IBM Security QRadar SIEM

整合式調查報告系統改善威脅保護與法規遵循管理

產品特性

- 將日誌管理功能與網路威脅保護技術整合至共用資料庫及儀表板式使用者介面
- 將數千筆安全事件簡化為一份易於管理的可疑攻擊清單
- 延長偵測及追蹤惡意活動的時段，協助發掘常遭其他安全解決方案忽略的進階威脅
- 進階的內部詐騙偵測功能
- 協助超越法規要求並支援法規遵循

現今網路世界的規模與複雜程度前所未見，如何保護網路免於惡意活動的危害，成為一件永無休止的工作。組織若想保護智慧財產和客戶資料，或避免業務中斷，需要進行的工作可不僅止於監視日誌和網路流程檔案，還必須善用進階工具，偵測各種可能的不當活動。組織無論規模大小，均可採用 IBM Security QRadar SIEM 作為安全作業中心的重點解決方案，利用多年的環境定義見解，收集可用的網路資料，並且將這些資料正規化和關聯化，最後成果便是所謂的安全情報。

本產品的核心部分是一個具備高度擴充性的資料庫，專為捕捉即時日誌事件與網路流程資料而設計，能揭露潛在攻擊者的足跡。QRadar SIEM 為企業級解決方案，可將散佈在網路上、數以千計裝置端點中的日誌來源事件資料加以合併，以原始形式儲存每個活動，再立即將資料關聯化，篩選出真正的威脅，免於誤判。此外，它也能捕捉即時的 Layer 4 網路流程資料，更獨特的是，還可藉由深度封包檢測技術，收集到 Layer 7 應用程式的資料。

QRadar 系列所有產品皆使用相同的直覺式使用者介面，可協助 IT 工作人員快速按照等級辨識並修復網路攻擊，並將上百件警告通知與異常活動模式，大幅簡化為少數攻擊，以便進一步調查。

威脅偵測的即時檢視與優先順序的判定

QRadar SIEM 所提供的監控功能係依據環境定義、可據以行動並涵蓋整個 IT 基礎架構，能協助組織偵測並修復常遭其他安全解決方案忽略的威脅。此類威脅包含應用程式濫用、內部詐騙，以及可能隱身在數百萬個事件之中的進階低速 (Low-and-Slow) 威脅。

