ThreatSonar ANTI-RANSOMWARE

威脅鑑識分析與回應平台

企業、政府和組織的資安團隊在偵測、調查和修復威脅攻擊時，面臨多重挑戰。資安團隊從不同的端點收集到的大量數據，需要相對應的分析調查能量，但在缺乏可視化、且手動搜索缺乏關聯性下，常難以獵捕異常行為。加上駭客攻擊行動往往被大量資訊淹沒，使得資安人員需耗時找出真正可疑的攻擊行為，拖累資安事件應變與調查的進展，影響生產力並增加運營成本。

情資驅動端點安全防護，強化企業組織面對威脅攻擊的防禦能量

長期研究全球威脅情資與追蹤惡意程式的 TeamT5 團隊，深知企業、政府與組織的資安威脅防禦需求，開發 ThreatSonar Anti-Ransomware 威脅鑑識分析與回應平台，以領先情資持續預測未來攻擊，並全時監控異常行為。一旦偵測到威脅入侵，發出即時警告、阻斷攻擊行動，有效回應威脅事件，降低入侵造成的損害。

效益

- **有效資安防護** 高偵測覆蓋率，精準阻擋潛在威脅。
- **縮短應變時間** 自動分析入侵威脅，加速事件處理。
- **緩解警報疲勞** 協助資安人員識別風險高低，將時間專注在高風險事件處理。
- **減輕人力偵測負擔** 自動化智慧威脅獵捕，主動發現環境中潛伏的威脅。
- **事件緩解，減少損失** 防堵橫向移動，修補威脅損害。

特色

① 全時監控，威脅無所遁形

藉由引擎自我學習機制，防範來自勒索軟體等惡意威脅，自動判斷常用程式或新進惡意程式 ， 有效掃描被加密檔案，揪出惡意行為。

② 可視化網路攻擊鏈，快速識別事件軌跡

藉由圖像化攻擊發生路徑 ， 查找事件軌跡 ， 並且根據事件資訊標籤，方便資安事件分析人員快速識別，並深入了解攻擊者的行為，進行緩解處置。

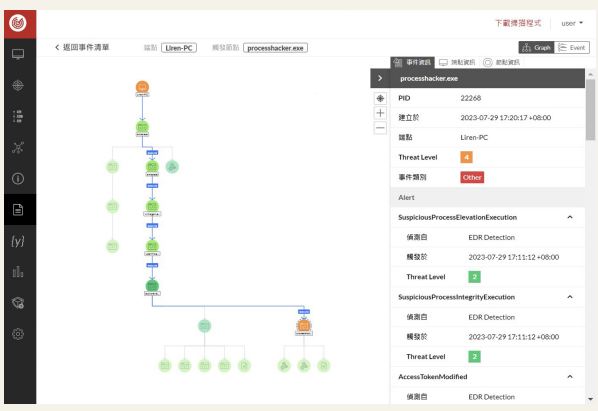
③ 對應 MITRE ATT&CK® 加速調查攻擊行為，強化資安策略

當攻擊發生時，可即時對應 MITRE ATT&CK® 框架，透過其已知的技術和戰術的關聯 ， 資安團隊可即時掌握攻擊行為過程中的戰術 、 技術和程序 (TTP)，查看自身對某些惡意族群的防範措施是否確實。

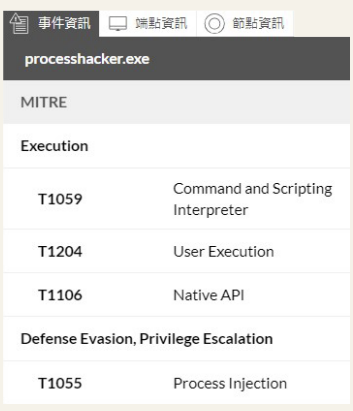
④ 時間軸呈現事件全貌，縮短事件調查時程

可透過事件時間軸 ， 呈現先後事件紀錄分析 ， 加速調查事件軌跡。時間軸呈現方式有兩種，一為以節點為主體，查看單一節點執行的時間序 ; 二是以事件為主體 ， 查看報告內每個事件發生的時間序。

② 可視化網路攻擊鏈



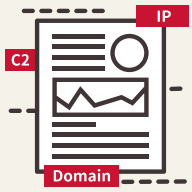
③ 對應 MITRE ATT&CK®



④ 時間軸呈現事件全貌

ThreatSonar 如何全面防堵勒索攻擊？

威脅預測 ···· ▶ ···· 檔案加密前 ···· ▶ ···· 檔案加密中 ···· ▶ ···· 檔案加密後



情資	端點	阻擋	還原
風險精準預測	監控新進程式	即時自動阻斷	保護備份檔案

持續預測未來攻擊，精準防禦

藉由 TeamT5 威脅情資團隊長期追蹤各大駭客族群的最新攻擊技術，以領先情資預測勒索攻擊的下一步。

主動獵捕勒索軟體，即時阻斷威脅攻擊

可識別上百種勒索程式，藉由在被保護檔案附近路徑鋪設陷阱檔案，若有非經允許的程式存取，將自動觸發處置措施，即時中斷軟體運行，阻擋惡意程式加密檔案行為。

阻止威脅傳播，立即採取隔離措施

偵測到具高風險的威脅時，發出即時告警。若藉情資比對，發現屬於威脅攻擊，則截斷該惡意程式運作，並隔離該台端點，讓攻擊者無法在內網橫向移動。

阻擋惡意破壞，有效保護還原備份資料

結合 Windows VSS 服務，快速啟用備份機制。當 ThreatSonar 主動偵測到攻擊者惡意破壞備份行為時，即時阻擋，確保企業或組織成功還原資料。

關於 TeamT5

廣受全球 300 家以上客戶信賴，橫跨政府單位、科技、製造、金融、醫療、軍事、電信等產業。

團隊具備超過 20 年的惡意程式與進階持續性滲透攻擊 (APT) 的經驗，基於地緣和語言優勢，我們有效掌握亞太地區的駭客攻擊 ， 更經常受邀於世界級資安會議中發表最新頂尖研究 ， 包含臺灣 HITCON、美國 Black Hat、日本 Code Blue / AVTOKYO、德國 Troopers，及國際組織辦理的 Hack In The Box 與 FIRST。更獲得美國 Bloomberg 及 CNN、日本產經新聞及朝日新聞、韓國 ET News 等採訪報導，我們於威脅情資研究與資安先進技術領域擁有世界領先地位。

TeamT5 杜浦數位安全股份有限公司 | Tel 02-7706-1299 | E-mail sales@teamt5.org