QRadar 中小企业集中日志管理系统

方案建议书

目 录

摘要

我们对您的目标的理解

各种组织机构都相当注重收集、分析、归档及安全地储存大量网络及安全事件日志，他们需要一个高性能、易于使用的综合日志管理系统。这对于当前这个更加物联化、互联化、智能化的世界尤其重要，互联的智能商务比以往产生并存储更多的信息。然而，多数机构依旧采用传统的手动方式来分析每天所产生的大量日志，这不仅非常困难且消耗大量的人力。

IBM 解决方案

通过分析来自不同的网络和安全设备、服务器和运行系统、应用程序及海量终端的全部的日志及事件数据，IBM® Security QRadar® Log Manager 提供对潜在威胁近于实时的可视性同时，符合持续的监控和合规要求。QRadar Log Manager 设备提供流线化、易于部署的解决方案来保障安全高效的日志管理。

我们推荐的方案产品，QRadar 2100 是专门为中小企业提供的、在单一设备上实现的 QRadar SIEM（安全信息和事件管理）方案。QRadar 2100 整合了 SIEM（安全信息和事件管理）、日志管理、内置的网络行为监控功能和特性。它提供了一个易于快速部署的集成的安全解决方案，您可以在数分钟内完成 QRadar 2100 一体化设备的部署，并就此开启你的网络安全之旅。

成功案例

台湾财团法人联合信用卡处理中心：

结合安全事件分析与管理、日志管理、风险管理和网络行为分析为一体得高价值、符合成本效益的产品。 Q1 Labs 具备高可用性、易于扩展、易于部署和使用的特性，可快速实现价值。能立即满足作业面之需求与PCI.ISO27001法规遵循要求。

为什么选择 IBM

IBM QRadar 解决方案开创先河、自成一派，成千上万的客户依靠 QRadar 进行安全与合规管理。QRadar 被世界各地的医疗保健机构、能源公司、零售机构、电力公司、金融机构、政府机构及高校广为采用。

第1章　我们对您的目标的理解

各种组织机构都非常注重收集、分析、归档及安全地储存大量网络及安全事件日志，他们需要一个高性能、易于使用的综合日志管理系统。这对于现今这个更加物联化、互联化、智能化的世界尤其重要，互联的智能商务比以往产生并存储更多的信息。然而，多数机构依旧采用传统的手动方式来分析每天所产生的大量日志，这不仅非常困难且消耗大量的人力。

如何通过对分布式的数据进行分析，找出潜在威胁并保护基础设施？

我们发现，促成当今现状的变化主要有以下几点：

- 企业需要收集、分析、归档和安全的储存大量网络及安全事件日志。
- 大多机构产生大量的日志。
- 为了保护全部数据，安全法规要求比以往更加严格。

这种新趋势带来了新的挑战：

- 手动分析大量日志不仅困难重重且消耗大量人力。
- 许多机构努力追赶安全法规要求。
- 他们需要一个全面的高性能的日志管理系统。

由于这些变化和挑战，他们需要改变思路和工作方式。

他们需要改变原有的计划方式。

IT 机构必须创造长期的 IT 规划来帮助收集、分析、归档和安全的储存大量事件日志。这些计划需要包含可以减轻人力负担的自动化威胁分析。

他们需要改变原有的购买方式。

除行政成本和效率以外，现今的购买决定还需要包含一系列的因素。组织机构需要可以加强安全和满足长期监管要求的合规方案。

他们需要改变原有的部署方式。

为了加强安全日志管理和促进合规审计，组织机构需要部署可以从不同的设备分析数据，从而针对潜在威胁提供近于实时可视性的解决方案。

第2章　QRadar 中小企业集中日志管理系统介绍

2.1 IBM 解决方案

通过分析来自不同的网络和安全设备、服务器和运行系统、应用程序及海量终端的全部的日志及事件数据，IBM® Security QRadar® Log Manager 提供对潜在威胁近于实时的可视性同时，符合持续的监控和合规要求。QRadar Log Manager 设备提供流线化、易于部署的解决方案来保障安全高效的日志管理。

IBM QRadar Log Manager，用于保护 IT 基础设施及满足合规要求的实时日志管理。

2.1.1 解决方案功能

- 通过汇总和关联各种各样的日志及事件，产生可行的 IT 鉴识。
- 在具有单一全球视角的联合资源库内，从安全和网络设备、服务器、终端和应用程序捕捉事件数据。
- 每个系统每秒支持成百上千的事件。