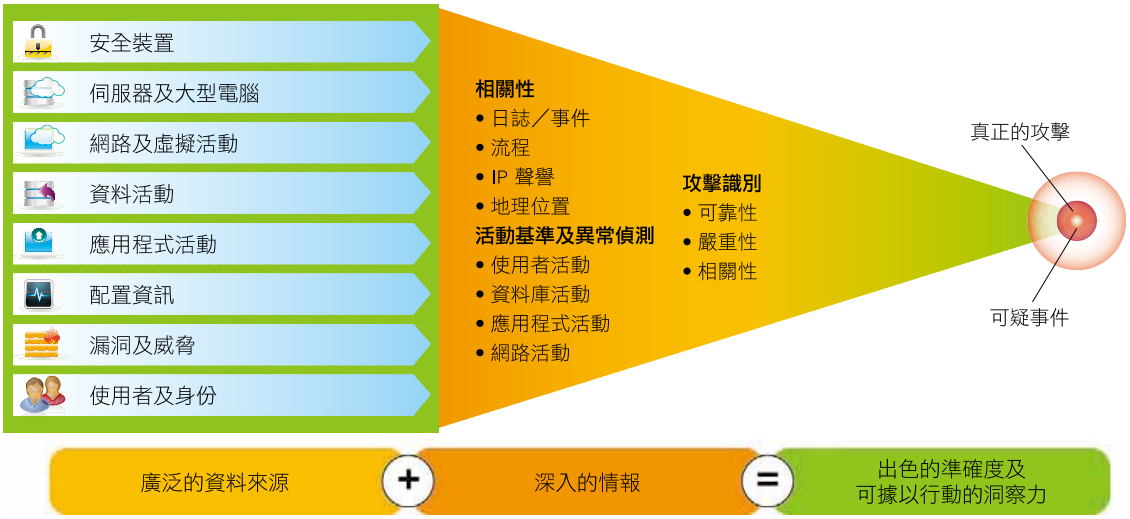
QRadar SIEM 收集的資訊包括：

- 安全事件：來自防火牆、虛擬私密網路、侵入偵測系統、侵入防護系統等的事件
- 網路事件：來自交換器、路由器、伺服器、主機等的事件
- 網路活動環境定義：來自網路與應用程式資料流量的 Layer 7 應用程式環境定義
- 使用者或資產的環境定義：來自使用者身分、存取管理產品及漏洞掃描程式的環境定義資料
- 作業系統資訊：網路資產的供應商名稱及版本號碼特性
- 應用程式日誌：企業資源規劃 (ERP)、工作流程、應用程式資料庫、管理平台及其他

減少警告並判定優先順序，讓調查聚焦於可處理的攻擊

許多組織能在一天之內產生數百萬、甚至數十億筆事件，因此，將資料精簡為一份依攻擊優先順序排序的摘要清單，是件驚人的大工程。QRadar SIEM 可自動搜索大部分網路日誌的來源裝置，並檢查網路流程資料以便尋找並分類網路上有效的主機及伺服器 (資產)，追蹤所使用的應用程式、協議、服務、通訊埠等等，此外還可收集、儲存並分析資料，對事件即時進行關聯化，以供威脅偵測與法規遵循報告和審核使用，數十億筆事件和流程因此能夠依據對業務可能會造成的影響，縮減並按照優先順序排列，精簡為少數可處理的攻擊事件。

如此一來，專業安全人士便可很快看出安裝 QRadar SIEM 的價值，且設定時不需花費高價聘請顧問幫忙。自動探索功能和立即可用的樣板和篩選器，搭配更為大眾化的 IT 作業工具，代表再也不必花上數個月將系統調整為最適合環境的狀態。架構採用事件處理器工具、事件收集工具、流程處理器工具與中央主控台等多重模組，皆可採取硬體式、純軟體使用，或是作為虛擬軟體工具。安裝程序簡便，只要一款多合一解決方案即可開始安裝，也能輕鬆升級至主控台配置，新增所需的事件與流程處理器工具。



QRadar SIEM 收集資料的來源範圍相當廣泛，但它會依照現有或客戶自訂的規則，將資料縮減為一份可處理的攻擊事件清單。

提出關鍵問題，實現更有效率的威脅管理

為了充分理解所面對的潛在威脅，安全團隊必須能夠回答下列關鍵問題：誰在攻擊？哪些地方受到攻擊？對於業務有何影響？需要調查哪些地方？ QRadar SIEM 能追蹤重要的事件和威脅，建立支援資料與相關資訊的歷程記錄，諸如攻擊目標、時間點、資產值、漏洞狀態、不當使用者身份、攻擊者檔案、作用中的威脅以及先前的攻擊記錄等詳細資料，都能讓安全團隊取得所需的情報，以便採取適切的因應行動。

事件與流程資料即時位置導向歷程檢索，專供分析與鑑識使用，可大幅改善組織架構在活動評估及事件解決方面的能力。使用簡便的儀表板、時間序列檢視、往下探查檢索、封包層級內容檢視以及上百種預定義搜尋，可讓使用者快速彙總資料，辨識並總結出異常狀況及最高的活動貢獻者。此外，也能針對分散各地的大型環境執行聯合搜尋。

提高應用程式的可見度及異常偵測能力

QRadar SIEM 可支援各種異常偵測功能，辨識會影響應用程式、主機、伺服器與網路區域的行為改變。例如 QRadar SIEM 能偵測應用程式或雲端服務是否有非正規時間使用或超出正常用量的情況，也能偵測網路活動型樣是否不符合過往平均移動概況及季節性使用型樣。QRadar SIEM 會學習分辨這些每日每周累積的使用檔案，協助 IT 工作人員快速辨識出有意義的異常行為。

