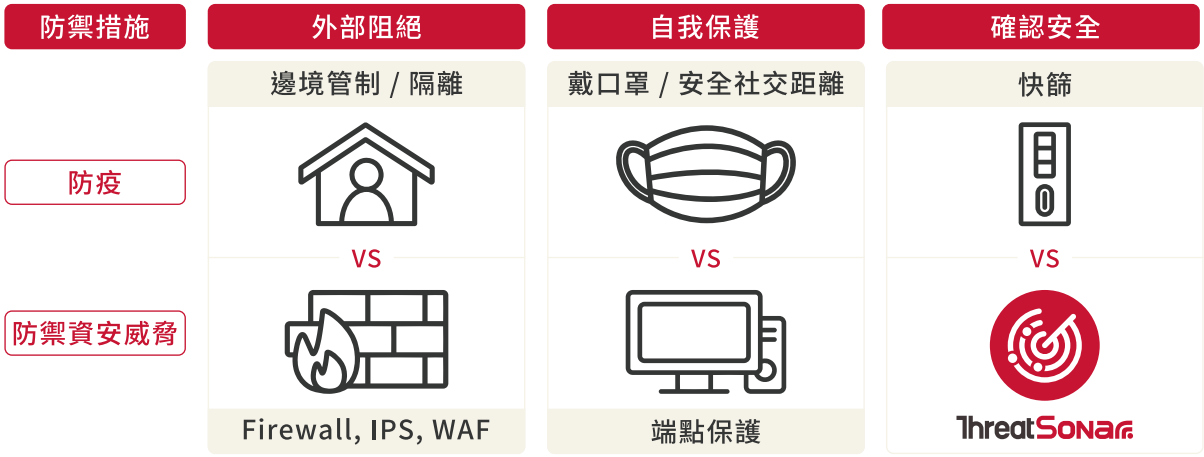
ThreatSonar 威脅鑑識分析平台

情資驅動威脅鑑識，獵捕已入侵 APT 攻擊

APT（進階持續性威脅，Advanced Persistent Threats) 攻擊手法日新月異，往往當攻擊事件被發現時，企業重要機敏資料早已落入駭客手中。因此，及早發現已潛入的威脅攻擊，減少入侵者橫向移動的時間，成為威脅鑑識的首要課題。

防駭如防疫，「知己知彼」情資主動獵捕潛藏 APT 威脅

防駭如同防疫，企業與政府組織採取各項措施來阻絕威脅攻擊，例如架設防火牆外部阻絕、安裝防毒軟體等被動自我保護，如同防疫時管制邊境、戴起口罩等防止疫情擴散。然而，企業與政府組織的資訊環境是否安全，仍需要透過快篩確認。



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，以威脅行為分析前瞻技術與真實案例訓練出的獨家 APT 風險模型，自行研發 ThreatSonar 威脅鑑識分析平台，能快篩檢驗資訊環境安全，真正發掘潛藏的入侵威脅。

效益

發現	超過	完成
1,000 起以上	**九成**	**100 萬台以上**
其他資安產品未發現的 APT 資安事件	台灣網路安全服務供應商採用	端點威脅鑑識

- **彈性部署** 支援落地、雲端管理機制，相容多種虛擬化架構。
- **主動威脅獵捕** 以全球威脅情資研究為後盾，精準鑑識惡意程式，及早發現已入侵攻擊，防範未知攻擊。
- **快速高效鑑識** 每小時可完成 5,000 台端點以上的大規模鑑識。
- **縮短應變時間** 自動調查分析入侵威脅，加速事件處理。
- **作業系統全面支援** Windows, Linux, MacOS

ThreatSonar 如何鑑識威脅？

資料收集與偵測

進階威脅獵捕技術，揪出端點可疑程式、檔案活動，找出潛在威脅。

情資導向鑑識

透過 IOC、威脅情報關聯性，驗證已識別的事件。

分析原因

確定事件如何發生，並鑑定威脅。

事件鑑識報告

包括已確定的威脅和根本原因，記錄評估過程中的所有活動，以供未來參考。

領先業界特色

情資導向的智慧威脅識別

內建數千種 APT 後門特徵，將最新情資帶到每個端點鑑識。同時，可匯入 hash、IP、domain、Yara Rule 與 IoC 等外部情資，高精準度打擊針對性強的潛在威脅。

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。

資安健檢從事件全貌著手，縮短事件調查時程

ThreatSonar 不只分析主機當下狀態，同時透過事件紀錄分析，調查過去的事件軌跡，以 Timeline 事件時間軸呈現先後，並藉由跨端點關聯，追蹤內網移動與資料外流路徑。

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

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