Q1Labs®
Total Security Intelligence

QRadar Log Manager

用於保護網路及符合法規要求的即時記錄管理

針對有安全性、稽核與報表需求，而欲收集、保存、防護與分析大量網路與安全性事件記錄的企業組織，提供全方位、高效能與前瞻性的記錄管理

可輕鬆符合法規要求

擁有超過2000個立即可用的規則與報表，讓企業組織能夠輕鬆達成稽核與報告需求，並符合PCI、沙賓法案 (Sarbanes-Oxley)、HIPAA、NERC CIP及 GLBA 等法規遵循要求。針對安全回應團隊的自動化警示可實現即時的原則執行。

加強記錄資料的可視性，提升可據以行動的 IT 營運及安全性鑑識

大多數的企業組織會產生數量龐大的記錄，而手動分析這些記錄會遭遇許多挑戰。利用 QRadar® Log Manager 靈活的佇列引擎，即可將不同的記錄資料彙總並關聯至可據以行動的IT鑑識，進而找出攻擊模式、異常狀況、機密資料的存取和使用與內部威脅。透過立即可用的相關規則，和預先定義的安全性、原則及法規遵循導向搜尋，即可讓企業組織以更快的速度調查並解析各種威脅，進而輕鬆分析所有記錄、產生全方位的報表並降低風險。

提升收集和保存記錄的效率

QRadar Log Manager 可以利用擴充的方式輕鬆收集和儲存大量資料，以支援每秒數十萬個事件。其卓越的壓縮方式可以大幅減少儲存空間，因此可以有效儲存記錄，進而免除外接式儲存裝置的需求。

統包解決方案可獲得立竿見影的結果

QRadar Log Manager 裝置的架構可讓您簡化並輕鬆部署安全和高效率的記錄管理解決方案。QRadar Log Manager 可降低複雜性，讓您能夠利用嵌入式記錄存放庫，輕鬆管理存放的資料，並且可以和收集自各種網路及安全性裝置的記錄進行整合。

QRadar® Log Manager

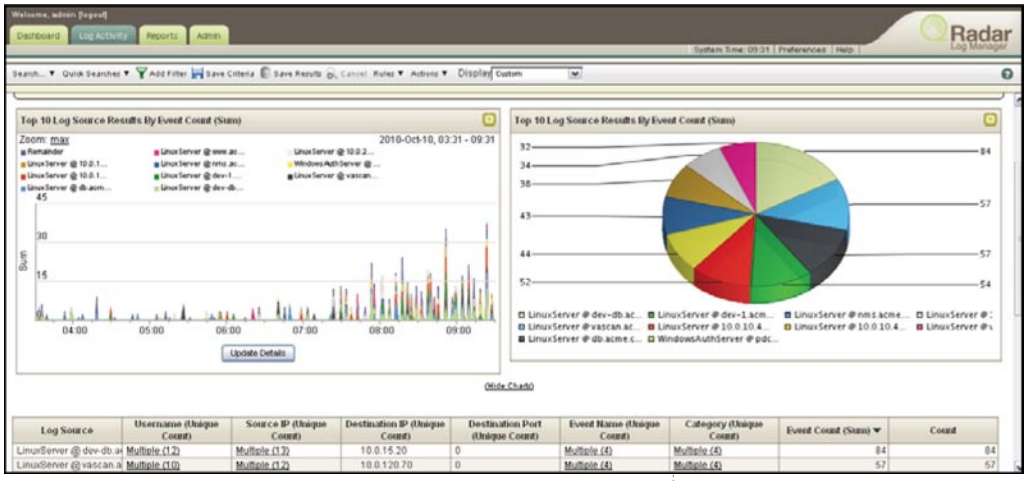
QRadar® Log Manager 可協助資安團隊、IT 營運人員、稽核人員和業務主管：

- 超越法規要求
- 更快解決各項威脅
- 保護網路
- 改善效率和營運項目

可自訂的儀表板可根據功能提供角色型存取，以及針對即時記錄分析、事件管理和報表的通用檢視。

QRadar Log Manager

Log Activity可提供記錄來源的自訂檢視，以及往下探索資料長期趨勢的時間序列檢視。



下層探索的功能可讓您掌控全局

QRadar Log Manager 擁有高度直覺的集中化使用者介面，可依據功能提供角色型存取，以及針對即時分析和報表的通用檢視，可為企業組織的安全或網路團隊提供穩固且直接的基礎架構。QRadar Log Manager 可根據功能提供各種預設的儀表板，且使用者可以建立和自訂專屬的工作區來監控特定活動，以及往下探查時間序列，以檢視資料長期趨勢。如此可以更容易找出異常狀況，或是可能危及企業組織的威脅。

可靠、可擴充及防止竄改的記錄儲存體

QRadar Log Manager 可提供每個裝置高達 6TB 的容錯儲存體，以保存事件記錄並支援廣泛的記錄檔完整性檢查，其中包括防止竄改記錄保存的 NIST 記錄管理標準 SHA-x (1-256) 雜湊。分散式的架構可讓儲存體的容量擴充至多達數百TB。以嵌入式為目的建立的資料庫可進行自我維護，不僅使用方便，而且可以降低整體擁有成本。

全方位的裝置支援

QRadar Log Manager 支援各種網路和安全性裝置的記錄管理，包括：路由器 / 交換器、防火牆、虛擬私有網路 (VPN)、入侵偵測/防護系統 (IDS/IPS)、防毒應用程式、主機與伺服器、資料庫、郵件及網頁應用程式、自訂裝置及專屬應用程式。QRadar Log Manager 可將所有資料標準化為簡單易懂但靈活的分類，有助於簡化跨不同安全性及整體網路裝置的搜尋、關聯與報告。

完整安全性資訊和事件管理(SIEM)的未來成長途徑

QRadar Log Manager 可處理所有的事件並將其標準化，此種作法可以輕鬆獲得安全性情報，同時也可為企業組織提供轉換為 SIEM 的前瞻性途徑。QRadar Log Manager 為 QRadar Security Intelligence Platform 的一部份，其可透過升級授權版本的方式，提供從簡單的記錄管理升級到完整 SIEM 的順暢轉換途徑。

自動容錯移轉的高可用性

加入 QRadar 高可用性後，企業組織即可利用系統之間的自動容錯移轉，以及全磁碟同步處理—此功能通常只有手動執行的昂貴軟體和儲存解決方案才具備。您可以透過架構精簡的隨插即用裝置，輕鬆部署資料儲存和分析的高可用性。

台灣國際商業機器股份有限公司
110 台北市松仁路7號3樓
市場行銷處：0800-016-888按1
技術諮詢熱線：0800-000-700

於台灣列印
2012年11月

DSQRLM0211