Datasheet

ThreatVision

TEAMT5

以專家情資驅動資安決策
強化防禦韌性

ThreatVision 威脅情資平台

ThreatVision 威脅情資平台根基於 TeamT5 逾 20 年來針對亞太地區惡意程式、進階持續性威脅 (APT) 攻擊族群與網路威脅的研究經驗，專為組織提供聚焦亞太的高品質情資。平台整合戰略、實戰與戰術層級的情資，支援決策者、風險管理人員與事件應變團隊，掌握威脅態勢、識別攻擊者，並強化整體防禦部署。

除了專業深入的情資報告，ThreatVision 同時也提供深暗網威脅情資，專為組織偵測早期警訊與資料外洩風險而設計，涵蓋深暗網論壇、交易市場、中文地下社群、社群媒體等範圍。搭配每週自動告警和客製化監控分析報告，讓組織能在威脅醞釀時就掌握狀況，無須等到威脅成為實際風險時，才著手應變。

平台關鍵數字

1,800+	670 萬+	2,600 萬+	3,100+	300+
情資報告	入侵指標	威脅樣本	惡意程式	攻擊族群

ThreatVision 核心特色

威脅入侵快速識別

整合多種 IoC 來源，迅速辨識潛藏攻擊與惡意活動，提升防禦效率。

威脅入侵快速識別

提供樣本上傳與分析，快速掌握惡意特徵，支援事件因應與調查。

完整掌握攻擊全貌

快速關聯惡意程式與攻擊族群，還原攻擊脈絡並掌握其動機與目標。

亞太威脅情資的專家

深耕亞太的專家團隊定期提供分析報告，詳解攻擊手法、目標與威脅態勢。

即時查詢所需情資

可即時查詢 IP、網域和樣本並取得原始情資，亦提供客製化報告與工具等進階服務。

快速整合與自動化

快速串接 TIP、SIEM 等平台，自動化推送情資，加快事件回應與處置流程。

威脅情資的重要性

TeamT5 將情資分為三大層面，分別支援各類型資安團隊中的不同角色，滿足從高階決策到第一線防禦的多元需求，包括：

戰略型威脅情資
協助決策者綜觀全局

對資安長與高階決策者而言，戰略型威脅情資至關重要，不僅能掌握網路威脅對營運的潛在衝擊，也可結合全球資安事件與政策變化，有利於制定整體防禦策略與資源規劃。

實戰型威脅情資
協助資安團隊有效應對

實戰型威脅情資著重於攻擊族群的動機、行動，以及其所使用的戰術、技術與程序 (TTP)，對資安營運中心 (SOC) 與事件應變團隊制訂優先應對策略至關重要。

戰術型威脅情資
協助前線人員快速應變

戰術型威脅情資提供可直接應用的 TTP 技術資訊，有助於偵測與防禦調整，是 IT 團隊與前線防禦人員應對威脅的實用工具。

深入了解 ThreatVision 報告

ThreatVision 提供四大類型的情資報告：亞太 APT 情資、漏洞情資、中文網路世界與中國網路政策，以及網路犯罪情資，協助組織進行明智決策，取得應變優勢。

APT 威脅情資週報
(APT in Asia Flash Reports，又稱 Flash Report)

聚焦最新 APT 攻擊事件，解析手法和技術細節，並提供相關入侵指標 (IoC)。Flash Report 每週發佈兩次，一年至少 100 份。

APT 威脅情資月報
(APT in Asia Monthly Reports，又稱 Monthly Report)

摘要過去一個月內亞太區 APT 攻擊動態，並連結地緣政治情勢與攻擊行為，平均涵蓋 13 至 16 起事件，提供相關入侵指標 (IoC)。Monthly Report 每月發佈一次，一年共 12 份。

APT 威脅族群追蹤季報
(APT Campaign Tracking Reports，又稱 CTR)

深度分析威脅族群、攻擊戰術、目標範圍，提升對亞太地區重要威脅族群和攻擊活動的全面了解。CTR 每季發佈兩次，一年共 8 份，包含 6 份威脅族群分析報告及 2 份半年威脅情勢分析報告。

