

威脅狩獵工具：主動防禦的利器

情資驅動的 主動防禦工具

ThreatVision 提供下載即用的威脅狩獵工具 (Threat Hunting Tools)，協助組織快速掌握自身環境中的潛在威脅，並強化內部資安流程。這些工具由 TeamT5 分析師團隊打造，旨在協助組織主動發現攻擊者使用的工具、後門與行動痕跡。

資安痛點的最佳解方

涵蓋多型態與變異樣本	精選規則減輕分析負擔	關聯情資構建攻擊脈絡	可直接部署於現有系統
惡意程式會持續變種並改變行為模式，我們提供涵蓋變異樣本的 YARA、Sigma 等偵測規則，可有效識別多型態攻擊行為。	當日誌與告警數量過大時，我們提供的精選規則可先行過濾低相關性事件，協助分析人員快速聚焦異常行為，減少誤報與不必要的調查。	僅有技術指標不足以判斷威脅真實性，我們提供關聯攻擊族群、相關樣本與 TTP 等可構建脈絡的情資，以利評估事件的影響範圍與應對優先順序。	在資源與人力有限的情況下，我們提供的工具可直接匯入現有資安系統 (如 SIEM、TIP)，縮短威脅狩獵啟動時間。

一鍵下載所需工具

在平台首頁即可查看最新釋出的威脅狩獵工具，分為偵測標的 (惡意程式或漏洞) 和工具類型 (YARA、Snort、Sigma 等)。系統會依發佈時間自動排序，便於使用者依需求一鍵下載。

效益

快速掌握威脅現況 協助使用者快速了解潛在威脅與異常行為，以利判斷與因應。	強化未知攻擊偵測 透過更新的偵測規則與進階分析工具，強化對變異型惡意程式與新型攻擊的識別能力。	整合自動化流程 偵測規則皆為 YARA、Snort、Sigma 等標準化格式，便於整合至現有資安架構與自動化流程。
提高漏洞應對效率 快速確認漏洞是否已遭利用，協助優先修補真正有風險的系統與資產。	擴大防禦範圍 不只能偵測惡意程式，也能識別漏洞利用，提升主動防禦能力。	

// 適用對象

組織資安團隊 主動導入威脅狩獵機制，強化整體偵測與應變力。	安全營運中心分析師 用於過濾告警、驗證 IoC 並輔助判斷威脅事件，提升調查效率。	事件應變人員 利用工具對樣本行為與 TTP 進行比對，快速建立攻擊脈絡與溯源。
資安工程師 整合 YARA、Snort、Sigma 規則至現有架構，提升偵測精確度與自動化程度。	資安決策者 依據偵測結果調整修補策略與資源分配，有助於策略性防禦規劃。	

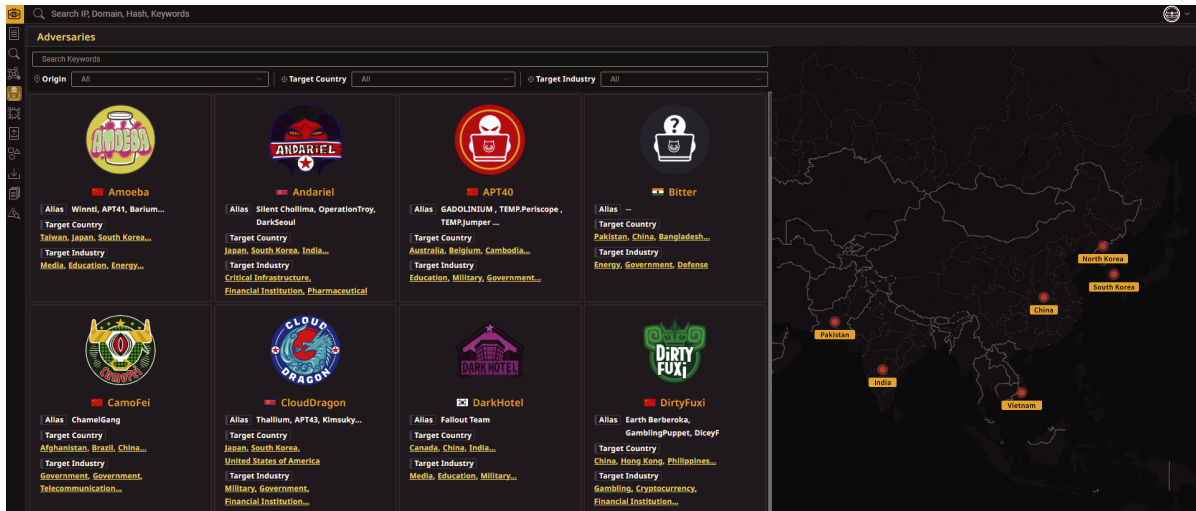
// 多元應用情境

ThreatVision 威脅狩獵工具涵蓋多種偵測需求與情境，主要分為三類：

- 多種偵測規則**
提供 YARA、Snort、Sigma 等規則，可自訂條件比對攻擊模式，協助快速偵測檔案或行為異常，適用於主機端或自動化平台的行為比對與樣本掃描。
- 惡意程式狩獵工具**
針對高風險惡意程式(如 ShadowPAD)所設計，辨識其變異行為與進階技巧，補強傳統防毒與簽章比對的不足。
- 漏洞偵測工具**
根據情資報告揭露的漏洞與攻擊行為而設計，可有效辨識漏洞是否遭利用及其影響範圍，並偵測與漏洞攻擊有關的惡意樣本或程式。

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。