ThreatVision

A Portal to See Through the Chaos

TEAMT5 杜浦數位安全

Email sales@teamt5.org
Tel +886-2-7706-1299

深入了解 ThreatVision 報告

ThreatVision 的情資報告分為三類：亞洲 APT 情資、漏洞和網路政策與事件。 這些報告為決策和應變提供了寶貴的洞察。

APT 威脅情資週報
APT in Asia Flash Reports

提供及時、準確和可行動的情資，與最新 APT 入侵的即時告警。快報每週發布兩次，詳細說明特定的目標攻擊，並提供所有必要的 IoC。

APT 威脅情資月報
APT in Asia Monthly Reports

提供了亞太地區的戰略性和可行動的情資，將網路攻擊與最近的政治事件、政策和外交事務串接起來。報告每個月發布一次，摘要過去一個月內，亞太地區 13 到 16 個 APT攻擊事件。

亞太區域網路政策雙週報
Cyber Affairs Biweekly Reports

提供有關中文網路世界的戰略網路情資，用戶可以了解新興強權中國的網路能力。雙週報每兩週發布一次，快速回顧中文網路世界的網路安全新聞、政策、法規和入侵事件。

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

提升對於亞太地區重要威脅族群和攻擊活動的全面了解。在每個季度末發布兩篇 CTR，深度分析威脅族群、攻擊戰術、目標範圍。此外，在第二季度和第四季度末，會提供一份半年度的 APT 威脅情勢報告。

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

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，每次專注於一個關鍵漏洞。

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

針對關鍵漏洞提供所有相關訊息，協助確認修補管理的優先順序。PMR 每週更新一次，摘要出約 100 個重大漏洞，與受影響的產品、修補的詳細資訊。

威脅情資的重要性

TeamT5 歸納出情資的三大層面包括

戰略型威脅情資

戰略威脅情資對於負責決策的 C 層級高階經理人至關重要，不僅能了解網路威脅對公司營運帶來的風險，更可借助於全球網路事件和政策的分析，做出明智的決策。

實戰型威脅情資

實戰型威脅情資側重於了解威脅族群、背後動機及其戰術、技術和程序 (TTP)，確立應變優先順序並調整策略，對於資安營運中心（SOC）和事件應變團隊來說至關重要。

戰術型威脅情資

戰術威脅情資提供實用的具體 TTP 技術資訊，可直接應用於改善防禦和偵測威脅，並調整安全措施以有效應對新興威脅，是 IT 團隊和第一線資安防禦者應對事件的利器。

如何開始使用 ThreatVision

請聯繫您的 TeamT5 代表並申請 14 天的 ThreatVision 試用帳戶。

若您希望了解此產品更多細節，請發送電子郵件至 sales@teamt5.org。

我們期待與您合作，確保您的組織免受網路威脅。

ThreatVision

A Portal to See Through the Chaos

TEAMT5 杜浦數位安全

Email sales@teamt5.org
Tel +886-2-7706-1299

什麼是 ThreatVision?

憑藉針對亞太地區惡意程式、APT（進階持續性威脅）族群和網路威脅的十多年研究經驗，ThreatVision威脅情資平台專為組織，提供以亞太地區為中心的豐富網路威脅情資。

平台透過提供戰略、實戰和戰術威脅情報，來滿足網路安全領域的不同角色，包括決策者、風險管理者和事件應變人員，協助 C 層級的高階經理人、風險經理和事件處理人員了解威脅形勢、識別惡意行為者並部署有效的網路威脅防禦。

ThreatVision 提供可客製情資調查與諮詢服務，以及其易於使用的介面和精選報告，協助組織能做出明智的決策，有效地分配資安資源，並增強網路安全。

ThreatVision 核心特色

01
威脅入侵指標 (IoC)

IoC　提供快速威脅辨識，並可做為追蹤企業內攻擊源的重要線索。

02
威脅狩獵工具

威脅狩獵工具提供直接檢測，能快速了解當前環境並識別潛在問題。

03
情資報告

情資報告提供駭客行為的分析、深度了解其攻擊手法與背後動機。

04
攻擊者與惡意軟體資料庫

提供惡意族群和程式的第一手資料庫，有助於了解威脅。

05
資訊需求服務 (RFI)

分析師提供用戶客製化報告與工具服務，實現個別化情資。

06
API 服務

快速整合平台資源，實現情資自動化。