使用Umbrella配置安全惡意軟體分析裝置

目錄

簡介

本文檔介紹如何配置受支援的第三方整合與安全惡意軟體分析裝置（以前稱為Threat grid）的整合並對其進行故障排除。

必要條件

需求

思科建議您瞭解以下主題：

- Cisco Secure 惡意軟體分析
- 思科資安防護傘

採用元件

本文件所述內容不限於特定軟體和硬體版本。

- Umbrella
- 安全惡意軟體分析裝置

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

為了提供已提交樣本的其他分析資訊，例如Umbrella風險評分，Malware Analytics Appliance通過API金鑰與Umbrella整合。

組態

提示：在TGA群集操作中，每個TGA節點都單獨配置。無法配置每個TGA節點可能導致結果不一致。

注意：來自裝置髒介面的整合源；必須連線髒介面並允許出站訪問才能正確操作。

步驟1.登入到您的Umbrella控制面板，然後在左側導航選單中按一下Admin > Licensing。您將看到您當前的包型別。

步驟2.確保您擁有SIG學位許可證
https://umbrella.cisco.com/products/umbrella-enterprise-security-packages

步驟3.在Umbrella控制面板中，點選Investigate > API keys > copy API Access Tokens

步驟4.登入到Malware Analytics裝置的Opadmin(Admin)介面。

步驟5.導航至Configuration > Integrations。

步驟6.使用API訪問令牌配置TGA。

配置後，按一下Save，然後按一下reconfigure。

步驟7.使用RASH向客戶裝置執行

systemctl — 無塊重啟tg-supervisor

步驟8.測試您的許可證是否具有適當的API層級：

curl —include —request POST —header "Authorization: Bearer 12345678910" —data-binary "["cnn.com"]" https://investigate.api.umbrella.com/domains/categorization

注意：您需要聯絡客戶的客戶經理以獲得許可證升級。
無法完成所需的操作，因為第1層許可證無權訪問批次終端。這需要許可證升級到第2層或第3層訪問。

步驟1.提交URL樣本進行分析。

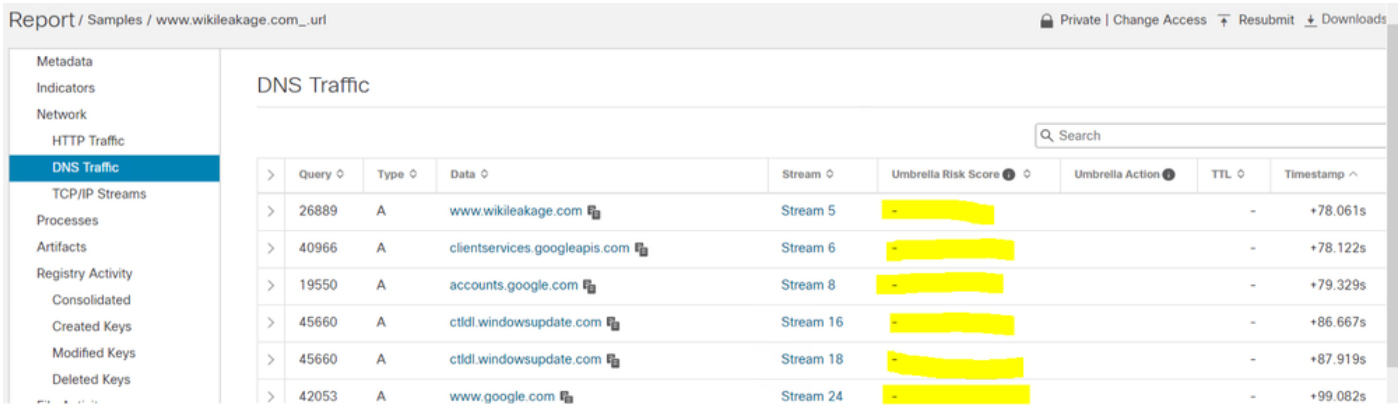
步驟2.完成示例後，檢視Samples>DNS流量。

步驟3.導航到Umbrella風險分數。

疑難排解

1.在DNS流量下的惡意軟體分析裝置示例中未顯示Umbrella風險評分

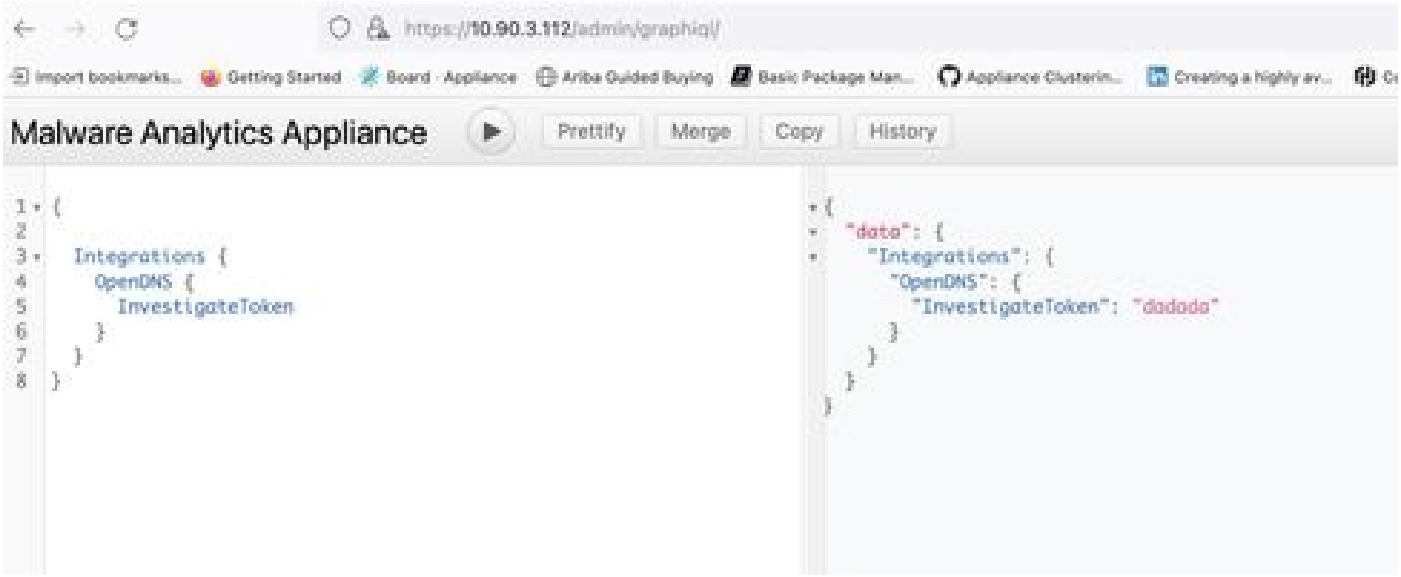
請確保在步驟8中未收到HTTP錯誤403。測試您的許可證是否具有適當的API層級別。



2.惡意軟體分析裝置中未儲存傘狀令牌

為了驗證API Umbrella令牌在裝置中是否正確硬編碼，您可以使用graphiql查詢配置檔案。響應應為從Umbrella儀表板獲取的正確API Umbrella令牌。

提示：用TGA的相應主機名替換<IP>，清除預設值並準確鍵入螢幕左側的內容，然後按播放按鈕。



graphiql

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）。