數聯資安

uSecure SIP
化繁為簡 掌握資安威脅

在巨量化事件資料中，及時有效的洞悉新興資安威脅。

uSecure SIP為新世代資安戰情平台，具備資安資訊事件管理(SIEM)功能所需能夠將企業環境中重要的資安防護裝置、各類作業系統與應用系統等，所發生的資安相關資訊紀錄進行彙集分析。更進一步提供四大優越特性：情境感知、智能化驅動、歷史資料回溯、及行為異常分析的機制，透過大數據分析、機械學習及人工智慧等先進的科技，能夠高效率粹取出更有實質助益的資安情資，並透過容易理解辨識的可視化方式表達呈現，避免傳統型態的SIEM系統對於資安訊息過於龐雜，造成企業資安管理者無法有效率掌握正確資安情資，適得其反而延宕主要資安威脅事件的處理作業。

監控　智能化驅動　大數據分析　即時預警

情境感知：
圖像化儀表板及資安天氣圖情境呈現資安狀態，協助資安管理者提前預測並採取抑制或防範措施

智能化驅動：
透過大數據演算能力搭配智能化事件關聯引擎，從乍看無關資訊發掘並主動列舉未知可能威脅

歷史資料回溯：
透過歷史回溯及軌跡資料分析，了解駭客入侵的真實時點，提早察覺已經潛伏且沉默的異狀變化

行為異常分析：
透過AI智能化的規則方法，察覺存在於特定裝置中，如大量連線、密碼猜測、異常帳號登入、異常網路連線等行為異常分析

數聯SOC維運經驗 x 大數據領導品牌Splunk

雙強聯手，豐富經驗更能有效著手解決您的問題

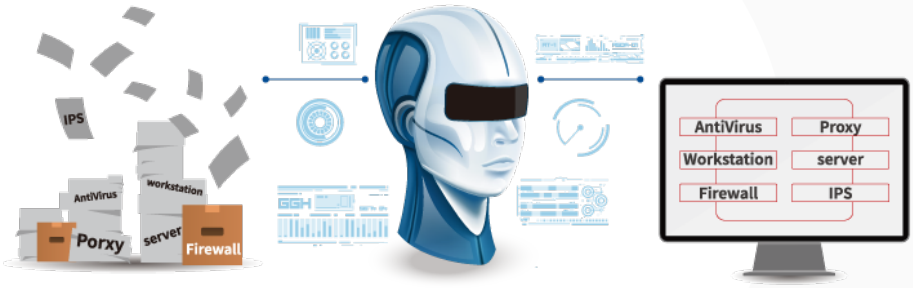
融入數聯資安長期在SOC資安維運服務上的專業經驗所彙集之新世代資安事件管理平台(NG-SIEM)，結合U-SOC資安監控服務超過180個客戶、1400台以上資安設備、及持續營運超過10年的在地經驗，孕育而生uSecure SIP資安戰情平台。

搭載業界最強的大數據引擎領導者Splunk Enterprise作為主要的處理核心，其運用No-SQL技術能大幅改善傳統的資安資訊事件管理(SIEM)方案在處理耗損效能及反應速度慢的問題瓶頸。對於企業面對駭客威脅得以即早察覺及預測，達到主動監控、鎖定、處理並遏止資安攻擊的發生。

uSecure SIP 優勢

資安情資彙整搜集，高效率資安戰情事件管理

- 支援多元資安防護裝置、作業系統與應用系統，快速收集各式日誌，無需複雜程式或語言，將資安設備無痛整合於uSecure SIP。
- 智能化情境感知監控機制，採取易讀易懂圖像表達呈現資安威脅狀態，協助管理者提前預測並採取抑制或防範措施。
- 透過大數據演算能力搭配AI智能化事件關聯引擎，以機器學習建立 Baseline，從乍看無關的資訊中發掘並主動列舉未知可能威脅。
- 串接最新資安情資單位情報，透過歷史回溯及軌跡資料分析，了解駭客入侵的真實時點，提早察覺已經潛伏且沉默的異狀變化。



uSecure SIP 效益

SIP資安戰情首選‧掌握資安威脅，準確即時告警

提升資安威脅管理協同作業：
上層管理者（CISO）、資安管理者（IT）、稽核人員、以及專家人員（資安顧問服務、設備系統廠商），都能在共同的SIEM資安情資基礎進行資安維運，建構完整SOC維運中心

提供資安的可視化與能見度：
具備關聯性的可視化檢視方法，資安管理者於uSecure SIP系統介面能夠快速、簡單、直覺的操作方式，進行事件根源的探查跟情報掌握

提升資安事件管理能力：
內方便簡易資安事件通報與指派處理的設計，有助於企業資安維運中心的管理者能夠追蹤資安事件處理，避免資安事件處理作業停擺或傳遞過程中斷的狀況

提升重要資安威脅事件的識別準確率：
可以從龐雜的資安威脅事件中淬濾出真正的關鍵資安威脅情資，有助於企業資安管理者的處理人力投入與資源分配

提升資安威脅的預測警覺能力：
攻擊發布前便已經透過各項關聯的異常行徑，預先察覺已經發生的威脅趨勢，幫助企業資安管理者提早做出預防性的決策