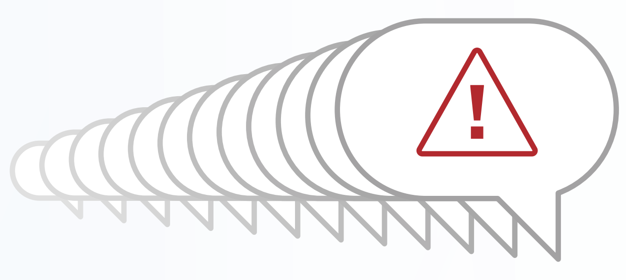
喊狼來了的SIEM

數千個警報中只有一個可能很重要。但是，今天的資安事件管理 (SIEM) 產品能否從真實威脅中識別出虛假警報？

警報超載



每天，世界各地的IT安全團隊平均被10,000條警報淹沒，遠遠超過了他們有足夠的資源進行調查。[1]更糟糕的是，用於集中化此數據的SIEM產品在為瑣碎警報進行排序 時，對整理重要警報毫無幫助。

很少有組織有資源來追踪每個警報，並且不可能對每個警報做出響應。

10K+	“Off”	67%
大多數資安運營中心每天都會收到警報[1]	大多數團隊會關閉自動阻止作應對	的組織認為他們的回應缺乏效率[2]

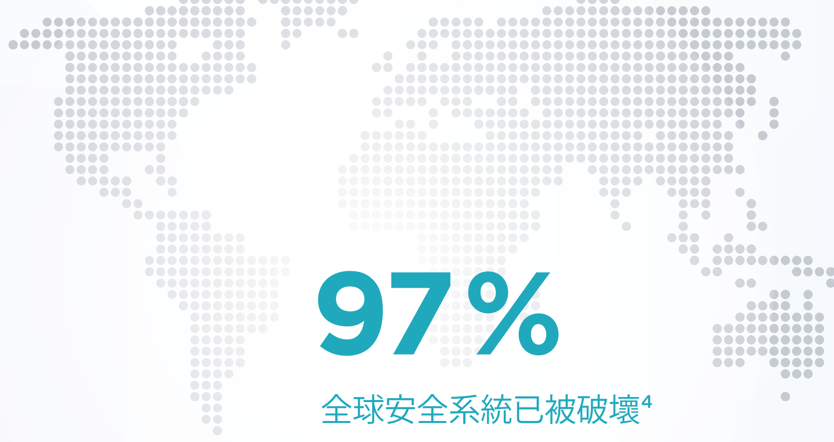
•••

在2013年對尼曼·馬庫斯（Nieman Marcus）的一次重大攻擊中，有60,000個警報（數量巨大）與入侵有關，但僅佔該時期警報總數的1%.[3]

危險上升

錯誤的安全感

資安團隊通常認為警報量高必意味著他們的工具正在捕獲最嚴重的威脅，但是在大多數情況下，這並非事實。



97%

全球安全系統已被破壞[4]

•••

誤報代表大量警報，導致團隊變得不敏感，他們可能將新警報視為令人討厭而不是警告。同時，僅對29%的警報進行了調查-與可能的威脅相距甚遠。[2]

一個安全事件可以觸發數百個警報。協同攻擊可以產生成千上萬.

一個高度複雜的問題

哪些警報值得關注？答案不是那麼簡單。大多數網路安全工具無法區分日常的惡意軟件和針對性的高級攻擊，這些攻擊要經過多個步驟，並且需要更複雜的響應。

進階攻擊

1 初步偵察
2 最初的妥協
3 立足點
4 特權升級
5 內部偵察
6 任務完成

預防 大多數安全解決方案都專注於檢測和預防攻擊的早期階段。

響應 如果逃避了早期發現的攻擊並發展到後期，則組織尤其容易受到攻擊。

先進的有針對性的攻擊可以以不同的形式進入組織，然後結合起來形成惡意的可執行文件。

無法檢測到精心策劃的攻擊團隊也無法過濾掉瑣碎的警報，確定警報的優先級別並合併相關警報。

一個資安運營中心平台可幫助團隊從預防到響應，揭示看似無關的活動如何在協同攻擊中建立聯繫。

新方向

傳統的SIEM可以聚合警報和其他安全數據，但是為了抵禦當今的高級攻擊，組織需要一個更具動態性的解決方案。資安運營平台超越了傳統的SIEM，可提供完整的可見性並幫助團隊控制事件-從警報到修復。

	傳統 SIEM	資安運營平台
先進的SIEM通過先進的用戶行為分析來集中安全數據，以監視用戶模式，檢測基於非惡意軟件的入侵並管理應用程序訪問	×	✓
資安協調可自動執行任務，例如包含端點，阻止IP地址以及針對惡意軟件數據庫進行搜索	×	✓
工作流管理工具可幫助跟踪分析人員之間的工作，管理案例並自動執行調查任務	×	✓
情境情報可提高威脅行為者及其策略，技術和程序的可見性和環境，有助於確定哪些威脅構成最大風險	×	✓
第三方工具集成可通過吸收外部事件和日誌的功能來連接和增強整個組織中的各個資安解決方案	×	✓

請訪問以下連結以下載完整報告

www.FireEye.com/next-gen-siem-tc

---

1 John E. Dunn (May 14, 2014). Average US business fields 10,000 security alerts per day, Damballa analysis finds.
2 Ponemon Institute (March 16, 2016). The State of Malware Detection and Prevention.
3 Bloomberg (February 24, 2014). Neiman Marcus Hackers Set Off 60,000 Alerts While Bagging Credit Card Data.
4 FireEye (May 2014). Cybersecurity’s Maginot Line: A Real-World Assessment of the Defense-in-Depth Model.

H-EXT-IG-US-EN-000181-01