Probleemoplossing voor Cisco XDR en Secure Malware Analytics - cloudintegratie

Inhoud

Inleiding

Dit document beschrijft hoe u Secure Malware Analytics Cloud-module met Cisco XDR kunt oplossen.

Bijgedragen door Javi Martinez, Cisco TAC Engineer.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Secure Malware Analytics-cloud
- Cisco XDR router

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende softwareversies:

- Secure Malware Analytics Cloud-console (gebruikersaccount met beheerdersrechten)
- Cisco XDR-console (gebruikersaccount met beheerdersrechten)

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

Cisco Secure Malware Analytics Cloud is een geavanceerd en geautomatiseerd platform voor malware-analyse en malware-bedreigingsinformatie waarin verdachte bestanden of webbestemmingen kunnen

worden ontploft zonder dat dit gevolgen heeft voor de gebruikersomgeving.

In de integratie met Cisco XDR is Secure Malware Analytics een referentiemodule en biedt de mogelijkheid om in het Secure Malware Analytics Portal te draaien om extra informatie te verzamelen over bestandshashes, IPâ€™s, domeinen en URLâ€™s in de Secure Malware Analytics Cloud (SMA Cloud)-kennisopslag.

Raadpleeg de meest recente Secure Malware Analytics Cloud Integration Guide,

- NAM Cloud.
- EU Cloud.

Problemen oplossen

Licentie

- Controleer of u over een juiste SMA-licentie beschikt om toegang te krijgen tot Secure Malware Analytics Cloud-console

Moduletegels

- Controleer of u de juiste ***Tegels*** selecteert voor Secure Malware Analytics Cloud Module
  Navigeer naar Cisco XDR portal > Dashboard > Aanpassen knop > Selecteer de SMA Cloud module > De juiste Tegels toevoegen

Beheerdersrol

- Controleer of u een Secure Malware Analytics-account hebt met beheerdersrol in Secure Malware Analytics-portal
  Navigeer naar Cisco XDR-portal > Beheer > Uw account

- Controleer of u een SecureX-account met beheerdersrechten in SecureX-portal hebt
  Navigeren naar Malware Analytics portal > Mijn Malware Analytics account

Opmerking: als u geen beheerdersrol hebt in de Secure Malware Analytics-console en Cisco XDR-console, kan uw beheerder de accountrol rechtstreeks wijzigen via het betreffende portal

Tijdlijnen

- Controleer of de tijdstempel op de juiste manier op het Cisco XDR-portal is ingesteld.
  Navigeer naar Cisco XDR-portal > Dashboard > Tijdframe optie > Selecteer het juiste tijdframe op basis van de SMA-activiteit

Recreatiemodule

- Verwijder de oude SMA module en maak een nieuwe SMA module.
  Navigeren naar Secure Malware Analytics Cloud-console > Mijn Malware Analytics-account > API-sleutel > De API-sleutel kopiëren
  Navigeren naar Cisco XDR-portal > Integratiemodules > Selecteer de SMA Cloud-module > De API-toets en de URL toevoegen (selecteer de SMA Cloud) > Het Dashboard maken

Opmerking: alleen gebruikers met de Org Admin of Gebruikers rol kunnen de API-sleutel verkrijgen die de

Secure Malware Analytics-integratiemodule in Cisco XDR inschakelt.

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.