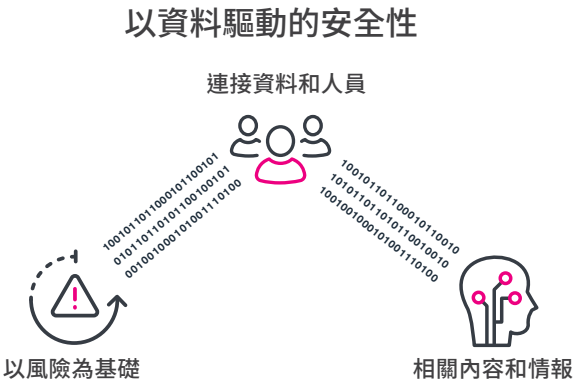
Splunk Enterprise Security

透過以資料驅動的洞察力，實現全面性的可見性、偵測和調查

- **在您的多雲、混合和本地環境中實現全面性的可見性**，改善安全狀態。
- **透過以風險為基礎的警示、整合的威脅情報和立即可用的安全內容**，加速威脅偵測和調查。
- **透過具彈性的資料平台和對多廠商工具和技術的整合能力**，快速從您的技術投資中收集相關資訊。



您的安全團隊面臨著不斷變化的威脅環境、新出現的攻擊策略和不斷演進的業務需求。然而，為了應對這些挑戰，您的團隊需要以資料驅動的能力、相關內容洞察力和準確且迅速的威脅偵測技術。這些能力可以幫助您減少偵測威脅的平均時間，並做出明智的決策，以加強業務成果。

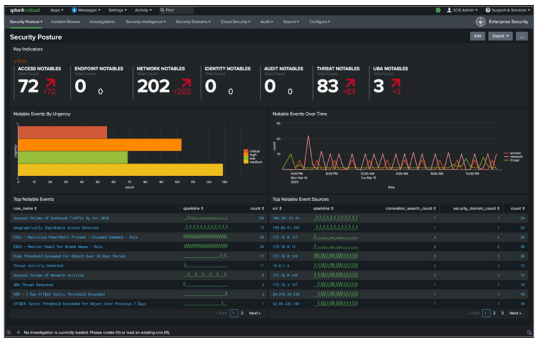
Splunk Enterprise Security (ES) 是一種以資料為中心的現代安全資訊和事件管理 (SIEM) 解決方案，可提供以資料驅動的洞察力，為您的安全狀態提供全面的可見性，使您能夠保護業務並大幅減輕風險。憑藉著無與倫比的搜尋和報告功能、先進的分析、整合的情報和預建的安全內容，Splunk ES 能加速威脅偵測和調查，讓您確定對環境構成高優先性威脅的範圍，以便快速採取行動。Splunk ES 採用開放且可擴展的資料平台所打造，使您能夠靈活地應對不斷演變的威脅和業務需求。

Splunk ES 可幫助各種規模和專業程度的安全團隊最佳化安全營運工作。它提供：

- **超過 1170 個現成的偵測**，符合多種業界框架 (如 MITRE ATT&CK、NIST、CIS 20 和 Kill Chain)。
- **可採取行動的情報**，其中包含相關的正規化風險分數和情報來源所需的必要相關資訊，以便偵測、優先處理和調查安全事件。
- **使用以雲端為基礎的串流分析技術**，可即時偵測可疑和惡意行為。
- **超過 2700 個由 Splunk、合作夥伴和社群成員建立的安全性和 IT 整合功能**，讓您可以輕鬆地將安全工具和資料來源饋入 Splunk。
- **減少 80% 的警示量**，以減少警示疲勞，為分析師提供明確的優先等級和分類，將解決案件的時間從幾週縮短到幾分鐘。
- **使用視覺化矩陣**將 MITRE ATT&CK 框架實際運用在工作中，該矩陣會強調顯示在風險事件中觀察到的策略和技術，以節省調查事件的時間。
- **快速找出事件的範圍**，並透過從機器和用戶觀察到的惡意可執行檔和威脅行為者進行全面查看，精確地做出回應。
- **支援所有部署類型**，包括雲端、多雲、本地部署和混合部署，以滿足業務需求和發展。

