善用資料智慧創新轉變 Intel 的資訊安全狀態

執行摘要

難以低估 Intel 的科技貢獻對社會帶來的影響和重要性。該公司的工程專業知識能協助保護、強化和連結數十億台裝置，以及智慧型網路連線世界的基礎結構。同樣讓人難以低估的是將安全資料視為企業最受保護的資產的重要性。

以 Splunk® 和 Apache Kafka 為基礎，Intel IT 發展出全新的網路智慧平台，透過以下方式，改變維護資訊安全性的方法：

- 加速資料分析並減少偵測與回應進階威脅的時間
- 使協同合作企業具備共同語言和通用工作平台
- 提供串流處理和機器學習工具，在資訊安全作業和系統運作情況等其他領域提供商業價值

資料就是一切

Intel 已經從以 PC 為中心的公司轉變為一家以資料為中心的公司。該公司不斷開發新產品、進入新市場，並以創新的方式吸引新客戶。

「資料就是一切；資料才是王道。資料推動我們的業務，是一切行動的推手。」Intel 首席資訊安全總監 Brent Conran 說：「資料正在改變傳統產業，以及誕生於雲端的產業。從資料中取得深入見解的能力，是成功企業與失敗企業之間的差別。」

這種對資料的更加重視和依賴，讓 Intel 資訊安全組織必須建立和維護一個全面性「深度防禦」策略。該團隊將多個層級 (包括周邊、網路、端點、應用程式和資料分層) 的預防和偵測工具自動化，以處理 Intel 環境中所面臨 99% 的威脅。

狩獵那百分之一

進階威脅的發生頻率和複雜程度持續增加。該公司使用的舊版 SIEM 不僅無法滿足其需求，還成為他們的負擔。只有少數專家知道如何使用舊版 SIEM，而且面對公司對越來越多不同資料類型的需求，這個舊版 SIEM 根本無法經由擴充來加以因應。

產業

- 科技產業

Splunk 使用案例

- 資訊安全
- 網路資訊安全事件回應管理
- 安全性監控
- 應用程式監控

挑戰

- 轉為以資料為中心的業務模式雖然能增加資料價值，但同時也增加了弱點
- 舊版 SIEM 已無法滿足目標
- 多個無法連接的資料孤島和團隊各自提供不同的資料分析解釋

業務影響

- 轉型資訊安全管理和控制方式
- 在幾分鐘或幾小時內偵測複雜的威脅，不需要花上幾天或幾週
- 提供協作及整合的方法，管理網路安全
- 為整個資訊安全團隊提供網路智慧平台

Splunk 產品

- Splunk Enterprise
- Splunk Enterprise Security
- Splunk IT Service Intelligence (ITSI)
- VictorOps
- Splunk Mission Control

Intel 資訊安全組織需要一種策略來偵測試圖滲透企業環境的複雜威脅。Intel 資訊安全組織將這種策略稱為「**狩獵那百分之一**」。這項策略催生了 **Intel 網路智慧平台 (CIP)**，該平台以 Splunk 和 Apache Kafka 在內的尖端技術為中心。全新網路智慧平台以 Intel® Xeon® Platinum 處理器、Intel 3D NAND 固態硬碟和 Intel® Optane™ 固態硬碟為基礎，每天接收超過 12 TB 的資料，並儲存 15 PB 的資料。資料從數百個來源流向 Kafka 訊息匯流，然後進入 Splunk 平台。在此平台上，使用者每週搜尋 130 多萬次。

有了 Splunk 的「數據萬物」平台和數百個第三方工具，資訊安全組織現在能夠掌握豐富內容和通用工作介面，進而提高整體資訊安全組織的效率。與之前花數週或數小時來偵測並回應威脅相比，該團隊現在只需要數小時或數分鐘內就能完成這個工作。

擴充 Intel 網路智慧平台

網路智慧平台的成果帶來更多的資料來源、全新使用案例和更多資料模型。很快地，網路智慧平台的使用範圍便擴充至漏洞管理、法規遵循和執行、風險管理等團隊，這些團隊對基礎架構提出額外要求，同時也需要更快的運算和儲存能力。為了將平台效能最大化，Intel 的資訊安全解決方案架構師和工程師需要更深入瞭解 Splunk 平台和 Intel 技術。

Splunk 和 Intel 團隊合作開發了聯合**參考設定**，協助指導網路智慧平台使用最新的 Intel 產品和技術來擴充運算能力、記憶體和儲存空間。Splunk 和 Intel 現在與 IT 同行分享其成功經驗，協助其他公司擴充並部署 Splunk 和 Apache Kafka，以便更有效地將原始資料轉換為營運、業務和資訊安全情報。

「我們看到了可能性，且正因為如此，我們投入時間、精力和資源。我們希望 Splunk 能成功，因為我們深信 Splunk 能協助我們完成使命。」

— Intel 資訊安全長 Brent Conran

為今世和未來創造價值

Intel 的資訊安全團隊不斷拓展 Splunk 和 Kafka 的使用範圍。分析師和資料科學家轉換、豐富、參與、篩選並操作串流中的資料。該團隊還新增更多機器學習工具，從事件回應、營運和系統運作情況，到工作流程編排和警示等，遍及各種領域。透過與 Splunk 合作，Intel 正在為今世和未來發掘價值。

「Intel 資訊安全組織已達成史無前例的靈活性。」Conran 表示。「我們建立全新的 Splunk 資料湖，並將我們使用的工具進一步現代化。將資料放在正確的位置，並重新培訓員工，使我們得以擁有極為強大的能力。我們正在使用機器學習來大幅提高網路情報的深度和速度。」

「為了處理每日數十甚至數百 TB 的資料，並支援數百名使用者建立臨機操作搜尋、已排程的搜尋、資料模型加速和機器學習模型，我們建構了 CIP。為了能大規模展現效能，我們需要搭載 Intel Xeon 可擴充處理器和 Intel 固態硬碟來進行高效能運算和儲存。當你的任務是要『讓 Intel 安全快速發展』時，分秒必爭。」

— Intel 資訊安全解決方案架構師 Jac Noel

免費下載 Splunk 或先從**免費雲端試用版**開始。無論是雲端或內部部署環境還是大型或小型團隊適用，Splunk 都能提供符合您需求的部署模型。

2020-Splunk-RET-Intel-101-CS