Cisco XDR已知問題

目錄

簡介

本文記錄當前已知的Cisco XDR技術問題。

技術問題可由思科確認、審查、待解決或視為按預期工作。

已知的問題:

事件

目前此XDR功能沒有已知問題。

調查

目前此XDR功能沒有已知問題。

控制中心

目前此XDR功能沒有已知問題。

思科整合

1. Cisco XDR — 思科安全防火牆完全整合

詳細信息：為了確保在Cisco Defense Orchestrator(CDO)、安全服務交換(SSX)和安全分析和

記錄(SAL)之間實現無縫整合，需要手動對映。此過程涉及到聯絡Cisco TAC以執行必要的配置和對映。

解決方法：與TAC聯絡，以協助連結相關帳戶並確保系統的正確整合。

預期解析度：待定

第三方整合

1. — 具有G型別許可證的Microsoft客戶無法使用XDR Microsoft整合。

狀態：按設計工作

詳細資訊:Microsoft G型別權利只在受控環境中為政府實體調配訪問許可權。

後續步驟：思科正在與Microsoft合作，以瞭解將Microsoft G-type權利整合到Microsoft GCC環境的要求。如果可行,Cisco XDR計畫與Microsoft G型別的許可證整合，用於Microsoft Defender for Endpoint、O365和EntraID。

預期解決方案：已解決，在此處提供整合。

資產

目前此XDR功能沒有已知問題。

XDR自動化

目前此XDR功能沒有已知問題。

裝置/感測器

目前此XDR功能沒有已知問題。

安全使用者端

若要諮詢Secure Client的問題，請遵循文章。

XDR分析

1. — 多個IP地址和/或多個主機名可以與XDR-A中的單個裝置名稱關聯

狀態:未解決/延遲

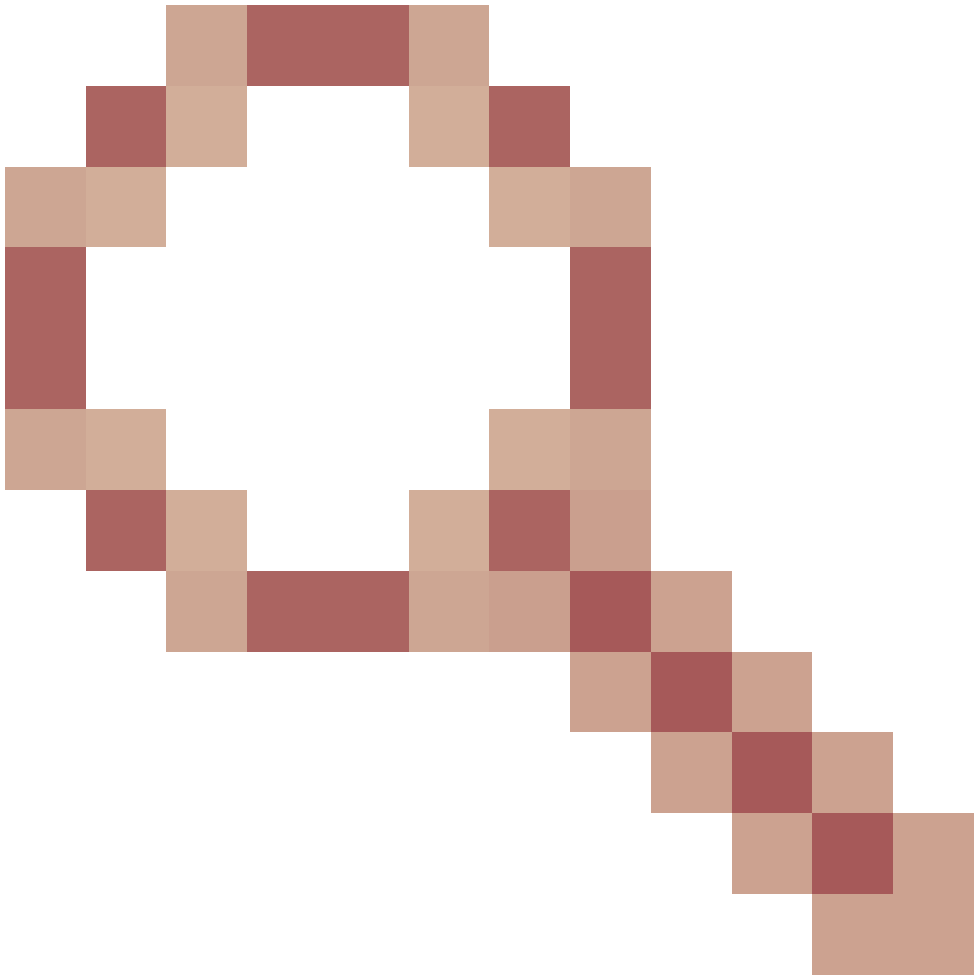
詳細資訊：多個活動IP地址可以與SNA/XDR-A門戶中的單個裝置相關聯。這可以包括NVM和非NVM裝置。某些裝置也具有多個主機名。根據當前實施，註冊裝置可能導致裝置具有多個IP地址（位置）。 其中一些IP地址可能來自使用者的家庭網路，並且可能與組織網路中的IP地址衝突。