亞太區域網路政策雙週報
(Cyber Affairs Biweekly Reports，又稱 Biweekly Report)

深入分析新興強權中國的網路能力，以及中文網路世界的網路安全新聞、政策法規和資安事件。Biweekly Report 每兩週發佈一次，一年共 24 份。

漏洞情資暨應對緩解雙週報
(Vulnerability Insights Reports，又稱 VIR)

每次專注於一個關鍵漏洞，提供關鍵漏洞的詳細技術情資，以及可能的攻擊情境與檢測工具。VIR 每兩週發布一次，一年共 24 份。

漏洞修補管理週報
(Patch Management Reports，又稱 PMR)

彙整約 100 個高危漏洞，包含攻擊概念驗證 (PoC)、受影響產品與修補建議，有利排定修補優先順序。PMR 每週更新一次，一年共 52 份。

網路犯罪情資報告
(Cybercrime Reports，又稱 CC Report)

奠基於長年對深暗網、地下論壇與犯罪社群的追蹤與研究，內容包含網路犯罪活動研析報告 (每月發佈一次，一年共 12 份)；暗網論壇動態與勒索軟體動態 (兩種每月至少各 4 篇，一年至少各 48 份)。

ThreatVision 關鍵亮點

APT / 網路犯罪 IoC

APT IoC 聚焦於國家級攻擊；網路犯罪 IoC 強化對大規模網路犯罪活動的防禦能力。兩種 IoC 皆為每週 1 份，1 年各 52 份。

威脅狩獵工具

提供專家設計的規則，用於掃描環境、發現威脅並加速調查。

資訊需求服務 (RFI)

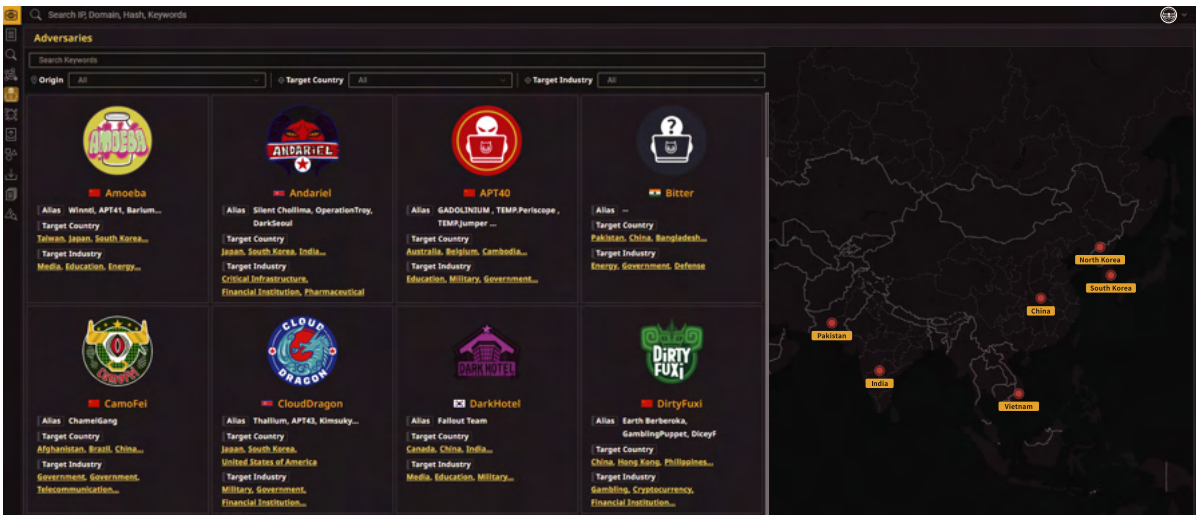
針對特定議題或攻擊行動，提供量身定制的研究，協助進行風險評估與防禦。

API 服務

支援將情資自動化整合至既有平台，加速部署並確保穩定運作。

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。

Tel 02-7706-1299
E-mail sales@teamt5.org

TEAMT5 | THREAT INTELLIGENCE PIONEER, BORN IN ASIA