趨勢科技

網路惡意行為分析半年報表系統
運用資安情資分析系統挖掘潛藏的網路攻擊事件

進階持續性威脅是今日網路攻擊常用手法，駭客透過目標式攻擊進行滲透，長時間潛伏在您的網路環境或資訊系統中，隱密的竊取機敏資料與收集各種情報。您必須在眾多看似獨立不相干的警示中，做出有效且即時的回應。

網路惡意行為分析半年報表系統 是一套專為此目的設計的資安威脅與情資分析平台，可在您現有的防禦之上，架構專屬於您的資安情報系統，提供進階攻擊偵測及整合性預警的能力，成為您精準的防護雷達，達成偵測攻擊並快速反應的目標。

網路惡意行為分析半年報表系統 採用大數據分析與人工智慧機器學習技術，分析駭客行為軌跡、建立情資系統，並結合趨勢科技全球資安情資中心作為後盾，能即時掌握全球網路攻擊情報與資安威脅元素。

為了有效釐清攻擊事件脈絡與軌跡， **TIA** 包含兩套系統模組，分別針對惡意程式與網路流量提供情資分析。您可依單位環境與需求分別佈署、或結合惡意程式與網路流量分析進行關聯式分析，達到層次性整合防禦的目標。

TIA - 動態沙箱情資分析系統

運用客製化沙盒模擬分析技術，對惡意程式進行分析，可偵測並分析多重階段下載、網址、幕後操縱 (C&C) 通訊等等，並擁有靜態分析、經驗式分析、行為分析、網站信譽評等等，提高進階威脅的偵測率。

TIA - 網路流量情資分析系統

運用檔案、網站、IP 位址、行動應用程式等信譽評等，再配合經驗式分析、進階威脅掃描、以及交叉關聯威脅情報，檢查所有網路內容。自內送與外流的網路通訊流量中，偵測針對性攻擊、勒索病毒、零時差漏洞攻擊、進階惡意程式和駭客行為、並且偵測橫向擴散、C&C 通訊以及攻擊行動所有階段的其他駭客行為。

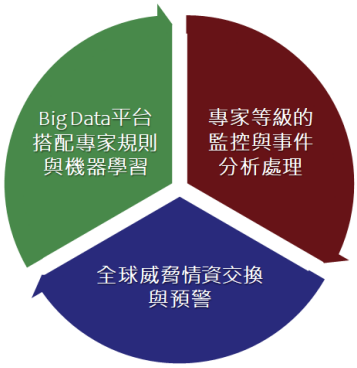
更好的偵測能力

動態沙箱情資分析系統

- 提供比一般通訊虛擬環境更優異的偵測能力
- 更好的躲避技巧防範能力

網路流量情資分析系統

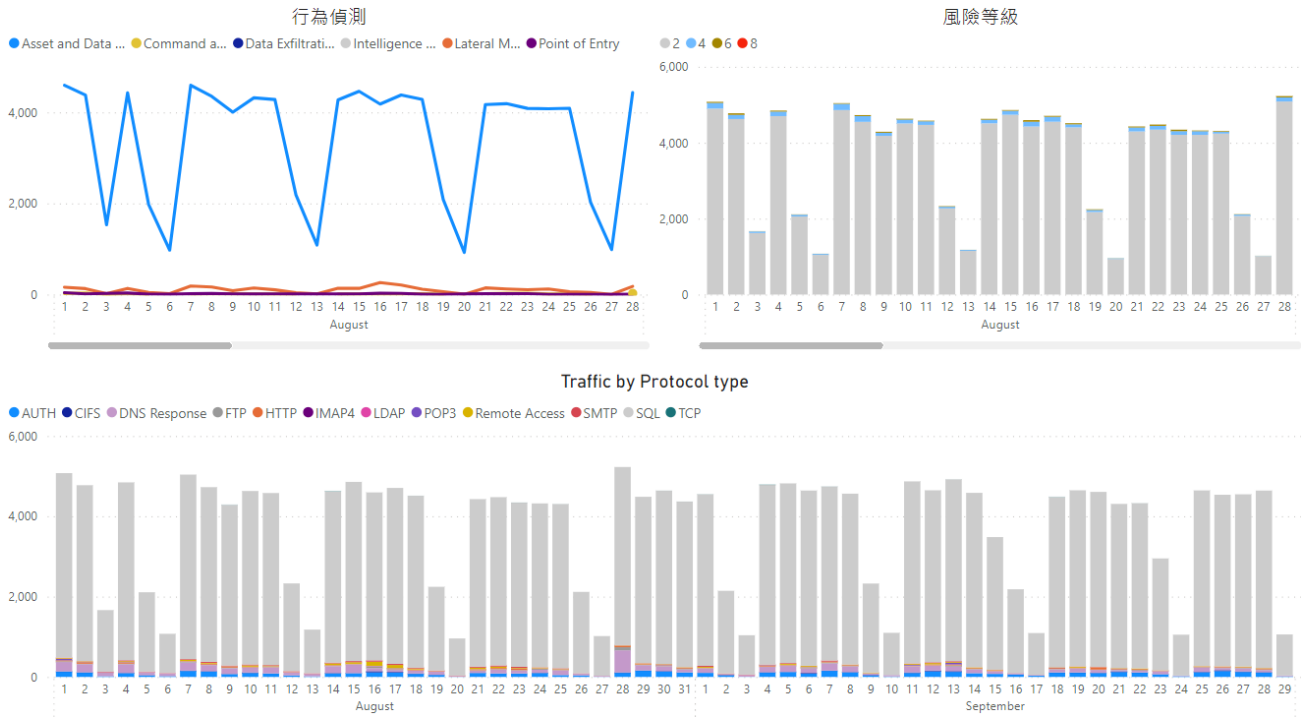
- 多重偵測技巧
- 經由產業標準格式分享威脅情報
- 運用機器學習提高偵測率



©2022年版權所有。趨勢科技股份有限公司及其相關機構保留所有權利。Trend Micro 與 t 字球形標誌為趨勢科技股份有限公司及其相關機構在美國或其他國家的商標或註冊商標。本文提及之第三方商標皆為其擁有人之財產。本文件內容若有變動，恕不另行通知。

Securing Your Connected World

流量分析圖 Traffic by Protocol



惡意連線圖 Dangerous URL in WRS