標題幻燈片

"通過分析Incribo 合成網路數據集增強網路安全"

**資訊安全分析師 | 數據分析師**

* 具有數據分析能力。熟悉 SQL、Python 和 Tableau 將資料轉換為簡單圖表。培養網路安全分析技能，以確保資料完整性並防範基本威脅，從而做出明智的決策。

**技能**

* Python
* SQL
* Excel
* Power BI
* Google Analytics
* Splunk
* Splunk Phantom
* Wireshark
* Tenable Nessus
* Autopsy

教育

* Cisco CCST 思科認證技術人員原廠國際認證
* Pearson VUE ITS 資訊科技專家國際專業認證
* Google Advanced Data Analytics Professional Certificate
* Google Cybersecurity Professional Certificate
* IBM Data Analytics with Excel and R Professional Certificate
* Google Analytics (分析) 個人認證

**自我介紹**

情境

- 關於公司:

Incribo提供定制的合成數據生成,專門針對網路安全需求。

該公司使用合成網路攻擊資料集來説明組織識別和緩解網路安全威脅。本文檔展示了 Incribo 合成網路資料集在威脅檢測和緩解方面的價值，同時還展示了分析師在資料解釋和戰略制定方面的專業能力。

- 問題陳述:

滿足對精確且可操作的見解的需求，以增強網路安全態勢。

日益嚴峻的網路威脅形勢要求採取強有力的安全措施來保護敏感性資料和關鍵基礎設施。精心設計的合成網路資料集可以類比現實世界中的網路流量模式，為增強網路安全態勢提供寶貴工具。Incribo 的合成網路攻擊資料集為組織提供了一個安全和可控的環境來測試其安全系統、識別漏洞並制定有效的緩解策略。

- 策略:

利用合成數據集提取可行動的洞見,支援網路安全決策。

- 交付成果:

1. 業務任務說明:明確定義網路安全目標和任務。

2. 數據來源描述:概述數據源及其相關性。

3. 數據清洗文檔:詳細說明確保數據完整性的清洗過程。

4. 分析摘要:呈現分析方法和發現。

5. 可視化和關鍵發現:通過視覺數據呈現突出關鍵洞見。

6. 主要建議:根據分析提供優先次序的建議。

任務:

展示Incribo合成網路攻擊數據集在識別和緩解網路安全威脅方面的重要性,展示分析師在數據解讀和戰略制定方面的專業能力。

準備

- 數據來源:

所用數據需經過嚴格清洗,符合ROCCC (相關性、原創性、全面性、一致性和正確性)標準,確保高質量的分析輸入。

- 數據清洗:

分析師使用Jupyter Notebook中的Python進行高效的數據清洗和處理。每個步驟都有詳細記錄,確保可重複性和透明度,體現分析師的技術熟練度。

過程:

數據分析:

- 檢查網路流量量趨勢,以識別潛在的威脅,如DDoS攻擊和密碼注入嘗試。

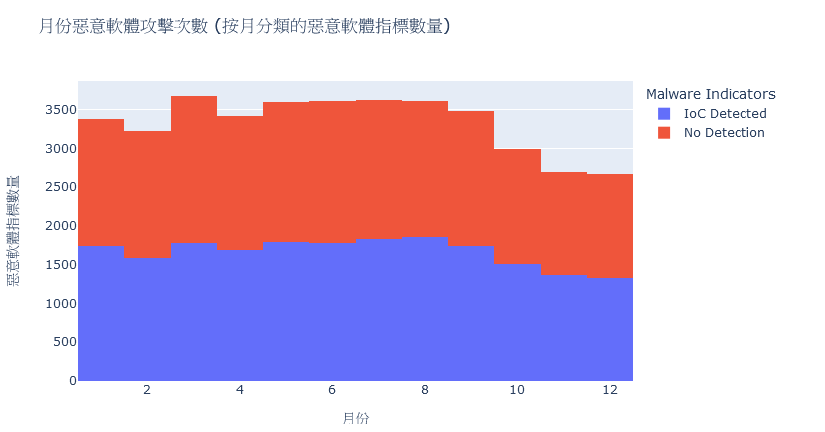
- 集中應對潛在攻擊者,優先處理威脅響應,採取針對性緩解措施。

- 進行趨勢分析,預測潛在的升級點和異常認證模式,為修補和緩解制定策略。

分析

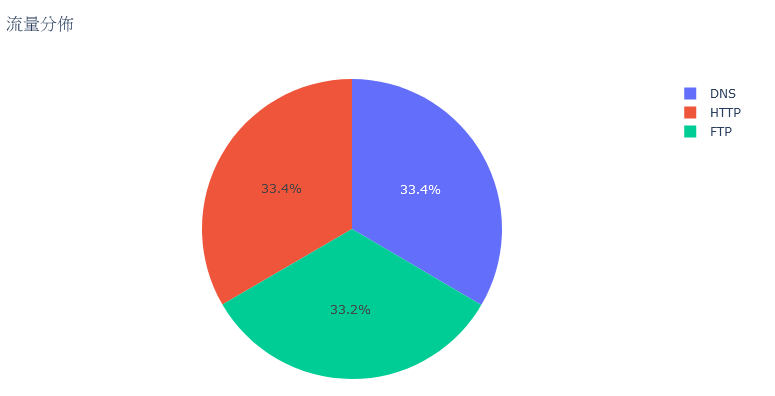
1. 隨時間變化的網路流量:

