Cisco XDRとSecure Malware Analyticsのクラウド統合のトラブルシューティング

内容

概要

このドキュメントでは、Cisco XDRを使用してSecure Malware Analytics Cloudモジュールをトラブルシューティングする方法について説明します。

著者：Cisco TACエンジニア、Javi Martinez

前提条件

要件

次の項目に関する知識があることが推奨されます。

- セキュアマルウェア分析クラウド
- Cisco XDR

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアのバージョンに基づいています。

- Secure Malware Analytics Cloudコンソール（管理者権限を持つユーザアカウント）
- Cisco XDRコンソール（管理者権限を持つユーザアカウント）

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このド

キュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

Cisco Secure Malware Analytics Cloudは、高度で自動化されたマルウェア分析およびマルウェア脅威インテリジェンスプラットフォームです。ユーザ環境に影響を与えることなく、疑わしいファイルやWebの宛先を起爆可能です。

Cisco XDRとの統合において、Secure Malware Analyticsは参照モジュールであり、Secure Malware Analytics Portalにピボットして、ファイルハッシュ、IP、ドメイン、およびURLに関する追加のインテリジェンスをSecure Malware Analytics Cloud(SMA Cloud)ナレッジストアに収集する機能を提供します。

最新の『Secure Malware Analytics Cloud Integration Guide』を参照してください。

- NAMクラウド。
- EUクラウド。

トラブルシュート

ライセンス

- Secure Malware Analytics Cloudコンソールにアクセスするための適切なSMAライセンスがあることを確認します。

モジュールタイル

- Secure Malware Analyticsクラウドモジュールに適切なタイルを選択していることを確認します。
  Cisco XDRポータル>ダッシュボード>カスタマイズボタン> SMAクラウドモジュールの選択>適切なタイルの追加に移動します。

管理者ロール

- Secure Malware Analyticsポータルで管理者ロールを持つSecure Malware Analyticsアカウントがあることを確認します
  Cisco XDRポータル>管理>アカウントに移動します。

- SecureXポータルで管理者権限を持つSecureXアカウントを持っていることを確認する
  Malware Analyticsポータル> My Malware Analyticsアカウントに移動します

注：Secure Malware AnalyticsコンソールおよびCisco XDRコンソールに管理者ロールがない場合、管理者は問題のポータルからアカウントロールを直接変更できます

期間

- Cisco XDRポータルでタイムスタンプが正しく設定されていることを確認します。
  Cisco XDRポータル>ダッシュボード>タイムフレームオプション> SMAアクティビティに基づいて適切なタイムフレームを選択します

モジュールの再作成

- 古いSMAモジュールを削除し、新しいSMAモジュールを作成します。
  Secure Malware Analytics Cloudコンソール> My Malware Analyticsアカウント> API Key > Copy the API keyに移動します。
  Cisco XDRポータル> Integration modules > SMA Cloudモジュールの選択> APIキーとURLの追加（SMA Cloudを選択） > Create the Dashboardに移動します。

注：Org AdminまたはUsersロールを持つユーザだけが、Cisco XDRのSecure Malware Analytics統合モジュールを有効にするAPIキーを取得できます。

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。