uSecure SIEM 資安事件管理系統

提升資安威脅管理、協同作業、與事件識別準確率

uSecure SIEM是一款以日誌管理與分析為核心功能的 SIEM 產品。能協助集結所有事件管理與分析需求為一身，提供完整資安日誌分析、資安情資報表與關聯告警SIEM功能，以輕鬆掌握資安維運狀態。

現今網路設備、伺服器與資安產品繁多，對 IT 人員來說，訊息完整的 Syslog Data 日誌軌跡保存與資安稽核調閱需求極為重要，資安法與個資法符規要求也與日俱增，uSecure SIEM能協助您集結所有事件管理與分析需求為一身，提供完整資安日誌分析、資安情資報表與關聯告警SIEM功能，使企業輕鬆掌握資安維運狀態。

- 資安設備系統日誌彙整收集
- 原始日誌保存稽核
- 異質紀錄綜合查詢
- 圖形化彙整分析
- 異常行為關聯警訊能力

功能特色

- ✓ 多樣化日誌收容及完整保存機制，確保資安事故管理完整性與可靠性
- ✓ 直觀視覺的儀表板與分析圖，資安事件可視化
- ✓ 日誌收容與情報收集，原始日誌保存稽核
- ✓ 內建關聯告警快篩功能，異常行為關聯警訊分析能力
- ✓ 持續依內建關聯規則，篩檢侵入行為或可疑事件，洞察資安威脅、預警通報
- ✓ 採已知特徵基礎及行為模式，自動偵測及發現異常
- ✓ 參考資安攻擊鏈各階段設置對應，制定精要的關聯機制
- ✓ 內建支援多項資安設備整合，自動解析關鍵資訊做為儀表分析及關聯分析的分析因子
- ✓ 支援ISAC STIX情資交換格式

uSecure SIEM 資安事件管理系統 / 每套 / 1年軟體授權

- 系統安裝需求:
  - 作業系統：虛擬化系統
  - 處理器 ： 8 核心(含)以上
  - 記憶體 ： 32 GB(含)以上
  - 安裝磁碟： 100 GB(最少) (日誌儲存之硬碟空間由使用單位自行準備)
  - 處理效能： 1,000 EPS (Events per Second)