



情資主導獵捕威脅，專家服務即刻應變

隨著網路安全威脅複雜度日增，面對海量的威脅告警，企業與組織的資安團隊處理量能有限，若遇到入侵事件發生，難以及時應變。因此，更需要專業資安團隊協助威脅事件分析與調查。

TeamT5 威脅偵測應變代管服務 - 全時監控、處置、調查服務一次到位

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，提供專業的威脅偵測應變代管服務 (Managed Detection and Response, MDR)，將領先情資轉為主動防禦。企業等組織可以安心將威脅監控、分析、處置、調查等資安防禦任務交由 TeamT5 專業團隊，讓企業與組織的資安團隊能夠更專注於戰略性的行動措施。

藉由部署 TeamT5 自主研發的 ThreatSonar Anti-Ransomware 威脅鑑識分析與回應平台，提供 24/7 全時監控，並配合第一手掌握的網路威脅情資，包括攻擊族群分析、動機、攻擊手法、入侵指標等，TeamT5 MDR 可提供威脅入侵前、中、後的相對應服務，達到全面風險控管。

效益

- 事件應變程序符合 NIST SP 800-61r3，提升資安事件處理效率
- 根據威脅情資，MDR 專家團隊精準辨識資安事件，達到有效防禦
- 採用 ThreatSonar Anti-Ransomware 識別最新攻擊手法，及早發現，及早根除
- TeamT5 專家代管，節省企業資安人力負擔，提升應變時效
- 服務流程標準化，整合案件處理過程，利於高風險事件追蹤
- TeamT5 具專業事件應變處理經驗，掌握事件根因，強化資安韌性



一旦偵測到組織環境內有高風險威脅，TeamT5 協助分析，並在第一時間通報威脅初判結果與處置建議，如：斷網、關閉特定服務等，以協助組織快速反應，阻止可能正在進行的攻擊，最大程度地減少組織營運因此中斷的風險。TeamT5 專家團隊在通報後，會持續追蹤可疑事件，若判定有入侵跡象，及時提供企業和組織資安團隊啟動事件調查的行動計畫。

啟動事件調查後，TeamT5 專業的事件應變處理 (Incident Response, IR) 團隊將協助調查事件根因，並依案場實際狀況提出後續處置建議，保護未受影響的資產和備份、重建安全環境，並提供強化資安防禦建議，以防未來類似的攻擊。

TeamT5 MDR 服務特色



化被動為主動防禦，
制敵機先

- 提供最新網路威脅報告，組織可主動掌握威脅現況
- 從 TeamT5 情資研究萃取出 APT 入侵指標 (IOC)，及早發現威脅，有效防禦



專業識別高風險事件，
減輕資安人員負擔

- ThreatSonar 自動化識別威脅優先級，即時通報
- 專業分析師團隊針對高風險威脅，提供事件分析



專業處置
縮短入侵停留時間，
降低損害

- 藉由惡意程式特徵、攻擊手法研究，提供精準處置建議
- 威脅事件關聯獵捕，協助防堵近期重大資安事件類似威脅手法



詳盡事件調查
與補強建議，
降低再次入侵風險

- 專家團隊提供完整事件調查報告，包括根因分析、攻擊手法、補強建議等
- 結合情資研究與事件調查分析，協助企業組織強化主動防禦

情資驅動平台與專家團隊聯防，打造多層次資安防禦架構



威脅鑑識分析與回應平台

引擎自我學習機制，自動判斷惡意程式，快速鑑識事件軌跡



威脅情資平台

第一手威脅研究轉化特徵與規則，精準掌握潛在威脅



監控、分析、應變三方人員無縫合作，完備風險控管

TeamT5 MDR 專家團隊由第一線監控人員、二線的分析人員，以及事件應變人員組成，三層式過濾與控管風險。一線的監控人員協助釐清異常狀況，排除誤判；二線人員分析判斷是否為惡意入侵，若確定為惡意入侵，提供客戶精準的處置建議，同時由事件應變分析師主動介入調查，持續追蹤高風險事件，防止任何潛在的有害因子在環境內擴散。

MDR 專家團隊

- 專家經驗判斷風險等級，快速通報。
- 快速分析威脅，第一時間提供緩解措施。

分析師團隊

- 第一手惡意程式研究，了解駭客最新手法。
- 惡意程式逆向分析，提供精準防護建議。

事件應變處理團隊

- 匡列事件影響範圍，專業調查與分析事件根因與軌跡。
- 結合 TeamT5 威脅情資研究，提供完整事件調查報告與資安強化建議。

國家級事件調查經驗

逾 20 年惡意程式與 APT 研究經歷，具豐富資安事件應變實務經驗。

長期駭客攻擊研究

擅長駭客攻擊手法分析、駭侵威脅獵捕、漏洞弱點研究與入侵根因分析。

擁有多項專業證照

取得多項專業證照，如 OSCP、CCD、ECSA、CISSP、CEH、CHFI 等。

講師級資安專家

參與國內外專業資安研討會並發表研究，如美國 Black Hat、日本 JSAC、CodeBlue 等。

接軌國際資安組織

TeamT5 CSIRT 為國際最大資安事件應變組織 FIRST 會員。

關於 TeamT5

廣受全球 550 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。

頂尖專家團隊

團隊成員常在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，於威脅情資研究與資安先進技術領域擁有世界領先地位。

外界肯定

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。更於 2022 年獲得日本三大巨頭投資，包含日本最大創投 JAFCO 集富集團、日本最大跨國企業並在全球皆有商業投資的 ITOCHU 伊藤忠商事，與日本最大資安解決方案提供商 MACNICA。

Tel 02-7706-1299
E-mail sales@teamt5.org

v.202605



THREAT INTELLIGENCE
PIONEER,
BORN IN ASIA