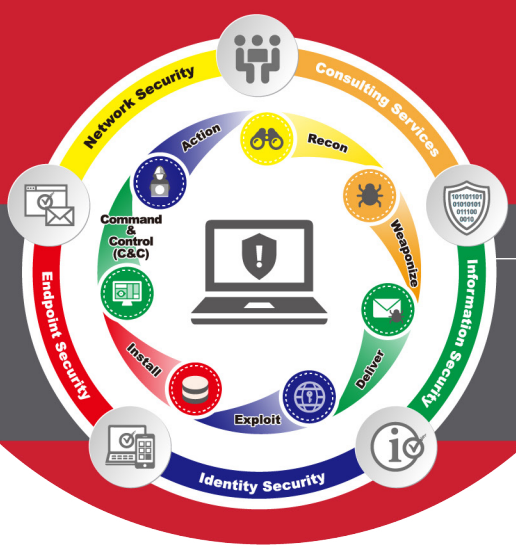


破除雜訊：智慧型異常分類如何強化資安營運中心(SOC)作業

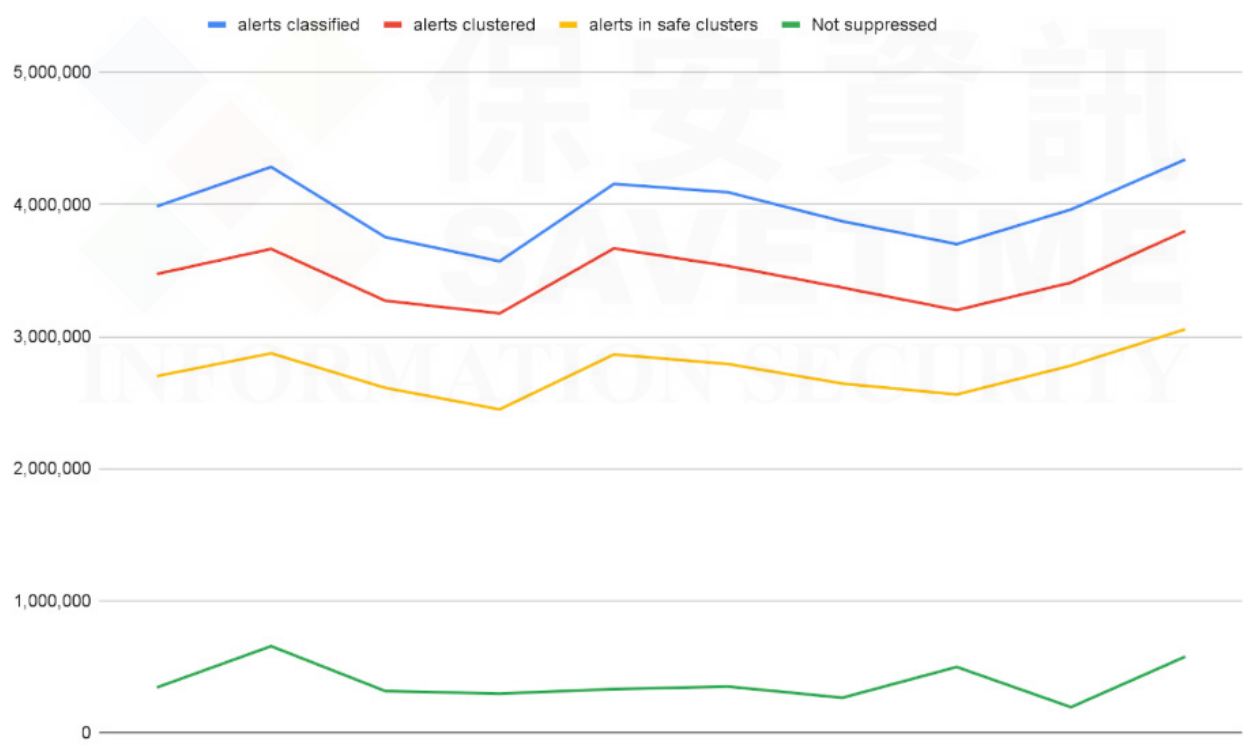
2025 年 8 月 5 日發布

資安營運中心 (SOC) 的效能經常受到一個無聲無息、無處不在的敵人影響：「警報通知疲勞轟炸」。當資安營運中心 (SOC) 分析師被大量的安全警示淹沒時，就會出現這種現象，其中許多都是誤報、低優先順序或多餘的警示。不分優先順序的警報持續不斷，會導致敏感度降低、倦怠，最重要是可能真的會遺漏真正的重要威脅。

