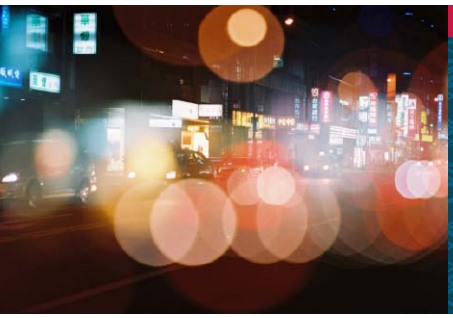

SIEM：可解決重大企業問題的五項需求

憑藉這十幾年來在生產環境中的運作經歷，安全性資訊和事件管理 (SIEM) 解決方案現已被視爲發展成熟。事件收集、關聯、警示以及展現法規遵循狀態等功能均屬基礎，而多數的 SIEM 解決方案皆可因應這些需求。但局面隨時都在變化。組織面臨到目標鎖定式和持續性攻擊等新型威脅；行動裝置、雲端及虛擬化等全新趨勢；以及在招攬客戶、營運效率及成本節省方面不停轉變的企業要務。因此，SIEM 使用案例需要更多進階功能來解決更重大的企業問題。

McAfee 與 SIEM 使用者洽談，並要求他們告知使用 SIEM 時所遭逢的主要問題。以下是他們面臨的五大問題：

- 巨量資料安全性
- 情境感知
- 即時內容
- 管理作業簡易性
- 整合式安全性

爲讓 SIEM 以更有效的安全性與風險管理策略來協助使用者，特別是在他們與降低風險、適應趨勢以及配合企業要務有所關聯的情況下，這五大問題更必須予以正視。下面介紹每個問題以及對應的客戶案例研究與使用案例。

使用案例：巨量資料安全性

- 採用更多來源的更多摘要來擴充資料擷取。
- 針對超大資料集執行分析與鑑識作業。
- 針對巨量資料安全性的速度與容量需求進行最佳化。
- 提高員工和處理流程效率。

1. 巨量資料安全性

如果您能夠善用巨量資料安全性，這項特點就可謂極具價值。傳統 SIEM 解決方案的設計並非旨在與數量如此龐大的端點、網路及資料來源進行整合，也不是用於處理如此高的事件發生率或保存如此長久的原則。因此，關聯式資料庫與相似的傳統 SIEM 缺點主要是針對以網路爲中心的事件重點而設計，在時下多變的 IT 基礎架構下根本無法滿足該架構的安全性需求。由於缺乏速度、擴充性及延展性，導致效力低又不實用。

案例研究：美國聯邦政府

大型政府機構想要將進階分析應用於儲存在 SIEM 數以 PB 計的關聯式資料庫中的「巨量資料安全性」。不過，即便是簡單報告也需花上數小時才能處理完畢，部分資料甚至得耗費一天以上，使得機構的 SIEM 無法用於鑑識工作。

機構若改用 McAfee® Enterprise Security Manager 作爲 SIEM 解決方案，便可擴充整合式裝置的數量與類型，進而加入更多以資料和使用者爲中心的內容至分析數據中。機構亦可提升事件發生率並增加儲存的資料量。現在，不僅可在數分鐘之內取得報告，還能改進鑑識分析的整體運作方式。

使用案例：情境感知

- 利用更多身分識別解決方案來充實情境感知的內容。
- 釐清人員、時間、方式、地點及內容。
- 瞭解持續時間、參與人員與其他事項。
- 納入 BYOD 資產，例如：筆記型電腦和智慧型手機。

2. 情境感知

SIEM 以前曾經只是爲防火牆與入侵偵測系統間的事件建立關聯的工具，後來也許應用於部分弱點評估資料。時至今日，仍有一些 SIEM 主要仰賴著網路流量資料。雖然這些資料來源很重要，但還需要應用程式、資料內容、身分識別資訊來充實內容。若未這麼做，就須花費更多時間與資源及充足的情境情報來瞭解並優先處理事件，進而達到可行且即時的成效。

案例研究：醫療保健機構

地區性的醫療保健機構採納了「自行攜帶裝置」(BYOD) 的概念，以支援個人平版電腦的方式來提高員工機動性。但是，因發生過事故，讓該機構十分擔心內部濫用的情況。無論使用的裝置爲筆記型電腦、桌上型電腦、平板電腦或虛擬桌面，這間醫療保健機構先前的 SIEM 解決方案都無法得知哪位使用者正與機密資料進行互動。

有了 McAfee Enterprise Security Manager，醫療保健機構便可與身分識別和行動性管理、Active Directory 及 LDAP 產品進行連線，以便感知使用者及裝置活動。由於與結構性和非結構性資料儲存 (例如：原生資料庫支援) 整合，也與資料遺失防護 (DLP) 和 Database Activity Monitoring (DAM) 整合，造就更完善的情境感知以及更優良的內部威脅降低效果。

使用案例：即時內容

- 瞭解環境內外部的威脅。
- 利用即時內容來改善 SIEM 情報。
- 減少事件識別與回應的次數。
- 透過額外安全性情報，找出威脅並排定優先處理順序。

3. 即時內容

最早期的 SIEM 使用案例之一是日誌管理，意即使用一些華而不實的額外功能來收集、儲存及查詢。日誌仍是 SIEM 的基本元件，不過現今的 SIEM 也需要即時內容。

這一類內容的範例是 McAfee Global Threat Intelligence (McAfee GTI) 與 McAfee Vulnerability Manager。McAfee GTI 可提供即時的雲端型信用評價服務，而 McAfee Vulnerability Manager 則可收集有關資產弱點的組織資訊。