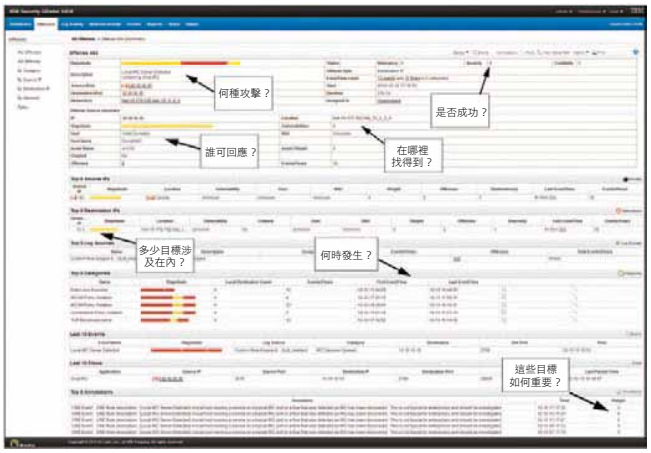
QRadar SIEM 集中式資料庫可同時儲存日誌來源事件與網路流量，協助建立個別事件，以及來自相同 IP 來源的雙向網路流程活動之間的關聯性。此外，它也能分類網路流程的流量，並將短時間內發生的操作記錄視為單一資料庫項目，以減少佔用的儲存空間與軟體使用權。

針對 Layer 7 層的應用程式流量的偵測功能，可讓 QRadar SIEM 針對原則、威脅及一般網路活動監視等方面，提供精準的組織結構分析與解讀。可搭配 IBM Security QRadar QFlow 或 VFlow Collector 軟體驅動裝置，QRadar SIEM 可監視 ERP、資料庫、Skype、網路電話 (VoIP) 及網路社交媒體等應用程式使用，能夠深入剖析誰在使用什麼程式，對內容傳輸進行分析與警告，讓其他網路與日誌活動產生關聯性，以顯示不當的資料傳送或過度的使用型樣。雖然 QRadar SIEM 已附帶有許多異常行為和行動偵測規則，但安全團隊仍可以自行建立篩選功能，以適用於時間序列資料的異常偵測。

採用高度直覺式的單一主控台安全解決方案，進行指揮工作

QRadar SIEM 為組織的安全作業中心提供了一個穩定基礎，集中式的使用者介面可根據角色提供存取功能，並提供全域視圖，可近乎即時地進行分析、管理發生事件並產生報告。五種預設儀表板可供使用，包括安全性、網路活動、應用程式使用、系統監視與法規遵循，使用者也可以自行建立並自訂專屬的工作區。

透過這些儀表板，安全人員能輕鬆觀測警示活動中代表攻擊開始的高峰。按一下圖形即可執行往下探查功能，讓安全團隊能快速調查重點事件，或與可疑攻擊相關的網路流程。除此之外，還有上百種與特定角色相關的樣板、裝置、法規遵循規則及垂直產業等可供使用，有助加速報告產生。



QRadar SIEM 可針對每個可疑攻擊，提供豐富的監測詳細資料，且能夠微調現存規則或新增規則，以減少誤判。

將安全保護擴展至虛擬環境

由於虛擬伺服器與實體伺服器同樣易受安全性漏洞影響，因此完善的安全情報解決方案必須包含適當的方法，才能保護虛擬資料中心內的應用程式與資料。QRadar VFlow Collector 軟體驅動程式能讓 IT 專業人士檢視更多虛擬網路中大量的商業應用程式活動，並更迅速地識別應用程式的安全監視、應用程式層行為分析與異常偵測。操作人員也能收集應用程式內容以進行深入的安全與原則監控。

產生詳細的資料存取以及使用者活動報告以管理法規遵循

QRadar SIEM 具備透通性、責任可追查性、可測量性，能使組織成功符合法規要求以及法規遵循報告。本解決方案能針對監控饋送進行關聯化與整合，可為監控人員帶來更完整的 IT 風險指標報告，以及上百種報告與規則的樣板，滿足企業對於法規遵循方面的需求。

