IBM Security

IBM QRadar Data Store
無限制授權的日誌管理解決方案

IBM QRadar Data Store能夠建立一個成本效益的日誌管理解決方案，用於深度報告和分析。

- 需要儲存日誌用於報告、搜索、調查、審計、合規和分析？
- 基於EPS（每秒處理事件數）或 GB/Day的授權許可太貴？

IBM QRadar Data Store，規範化和儲存安全和操作日誌，用於將來的分析和審查。

該產品支持無限數量的日誌儲存，而不限制EPS或GB/Day的授權許可，並使您的組織能夠基於儲存的日誌構建靈活的分析、查詢與報告，以獲得對您的IT環境的更深入的瞭解。

方案優勢

1. 解放數據

- 收集、解析、正則化和儲存
- 對每個設備/節點沒有日誌容量的許可限制
- 可對日誌進行搜索、報告、儀表板和構建應用程序
- 針對每個設備/節點使用簡單、固定、低成本的許可

2. 一切由您掌控

- 針對已經部署了（QRadar SIEM的用戶）可使用現有的已部署的能力，不需要額外硬體設備
- 您來定義哪些數據儲存到日誌儲存區（Data Store）
- 可以按照IP，CIDR（網段），日誌來源，正則表達式等來確定什麼樣的日誌進入日誌儲存區（Data Store）
- 當需要時，可將日誌移動到威脅檢測功能（需EPS許可證）

關鍵特徵

- 將提供無限量設備的日誌收集和儲存，而不限制EPS或GB/Day的授權許可
- 可以根據業務需求添加QRadar SIEM EPS許可證，以獲得事件關聯和使用案例的能力，達到安全監控的目的。
- 可規範化和儲存安全以及操作日誌，用於將來的分析和審查。
- 使組織能夠基於該系統儲存的數據，透過API，構建自定義的集成和報告，以獲得對其IT環境的更深入的洞察。
- 將提供超過300種網路安全設備的支援，包括路由器和交換機、防火牆、虛擬專用網路（VPNs）、入侵檢測和預防系統（IDS和IPS）、防毒軟體、主機和服務器、資料庫、郵件和Web應用。
- 能為各種用途和用戶提供儀表板，具備查詢長時間特定時間序列和數據點的能力，用於識別異常和威脅，或審閱日誌活動。
- 提供搜索和合規報告模板，幫助組織解決稽核和法規要求，例如PCI、HIPAA、GLBA、ISO27001、GPG-13等。
- 透過用戶界面查看日誌時，支持數據混淆，以隱藏用戶身份或敏感信息，同時仍保留完整的產品功能，以達到遵守隱私合規的目的。

IBM QRadar Data Store配置

Part #	描　　述
D1RNCLL	IBM QRadar Software Install License
D1S2JLL	IBM QRadar Software Node Install License
D1VRWLL	IBM QRadar Data Store Connection License

推薦硬體配置

型號	Lenovo xSeries 3650 M4 BD
尺寸	29.5"D x 17.6" W x 3.4" H
CPU	2 x E5-2680V2, 2.8 GHz, 10Core, 25 MB Cache (Long Life Processor)
記憶體	128 GB 8 x 16GB 1866 MHz RDIMM
硬碟	12 x 4TB SAS 7.2K rpm (/w Raid 10) RAID Controller: ServeRaid M5210 + 2GB cache
網卡	2 x 10/100/1000 Base-T network monitoring interfaces 1 x 10/100/1000 Base-T QRadar management interface 1 x 10/100/1000 Base-T integrated system management Interface (IMM) 1 x 2 port 10Gbps Intel X520 SPF+ Embedded Adapter

*使用以上硬體配置可最高支持高達30,000 EPS
*以上硬碟僅為推薦配置，可配置更大硬碟以保存更多日誌

可通過增加QRadar EPS授權，支持更多高級安全場景

	高級持續威脅	內部威脅	保護雲	關鍵數據保護	風險和漏洞管理	合規	事件應變
防火牆/路由器	✓	✓	✓	✓		✓	✓
IDS/IPS	✓			✓	✓	✓	
Web代理	✓	✓	✓	✓		✓	
VPN	✓	✓	✓			✓	
DNS	✓		✓		✓	✓	
DHCP	✓	✓				✓	✓
郵件日誌	✓	✓		✓			
DLP	✓	✓		✓		✓	
終端	✓	✓		✓		✓	✓
LDAP/AD/Radius	✓	✓	✓		✓	✓	✓
防病毒	✓	✓	✓	✓	✓	✓	✓
QNI/網絡流	✓	✓	✓	✓	✓	✓	✓
資料庫	✓	✓			✓	✓	✓
終端檢測與應變	✓					✓	✓
AWS/Azure	✓	✓	✓	✓		✓	
Office 365	✓	✓	✓	✓		✓	✓

與我們連繫

若您有任何與IBM資安情報、資安產品或資安服務等疑問，歡迎您來電0800-016-888 按 1，或前往https://www-03.ibm.com/security/tw/zh/ 與線上業務代表互動。