ThreatSonar EDR

Designed for APT & Ransomware Protection

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，能真正發掘潛藏企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。

作業系統全面支援

- Windows
- Linux
- macOS

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。

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。

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。

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。

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。

24 HOURS

支援常駐模式，以及7/24全時監控，持續監視端點活動，一旦發現異常行為，系統即時告警，呈現分析結果。

TEAMT5 杜浦數位安全

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

ThreatSonar EDR

Designed for APT & Ransomware Protection

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

風險訂閱

- 風險防護客製化，可自行定義風險追蹤項目
- 風險等級可調整，彈性定義風險程度
- 簡化事件調查，加速風險告警

情資驅動

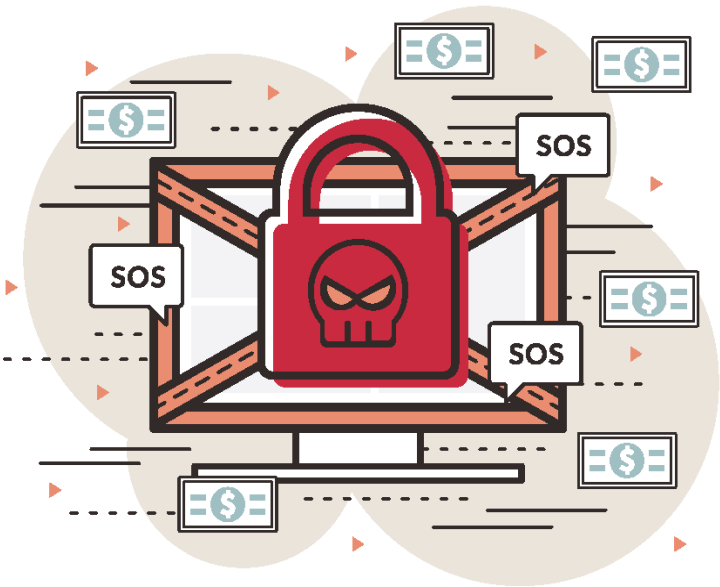
- 將第三方情資帶到每個端點
- 內建數千種 APT 後門特徵
- 可匯入 hash、IP、domain、Yara Rule 與 IoC 等外部情資
- 可雲端比對情資或離線斷網運作

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

防堵勒索軟體

防駭所面臨的對象是人類，以人工智慧或單一解決方案效果有限，因為駭客也會適應與變化，設法規避現有防護，唯有「全面防堵」的策略才能有效且持續對抗勒索軟體。



隔離新進程式

採不信任策略，嚴格觀察新進程式，避免非必要的系統互動與資料存取。

誘捕勒索軟體

置放陷阱檔案，誘捕勒索軟體，即時中斷惡意程式運行與檔案加密動作。

監控可疑行為

檢視是否有檔案加密或系統破壞的可疑行為，包含檔案系統、記憶體、註冊機碼、系統備份等。

還原備份檔案

獨家備份機制，有效還原關鍵檔案，保護公司重要文件資產不流失。

阻止傳播擴散

當攔捕到威脅時，快速隔離該惡意程式，避免威脅於企業內網持續橫向擴散。

預防最新手法

持續研究與追蹤各大勒索軟體族群的最新手法，以領先情資預測勒索軟體的下一步。

採購資訊：

- ☐ ThreatSonar EDR - APT與勒索威脅防護系統雲端版 (10端點/1年授權/支援Windows、Linux及Mac)
  - 雲端平台專屬使用帳戶一組
  - 端點掃描程式軟體
  - 即時威脅情資更新
  - 10個端點連線授權一年
- ☐ ThreatSonar EDR - APT與勒索威脅防護系統標準版 (5端點/1年授權/支援Windows)
  - ThreatSonar管理平台
  - 端點掃描程式軟體
  - 管理平台使用與更新(一年授權)
  - 威脅情資更新(一年授權)
  - 5個端點軟體使用與更新(一年授權)
- ☐ ThreatSonar EDR - APT與勒索威脅防護系統旗艦版 (5端點/1年授權/支援Windows、Linux及Mac)
  - ThreatSonar管理平台
  - 端點掃描程式軟體
  - 管理平台使用與更新(一年授權)
  - 威脅情資更新(一年授權)
  - 5個端點軟體使用與更新(一年授權)
- ☐ ThreatSonar EDR - APT與勒索威脅防護系統進階版 (5端點/1年授權/支援Windows及Linux)
  - ThreatSonar管理平台
  - 端點掃描程式軟體
  - 管理平台使用與更新(一年授權)
  - 威脅情資更新(一年授權)
  - 5個端點軟體使用與更新(一年授權)
- ☐ ThreatSonar EDR - APT與勒索威脅防護系統專業版 (5端點/1年授權/支援Windows及Mac)
  - ThreatSonar管理平台
  - 端點掃描程式軟體
  - 管理平台使用與更新(一年授權)
  - 威脅情資更新(一年授權)
  - 5個端點軟體使用與更新(一年授權)

端點掃描程式系統需求

Windows：Windows 7以上；Linux：Kernel 2.6以上；Mac：MacOS 10.13以上

TEAMT5 杜浦數位安全

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