

原始情資：掌握威脅的關鍵起點

來自專家團隊的 ThreatVision 原始情資

ThreatVision 的原始情資 (Raw Intel) 由 TeamT5 分析師於第一線研究過程中產出，提供尚未公開、具潛在風險的重要觀察結果。對於需要即時判讀可疑活動的資安團隊而言，這些原始情資能在完整情資報告產出前，先行掌握潛在威脅的線索，補足時效性與細節不足的情資空窗。

舉例來說，當分析師在追蹤惡意樣本或基礎設施時，發現可疑的 IP、網域或雜湊值，即會以原始情資形式記錄在案，供使用者查詢與比對。這項功能讓具備分析能力的團隊能快速研判後續調查方向，或強化現有的防禦邏輯與回應效率，進而加快威脅識別流程、降低錯失先機的風險。

資訊 vs. 情資

ThreatVision 的原始情資屬於資訊，而非情資。資訊 (Information) 通常是尚未經過完整驗證和分析歸納的原始觀察結果，具有即時性與潛在線索價值，但仍需仰賴分析師判讀與交叉比對。情資 (Intelligence) 則是在大量資訊基礎上，經過驗證、研判與架構化整理後所產出的成果，能夠提供明確的行動依據與策略價值。原始情資的價值，在於補足時效性與潛在威脅相關細節的空缺。在正式情資報告尚未產出前，分析師會先紀錄可疑的 IoC、惡意樣本或相關基礎設施等初步觀察結果，作為後續調查的基礎。對具備分析能力的組織而言，這些內容能快速指引後續研判方向，或補強事件調查中尚未掌握的環節。因此，TeamT5 建議資安團隊可視風險需求，將原始情資納入初步分析流程，並在必要時聯繫 TeamT5 取得完整情資或支援。

原始情資的效益

在取得情資報告前即可獲得相關線索，
即時掌握新興威脅

原始情資提供尚未公開的最新觀察結果

協助分析團隊提早掌握可疑活動

加快事件反應速度與風險判讀能力

兩步驟取得 ThreatVision 原始情資

步驟一：根據搜尋結果來識別

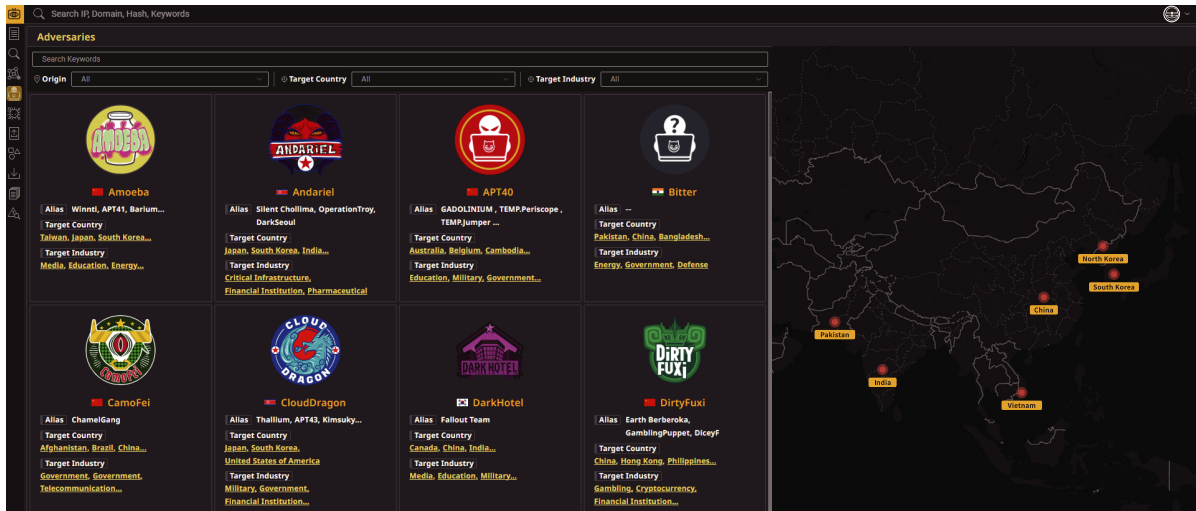
在以關鍵字查詢（如 IP、網域、雜湊值等）後，若該項目有對應的原始情資，系統將於結果頁面的「原始情資」分頁標示數量，使用者切換至該分頁即可檢視初步內容。

步驟二：使用點數解鎖以取得原始情資

為控管存取權限，詳細內容會先予以遮蔽。使用者可用點數解鎖以取得完整資訊，內容包含受害對象、關聯攻擊族群、惡意程式與野外利用狀態等，協助快速掌握威脅脈絡。

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。