Cisco XDR和安全惡意軟體分析雲整合故障排除

目錄

簡介

本檔案介紹如何使用Cisco XDR對安全惡意軟體分析雲模組進行故障排除。

作者：Javi Martinez，思科TAC工程師。

必要條件

需求

思科建議您瞭解以下主題：

- 安全惡意軟體分析雲
- Cisco XDR

採用元件

本檔案中的資訊是根據以下軟體版本：

- 安全惡意軟體分析雲控制檯（具有管理員許可權的使用者帳戶）
- Cisco XDR控制檯（具有管理員許可權的使用者帳戶）

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

Cisco Secure Malware Analytics Cloud是一個高級且自動化的惡意軟體分析和惡意軟體威脅情報平台，可在其中觸發可疑檔案或Web目標，而不會影響使用者環境。

在與思科XDR的整合中，安全惡意軟體分析是一個參考模組，它提供透視到安全惡意軟體分析門戶的功能，從而在安全惡意軟體分析雲（SMA雲）知識庫中收集有關檔案雜湊、IP、域和URL的額外情報。

請參閱最新的Secure Malware Analytics雲整合指南，

- NAM雲。
- EU雲。

疑難排解

授權

- 驗證您擁有適當的SMA許可證，以便訪問安全惡意軟體分析雲控制檯

模組磁貼

- 驗證您是否為安全惡意軟體分析雲模組選擇正確的磁貼
  導航到Cisco XDR門戶>控制面板>自定義按鈕>選擇SMA雲模組>新增正確的磁貼

管理員角色

- 驗證您是否具有安全惡意軟體分析門戶中具有管理員角色的安全惡意軟體分析帳戶
  導航到Cisco XDR門戶>管理>您的帳戶

- 驗證您在SecureX門戶中具有管理員許可權的SecureX帳戶
  導航到Malware Analytics門戶> My Malware Analytics帳戶

注意：如果您在安全惡意軟體分析控制檯和Cisco XDR控制檯中沒有管理員角色，您的管理員可以直接從相關門戶更改帳戶角色

時間範圍

- 驗證在Cisco XDR門戶上是否正確設定了時間戳。
  導航到Cisco XDR門戶>控制面板>時間框架選項>根據SMA活動選擇適當的時間框架

重新建立模組

- 刪除舊的SMA模組並建立新的SMA模組。
  導航到Secure Malware Analytics Cloud Console > My Malware Analytics account > API Key > Copy the API key

導航到Cisco XDR門戶>整合模組>選擇SMA雲模組>新增API金鑰和URL（選擇SMA雲）>建立儀表板

注意：只有具有「組織管理員」或「使用者」角色的使用者才能獲得在Cisco XDR中啟用安全惡意軟體分析整合模組的API金鑰。

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。