie van de Orbital Advanced Se Console wordt weergegeven in het SecureX Dashboard.

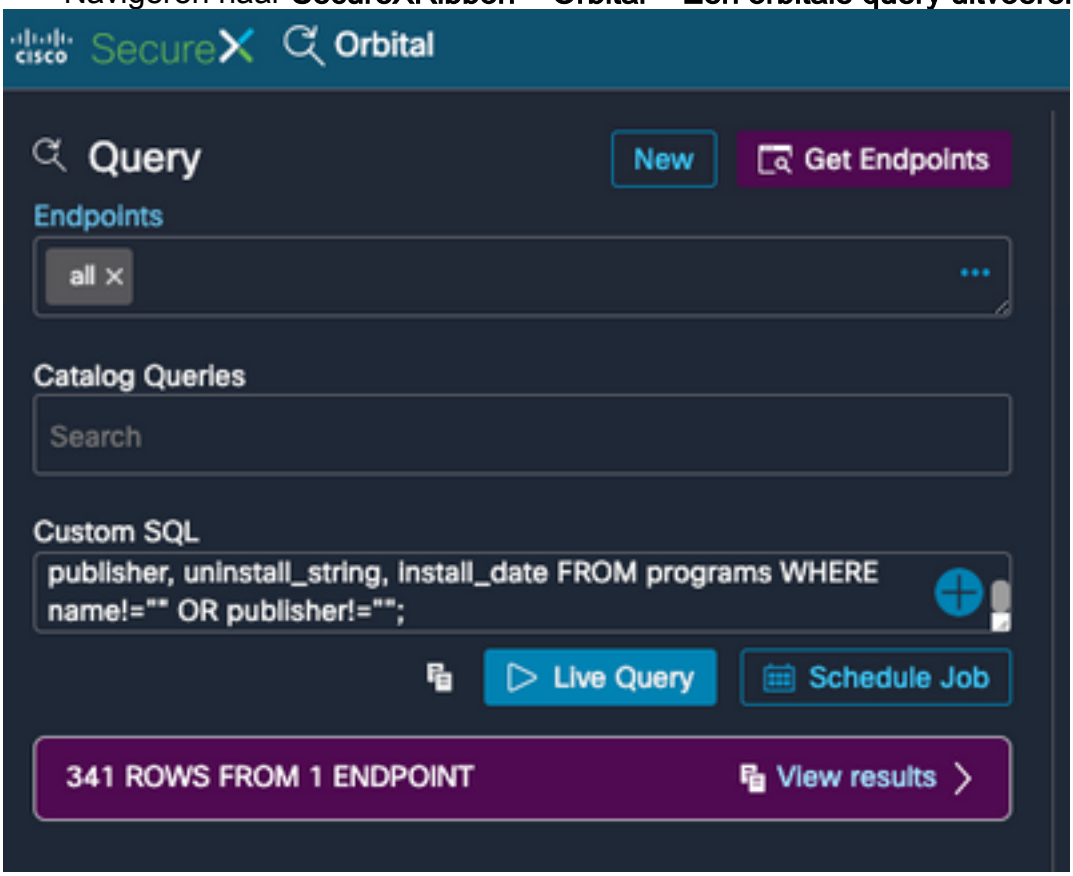
- Navigeer op SecureX naar **Dashboard**
- Klik **op Nieuw Dashboard** en geef het een naam
- Selecteer de eerder gegenereerde orbitummodule
- Selecteer de tegels, voor deze gids worden alle toegevoegd
- Klik op Opslaan



- Selecteer de **tijdlijn** en controleer of gegevens van Orbital in SecureX worden weergegeven



- Een onderzoek kan worden gestart vanuit het SecureX-lint
- Navigeren naar **SecureXRibbon > Orbital > Een orbitale query uitvoeren**



Gerelateerde informatie

- Hier vindt u video's over het configureren van productintegraties.
- 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.