ThreatSonar
An Engine to Hunt down Intruders

# 威脅鑑識分析平台
# MDR服務

## ThreatSonar 設計理念

APT (進階持續性威脅，Advanced Persistent Threats) 攻擊事件持續發生，企業每年投資愈來愈多預算採購資安防護產品與服務，卻依舊無法有效阻擋 APT 攻擊行為。當攻擊事件被發現時，往往企業內部重要機敏資料早已經落入駭客手中。

ThreatSonar 惡意威脅鑑識分析平臺，源自 TeamT5 安全團隊長期對全球威脅情資與惡意程式研究的成果，結合自行開發的遠端智能鑑識與威脅行為分析前瞻技術，以及真實案例訓練出的獨特 APT 風險模型，能真正發掘潛藏啟業資訊環境內的入侵威脅，進而協助企業對抗 APT 攻擊，是構建企業資訊安全防護最有效的入侵威脅解決方案。


威脅鑑識報告簡單易懂，立即遠端啟動事件反應 (Incident Response)，掌握每個端點狀況，更可離線執行的威脅狩獵工具。

架構彈性部署容易，支援落地 (On-Premise) 或雲端管理機制，可安裝於筆記型電腦，並且相容於多種虛擬化架構。

具備威脅情資匯入功能，透過 Yara Rule 與 Blacklist 整合第三方情資資訊。

透過企業軟體派送機制部署到端點主機，執行時僅需少量網路頻寬、系統資源與檢測時間，即可迅速完成單次鑑識工作。

快速高效率鑑識工作，平均每台端點檢測僅花費 30 分鐘。硬體資源充足下，可達每小時 5,000 台端點以上的大規模鑑識。

## ThreatSonar 主要特色

### 智能鑑識

- 真實案例訓練的 APT 風險模型
- 自動鑑定數百種動態行為異常

e.g. 記憶體、檔案、網路連線、系統登入檔、事件紀錄、工作排程、開機磁區、WMI、啟動程序等

### 威脅狩獵

- 統計關聯分析找出未知攻擊手法
- 建立基準線鎖定異常行為
- 主動威脅狩獵，標示潛伏未知威脅

例如組織中稀有程式或目錄、合法系統工具遭到濫用，或是具數位簽章的惡意程式等

### 情資驅動

- 將第三方情資帶到每個端點
- 內建數千種 APT 後門特徵
- 可匯入 hash、IP、domain、Yara Rule 與 IoC 等外部情資
- 可雲端比對情資或離線斷網運作

### 自動聯防

- 開放 API 整合既有防護設備
- 自動化傳遞告警及更新情資
- 發送 CEF 告警到 SIEM 設定規則阻擋
- Restful API 下載報告及樣本
- 程式化更新情資，調整偵測規則

### 自動調查分析

- 發掘攻擊事件起源及過程
- 追蹤內網移動足跡與資料外流路徑
- Timeline 事件時間軸呈現先後
- 圖形視覺化方式呈現威脅事件
- 主動發現駭客族群常用 TTPs 的隱藏威脅

### MDR 服務

- 專家進行深度入侵威脅獵捕服務
- 威脅案件調查、報告與應變建議
- 重大網路威脅事件關聯獵捕服務


TEAMT5 杜浦數位安全

Website https://teamt5.org/ | Facebook TeamT5.org | E-mail sales@teamt5.org | Tel +886-2-7706-1299