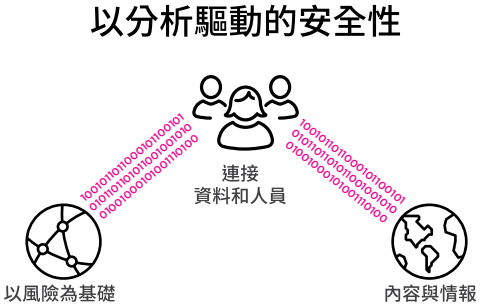
SPLUNK® ENTERPRISE SECURITY

以分析驅動的安全性與對當今威脅的持續監控

- 使用可調適的回應與調查工作台，以更快速的回應時間**最佳化安全維運**
- 使用包含雲端和內部部署的所有機器資料的端對端可見度**改善安全狀態**
- 使用使用者行為分析偵測異常狀況與威脅**提升調查能力**
- 利用威脅情報**做出更明智的決策**



您眼前的難題包括適應動態威脅環境、不斷演變的敵人策略、先進的威脅，以及不斷變化的業務需求 - 而您現有的安全技術卻跟不上。為了解決這些新挑戰，現代的安全團隊需要分析能力與關聯式事件回應；而且他們必須能迅速實作新的威脅偵測技術，以縮短回應威脅時間，並做出以業務為中心的決策。藉著集中處理及利用所有機器資料，安全團隊得以更快速偵測、回應及中斷攻擊。

Splunk Enterprise Security (Splunk ES) 是一款**安全資訊和事件管理 (SIEM) 解決方案**，可讓安全團隊快速偵測及回應內部與外部攻擊、將風險減到最小，同時簡化威脅管理，並保護您的業務安全。**Splunk ES** 可讓您的安全團隊使用所有資料以取得整個組織的可見度和安全情報。不論部署模型為何 (包括內部部署、公用或私有雲端、SaaS 或任何組合)，**Splunk ES** 都能用來進行持續監控、事件回應、執行安全維運中心，或為高階主管提供對業務風險的了解。**Splunk ES** 可搭配 **Splunk Enterprise** 部署成軟體，或搭配 **Splunk Cloud** 部署成雲端服務。

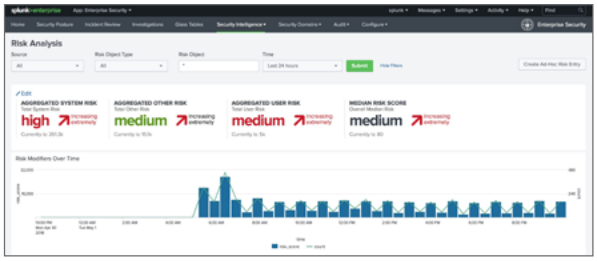
Splunk ES 可協助安全團隊，為所有規模與專業等級的組織簡化安全維運。它提供：

- **對資料的深入見解**，從網路、端點、存取、惡意軟體、UBA 異常、弱點和身分識別技術自動擷取資料，並使用預先定義的規則或透過隨選搜尋，來共用以產生關聯
- **現成的警示管理功能**和強大的動態探索、關聯式搜尋，以及快速偵測與**分析先進威脅**
- **彈性的自訂化**：不論其部署目的是為了持續監控、事件回應、安全維運中心 (SOC)，或是需要檢視業務風險的主管，皆可自訂關聯搜尋、警示、報告和儀表板，以滿足特定需求
- **提升營運效率**，使用以工作流程為基礎的內容，實現自動與人為輔助的決策

以分析驅動的安全性，定義了所有安全相關資料 (包括 IT 基礎架構、端點安全產品和所有機器產生的資料) 的關係探索程序，可迅速適應不斷變化的威脅狀況。

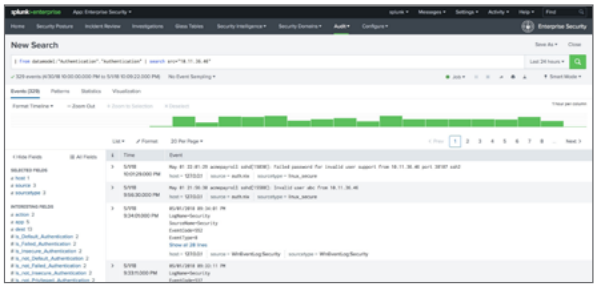
持續監控安全狀態

使用全方位預先定義的儀表板、具備重要安全指標、重要效能指標、統計與動態閾值的自訂單一管理平台檢視，以及趨勢指標，可清楚了解您組織的安全狀態。



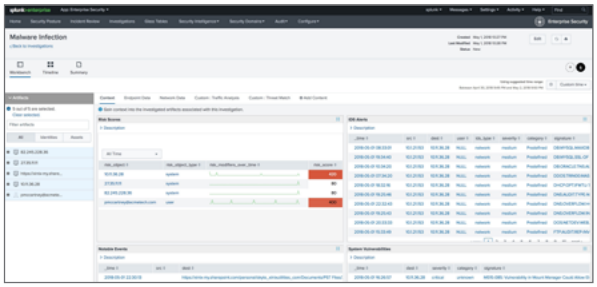
排定事件的優先順序並採取行動

使用集中的日誌、警示和事件、UBA 異常、預先定義的報告和關聯性、具備風險分數的事件回應工作流程，以及安全特定檢視的相關性，為個別分析師或調查團隊最佳化事件回應工作流程。使用調查工作台，在單一檢視中調查一或多個值得注意的事件，可簡化調查並加速事件回應。



快速調查威脅

使用隨選搜尋來執行快速調查，並使用靜態、動態和視覺相關性來提升回應時間。調查從安全性與 IT 堆疊自動擷取的所有資料及跳轉到任何欄位，可快速開發威脅關聯性，並追蹤攻擊者步驟以驗證證據。使用可調適的回應動作來自動化及最佳化威脅偵測與補救，以便在多供應商的環境中自動擷取、共享及回應。



處理多步驟調查

執行入侵與調查分析，以追蹤與遭駭系統相關聯的活動。使用隨選搜尋和所有 ES 功能，結合調查時間軸與調查工作台，來套用獵殺鏈方法並調查攻擊生命週期。此外，ES 內容更新 (一項訂閱服務) 可讓分析師和調查員持續改進並加速對威脅的回應，不受定期軟體更新的影響。

立即試用 Splunk Enterprise Security 體驗 Splunk Enterprise Security 的力量 — 無需下載、不用安裝硬體，也不需要任何設定。Splunk Enterprise Security 線上沙箱是一個 7 日評估環境，具有預先填入的資料，佈建於雲端，可讓您搜尋、可視化及分析資料，並徹底調查廣泛安全使用案例的事件。您也可以遵照逐步教學課程，引導您完成 Splunk 軟體所提供的強大視覺化與分析功能。了解更多資訊。

聯繫Splunk台灣團隊：https://www.splunk.com/zh_tw/talk-to-sales.html
www.splunk.com
台北市信義區松仁路 100 號 台北南山廣場 37 樓