惡意軟體攻擊在 12 個月內出現明顯波動，2 月、4 月和 6 月是攻擊高峰期。這強調了在此期間需要提高警惕。



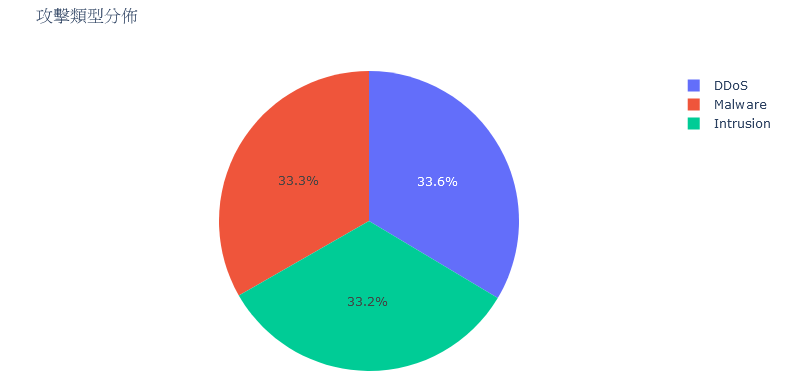
2. 惡意流量的主要源頭:

DNS（33.4%）、HTTP（33.4%）和 FTP（33.2%）協議的流量分佈相對均勻。組織應監控所有這些協定的流量以檢測異常。



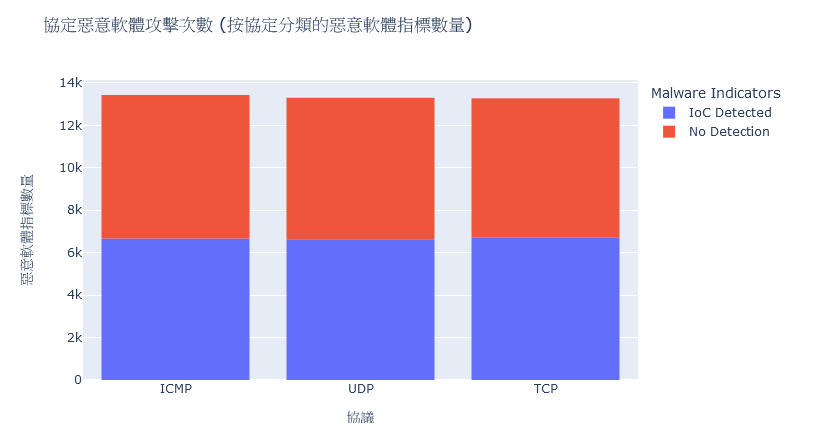
3. 檢測到的威脅類型:

DDoS（33.6%）、惡意軟體（33.3%）和入侵（33.2%）成為最普遍的威脅類型。這需要一個全面的安全性原則，涵蓋所有三個威脅類別。



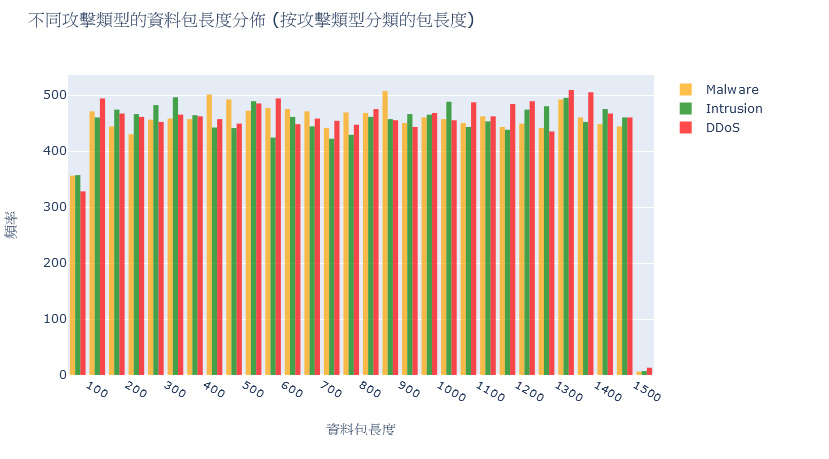
4. 用戶認證嘗試:

TCP 協議的驗證嘗試數量最多，其次是 UDP 和 ICMP。監控這些協議的驗證嘗試可以揭示可疑活動。



5. 按系統和嚴重性劃分的漏洞狀況:

不同攻擊類型（惡意軟體、入侵、DDoS）的資料包長度差異很大。這種差異可用於異常檢測和基於簽名的保護。



分享:

DDoS攻擊檢測:

流量異常激增和特定資料包特徵表明 DDoS 攻擊。立即部署 DDoS 緩解工具並通知 IT 安全團隊至關重要。

密碼注入:

在短時間內從不同 IP 位址進行多次登錄嘗試表明密碼注入攻擊。建議實施多因素身份驗證（MFA）並在多次失敗嘗試後鎖定帳戶。

內部威脅:

內部員工對敏感性資料的異常訪問模式引發了對潛在內部威脅的擔憂。需要進行徹底調查並實施最小特權存取控制。

行動:

1. 建議:

- 持續監控:定期監控和更新可視化,捕捉網路行為和威脅格局的實時變化。

- 協作分析:促進分析師和利益相關方之間的協作,解釋可視化洞見並實施有效的安全措施。

- 適應性策略:根據不斷演變的威脅趨勢和可視化洞見,制定適應性策略。

2. 理解模式:

- 模式識別:

o 威脅檢測:識別出DDoS攻擊和密碼注入等潛在威脅的特徵模式。

o 針對性策略:根據識別的模式制定針對性的漏洞管理和事件響應策略。

- 提高成果:

o 展示如何通過理解這些模式來提高事件響應和整體網路安全成果,證實分析師專業能力的價值。