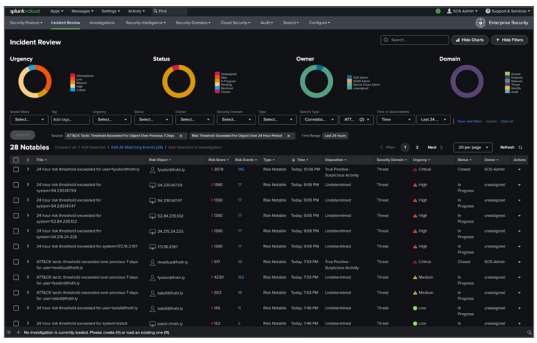
以資料驅動的安全性

Splunk Enterprise Security 能夠對驅動和保護業務的資料提供可見性和洞察力，使分析師能夠以快速和準確的方式做出關鍵決策，無縫地進行偵測和保護企業。



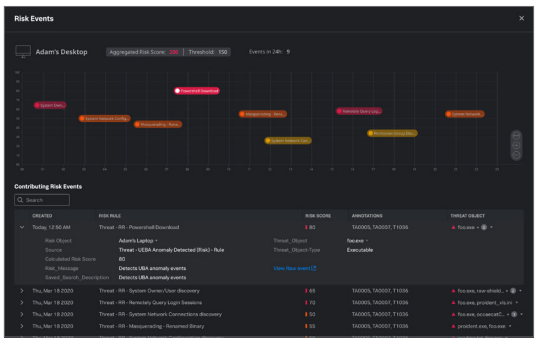
全面可見性

打破資料孤島，深入了解您的整體安全狀態並獲取可操作的情報。每天監控數十 TB 的資料——包含來自任何地方的任何結構化或非結構化資料。您可以一個無與倫比的資料平台做出以資料驅動的決策，保護您的業務並減少風險。您不僅能在安全性，也能在涵蓋 IT、開發安全營運和其他方面實現成果。



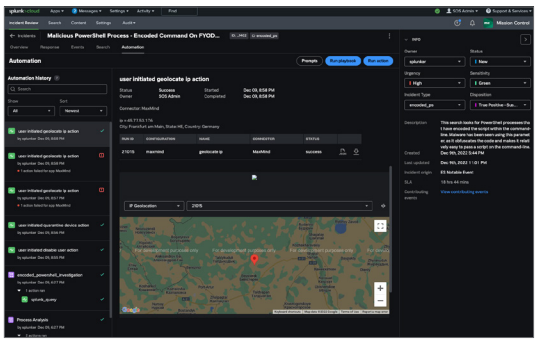
提升彈性和相容性

在面對不斷變化的威脅和業務需求時，透過一個可調適的資料平台，能夠讓組織保持敏捷，無論組織處於那一個雲端或混合式過程的階段。快速蒐集多廠商安全生態系統的背景資訊，透過 Splunk、合作夥伴和社群在 Splunkbase 上所建立的超過 2,500 個應用套件和元件進行技術整合。



加快威脅偵測

使用無監督式的機器學習技術，偵測未知威脅和異常行為，可以將安全調查的速度提高 50% 以上。加速調查並透過整合威脅情報來補充和優先處理高度真實的警示，以提高安全中心 (SOC) 的生產力和減少人員的疲勞。



統一您的安全營運作業

Mission Control 是供 Splunk Enterprise Security 使用者使用的應用程式，它可以讓你的安全作業更有秩序。Splunk Mission Control 能夠在同一個工作平台上統一安全事件的偵測、調查和回應能力，將您的流程編碼成易於遵循的回應範本，可簡化安全工作流程，並透過自動化減少分析人員的工作量，以加快回應速度。

準備好使用以雲端型資料驅動的 SIEM 解決方案來強化安全營運了嗎？了解如何開始使用 Splunk。

Splunk、Splunk> 和 Turn Data Into Doing 是 Splunk Inc. 在美國和其他國家/地區的商標和註冊商標。所有其他品牌名稱、產品名稱或商標均屬於其各自所有者。
© 2023 Splunk Inc. 保留所有權利。

23-165055-Splunk-Enterprise Security-PB-104