ThreatVision

A Portal to See Through the Chaos

ThreatVision 如何協助亞太地區政府應用威脅情資

許多亞太地區政府部門採用 ThreatVision，希望藉其增強網路安全態勢，並改善對亞太地區主要攻擊者如中國、北韓、南韓、巴基斯坦、越南和印度等地的防禦。

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、營運和戰術威脅情資，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。

亞太地區政府的情資需求

一般來說，我們的亞太地區政府客戶需要威脅情資平台，但他們沒有足夠的資源來自行過濾和分析數據。他們期望能夠了解對手的活動、研究誰是攻擊背後的攻擊者，並知道誰在亞太地區受到攻擊。如果沒有這類情資，就會面臨很高的被攻擊風險。

ThreatVision 對亞太地區政府的效益

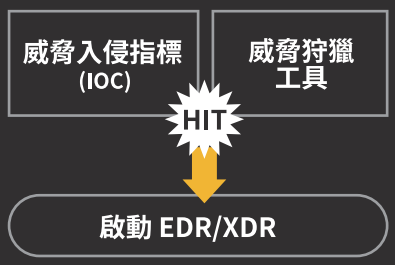
ThreatVision 所提供詳細的報告和技術工具，可滿足亞太地區政府客戶的情資需求。ThreatVision 能讓亞太地區政府深入了解對手的活動、戰術、技術和程序，並加強主動防禦措施，面對不斷變化的網路威脅保持領先。除了為合作夥伴提供威脅入侵指標（IoC）、為管理階層提供詳細簡報外，能夠進行樣本分析，以及客製化分析環境中發現的可疑樣本。

TEAMT5 杜浦數位安全 | Tel +886-2-7706-1299 | E-mail sales@teamt5.org

亞太地區政府如何使用 ThreatVision

亞太政府客戶如何應用 ThreatVision 威脅偵測？

01 偵測



02 研究

- 威脅態勢
- 攻擊族群
- 惡意程式
- 樣本管理

03 結果

- 惡意程式偵測
- 了解威脅
- 了解攻擊者 TTPs
- 防堵未來的攻擊

在威脅偵測方面，亞太地區政府客戶通常使用 ThreatVision 的威脅入侵指標（IoC）和威脅狩獵工具來偵測入侵。在啟動 EDR / XDR 後，透過 ThreatVision 提供的威脅態勢、攻擊者族群、惡意程式和樣本管理功能，啟動威脅研究。最終達成能夠偵測惡意程式、更了解威脅與攻擊者的 TTPs，並阻絕未來的攻擊。

亞太政府客戶如何應用 ThreatVision 威脅情資？

01 洞察

- APT 威脅族群追蹤季報
- 亞洲 APT 威脅情資快訊報告
- 亞洲 APT 網路威脅情資月報
- 亞洲網路政策雙週報
- 漏洞情資暨應對緩解雙週報
- 漏洞修補管理雙週告

02 報告與防禦

- 項管理階層報告
- 執行防禦措施以減少風險

03 結果

- 優化資安政策
- 預算決策更加輕鬆
- 強化資安環境
- 高豐富度的洞察

在威脅情報方面，客戶可從 ThreatVision 的許多不同報告中獲得情資洞見。協助他們隨後向上級報告調查結果，並採取預防措施，以降低風險。最終達到資安政策優化、預算決策變得更加輕鬆、強化資安環境，並且獲得高豐富的威脅形勢洞察。

如何開始使用 ThreatVision

請聯繫您的 TeamT5 業務並申請 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。

TEAMT5 杜浦數位安全 | Tel +886-2-7706-1299 | E-mail sales@teamt5.org