案例研究：零售商

身爲財星前 100 大公司的零售商不具可實際執行的 SIEM，也沒有採用 McAfee 解決方案來執行概念驗證。零售商在頭一週就發現到嘗試進入自家網路的流量中，有超過 30% 是來自惡意來源並/或含有惡意承載。

使用 McAfee Enterprise Security Manager 來將事件資訊與 McAfee GTI 建立關聯後，零售商得以迅速地找出自家所有的儲存位置和資料中心裡有哪些資產正遭到鎖定，並且進一步瞭解把矛頭指向組織的攻擊類型。McAfee SIEM 解決方案判定出嚴重性的最高層級，接著優先處理回應。SIEM 搭配即時內容可以打造出更加迅速的威脅偵測、優先處理及修補程序。

使用案例：管理作業簡易性

- 藉由動態白名單以及由硬體輔助的安全性功能來部署 SIEM，以便保護固定功能裝置。
- 透過可自訂的深入查詢功能來簡化鑑識程序。
- 將 SIEM 與防火牆和入侵預防系統 (IPS) 整合，以迅速回應事件。
- 由於安全性獲得改善，傳統資產的使用壽命也能延長。

4. 管理作業簡易性

傳統的 SIEM 架構十分僵化，且缺乏一些必要功能。例如，這些 SIEM 無法輕易地與原本不支援的裝置整合，讓資訊可供使用。相反地，新一代 SIEM 卻能輕鬆地進行自訂，其靈活性也足以因應任何特定環境。這也就是爲何眾多組織會將新一代 SIEM 納入策略中。

案例研究：公用事業公司

一家大型公用事業公司需要導入安全性控管措施，防止類似 Stuxnet 的攻擊影響基礎架構而導致數百萬名客戶遭逢停電事件。有了 McAfee Enterprise Security Manager，這家公用事業公司得以使用原生的裝置、應用程式和通訊協定支援，在整個企業 IT、SCADA 及工業控制系統 (ICS) 區域內落實情境感知能力。

McAfee SIEM 提供工具給客戶，助其自行與 SCADA 和 ICS 裝置進行自訂整合。如此一來，上述三個區域就能彼此建立關聯、執行異常偵測並進行趨勢分析。除了自訂事件收集之外，客戶還能迅速輕鬆地建立唯一的儀表板、報告、關聯規則及警示。這讓 SIEM 成爲安全性、展現法規遵循狀態以及資產可用性方面的無價工具；也就是說，它能讓營運從此不間斷。

使用案例：整合式安全性

- 簡化安全性與業務工作流程。
- 透過自動化與簡易自訂來簡化複雜性。
- 將多種安全性解決方案綜合運作，以改善可見性與情境感知能力。
- 利用情報與整合，打造更優質的安全性。

5. 整合式安全性

SIEM 是所有策略性安全企劃的起始要素，但也只是眾多要素之一。涵蓋所有安全性與法規符合性解決方案的整合可帶來更爲緊密結合而非單獨的解決方案，然後非整合式架構卻衍生了複雜性。複雜性使得安全性時常流於紙上談兵，而無法更具策略性並配合企業要務。

案例研究：金融服務

跨國銀行客戶擁有不同廠商的各種不同產品。某些產品已實際運作，不過許多產品因資源有限而未經定期使用或維護。銀行利用 SIEM 搭配整合式端點、網路及資料控制來作出這類判斷，以便更有效地緩解風險並降低成本，同時也讓安全性與業務的關係更加緊密。

銀行減少了廠商數量，並獲得規模經濟。這家銀行降低了培訓成本，並減少代理程式、主控台、伺服器等項目的數量。此舉也降低了合約成本以及大量相關費用。除了節省成本外，銀行也確保所有現有及未來的解決方案與 McAfee Enterprise Security Manager 完全整合，以確保更能瞭解並掌控自身的安全性狀態。

主要考量因素

- 由巨量資料安全性來呈現，且可輕鬆處理收集、儲存、存取、處理及分析難題的能力到底有多重要？
- 您的安全性利益相關者是否取得所需資訊，以便作出明智決策並及時採取行動？
- 您的安全性團隊是否有所需的即時內容，以便在風險與攻擊實際造成危害前先找出它們？
- 如果您使用 SIEM 的直覺式深入查詢與易於自訂的檢視功能，對安全性和資源會造成什麼影響？
- 涵蓋整個基礎架構的整合方式如何改善安全性、可見性、程序與回應能力？

在過去十年所使用的傳統 SIEM 方法根本無法因應現今的需求。隨著對巨量資料、安全性情報、情境感知、效能、實用性及整合的需求日新月異，SIEM 使用案例也更加多元。SIEM 解決方案應該是降低複雜性，而不是雪上加霜。您可期待 SIEM 做更多。

SIEM 目前必須融入企業與安全性要務達成一致的大型連線安全性架構才能有效運作。SIEM 在打造更具策略性的安全性並提供實際的企業價值方面扮演了十分重要的角色。

若要深入瞭解 McAfee 的各項 SIEM 解決方案，請造訪：www.mcafee.com/tw/products/siem/index.aspx。

Security Connected

McAfee 的 Security Connected 平台能爲數百種產品、服務及合作夥伴提供統一化架構，助其彼此瞭解、即時共用特定內容的資料，並以團隊的身分來保護資訊和網路的安全。任何組織均可透過該平台的創新概念、最佳化程序及實際節約，來改進自身的安全性狀態並將營運成本降至最低。

McAfee
An Intel Company

邁克菲有限公司台灣分公司
台北市 110 基隆路一段
333 號 22 樓 2210 室
886-2-2757-6677
www.mcafee.com/tw