

威脅入侵指標：精準識別，阻斷威脅

現代資安團隊的困境

隨著組織數位化程度提升，日常資安營運面臨大量無法即時判斷的告警。若缺乏具可信度的線索佐證，將導致調查成本增加、資源浪費，甚至錯失入侵前兆。如果全面依賴外部調查服務，則會受限於成本與反應時效，難以建構持續性防禦。

ThreatVision 提供的高可信度入侵指標 (Indicators of Compromise, IoC) 正是解決此困境的關鍵，能在不增加資安團隊負擔的前提下，有效提升偵測準確度與應變效率，建構持續有效的防禦能力。

5 大特色

跨場景應用 IoC

高可信度資料來源

精準告警觸發

關聯情資整合

自動化整合

4 大效益

降低誤報與告警疲勞

連結威脅來源與攻擊脈絡

支援主動式威脅偵測與追蹤

快速部署有利強化防禦

ThreatVision 威脅入侵指標為何與眾不同？

TeamT5 長期專注於追蹤亞太地區的進階持續性威脅 (Advanced Persistent Threat, APT) 與網路犯罪 (Cyber Crime, CC) 活動，並將第一手觀察轉化為具行為脈絡與技術細節的 IoC。這些獨家 IoC 具備其他平台無法提供的行為脈絡與技術細節，並可直接整合至組織現有的防禦架構，有效提升告警判斷準確度，加快事件回應速度。

ThreatVision 提供的每筆 IoC 均經分析師驗證，使用者可在平台上查詢特定 IP、網域或檔案雜湊值，進一步了解其所涉及的攻擊事件、惡意程式、使用手法與攻擊族群，快速建立事件全貌，採取對應行動，強化組織對高風險攻擊的整體防禦能力。

ThreatVision APT 與 CC IoC 特色

APT IoC	CC IoC
• 聚焦由國家支持或特定任務導向的進階持續性攻擊 • 提供與攻擊族群、惡意程式、使用技術相關的完整脈絡 • 適用於高敏感產業 (如政府、國防、關鍵基礎設施) 進行威脅監控與風險分析 • 每週 1 份，1 年共 52 份	• 涵蓋大規模、非針對性的網路犯罪活動 • 適用於偵測常見威脅，如勒索病毒、釣魚攻擊與憑證盜用等 • 有助於提升日常告警品質，強化對高頻攻擊的即時防禦 • 每週 1 份，1 年共 52 份

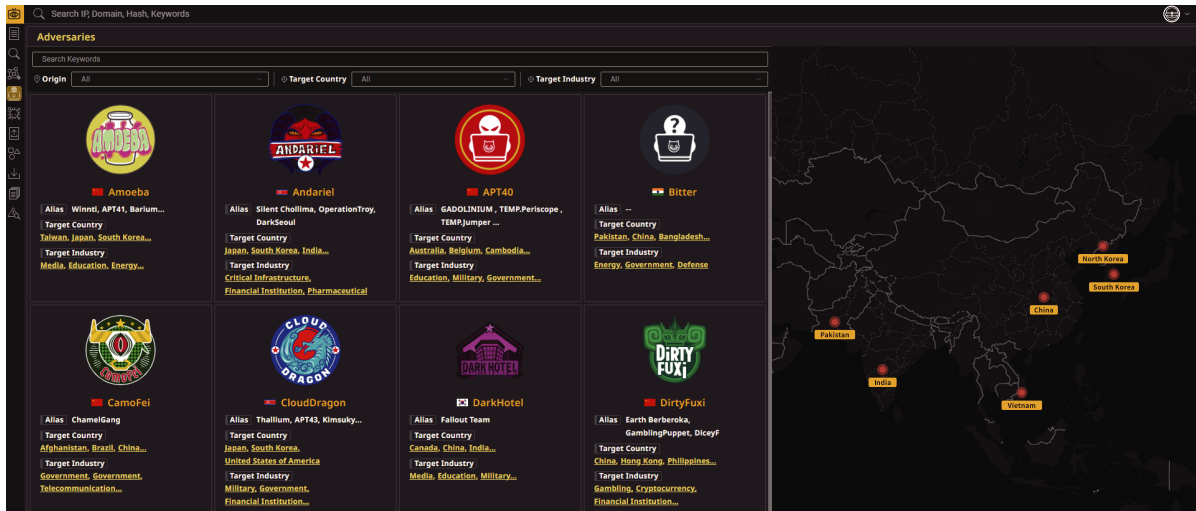
備註 | 在進行 APT 調查時，可能會發現與網路犯罪有關的情資。然而，本文中的 IoC 分類標準係依據事件是否被識別為 APT 攻擊，而非根據具體的網路犯罪類型。

ThreatVision IoC 的多元應用

組織需求	應用實例
需要涵蓋多種威脅來源 以建立有效偵測策略	某高科技製造業導入 ThreatVision APT 與 CC IoC，並分別配置對應的偵測與處理邏輯，顯著提升告警回應準確度與效率
需要可信任的指標 以提升威脅掌握能力	某政府單位需針對特定國家級攻擊行動進行威脅監控，導入 ThreatVision APT IoC，確保情資具可追溯性與技術脈絡，作為資安風險分析的依據
需要提高告警品質與準確性 以強化即時防禦	某金融服務業者導入 ThreatVision CC IoC，用於偵測異常登入行為與連線，降低資料外洩風險
需要自動化情資串接 以提高防禦效率	某大型企業利用 API 串接將 ThreatVision IoC 自動導入其 SIEM 平台，實現即時更新與策略規則套用，大幅減少人工處理時間與錯誤風險
需要快速掌握攻擊脈絡 加快事件調查速度	事件應變人員於 ThreatVision 中查詢某個已觸發的 IoC，進一步取得對應的惡意程式分析與攻擊族群資料，快速建立攻擊脈絡，加速調查行動
需要標準化格式 簡化跨平台整合與應用	某資安代管廠商透過 ThreatVision 的 STIX 與 CSV 格式 IoC，無縫整合入服務流程，快速部署於客戶的防禦系統，並支援報告自動化作業

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。