McAfee Enterprise Security Manager

排定優先順序。調查。回應。

最有效的安全機制就從監看系統、網路、資料庫及應用程式上的所有活動開始。安全性資訊和事件管理 (SIEM) 是實現有效安全架構的基礎。McAfee® Enterprise Security Manager 是 McAfee SIEM 解決方案的核心，能以資安部門所需的速度和規模，提供效能、可行的情報及解決方案整合。如此可讓您針對隱藏的威脅快速排定優先順序，加以調查並做出回應，同時符合規範要求。

McAfee Enterprise Security Manager 不僅能提供真實現況 (威脅資料與信用評價摘要) 的即時資訊，也能讓您瞭解企業內的系統、資料、風險和活動。您的安全性團隊將可存取完整且相關的必要內容，然後迅速依據風險考量制定決策，讓您得以投入相關資源以妥善因應變動的威脅與營運態勢。這對於調查「潛伏式」攻擊、搜尋入侵指標 (IoC) 或修正稽核結果而言，是左右成敗的關鍵。為了讓威脅與符合性管理工作成為安全性作業不可或缺的一部分，McAfee Enterprise Security Manager 也提供整合式工具，讓您管理組態和變更、管理個案及集中管理原則等，執行一切必要工作，來改善工作流程並提高安全性作業團隊的效率。此外，McAfee Enterprise Security Manager 亦提供內容包，內含進階安全性使用案例的預先建置組態，有助於簡化安全性作業。

為企業規模而打造

安全性作業團隊極需更高的效率，才能從現今的動態及分散式企業架構中收集日漸龐大的原始與剖析資料量，並快速進行探索。為了克服這項挑戰，McAfee Enterprise Security Manager 採用專為處理大量資料而設計的可擴充的開放式資料匯流排。此外，具高度擴充性的資料架構也能支援擷取、管理和分析工作，以維持收集、搜尋及留存資料的能力。如果這類能力有所減損，便可能發生無法在日後取得重要資料、查詢回應減慢分析速度，或是因效能問題致使只能執行部分搜尋的情形，進而損及調查結果。

主要優勢

- **情報導向：**進階分析資料和豐富的內容可協助您偵測威脅並排定優先順序。
- **可付諸施行：**您需要的資料都會以動態效果呈現，並提供可行的選項，包括針對重要的警示和模式進行調查、遏止、修正及調整。
- **整合式：**此解決方案可從廣泛的異質安全基礎架構監控及分析資料，並透過開放式介面提供雙向整合。如此還可讓許多初期回應動作自動執行。

與我們聯絡

在幾分鐘內找出關鍵事證，而無需延宕數小時

在調查事件、搜尋進階攻擊的證據、或試圖補救失敗的符合性稽核時，能否快速存取長期儲存的事件資料將是關鍵，因為這些作業全都有賴於詳查歷史資料，以及完整存取每起特定事件的所有詳細資料。

經高度調整的裝置可依照您所需的速度收集及處理數年來累積的記錄事件，並與其他資料流相關聯，包括 STIX 威脅情報摘要。McAfee Enterprise Security Manager 可儲存數十億筆事件與流程資料，讓所有的資訊皆可立即用於特定查詢，同時長期保留資料以供鑑識、規則驗證及符合性工作。此外，資料可立即複製到多個儲存位置，以維護業務持續性。

內容感知

有可用的內容相關資訊時 (包括威脅資料和信用評價摘要、身分和存取管理系統、隱私權解決方案或其他支援的系統)，每起事件中都會加入對應的內容。這種添加內容的作法可讓您根據網路和安全性事件與資產屬性、實際商業流程及原則的關聯程度，進一步瞭解分類並使分類更準確。

McAfee Enterprise Security Manager 的可擴充性與效能可讓您從更多來源收集更多資訊 (包括文件、交易及通訊等應用程式內容)，進而獲得更深入的鑑識價值。這些資訊全都經過縝密的索引編排、標準化與關聯化，以協助您擴大偵測風險與威脅的範圍。

進階威脅解譯

無論是網路流量、使用者活動還是應用程式使用情形，任何異於正常型態的活動，都可能意味著潛在的威脅，或是您的資料或基礎架構正面臨風險。McAfee Enterprise Security Manager 可對所有收集到的資訊計算基準活動，這是為了在潛在威脅出現前，依照優先順序對您發出警示，同時分析該資料的模式中是否潛藏更大的威脅。McAfee Enterprise Security Manager 還能運用內容相關資訊，為每起事件加入對應的內容，以進一步瞭解安全性事件對實際商業流程有何影響。

McAfee Enterprise Security Manager 的 Cyber Threat Manager 儀表板不但有加強的即時監控功能，還能讓您瞭解新興威脅。透過 STIX/TAXII、McAfee Advanced Threat Defense 及/或第三方 Web URL 回報可疑或經確認的威脅資訊時，可以近乎即時的速度或以歷史記錄的方式 (運用追溯功能)，根據事件資料彙總及關聯這些資訊，讓安全性團隊深入瞭解環境中的威脅散佈情況。這些情報可讓組織正確對應資料與人員，以近乎即時的速度採取行動，並做出更明智的決策。

