Fehlerbehebung bei Cisco XDR und Secure Malware Analytics Cloud-Integration

Inhalt

[Einleitung](#)
[Voraussetzungen](#)
[Anforderungen](#)
[Verwendete Komponenten](#)
[Hintergrundinformationen](#)
[Fehlerbehebung](#)
[Lizenz](#)
[Modulkacheln](#)
[Administratorrolle](#)
[Zeitrahmen](#)
[Modul neu erstellen](#)

Einleitung

In diesem Dokument wird die Fehlerbehebung für das Secure Malware Analytics Cloud-Modul mit Cisco XDR beschrieben.

Beitrag von Javi Martinez, Cisco TAC Engineer.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Sichere Malware-Analyse-Cloud
- Cisco XDR

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf folgenden Software-Versionen:

- Secure Malware Analytics Cloud-Konsole (Benutzerkonto mit Administratorrechten)
- Cisco XDR-Konsole (Benutzerkonto mit Administratorrechten)

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten

Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Hintergrundinformationen

Cisco Secure Malware Analytics Cloud ist eine erweiterte und automatisierte Plattform mit Malware-Analyse und Malware-Bedrohungsinformationen, über die verdächtige Dateien oder Webziele ohne Auswirkungen auf die Benutzerumgebung zur Detonation gebracht werden können.

Secure Malware Analytics ist ein Referenzmodul für die Integration mit Cisco XDR und bietet die Möglichkeit, in das Secure Malware Analytics-Portal zu wechseln, um zusätzliche Informationen zu Dateihashes, IPs, Domänen und URLs im Wissensspeicher der Secure Malware Analytics Cloud (SMA Cloud) zu sammeln.

Weitere Informationen finden Sie im neuesten Secure Malware Analytics Cloud Integration Guide,

- NAM-Cloud.
- EU-Cloud.

Fehlerbehebung

Lizenz

- Vergewissern Sie sich, dass Sie über eine richtige SMA-Lizenz verfügen, um Zugriff auf die Secure Malware Analytics Cloud-Konsole zu erhalten.

Modulkacheln

- Wählen Sie die richtigen Kacheln für das Secure Malware Analytics Cloud-Modul aus. Navigieren Sie zum Cisco XDR-Portal > Dashboard > Schaltfläche Anpassen > Wählen Sie das SMA Cloud-Modul aus > Fügen Sie die gewünschten Kacheln hinzu.

Administratorrolle

- Vergewissern Sie sich, dass Sie über ein Konto für sichere Malware-Analysen mit Administratorrolle im Portal für sichere Malware-Analysen verfügen.
  Navigieren Sie zum Cisco XDR-Portal > Administration > Ihr Konto
- Überprüfen Sie, ob Sie über ein SecureX-Konto mit Administratorrechten im SecureX-Portal verfügen.
  Navigieren Sie zum Malware Analytics-Portal > Mein Malware Analytics-Konto

Hinweis: Wenn Sie in der Secure Malware Analytics-Konsole und der Cisco XDR-Konsole keine Administratorrolle haben, kann Ihr Administrator die Kontorolle direkt über das betreffende Portal

ändern.

Zeitrahmen

- Überprüfen Sie, ob der Zeitstempel im Cisco XDR-Portal richtig eingestellt ist.
  Navigieren Sie zum Cisco XDR-Portal > Dashboard > Zeitrahmen-Option > Wählen Sie den richtigen Zeitrahmen basierend auf der SMA-Aktivität aus.

Modul neu erstellen

- Löschen Sie das alte SMA-Modul, und erstellen Sie ein neues SMA-Modul.
  Navigieren Sie zu Secure Malware Analytics Cloud-Konsole > My Malware Analytics-Konto > API-Schlüssel > API-Schlüssel kopieren
  Navigieren Sie zum Cisco XDR-Portal > Integrationsmodule > wählen Sie das SMA Cloud-Modul > fügen Sie den API-Schlüssel und die URL hinzu (wählen Sie die SMA Cloud) > erstellen Sie das Dashboard.

Hinweis: Nur Benutzer mit der Rolle "Organisations-Administrator" oder "Benutzer" können den API-Schlüssel erhalten, der das Integrationsmodul für Secure Malware Analytics in Cisco XDR aktiviert.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.