McAfee Advanced Correlation Engine

根據您重視的要項來偵測威脅

面對現今難以察覺的威脅，以標準規則為準的威脅偵測功能已不敷使用。部署附有 McAfee Enterprise Security Manager 的 McAfee® Advanced Correlation Engine 解決方案，可使用以規則與風險為基礎的邏輯即時識別威脅事件，並加以評分。您只要在 McAfee Advanced Correlation Engine 解決方案中指定您所重視的要項 (使用者或群組、應用程式、特定伺服器或子網路)，即會在此資產受到威脅時對您發出警示。審查追溯和歷程重播可支援鑑識、符合性和規則微調。

McAfee Advanced Correlation Engine 解決方案以兩部專用的關聯引擎以及針對特殊目的建置的效能，補強 McAfee Enterprise Security Manager 的事件關聯功能：

- 一部風險偵測引擎，可使用非規則型風險分數關聯產生風險分數
- 一部威脅偵測引擎，可使用傳統規則型事件關聯來偵測威脅

獨立式 McAfee Advanced Correlation Engine 解決方案可提供足夠的處理能力，支援您針對整個企業環境使用此種多樣化的事件關聯功能。其資料引擎可調整規模，甚至可因應最大型網路的需求。

即時與歷程威脅偵測

McAfee Advanced Correlation Engine 解決方案可部署為即時模式或歷程模式。在即時模式下，McAfee Advanced Correlation Engine 解決方案會在收集事件時就對事件進行分析，以立即偵測威脅與風險：

- 當威脅發生時，採用即時事件資料的規則型關聯進行偵測
- 針對發展中威脅，採用即時事件資料的非規則關聯進行偵測

在歷程模式下，任何收集到的資料皆可透過這兩部關聯引擎進行「重播」，以執行威脅與風險的遞迴偵測。發現零時差攻擊時，McAfee Advanced Correlation Engine 解決方案可回溯確認您的組織過去是否曾遭受該攻擊，進行零時差威脅子偵測。

主要優點

- 可簡單啟動：無需更新規則、調整特徵碼或執行其他麻煩的作業
- 在威脅鎖定您優先重視的使用者、資產、應用程式與活動時發出警示
- 同時運用規則型與非規則型關聯，準確地執行評分
- 可讓您針對歷程記錄檢查新的攻擊與弱點，以偵測過去的事件
- 為 McAfee Enterprise Security Manager 加入了特殊的關聯與處理資源
- 在裝置與虛擬部署中均可使用

在需要時提供專屬的效能

McAfee Advanced Correlation Engine 解決方案是具有獨立運作能力的裝置或虛擬產品，因此絕對不會影響到 McAfee Enterprise Security Manager 的事件收集與事件管理方面的效能。您可以完全利用 McAfee Advanced Correlation Engine 應用程式的所有功能而不需妥協，同時讓 McAfee Enterprise Security Manager 公用程式發揮最大效用。

規則型事件關聯

規則型關聯會採用傳統關聯邏輯來分析即時收集的資訊。所有記錄、事件與網路資料流及內容資訊 (例如身分識別、角色、弱點等) 都會彼此產生關聯，以偵測有可能為較大威脅的型態。雖然所有的 McAfee Enterprise Security Manager 解決方案均已直接支援全網路規則型的關聯，但 McAfee Advanced Correlation Engine 解決方案所提供的專用處理資源可為更大量的資料建立關聯，以補強或完全擔負起現有的關聯工作。

無規則的風險分數關聯

雖然規則型關聯對於任何傳統安全資訊與事件管理 (SIEM) 而言，都是必要且很有價值的功能，但這些系統只能偵測已知的威脅型態，而且必須持續調整特徵碼並進行更新，才能維持效用。以「非規則型」關聯技術補強傳統事件關聯，可成功解決這個問題。在非規則型關聯系統中，偵測特徵碼會替換為簡易的一次性組態設定：您只要讓 McAfee Advanced Correlation Engine 解決方案瞭解對您業務最重要的部分即可。可以是特定的服務或應用程式、某個使用者群組，或是特定類型的資料。