最佳化安全性作業

McAfee Enterprise Security Manager 以分析人員為中心的使用者經驗可提供更多彈性、自訂能力，並更快就調查結果做出回應。簡化的工作流程能更及時有效地管理事件。由於可迅速且聰明地存取威脅資訊，不論何種經驗程度的分析人員 (從新手到專家) 都會發現，針對演進中威脅排定優先順序、進行調查並做出適當回應，都比以往更為容易。

您可以立即使用 McAfee Enterprise Security Manager 以及數百種現成的報告、檢視、規則和警示，更可以輕鬆加以自訂。無論是想設定基準以便瞭解一般網路使用情形，或只是想要自訂警示，McAfee Enterprise Security Manager 的儀表板都能輕鬆顯示、調查並報告最相關的安全性資訊。您的組織現在可以存取所有需要的相關資料與內容，迅速做出明智決策。

此外，McAfee Enterprise Security Manager 還提供內容包，以預先設定且已「準備就緒」的安全性使用案例簡化安全性作業，讓您擁有快速處理進階威脅或管理符合性的能力。內容包為常見安全性使用案例的預先建置組態，可提供一系列規則、警示、檢視、報告、變數及觀察清單。許多內容包都提供預先封裝的行為觸發程序，或許可以保證帶來額外的安全性或自動修正能力。

簡化規範

McAfee Enterprise Security Manager 可將符合性監控與報告作業集中化和自動化，藉此免除耗時的人工作業。此外，整合 Unified Compliance Framework (UCF) 便可實現「收集一次，多項遵守」的方法，藉此滿足符合性需求，盡可能減少稽核的工作量與支出。支援 UCF 後即可將各項法規的細節標準化，以便將一組集合事件對應到相關法規，藉此提高符合性效率。

McAfee Enterprise Security Manager 提供數百種預先建置的儀表板、完整的稽核追蹤項以及適用於超過 240 種全球法規和控制架構 (包括 PCI-DSS、HIPAA、NERC-CIP、FISMA、GLBA、GPG13、JSOX 及 SOX) 的報告，以簡化並加快符合性管理作業。McAfee Enterprise Security Manager 除了提供廣泛的立即可用支援之外，還可讓您完全自訂所有符合性報告、規則及儀表板。

連結您的 IT 基礎架構

跨安全性基礎架構的整合提供了前所未有的即時可見性，讓您掌握組織的安全計劃。McAfee Enterprise Security Manager 可從數以百計的第三方安全性廠商裝置，以及從各筆威脅情報摘要收集有價值的資料。與 McAfee Global Threat Intelligence (McAfee GTI) 的整合，可帶來 McAfee Labs 超過 1 億個全球威脅偵測器的資料，持續提供最新的已知惡意 IP 位址摘要。McAfee Enterprise Security Manager 還能接收透過 STIX/TAXII 和/或第三方 Web URL 回報的威脅資訊，並根據分析結果採取行動。

McAfee Enterprise Security Manager 也主動整合各個項目，以提供輔助性事件管理功能和分析解決方案，包括 McAfee 解決方案和 McAfee Security Innovation Alliance 合作夥伴解決方案。

舉例來說，McAfee Threat Intelligence Exchange 能以端點監控為基礎，利用全球第三方與本機威脅情報，彙整低普遍性的攻擊資料。McAfee Threat Intelligence Exchange 還能利用其他整合式產品 (例如 McAfee Advanced Threat Defense)，進一步分析和判定檔案。

分析人員也可受惠於與 McAfee Behavioral Analytics 的整合，這個專屬的使用者與實體行為分析解決方案可將數十億筆的安全事件去蕪存菁，轉化為數百筆異常狀況，藉此產生經過排定優先順序的豐富威脅線索，使分析人員得以發掘其他解決方案常無法辨識、具有高風險且不尋常的安全性威脅。同樣地，McAfee Enterprise Security Manager 與 McAfee Investigator 整合，可協助分析人員搖身一變，成為專業調查人員，並判斷出根本原因，從而在更短時間內胸有成竹地解決更多案例。

安全性事件回應團隊和管理員可使用 McAfee Active Response 尋找潛伏在系統以及記憶體內作用中處理序中的惡意零時差檔案。McAfee Active Response 亦可利用持續運作的收集器來不斷監控端點是否有具體 IoC；如果環境中某處出現 IoC，便會自動向您發出警示。有別於標準安全機制作法，這兩者的結合能為組織提供從發現攻擊到遏止及修正攻擊為止的封閉迴路式詳細工作流程。

McAfee 提供整合式安全性系統，可讓您抵禦新興威脅並予以回應。我們可協助您以更少的資源更快解決更多威脅。而我們互相連結的架構和集中式管理更可降低複雜程度，並改善整個安全性基礎架構的作業效率。McAfee 致力於成為您首選的安全性合作夥伴，為您提供完整的整合式安全性功能組合。

深入瞭解

如需 McAfee Enterprise Security Manager 的詳細資訊，請造訪 **www.mcafee.com/tw/products/siem/index.aspx**。

如需整合式解決方案的詳細資訊，請造訪 **https://www.mcafee.com/tw/solutions/intelligent-security-operations.aspx**。

McAfee Together is power.

台灣
台北市信義區忠孝東路五段 68 號 29 樓，11065
電話：+886 2 8729 9222
www.mcafee.com/tw