解決方法：目前沒有解決此問題的方法，並且此問題仍存在於當前體系結構中。人們希望，一

旦實施新的架構，將來這個問題可能會得到更好的解決，該架構將允許來自ONA和NVM的網路活動規範化為OCSF，並集中在一起。

後續步驟：不適用

解析度：未來/待定



跟蹤CDET:CSCwo67299

已解決的問題

1.- Cisco XDR - Cisco Secure Endpoint integration link not working on Cisco XDR Portal

狀態:已發現問題並等待解決

詳細資訊：在Admin > Integrations頁籤中，Secure Endpoint「Enable」連結斷開。按一下enable按鈕後，它會重定向到Threat Response頁面，並循環到XDR組織選擇器頁面，而不是轉到Secure Endpoint Console。

因應措施：可以從思科安全終端門戶執行整合

後續步驟：思科正致力於實施此問題的修補程式

預期解決方案：此問題已解決。

2.- XDR自動事件自動化規則意外停止運行

狀態：已識別的問題和待決問題

詳細資訊：由工作流和觸發器支援的事件自動化規則意外停止運行。在XDR使用者介面中，除了複查Workflows Run Over Time的度量之外，不顯示此值。執行此操作時，客戶將看到工作流運行減少或為零，具體取決於問題持續的時間長短。

後續步驟：思科已將此問題確定為XDR後端中的一個問題，並正在努力解決此問題。思科還計畫實施其他監控和狀態跟蹤功能，以避免將來發生此問題。

解決方法：禁用並重新啟用規則以啟動工作流規則觸發和處理的重新啟動。

預期解析度：已解決。

3.- Cisco XDR-Analytics — 虛擬環境中的ONA安裝失敗，錯誤指示「校驗和驗證失敗」
狀態：已識別的問題和待決問題

詳細資訊：在虛擬環境中部署ONA感測器時，ISO無法完成安裝過程並發生錯誤。

因應措施：使用Ubuntu ISO獨立安裝Ubuntu Server 24.04，並按照高級安裝步驟運行ONA即服務。使用7.0 U2相容性

後續步驟：不適用

解析度：此問題已在最新版本的ONA感測器中解決

4. — 控制中心上的MTTR圖塊顯示已使用一種新狀態(如「已關閉：False Positive"、"Closed:已確認威脅」或其他。

狀態:已發現問題並等待解決

詳細資訊：1月15日，新的事件狀態被引入，磁貼沒有考慮這些狀態。新決議狀態被解釋為進行中工作，因此即使該事件已使用其中一個新狀態結束，也將其視為正在進行中的工作。

解決方法：無

後續步驟：無

預期解決方案：已解決

如果您需要與思科支援聯絡，請依照此連結中提供的說明操作。

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）。