



Protect Your Business Against API Vulnerabilities

儘管大家對 API 安全意識體認日益增強,但涉及 API 的攻擊和數據洩露仍然頻繁發生

根據 Gartner 的 API 安全報告:「使用通用應用程式安全解決方案保護 Web API 仍然是無效的,因為每個新的 API 端點都會在系統中增加一個潛在並獨特的攻擊媒介。



現有解決方案未能兌現其安全承諾:

現有解決方案基於規則/啟發式,但業務營運和 API 非常複雜且是動態的.因此,現有方案不可能創建一個穩定的數據規則庫,而且這個規則庫會隨著時間的推移覆蓋所有可能的情況

IMVISION API 異常管理平台

API Anomaly Management Platform (AAMP)

✚ 在商務流程執行下分析提供服務的 APIs

✚ 使用 NLP 技術來自動學習，並建立適當的 API 使用模式



功能：

- ✓ 自動識別並顯示網域內的所有 APIs，為每個端點提供風險估量分析
- ✓ 自動學習 API Calls 的行為模式並發現其商業邏輯及流程，檢測到任何影響業務活動的異常情況
- ✓ 對有危害的 API 交易異常進行嚴重性對應分析，在攻擊到達公司核心資產前將其自動阻擋
- ✓ 自動偵測有攻擊意圖的 API 事件，早期發現-定義具攻擊意圖的模式，易讀取的攻擊事件描述

商業價值：

- ✚ 完全的自動化 – 無須人為的調校
- ✚ 高準確性- 0.001% 錯誤判斷率
- ✚ 自動化的判定及預防

