資料工作表

McAfee Global Threat Intelligence for Enterprise Security Manager

將 McAfee® Labs 的威力運用於情境感知功能。

McAfee® Global Threat Intelligence for Enterprise Security Manager 將 McAfee Labs 的威力帶入企業安全性監視用途。由 McAfee Labs 自超過 1 億個全球威脅偵測器收集而成的 IP 信用評價，首次可用於安全性資訊和事件管理 (SIEM) 解決方案。本產品向 McAfee Enterprise Security Manager 不斷提供豐富摘要並持續更新，可透過啟用快速探索涉及與可疑或惡意 IP 通訊的事件，來增強態勢感知功能。這使安全管理員能夠決定哪些主機曾經或正在與惡意對象通訊，並在已知惡意對象為威脅活動來源時快速識別狀況。

對外部內容的需求

安全性事件可及時提供安全相關活動的資訊。雖然 SIEM 有關聯這些事件的能力，仍然有幾個問題尚待操作員解決：這個活動可接受嗎？怎麼知道哪些事件是最緊急的？如何偵測不易察覺的複雜攻擊？將一般企業數量逾 2.5 億的日常事件與這些問題疊加後，會清楚發現舊版 SIEM 所專注的已知模式偵測作業，顯然只是安全性監視龐雜作業中的冰山一角。在此未知情況背後，最重要的內容因素之一是對於外部系統信用評價的瞭解。到目前為止，要對於安全性事件有如此透徹的瞭解，都並非可能。

McAfee Labs 的威力導向 SIEM

McAfee Global Threat Intelligence for Enterprise Security Manager 可透過 McAfee SIEM 專為大型安全性資料所打造之高速、高智慧特性，將 McAfee Labs 的威力直接導入安全性監視流量中。這項選用的訂閱服務將持續提供並調整超過 1 億 4 千萬筆 IP 位址的來源信用評價，將外部系統信用評價的內容直接帶入安全性事件串流，可迅速識別目前及過去與已知惡意對象的互動。McAfee Global Threat Intelligence (GTI) IP 信用評價源於所有主要威脅媒介之威脅情報的關聯，使用超過 1 億個全球偵測器，並集結超過 500 位研究員的心力。

主要優勢

- 將 McAfee Labs 的威力帶入 SIEM。
- 正確瞭解與事件相關聯的風險。
- 充分利用 McAfee GTI 大量的威脅摘要，同時不影響效能。
- 在 McAfee Enterprise Security Manager 中自動接受和處理來自新來源的信用評價。
- 提高威脅偵測的精確度，同時減少回應時間。
- 快速識別與殭屍網路/分散式阻絕服務 (DDoS)、主控網路探測的郵件/垃圾郵件發送惡意軟體、惡意軟體之存在、DNS 代管和入侵攻擊所導致的活動相關聯之已知惡意行為者的攻擊路徑和過往互動。

McAfee Global Threat Intelligence for Enterprise Security Manager 的效益

- **增強對整個網路的保護：**當網路上任何節點與可疑或已知惡意行為者進行通訊時，McAfee Global Threat Intelligence for Enterprise Security Manager 能夠立刻偵測並迅速瞭解該威脅的路徑。
- **風險型優先順序：**IP 信用評價自動併入 McAfee Enterprise Security Manager 較少規則風險計分演算法之中，能夠自動計算出回應的必要性。
- **24/7 威脅監視：**McAfee Labs 持續搜尋威脅資訊以偵測最近受感染和惡意的系統，以及那些系統被清除的時間，使組織對全球威脅環境有最新且正確的瞭解。

即時鎖定惡意活動

組織擁有 McAfee Global Threat Intelligence for Enterprise Security Manager 後，即可掌握任何事件，瞭解異質性防火牆、入侵預防系統、路由器和端點的 IP 信用評價等事件之內容。利用 McAfee Enterprise Security Manager 的動態關注清單功能，事件會自動與來源信用評價分數相關聯，進而調整風險。隨著全球威脅不斷改變，McAfee GTI 確保 McAfee Enterprise Security Manager 處於最新狀態，讓伺服器和系統持續具備精確的信用評價分數。這不僅可協助組織瞭解風險，也能夠即時指出緊急問題、縮短事件回應時間範圍，和提供正確的風險分析結果。

發現你還不知道的事

McAfee Enterprise Security Manager 的核心優勢是能夠對數年的資料進行儲存、擷取並執行歷程關聯作業的能力。現在，McAfee GTI 讓安全分析人員能夠回溯數年的資料，瞭解過去與惡意對象的互動情形。偵測「低調且緩慢」的攻擊、來自殭屍網路的反復活動、跨站台指令碼處理和 SQL 植入嘗試，這些均至關重要。

縮短回應時間

McAfee GTI 與 McAfee Enterprise Security Manager 警告和警示機制緊密整合，確保與已知惡意系統的互動能得到應有的注意。

有 McAfee 資料庫作為強力後盾，為大型安全性資料量身打造。

關於資料日益龐大的討論不知凡幾，這些討論內容也包含將 McAfee Labs 豐富的安全性相關知識帶入 SIEM。McAfee Enterprise Security Manager 具有儲存、關聯和更新大量 McAfee GTI IP 信用評價資料儲存的獨特能力，並且不會產生不可接受的效能影響。McAfee Enterprise Security Manager 擁有專有資料庫，不僅為 SIEM 免除曠日費時的資料庫管理程序，其也是專門為以極高速大量攝入和處理事件及關聯式資料的作業所打造。擁有 McAfee Global Threat Intelligence for Enterprise Security Manager，客戶可以確信 McAfee GTI 知識將會即時傳送。

規格

支援的版本

《McAfee Enterprise Security Manager 9.4》和《McAfee Event Reporter Appliance 9.4》

- McAfee Labs 威脅情報網路：在超過 120 個國家中擁有超過 1 億個節點
- 平均 IP 信用評價：依威脅環境而有所不同

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

2014 年 9 月