ACE 交易所導入 Splunk 完成 ISO 27001:2022 資安規範升級效能降低 10% 成本

主要挑戰

導入 Splunk 前，ACE 難以集中關聯資安資料和分析多設備資料，對於多雲架構缺乏全面的可見度。由於監控資料過於分散，導致事件回應效率低落，而且實做 ISO27001:2022 資安監控的人力成本相當高。

主要結果

導入 Splunk 後，ACE 可以更快預測威脅和即時回應事件，優化資安監控。這不只省下了 10% 的資安管控成本，更可以簡化系統維護，進一步優化員工的工作效率，最終達成保障用戶資產安全。

ACE Exchange

行業：金融服務

解決方案：資訊安全、平台

資安平台不對勁，問題自然接踵而至

ACE 王牌於 2018 成立之際即為台灣首家合法合規虛擬貨幣交易所，提供新台幣就可以買比特幣 (BTC)、以太幣 (ETH)、USDT (泰達幣) 等主流虛擬幣種，24 小時隨時輕鬆買賣，也是目前提供最多理財工具，企圖將 DeFi 搬到 CeFi，更是擁有最全面的跨鏈服務，ACE 集團建立龐大區塊鏈交易及孵化生態系統，更需要一套有效的資安監控平台，ACE 穩定茁壯發展之際，保障用戶資產安全，秉持「合法合規」及「永續經營」初衷不變。

然而，ACE 過去採用的開源分析平台表現未如理想，無法集中收集資料和關聯日誌以偵測異常交易，又未能夠讓 ACE 在日漸成長壯大的多雲架構中，好好監察資源運用及分配。結果 ACE 的資安團隊往往需要大費周章，花時間登入不同的控制台去調查同一警示，使平均檢測時間 (MTTD) 變得很長，也不容易預測層出不窮的進階持續性威脅 (APT)。平台維護更加是困難重重，例如資料匯入和儀表板的客製化都需要耗費較多人力，不只為團隊帶來時間及心理壓力，同時也限制了硬體運算的效能。

為了在複雜的營運環境中呈現細緻的數據可視化，ACE 決定轉向 Splunk 平台，以數據驅動加強資安部署，同時使威脅狩獵變得更完善、整體運作更有效率。

成效

資安監控需要的人力資源減少 70%

從閒置的雲資源中省下來的成本達到 10%

24/7 運作無間、服務隨時可用 – 基於對業務運作的即時可見度

集中化資安監控體現更大生產力

ACE 資安長 (CISO) 徐方繹表示：「Splunk 為我們提供了夢寐以求的資安分析平台。」Splunk 自動從各公有雲端平台收集日誌資料，恰如其分管理好 ACE 複雜的多雲環境升級更快速的威脅預測和即時事件回應，優化監控可靠性 (Multicloud)。當中包括 Google 雲端平台、亞馬遜網路服務及 Microsoft Azure 公用雲端服務。然後 Splunk 的分析平台會產生有關資安狀態的完整概況，一目瞭然。ACE 的資安團隊還可以在簡單易用的 Splunk 儀表板上，預測、偵測與回應各種資安威脅。

Splunk 的解決方案大幅減輕了 ACE 資安團隊的工作量。徐方繹解釋：「Splunk 的搜尋處理語言簡單方便，而且容易學習，不只解決了舊有平台搜尋緩慢的問題，還容許我們靈活調整儀表板，又可以快速改變警示設定，滿足實作 ISO27001:2022 新增控制項 A8.16 監視活動 (a.8.16 Monitoring Activities)。此外，Splunk 的行動應用程式也功不可沒。現在我們無論身處任何地方，都可以通過單一介面使用儀表板、報告及警示功能。我們的團隊在晚上再不用留在公司輪夜班，因為大家可以隨時、隨地連接 Splunk 平台，如常運作。」

ACE 還利用 Splunk 的技術開發機器學習模型預測網路威脅，並提供有關資安事件的警示，省去重複的人手程序。過去 ACE 需要安排七人天執行的資安監控變更工作，現在兩人天就足夠了。生產力的提升，使團隊中的人員可以專心處理更重要的工作，ACE 也可以更好地運用本身的資源，加強執行更重要的資安計劃。

> 有了 Splunk，我們可以在多雲環境中體現最完善的運作，創造最大的投資回報。
>
> ACE 王牌交易所 (ACE Exchange)
> 資安長徐方繹

即時資源管理實現最大投資回報

由於 ACE 對多雲環境有更大的可見度，資源管理因而得到改善。通過 Splunk 平台，ACE 可以準確洞悉不同雲端服務的支出，甚至查找出不必要的服務；又可以把資源即時重配，提升整體的投資回報。徐方繹指出，ACE 現在可以辨別出閒置的雲端資源，成功降低超過 10% 的成本。

整體來說，ACE 團隊一致認同 Splunk 平台的易用性。徐方繹表示：「Splunk 提供很多開箱即用的應用程式，可以支援雲端和內部部署中不同品牌的產品，使我們的資料載入及整合過程變得更暢順。後續的維運也相當簡單，只要更新應用程式就可以了。單一資料源可以擴展到不同案例，例如資安、IT 運作及商業分析，無須裝設多套監控軟體。」

繼往開來

Splunk 使 ACE 的網路安全性邁向新境界，不過這只是開始而已。徐方繹分享：「在未來，我們肯定會利用 Splunk 的技術成就更多、走得更遠，下一步就是提升資安自動化的水平。」為了達到這個目標，ACE 正在考慮採用 Splunk SOAR 解決方案，進一步提高資安運作的效率，並且加快事件偵測和復原的速度。此外，ACE 還在計劃以 Splunk 去偵測詐騙和減少內部的異常交易，以保障 ACE 的資安韌性 (Resilience)，同時支持新的交易途徑，為未來作好準備。

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。

23-ACE-Splunk-CS