趨勢科技
APT網路惡意活動檢視事件處理系統
運用資安情資分析系統串聯資安事故調查

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。

從常見惡意程式行為與駭客行為角度出發，掃瞄系統記憶操作與存取內容、系統設定值，識別可疑程式、疑似駭客攻擊後跡像，補足防毒特徵碼(pattern)偵測已知惡意程式能力，整合趨勢檔案白單大數據資料庫 CENSUS 與 GIRD、外部情資資料庫，比對檔案的 SHA 與數位簽章等資訊，彙整趨勢科技台灣與全球 IR 案例、鑑識社群研究，進行單一端點與跨端點數位跡證搜尋、關聯、分析的協同作業時，即時處理與分析，識別可疑端點與入侵跡證，必要時可搭配 QS Query 互動調查。

項次	分析項目	分析內容
1	惡意程式檢測分析	☐ 執行中惡意程式 ☐ 駭客遺留檔案 ☐ 惡意程式動靜態分析 ☐ APT 惡意程式分群分類
2	系統異常行為分析	☐ 作業系統日誌檢視 ☐ 系統程序 (Process) 檢視 ☐ 系統操作歷程檢視 ☐ 系統設定檔檢測 ☐ 網路設定資訊檢視 ☐ 檔案時間線分析
3	網站惡意網頁檢測	☐ 網頁存取日誌檢視 ☐ 網頁程式掃描與分析

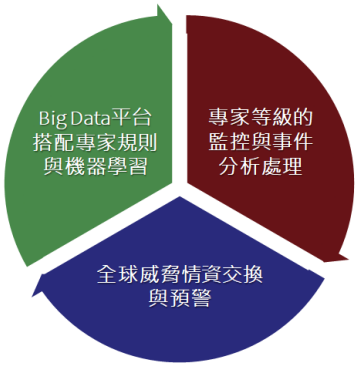
更好的偵測能力

提升分析能力

- 整合趨勢科技獨立與第三方威脅情資、趨勢科技 Yara、自行定義 Yara 或條件，趨勢科技 IR 關聯引擎

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