



雲端將主宰網路安全分析 與營運

雲端防禦趨勢(1)

需求與供應端的改變，致使 SIEM 系統由本地伺服器轉移到雲端平台。

文／Jon Oltsik 譯／曾祥信

SIEM（安全性資訊與事件管理）是 Security Information and Event Management 的縮寫，SIEM 系統最早出現是在 2000 年左右，由 Intellitactics、NetForensics 與 eSecurity 等廠商推

出的解決方案。最初的功能主要是「安全事件關聯」，也就是將入侵偵測系統（IDS）、入侵防禦系統（IPS）與防火牆等安全防護裝置搜集到的事件，關聯起來以進行分析。

過去 19 年間 SIEM 市場不斷演進，無論是功能、使用案例及供應商皆有所變化，如今 SIEM 已成為總值 25 億美金的市場，最主要的供應商為 Splunk、IBM、LogRhythm 與 AT&T (AlienVault)。

儘管 SIEM 系統歷經許多發展，現今的 SIEM 產品仍可視為只是過往產品的巨大規模版本。事實上，SIEM 最初的設計看起來就像是網路與系統管理工具 CA Unicenter、HP OpenView 與 IBM Tivoli 的仿冒品，SIEM 產品的基礎是由分散式資料收集器 / 索引編集器 / 處理器組成的多層式架構，加上一套負責資料分析、視覺化與產生報表的中央資料庫。

根據研究顯示，28% 的組織機構收集、處理與分析的安全資料量，比過去兩年大幅增加，另外有 49% 的組織出現小幅增加，這意謂組織需要更多基礎設施、更多人力以及營運工作。

隨著 SIEM 的規模日益擴大，企業組織需要更多的硬體階層，來支撐及維護 SIEM 系統的效能與規模延展性。這種發展狀況使得負責威脅偵測、應變處理與鑑識研究等任務的資安監控中心人員，必須倚賴 SIEM 基礎設施團隊，等待他們升級硬體與負載平衡伺服器，以及增加儲存空間。

SIEM 系統將由本地伺服器轉移到雲端

2019 年安全分析及營運技術模型正處於巨大的架構轉變，接下來幾年，SIEM 的後端平台將由本地伺服器（on-premises server）轉移到公有雲端設施上。我堅信，在 2020 年結束前，即使是對本地伺服器抱有偏見般堅持的產業組織，例如金融服務業、政府機關與軍事武器製造業，也會放棄本地伺服器，改用雲端設施來維護 SIEM 系統。

這項轉變不但已經發生，而且由於供需的變化，轉變過程將會非常迅速。資訊安全長（CISO）將開始尋求雲端的 SIEM 解決方案，理由如下：

- 安全資料的巨幅成長：根據 ESG 研究顯示（ESG 為環境、社會及治理研究機構），28% 的組織機構，收集、處理與分析的安全資料量，比過去兩年大幅增加，另外有 49% 的組織出現小幅增加（註：筆者本身是 ESG 的雇員）。至於增長的資料涵蓋哪些資料類型呢？網路威脅智慧（CTI, cyber threat



intelligence)、網路封包擷取、雲端日誌、企業應用程式日誌，任何你能想到的資料都有可能。安全資料的持續成長意謂組織需要更多基礎設施、更多人力以及營運工作。

- 更高的軟體成本：除了基礎設施與人力成本外，有些 SIEM 供應商會根據管理的資料量來決定計費，我曾聽過資訊安全長抱怨 SIEM 預算暴增，在一年內就花掉三年的預算，而且這種情況頗常發生。

- 難以接受的利弊權衡：因為 SIEM 軟體可能會以資料容量作為計費標準，許多組織不得不忽略或刪除具有收集與分析價值的重要安全資料，這是所有安全分析師

不樂見的情況。另一種常見的節省成本策略，是在 SIEM 系統外搭配開源碼的資料湖泊 (data lake)，以處理資料回顧與適合長期分析的資料。雖然這種作法可減少 SIEM 軟體支出，但也帶來系統互通性與營運上的挑戰，安全人員必須在 SIEM 與資料湖泊系統間轉換資料，還得同時管理兩套安全技術的基礎設施。

- 網路安全與 IT 人才的匱乏：由於技術人員嚴重短缺，科技長與資訊安全長必須謹慎考量是否要招募與聘用專門管理網路、伺服器與儲存裝置的人員。

雲端 SIEM 系統可以協助資訊安全長解決以上所有難題。

供應商推動雲端 SIEM 系統

在供應端，廠商察覺到增長迅速的市場機會，並將以下列幾種方式推動雲端 SIEM 系統：

- 傳統 SIEM 供應商看見雲端的優勢：雖然 SIEM 領導廠商 IBM 與 Splunk 在此議題著墨不多，但

他們已經察覺客戶用雲端平台部署他們產品的比例迅速增加，這項趨勢仍會持續進行。

- 新創公司都在做雲端系統：最新的安全分析及營運供應商，例如 DEVO、Empow Cybersecurity 與 JASK，全部都使用雲端為主的後端系統，專為資料管線、機器學習演算法與巨大規模所設計的平台。2019 年很可能還會出現更多新創公司加入這個市場。

Amazon、Google 與 Microsoft 擁有散落全球的分散式雲端基礎建設，並且積極投資人工智慧與機器學習領域，因此，「網路安全分析」這個使用案例自然成為與他們技術投資策略一致的絕佳機會。

- 雲端服務供應商的投入：Amazon、Google 與 Microsoft 擁有散落全球的分散式雲端基礎建設，並且積極投資人工智慧與機器學習領域，因此，「網路安全分析」這個使用案例自然成為與他們技術投資策略一致的絕佳機會。這些公司已經開始行動：Google/Alphabet 成立 Chronicle 公司，宣示其安全分析的意圖。Amazon 併購 Sqr1，顯示 Re:Invent 產品將更加專注安全分析與營運。Microsoft 對於自家的安全分析與營運仍然守口如瓶，不過該公司近期的公告暗示他們將在 2019 年加入戰局。

以我個人淺見來說，發展趨勢已經很清楚 - 安全分析與營運是一個巨大的資料應用，而大型的資料應用全都轉移到雲端了。對雲端依然抱持不信任態度的資訊安全長必須正視這項事實，他們必須學會如何與雲端為主的網路安全 / 營運技術和平共處，否則就只能等著被趨勢淘汰。

CIO