McAfee Database Event Monitor for SIEM

得以監看資料庫交易，且不會影響系統效能

對資料庫交易進行可靠的稽核，是符合性不可或缺的，但傳統的原生資料庫稽核解決方案卻可能拖累資料庫效能與資料庫管理員的生產力。McAfee® Database Event Monitor for SIEM (安全資訊與事件管理) 非入侵式的設計，可支援您愈來愈高的符合性稽核與報告需求，並可強化安全的操作。

McAfee Database Event Monitor for SIEM 能夠以非入侵的方式詳細記錄資料庫與應用程式的安全性，監視所有對公司與客戶敏感資料的存取。只需些許的部署工作，您即可深入監看資料庫交易、事件與特定的資料庫查詢及回應，包括資料的存取者是誰，及其原因為何。

McAfee Database Event Monitor for SIEM 是同類產品中，唯一可將資料庫活動合併到集中稽核存放庫，同時又能夠對該活動進行標準化、關聯、分析與報告的獨特產品。

藉由預先定義的規則與報告以及尊重隱私權的記錄功能，可讓您輕鬆符合法規遵循規定同時強化整體的安全性狀態。

內容的資料庫存取

McAfee Database Event Monitor for SIEM 不只可以記錄，還能進一步標準化資料，並將資料庫交易與其他資訊產生關聯，以協助您執行即時分析。

McAfee Database Event Monitor for SIEM 將可監看的範圍擴及使用者資訊、應用程式內容、作業系統活動、弱點甚至網路位置，而讓您能夠：

- 在應用程式間追蹤使用者
- 從登入到登出，檢查整個工作階段活動
- 偵測敏感資料，並識別原則違規的情形
- 透過授權的通道偵測資料遺失的情形
- 讓資料庫活動與安全性事件產生關聯
- 建立所有資料庫活動的稽核追溯
- 產生 PCI DSS、HIPAA、NERC-CIP、FISMA、GLBA、GPG13、JSOX、SOX 等標準的詳細報告

主要優點

- 使用被動式網路型監視，完全不會干擾資料庫效能
- 探索所有的資料庫例項，包括未經授權或未管轄的資料庫
- 可使用法規資訊來監視與記錄資料庫
- 存留登入至登出期間所有資料庫交易的詳細資料，以支援稽核作業
- 「一鍵」重新建構工作階段，以簡化分析工作
- 可與 McAfee Enterprise Security Manager完整整合，以在事件關聯與其他進階 SIEM 活動中使用資料庫交易
- 彈性的混合式傳送選項，包含實體裝置與虛擬裝置

完整監看每一項交易

McAfee Database Event Monitor for SIEM 可監視所有的資料庫交易，並且對所有的資料庫活動 (包括查詢、結果、驗證活動與權限提升等) 進行完整的稽核追溯。McAfee Database Event Monitor for SIEM 會保留所有交易的完整工作階段詳細資料，因此您將可輕鬆檢視從登入到登出，任何給定交易的之前與之後所發生的情形。

自動化符合性程序

預先建置的原則型偵測規則與符合性報告，可確保您能夠產生 PCI DSS、HIPAA、NERC-CIP、FISMA、GLBA、GPG13、JSOX、SOX 等標準所要求的資料存取資訊。此外，McAfee Database Event Monitor for SIEM 也能夠與 McAfee Enterprise Security Manager 和 McAfee Enterprise Log Manager 完整整合，而提供前所未見的事件分析與關聯功能，以及對活動記錄中的敏感資料提供的符合的儲存功能與遮罩功能。例外清單會顯示未受監視的資料庫伺服器，以及開放讓外界存取資料庫資料的非法連接埠。

使用者與帳戶追蹤

使用 McAfee 安全性管理產品系列的進階功能，可輕易地在不同的應用程式與帳戶間追蹤使用者與管理員，以提供所有使用者活動的端對端權責歸屬，無論他們存取資料庫的方式為何。

使用者活動資料設定

McAfee Database Event Monitor 會將每個 SQL 查詢 Token 化到命令中，在產生每個使用者行為的設定檔時，會在目標資料庫伺服器上存取物件 (表格、檢視、儲存程序)，進而同時顯示新活動與異常活動。

SQL 隱碼

所有的 SQL 查詢回應封包都會受到監視，無論查詢成功或失敗。語法錯誤等低嚴重性的失敗屬於 SQL 隱碼攻擊的特徵，若連續發生即會受到追蹤並進行關聯，進而確保可主動偵測出 SQL 隱碼攻擊的意圖。

風險與威脅偵測

McAfee Database Event Monitor for SIEM 可根據可自訂的原則規則集分析所有受監視的活動，並且偵測所有可疑活動，然後發出警示。此外，異常型偵測則會指出異常的使用者活動、查詢、回應與其他不適當行為。

功能強大，且不會造成額外負荷

McAfee Database Event Monitor for SIEM 裝置具有高效能的資料擷取引擎，可透過網路監視您的資料庫，而不會對資料庫本身造成額外負荷，並且可確實存留您所需要的稽核資料。

資料庫監視功能

- 監視並記錄所有的資料庫活動
- 支援符合性工作
- 防止竊聽
- 提高權責歸屬性
- 對物件、動作與原則違規發出警示
- 擷取寶貴度量以供資料庫服務層級/效能管理所用
- 監視資料的所有傳送途徑，包括：
  - 應用程式
  - 使用者
  - 惡意軟體
  - 公用程式
  - 後門程式
  - 查詢
  - LAMP 指令碼處理
  - Open Database Connectivity (ODBC)

McAfee Enterprise Security Manager 除了提供管理功能外，也可連結資料庫監視功能與您其他的安全性與符合性生態系統。若要能夠監看本機終端機活動，請使用選用性的主機代理程式，因為它所造成的效能影響低於競用的主機代理程式或原生稽核功能。

使用案例

法規遵循

McAfee Database Event Monitor for SIEM 可探索使用中的敏感資料，以協助您確保符合性。您可以監視這些資料庫，並為受保護的資料存取、使用者帳戶活動與變更建立稽核追溯。安全工作可與資料庫管理工作區隔開來，以便嚴格控制，而敏感資料則可加上遮罩以防記錄。報告中可突顯最常使用受保護記錄的客戶。可隨時產生針對不同法規所預先建置的報告。

資料庫的偵測與分類

McAfee Database Event Monitor for SIEM 可監視網路上的資料庫命令，以偵測所有的資料庫例項，包括不明或未管轄資料庫。此外，McAfee Database Event Monitor for SIEM 也可監視所有的交易 (包括查詢結果)，並根據原則規則與字典加以分析，以偵測哪些資料庫存有信用卡、身分證號碼或其他敏感資料。

安全性監視

McAfee Database Event Monitor for SIEM 可直接監視您的資料庫，並且可偵測暴力密碼破解登入、SQL 隱碼攻擊、異常存取型態，以及其他可能顯示您的資料庫伺服器可能遭入侵的跡象，同時立即對您發出警示。您可以監視後端應用程式活動並偵測可疑活動，包括詐騙式資料擷取與惡意使用者帳戶等。

如果攻擊來自網路內部，您可以追蹤使用者活動並根據網路流量資料進行關聯，以識別並找出攻擊者。如果攻擊來自於外部，則可以根據其他出埠的網路與應用程式活動，對安全性缺口進行關聯，以探索資料遺失、隱匿的訊通道與其他破壞媒介。

深入瞭解

如需詳細資訊，請造訪我們的網站，網址為：**www.mcafee.com/tw/products/database-event-monitor-for-siem.aspx**。

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