即時追蹤與警示

接著，McAfee Advanced Correlation Engine 解決方案即會開始追蹤所有與這些項目相關的活動，並產生隨著即時活動而上升或下降的動態風險分數。當風險分數超出特定閾值時，McAfee Advanced Correlation Engine 解決方案內即會產生事件。此事件可用來對安全性分析人員發出威脅情況加劇的警示，或者可供傳統規則型關聯引擎當作較大資安事件的產生條件。McAfee Advanced Correlation Engine 解決方案會保存風險分數的完整稽核追溯，以供日後長期完整分析及調查威脅情況之用。

使用案例

建立企業風險模型

McAfee Advanced Correlation Engine 解決方案提供可讓您有效建立企業風險模型的平台。具有高層級權限的員工能夠存取高度機密文件，這一點對於軍事防衛組織可能會構成風險，而診斷出名人罹患重大疾病的病歷若不慎外洩，則可能對醫院構成風險。McAfee Advanced Correlation Engine 解決方案會針對您組織最重視的屬性進行評分，為組織提供無懈可擊的風險模型——它可擬定基準，並於超出正常閾值時傳送通知。

根據關鍵資料進行主動式風險評估

使用 McAfee Advanced Correlation Engine 解決方案監視即時資料時，可同時使用這兩種關聯引擎，搶先在風險與威脅發生之前便加以偵測。傳統的關聯邏輯中可使用風險分數。例如，傳統規則型威脅偵測特徵碼可能會是「在暴力密碼破解登入事件後發生的惡意軟體事件」。在正常情況下，早在此特徵碼觸發之前，事件已經發生。不過，有了 McAfee Advanced Correlation Engine 解決方案，現在可改為加入風險係數，例如「在暴力密碼破解登入事件後將風險分數增加 20%」。在發現此事件時，McAfee Advanced Correlation Engine 解決方案可提供有資安事件即將發生的主動式警示，及早在損害造成前加以預防。

遞迴威脅評估

發現某個威脅或者揭露安全缺口的情況並不少見，只是我們更擔心此威脅或缺口是否已存在多時。只要將 McAfee Advanced Correlation Engine 解決方案部署為歷程模式，其中所含的任何歷程資料集都可透過傳統與非規則型關聯引擎進行重播。

在確認新發現的威脅首次現身的時間後，我們就更有可能找出該情況的真正成因。

操作模式

即時關聯模式：

- 當威脅發生時，採用即時事件資料的規則型關聯進行偵測
- 針對發展中威脅，採用即時事件資料的非規則關聯進行偵測

歷程關聯模式：

- 進行遞迴威脅偵測時，會對歷程事件資料採用規則型關聯
- 進行遞迴威脅評估時，會對歷程事件資料採用非規則型關聯

關聯功能

- 同時運用規則型與非規則型關聯
- 與所有支援的資料來源建立資料關聯
- 與分散式網路與收集器上的資料建立關聯
- 加入數百項預先定義的事件關聯規則
- 加入非規則型關聯的組態編輯器
- 加入易於使用的 GUI 事件關聯規則編輯器，以自訂規則或建立新規則

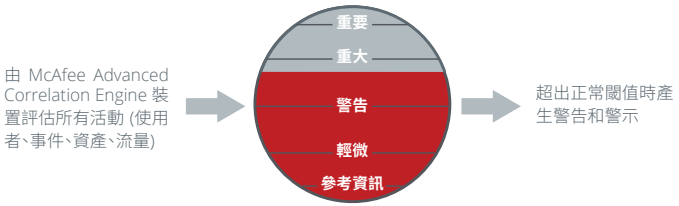

圖 1. 風險型關聯可協助您根據優先重視的資產偵測潛在的威脅。

深入瞭解

如需詳細資訊，請造訪 **www.mcafee.com/tw/products/siem/index.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