QRadar SIEM 可納入新定義、新規則，並且透過自動更新取得最佳執行常規，這種擴展性能讓組織更有效率地回應以法規遵循為主的 IT 安全需求。此外，網路資產的全部檔案皆可依照商業功能分組，例如受醫療保險轉移和責任法 (HIPPA) 規範審核的伺服器。

解決方案預先內建的儀表板、報告與規則樣板皆根據以下法規與控制框架而設計：CobiT、SOX、GLBA、NERC/FERC、FISMA、PCI DSS、HIPAA、UK GSi/GCSx、GPG 等等。

新增高可用性與災難回復功能

為了達到高可用性與災難回復功能，相同的輔助系統可與所有的 QRadar 工具系列搭配，包括事件處理器裝置、流程處理器裝置及多合一主控台 SIEM 裝置，使用者能隨時新增需要的穩固性與保護度，以確保作業的連續性。

對於尋求業務適應力的組織，QRadar 的高可用性解決方案能提供系統之間的整合式自動失效接手以及全磁碟同步處理。這些解決方案都能透過隨插即用的裝置輕鬆部署，不需額外添購第三方錯誤管理產品。

若是追求資料保護及回復的組織，QRadar 災難回復解決方案可從主要的 QRadar 系統，將現用資料（即流程與事件）傳送至位在分離設施上的輔助平行系統。

漏洞調查

IBM Security QRadar Risk Manager 能與 QRadar SIEM 相輔相成，識別網路中最脆弱的資產，當系統使用中的活動有暴露系統的潛在可能性時，IBM Security QRadar Risk Manager 可立即產生警告。例如，組織可以掃描網路，尋找未修補的應用程式、裝置和系統，決定何者要連接至網際網路，並依各應用程式的風險分析來排定修復的優先順序。更多相關資訊請見 QRadar Risk Manager 資料表。

廣泛的裝置支援協助收集網路事件與流程

QRadar SIEM 支援企業網路部署的 450 多種領導廠商產品，可提供跨越廣泛系統的資料收集、分析與關聯化功能，包括網路解決方案、安全解決方案、伺服器、主機、作業系統與應用程式。此外，QRadar SIEM 能夠輕鬆延伸，用於支援自有的應用程式或 IBM 和其他供應商提供的新系統。

為何選擇 IBM ？

IBM 擁有全世界最廣泛的安全研究、開發及服務能力。IBM 的解決方案能協助組織減少安全漏洞，更專注於策略性計畫的推動。

相關資訊

如需進一步瞭解 IBM Security QRadar SIEM 如何解決貴組織的威脅管理與法規遵循問題，請聯絡 IBM 業務代表或 IBM 企業合作夥伴，也可造訪以下網站：**ibm.com**/security。

關於 IBM 安全解決方案

IBM 安全解決方案提供最先進完整的企業安全產品與服務組合。IBM 安全解決方案獲得世界知名 IBM X-Force 研發團隊的支援，能夠提供安全情報，協助組織完善保護員工、基礎架構、資料及應用程式，並有多元解決方案可因應多種不同需求，包括身份與訪問管理、資料庫安全性、應用程式發展、風險管理、端點管理、網路安全等等。這些解決方案能協助組織有效管理風險，並採取整合式的安全保護措施，保障行動裝置、雲端、社交媒體和其他企業架構的安全。IBM 是全球安全研究、開發及服務最廣泛的企業之一，每天監控 130 多國的 130 億筆安全事件，且擁有超過 3000 項安全專利。

此外，IBM 全球租賃事業部能助您以最符合成本效益與最適切的方式，取得企業所需的軟體功能。我們會與符合信用資格的客戶合作訂定租賃解決方案，符合您的商業和發展目標、啟用有效的現金管理，降低您的總擁有成本。IBM 全球租賃事業部資助重要 IT 投資與推動企業向前邁進。如需相關資訊，請造訪：**ibm.com**/financing

110 台北市松仁路 7 號 3 樓
軟體事業處
技術諮詢熱線：0800-000-700
台北市松仁路 7 號 3 樓

台灣印製
2013 年 1 月

WGD03021-USEN-00