「警報通知疲勞轟炸」後果非常嚴重。分析師難疲於奔命，回應時間變慢，組織的整體安全狀態也會被弱化。大量的警報讓人很難從看似良性事件中分辨出真正的惡意活動，導致時間浪費、營運成本增加，以及遭成功入侵的風險提高。

為了避免這個關鍵問題，賽門鐵克開發創新的抑制技術：異常分類 (Anomaly Classification)。此系統利用人工智慧 (AI) 和機器學習 (ML) 的力量，同時採用監督和非監督模型來智慧地抑制良性警示，並提高真正惡意警示的能見度。我們的新監督模型是根據遙測特徵與數以千計的客戶回饋輸入進行訓練，讓我們能有效結合無監督與有監督技術，達到更高的抑制率。

有了新引入的模型，我們取得重大突破。在我們初步實驗中，我們已經壓制 94% 的警報，但隨著改良模型的到位，我們進一步將未壓制的警報減少原來值的三分之二，合計壓制率達到 98%。其餘的高優先級警報應由 SOC 小組進行分流。這可大幅降低 SOC 代理的工作量，讓他們能將專業知識專注在真正重要的威脅上。



為 SOC 團隊帶來的好處

實作我們的異常分類系統，可為飽受「警報通知疲勞轟炸」的 SOC 團隊帶來多種好處：

- 大幅降低警報量
- 更專注於真正的威脅
- 更快的事件回應
- 提高分析師士氣和留任率
- 提高效率並節省成本
- 主動的安全態勢

欲深入了解賽門鐵克的端點多層次防護解決方案中「進階機器學習」防護技術，請點擊此處。

關於賽門鐵克 (Symantec)

賽門鐵克 (Symantec) 已於 2019/11 併入全球網通晶片巨擘--博通 (BroadCom，美國股市代號 AVGO，全世界網際網路流量有 99.9% 經過博通的網通晶片) 軟體事業部的企業安全部門 (SED)，特別是近年以半導體的嚴謹、系統化以及零錯誤思維來改造核心技術、管理框架以及整合最完整的資安生態體系，讓賽門鐵克的解決方案在穩定性、相容性、有效性以及資安生態系整合擴充性，有著脫胎換骨並超越業界的長足進步。博通 (Broadcom) 是務實的完美主義者，致力於追求卓越、關注細節並且有系統和紀律地投入科技創新與嚴謹工藝，同時也大大降低交易複雜性。Symantec 持續創新的技術能為日新月異的資安問題提供更好的解決方案，近三年 Symantec 很少出現在由公關機制產生的頭版文章中，而且在全球前兩千大企業的市佔率及營收成長均遠遠高於併入博通之前，增長幅度也領先其他競爭對手，是科技創新驅動的解決方案非常穩健可靠深受大型企業信賴的實證，也顯示大型企業顧客對轉型中的新賽門鐵克未來充滿信心。(美籍華人王嘉廉創辦的企業軟體公司，組合國際電腦（CA Technologies）以及雲端運算及「硬體虛擬化」的領導廠商--VMware， 也是博通軟體事業部的成員)。2021 年八月，因應國外發動的針對性攻擊日益嚴重，美國網路安全暨基礎架構安全管理署（CISA）宣布聯合民間科技公司，發展全國性聯合防禦計畫 JCDC(Joint Cyber Defense Collaborative)，而博通賽門鐵克是首輪被徵招的一線廠商，如就地緣政治考量，Symantec 也絕對是最安全的資安廠商。擁有更強大資源與技術為後盾的賽門鐵克已更專注於整合各種最新科技於既有領先業界的端點、郵件、網頁以及身分認證等安全解決方案。

關於保安資訊 www.savetime.com.tw

保安資訊團隊是台灣第一家專注在賽門鐵克解決方案的技術型領導廠商，被業界公認為賽門鐵克解決方案專家。自 1995 年起就全心全力專注在賽門鐵克資訊安全解決方案的技術支援、銷售、規劃與整合、教育訓練、顧問服務，特別是提供企業 IT 專業人員的知識傳承 (Knowledge Transfer)、協助顧客符合邏輯地解決資安問題本質的效益上，以及基於比原廠更孰悉用戶使用情境的優勢能提供更快速有效的技術支援回應，深獲許多中大型企業與組織的信賴，長期合作的意願與滿意度極高。許多顧客樂意與我們建立起長期的友誼，把我們當成可信任的資安建議者、可以提供良好諮商的資安策略夥伴以及總是第一個被想到的求助暨諮詢對象。

保安資訊連絡電話：**0800-381-500**。