財星 100 大企業透過風險型警示改善偵測和調查能力

主要挑戰

這家一流金融機構所產生的大量警示，需要分析師花費大多數時間分類警示，幾乎消耗了機構中所有的分析師資源。

主要結果

這家金融服務機構善用 Splunk 大幅降低警示量，同時提高了真陽性率，並操作化 MITRE ATT&CK。

產業：金融服務業

解決方案：資訊安全與防詐騙管理、企業安全性

這家財星雜誌 100 大金融服務企業是美國最大的銀行機構之一，專擅以負責的方式管理風險

無論是在網際網路首次成為主流時推出線上交易，或是為客戶取消帳戶費用，多年來，他們總是搶先採用顛覆傳統的想法。

這個跨國機構的安全團隊負責保護公司的資訊安全狀態，使其免於遭受不必要的入侵。因此，他們持續密切關注技術和程序的轉型，以強化防禦能力。在 conf18 大會上，他們遇到了一個令他們印象深刻的主題：風險型警示 (RBA)。

團隊回國後，他們將落實 RBA 列為首要任務。RBA 強化了該機構原有的 Splunk Enterprise Security 解決方案，以「歸因」為基礎的全新方式來執行工作。這些在思維與程序上看似輕微的變化，卻讓團隊擁有更好的方法來收集相關資訊安全內容，並加速處理威脅。

這裡越來越忙碌了

過去，資訊安全監控中心 (SOC) 是個喧鬧忙碌的地方。為了查明違規而追求「完美」的關聯搜尋會產生太多誤報，絕對不是偵測活動的有效方式。

資料導向成果

65%
警示量減少 65%

~2x
警示精確性提高 2 倍

更佳
更好的複雜威脅偵測效果

「一天內產生的 200 個警示中，只有少部分需要進一步調查，其中大部份與違反政策有關。」機構中的資訊安全工程師表示。問題在於，如今每當 SOC 收到巨量警示時，資訊安全分析師都必須篩選所有警示，嘗試拼湊正在發生的狀況。SOC 通常缺乏有效機制來破解資料試圖呈現的狀況。該團隊將 RBA 視為改進 SOC 內廣泛採用之最佳實務的契機，同時也能改善其偵測、調查和處理複雜威脅的能力。

> 許多產品只是盡到商業或法規遵循責任，但其實不會影響資訊安全營運。Splunk Enterprise Security 提供的風險導向警示，能真正提升資訊安全，同時清楚展示資訊安全對企業的價值。」
>
> 金融機構
> **資訊安全工程師**

大家都喜歡好案例

安全性和企業間的關係必須更加緊密。從歷史層面上看，語言在中斷連線的狀況下是極重要的一環。資訊安全工程師表示，RBA 對團隊的早期好處之一是「風險型警示允許業務和安全性團隊使用相同的語言」。

資訊安全從業人員在說明狀況時傾向使用較多高技術性術語，這對大多數 SOC 之外的人員來說是項挑戰。風險歸因是 RBA 的核心組成，提供必要的通用語言，讓 SOC 和企業能掌握相同狀況。「以前我們要在許多不同地方之間來回切換，導致收集到的資訊失焦，又過度技術性。」資訊安全工程師表示。「RBA 為指定使用者/對象集中處理所有風險內容。我們現在可以向 SOC 以外的團隊，展示與使用者/對象相關的各種風險行為是如何交織在一起，演變成一場安全性事件。」

使用架構做為指南

資訊安全分析師承受過量的警示疲勞衝擊。這迫使許多分析師採用安全警示思維方式，這種作法特別著重於排定優先解決問題順序的活動。在 RBA 中，為重大事件找出根本原因，為資訊安全分析師提供瞭解整個安全性事件所需的背景。值得調查的根本原因可對應至 MITRE ATT&CK 等頂尖網路安全架構，因此分析師現在可花更多時間對真實威脅進行安全性調查。有了 Splunk 平台，這個一流機構的團隊誤報率大幅降低，同時提高了整體偵測涵蓋範圍。

想要瞭解 RBA 如何協助貴公司加強資訊安全作業嗎？請觀賞這部示範影片。

21-18016-Splunk-Tier2-Fortune100-FinServices-A4-CS-102