

威脅情資點數：提升情資運用效益

為了協助組織因應不同層級的資安需求，ThreatVision 提供兩種情資點數機制，支援從即時查詢到進階分析的完整流程：

威脅情資查詢點數

(Automated Analysis Points, AAP)

適用於即時查詢與樣本分析，用於快速判斷威脅是否與已知攻擊活動有關。

進階威脅情資分析點數

(Request for Assistance Hours, RAH)

適用於下載特定類型的報告與工具，或提出客製化情資需求。

ThreatVision 威脅情資查詢點數 (AAP)

AAP 提供即時、快速的查詢功能，讓使用者能在第一時間掌握潛在威脅，廣泛應用於告警分類、樣本分析與入侵指標 (IoC) 驗證等工作流程。

AAP 可用於下列功能：

IP / 網域 / 樣本查詢

搜尋可疑 IP、網域或雜湊值時，系統會自動比對並呈現相關攻擊族群、惡意程式與報告資訊。

查閱原始情資 (Raw Intel)

取得尚未產出完整報告的第一手觀測結果，包括攻擊者活動、目標產業與 IoC，讓您在威脅尚未擴大前就掌握初步線索。

可疑樣本分析

上傳可疑檔案後，平台將自動執行分析，提供惡意活動摘要與關聯情資，支援事件初判與主動應變。

AAP 使用提醒：

- 點數為預購制，可依需求彈性加購。
- 針對樣本分析，系統會出現提示訊息，告知將扣除的點數。
- 適用於需快速回應的場景，例如警示分類、IoC 驗證、樣本偵測等。

ThreatVision 進階威脅情資分析點數 (RAH)

RAH 是用於進階支援情境的點數機制，涵蓋特定類型的報告存取、工具下載與客製化情資服務，特別適合需深入分析特定攻擊或解讀威脅趨勢等情境。

RAH 可用於下列項目：

解鎖特定類型的情資報告	下載威脅狩獵工具 (Threat Hunting Tools)	提交客製化情資需求 (Request of Information, RFI)
視所訂閱的情資報告類型而定，使用者可按自身需求，以點數解鎖過往發佈的報告。	包括 YARA、Snort、Sigma 等規則，可立即部署於現有環境中，加速威脅偵測與追蹤。	可針對特定產業、地區或攻擊活動提出需求，並由 TeamT5 分析師團隊提供專屬研究成果與防禦建議。

RAH 使用提醒：

- 點數為預購制，系統會顯示下載項目所需點數。
- 所有使用紀錄可於後台查詢，便於資源管理與追蹤。
- RAH 適用於需深入判斷背景資訊、攻擊來源、關聯樣本等情境。

如何選擇使用 AAP 或 RAH？

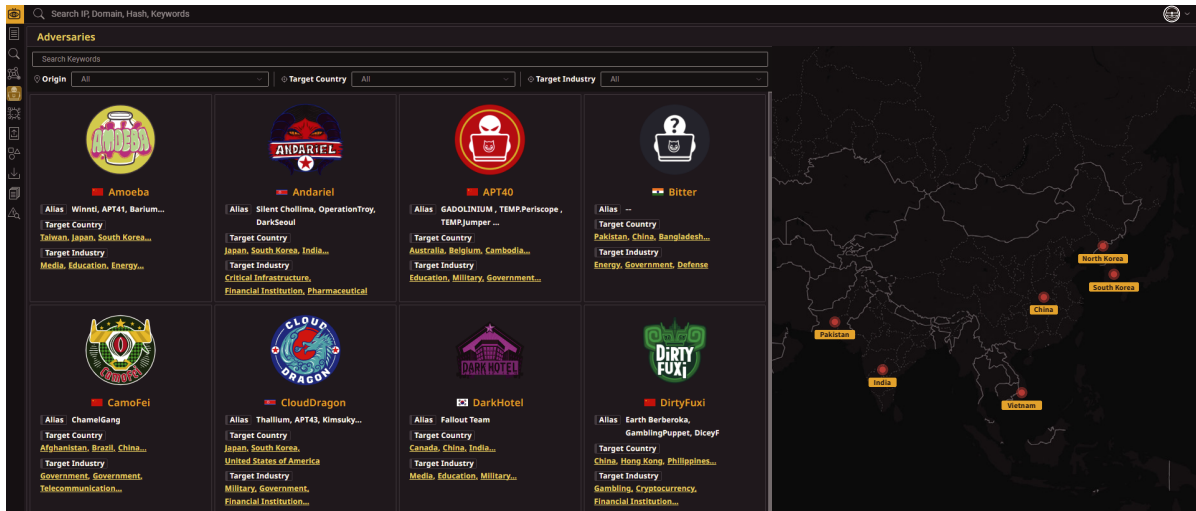
AAP	RAH
• 查詢可疑 IP / 網域是否涉及惡意攻擊 • 上傳樣本進行自動化分析 • 取得原始情資，以利判斷潛在威脅曝險程度	• 存取特定情資報告與威脅狩獵工具 • 提出特定議題的客製化分析需求 • 深入了解特定攻擊行動的技巧和手法

立即啟用，最大化情資效益

無論您是安全應變人員、安全營運中心分析師，還是需快速評估風險的資安長，AAP 與 RAH 點數機制為您提供彈性，可按自身需求取得客製化服務或特定類型的情資。如需進一步資訊，歡迎聯絡 TeamT5 業務團隊，我們將協助您部署最合適的使用策略。

ThreatVision 平台一覽

多元情資支援不同角色與任務，協助組織全面掌握攻擊族群的行為模式、預先部署防禦策略，是從資安戰略規劃到第一線防禦的最佳助力。



如何開始使用 ThreatVision

請聯繫 TeamT5 業務並申請 14 天的 ThreatVision 試用帳戶。如果希望了解產品相關的進一步資訊，請發送電子郵件至 sales@teamt5.org。我們期待與您合作，協助您的組織免受網路威脅。

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。