Datasheet

Incident Response

TEAMT5

領先業界威脅情資，全方位應變資安事件

企業組織為拓展業務、與客戶協作，廣泛利用網路系統提供服務。然而，駭客可能利用網路端口入侵攻擊，造成營運停擺，損害品牌價值和客戶權益。事件應變處理最重要的目標，是減少攻擊造成的損失，協助組織盡快恢復。

TeamT5 資安事件應變處理服務
專業分析、調查、處置

長期研究全球威脅情資與追蹤惡意程式的 TeamT5 團隊，深知組織面臨資安攻擊事件的緊急應變需求，提供專業的資安事件應變處理服務(Incident Response, IR)，協助組織迅速、有效應對資安攻擊，保護關鍵資訊資產，縮短網路服務中斷時間，確保營運恢復正常運作。

藉由部署 TeamT5 自主研發的 ThreatSonar 威脅鑑識分析平台，快速篩檢場域中可能的資安風險與威脅，並從事件中嚴重受駭的主機出發，全面盤點端點安全狀態。同時藉由分析關鍵網路系統紀錄，調查駭客可能的入侵存取點，獲取駭侵根因(root cause)、掌握駭客移動路徑、盤點威脅損害。為防範未然，更進一步提供網路系統架構改善，以及預防未來類似攻擊事件的建議。

效益

符合國際資安管理框架 ， 提升效能

- 事件應變程序符合 NIST SP 800-61r3 ， 提升資安事件處理效率

阻斷威脅 、 掌握收集跡證的關鍵時間

- 第一時間提供阻斷攻擊的建議 、 取證 ， 提升事件追溯能力
- 部署 ThreatSonar 快速篩檢 ， 釐清環境威脅風險

全面排查環境可疑因子 ， 根絕後患

- 啟動關鍵受駭主機調查時 ， 同步匡列受駭範圍
- 對事件執行關聯調查 ， 確認是否橫向移動

專業 、 精準事件分析 ， 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
- 掌握中繼站溝通方式 、 失竊帳號密碼等損害 ， 提供事發現場還原建議

詳盡事件調查與補強建議 ， 減少風險

- 專家團隊提供完整事件調查報告 ， 如根因分析 、 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

前期準備	偵測受害範圍	事件調查與抑制	改善建議
▪ 掌握事件現況 ▪ 訪談客戶需求 ▪ 緊急應變建議 ▪ 規劃作業項目	▪ 端點安全狀況掃描(ThreatSonar) ▪ 關鍵記錄取證與判讀 ▪ 確認場域受害範圍	▪ 調查取樣 ▪ 樣本與日誌分析 ▪ 威脅狩獵 ▪ 根因推論 ▪ 抑制建議	▪ 事件調查報告，專人報告解讀 ▪ 威脅情資回饋，及時防禦阻擋 ▪ 駭侵根因研判，資安強化建議

完整網路事件應變服務

從事件調查、遏制和分析流程，解決入侵事件的所有面向。

資安事件調查與應變

針對駭客入侵事件，提供緊急應變諮詢與現場 / 遠端 / 離線調查服務。協助確認場域中受害終端與影響範圍，辨識惡意程式與攻擊手法，釐清入侵根因，並提供資安防護機制與改善建議。

系統、網頁、設備日誌分析

分析客戶所提供的系統、網頁、資安設備日誌。

惡意程式分析

針對案發現場的可疑程式，提供自動化沙箱或專業人工分析。

TeamT5 IR 專業團隊受國際肯定

國家級事件調查經驗	20 年以上惡意程式與 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。

具備處理各種類型資安事件經驗

TeamT5 深入瞭解網路威脅趨勢，具長期資安事件調查經驗，涵蓋不同產業別和各種規模企業與組織的資安事件類型。

APT 攻擊	網站入侵	個資外洩	設備遭駭
勒索事件	SQL 注入 WebShell	VPN 帳密洩漏	詐騙事件

ThreatSonar

威脅鑑識分析平台

快速篩檢資安威脅，有效鑑識事件軌跡

	超過	完成	發現
	九成	**100 萬**	**1,000 起**
效益	**超過九成的台灣網路安全服務供應商採用**	**已鑑識 100 萬台以上端點**	**發現 1,000 起以上其他資安產品未發現的 APT 資安事件**

領先業界特色

輕量佈署、背景執行，不影響日常作業

ThreatSonar 執行程式可安裝到企業組織內上百千台電腦中，背景運行，系統資源使用量少，人員可照常進行電腦工作，不受此程式運行的負擔。

具備記憶體鑑識及行為分析能力，有效揪出未知惡意程式

辨識出隱匿於記憶體中的惡意程式、執行過以及將要執行的程式、攻擊者的駭客工具、攻擊後殘留於主機的紀錄，自動鑑定數百種動態行為異常。

主動威脅狩獵，可視化關聯潛在受害主機

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，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。

關於 TeamT5

v.202605

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

TEAMT5 | THREAT INTELLIGENCE PIONEER, BORN IN ASIA