SPLUNK® ENTERPRISE SECURITY

針對新型態威脅，以分析技術為基礎的資訊安全防護和持續監測，確保資安無漏洞

- **優化資訊安全的營運，**快速回應資安攻擊
- **提昇企業資安層級，**透過機器資料分析提供點對點的資安可見度
- **提升偵測防禦力，**利用分析技術找出未知的資安攻擊
- **做出最佳決策，**善加利用相關資安攻擊智慧和情報

企業面對各種動態攻擊場景、推陳出新的攻擊手法、進階資安威脅、以及瞬息萬變的商業需求，但既有的資訊安全技術卻無法跟上腳步。為應付這些新挑戰，先進的資訊安全團隊不僅須具備有分析與回應資安事件的能力，還需要有快速偵測新的進階攻擊能力，以縮短面對資安攻擊時的反應時間，以業務至上做出回應的決策。因此，資安團隊需藉由集中收集並分析所有機器資料，以更快偵測、回應並瓦解這些新型的攻擊行動。

Splunk Enterprise Security (Splunk ES) 白金級資訊安全解決方案，讓資安團隊能快速偵測並回應來自內部或外部的攻擊，藉此簡化資安攻擊的管理作業，同時將風險降至最低以確保企業業務的正常運作。有了 Splunk ES，資安團隊就能利用所有資料，取得整個組織的資安可見度與相關情報智慧。無論採用何種部署方式 — 包括企業自有機房、公有雲或私人雲、軟體即服務 (SaaS) 或結合以上方式 — 都能使用 Splunk ES 持續監測、回應事件、經營資訊維運中心 (SOC)，或為主管提供一個了解商業資安風險的窗口。

不論組織規模大小或屬於何種技術層級，Splunk ES 都能協助安全團隊簡化安全作業。它能提供：

- **資料洞察力：**利用預定義規則或透過隨機搜尋，找出網路、端點、存取點、惡意軟體、漏洞與身分認證技術所產生資料的關聯性。
- **開箱即用的警示管理功能、**和強大的動態偵測功能、情境搜尋功能，可快速偵測並分析未知的進階威脅。
- **提供客製化的彈性，**可針對特定需求進行關聯性搜尋、警示、報告與儀表板的客製化設定，無論您部署的目的是持續監測、回應事件、管理安全營運中心 (SOC)，或滿足主管了解商業風險的需求。

以分析技術為基礎的資訊安全應用，可從所有跟資安相關的資料中找出關聯性，包括來自 IT 基礎架構、個人終端資安產品和所有機器產生的資料，以快速適應不斷演進的攻擊環境。

持續監測企業資訊安全的健康度

提供一套完整的預定義儀表板、關鍵資安指標 (KSI) 與關鍵績效指標 (KPI)、靜態與動態臨界值與趨勢指標，透過視覺化圖表清晰呈現整個組織的資安健康程度。

針對資安事件，依嚴重性排序並採取行動

利用集中化的資安日誌、警示與資安事件、預定義的報告與關聯、事件回應工作流程以及關聯性，為各別分析師或調查團隊優化事件回應工作流程，提供單一清楚明瞭的資安專用介面。

迅速調查威脅

可利用隨機搜尋，還有靜態、動態與視覺關聯性來判定惡意活動。可調查任何領域或任何資料並進行樞紐分析，以便迅速發現進階威脅的可能場景、並追蹤攻擊者蹤跡，藉此分析和確認證據、找出額外資訊並與團隊成員進行協作。

多管齊下的調查處理

針對零日攻擊，可調查漏洞並進行分析，以追蹤被攻陷系統的相關活動。並運用狙殺鏈 (kill chain) 手法調查攻擊生命週期，利用隨機搜尋同時結合調查者日誌與調查時間軸、與所有 Splunk ES 功能，進行多方面全方位的調查分析。

請即刻試用 Splunk Enterprise Security。體驗 Splunk Enterprise Security 的威力 — 無須下載、設定硬體，也完全沒有組態限制。Splunk Enterprise Security Online Sandbox 提供 15 天評估環境，內含預建於雲端的資料，讓您能夠搜尋資料、加以視覺化並進行分析，藉此徹底調查來自各種安全使用案例的事件。還提供技術步驟教學，引導您試用 Splunk 軟體各種強大的視覺化與分析功能。**更多資訊請點擊此處。**

splunk>

台灣台北市大安區信義路四段 6 號 6 樓　886-2-5551 1266
splunktw@splunk.com　www.splunk.com

PB-Splunk-ES-109-A4