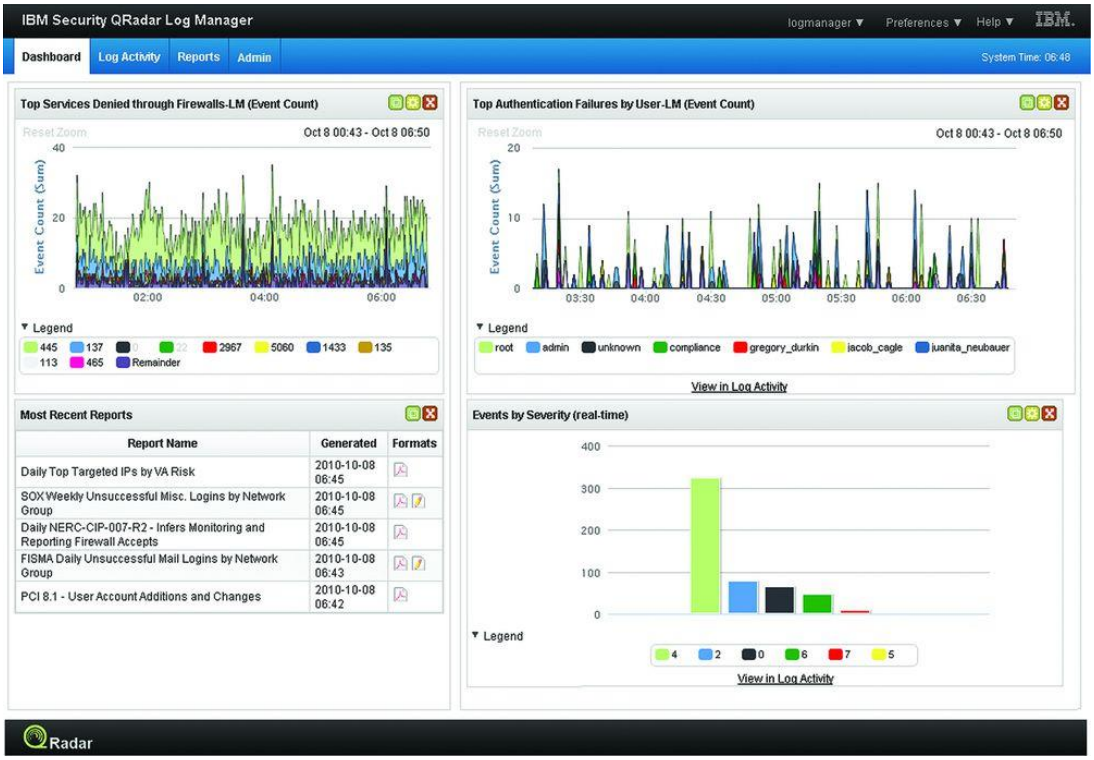
2.1.2 解决方案概述

- 具有丰富的合规性报告能力，帮助超越常规的要求。
- 通过启动集成安全信息和事件管理（SIEM）技术来保护投资。
- 提供高可用和灾难修复选项。

2.1.3 解决方案优势

- 灵活的问询引擎帮助鉴别攻击、异常情况、对机密数据的访问和使用，以及内部威胁。
- 高度直观的集中化用户界面为安全及网络团队提供一个坚实的、直接的基础。
- 分布式架构使存储空间可扩展至数百 TB。

2.2 QRadar Log Manager 功能概述



图：可定制的 QRadar Log Manager 仪表板提供按功能基于角色的访问及对实时日志分析、事件管理和报告的全球化视角。

要点

- 通过集合和互联各种各样的日志及事件，产生可行的 IT 鉴识。
- 在具有单一全球视角的联合资源库内，从安全和网络设备、服务器、终端和应用程序捕捉事件数据。
- 用于简化的搜索，简单地跨正常化数据执行鉴识、应用程序和网络故障排除。
- 每个系统每秒支持成百上千的事件。
- 具有丰富的合规性报告能力，帮助超越常规的要求。
- 通过启动集成安全信息和事件管理（SIEM）技术来保存投资。
- 提供对潜在威胁近于实时的可视性。
- 帮助满足 IT 服务级别的职责。
- 把来自不同日志的相同的部分分配至相似的事件。

- 通过简单的证书升级，从日志管理无缝升级到完整的 SIEM 方案。
- 提供高可用和灾难修复选项。

2.2.1 加强日志资料的可视性，提升可执行的 IT 鉴识

多数机构采用手动分析不断产生的大量日志，这不仅非常困难且消耗大量的人力。通过 QRadar Log Manager 灵活的问询引擎帮助鉴别攻击、异常情况、对机密数据的访问和使用，以及内部威胁。

2.2.2 下层探索的功能可让您掌控全局

QRadar Log Manager 通过一个高度直观的、集中的用户界面，为安全或网络专业人员提供了一个坚实的、简单的基础架构。默认提供仪表板功能，用户可以创建和定制他们自己的工作区，以监测特定的活动或往下探查时间序列以获取长期数据视图的趋势。这使得它更容易识别异常和可能的威胁，检查网络使用情况和性能，以帮助满足 IT 服务级别要求。

2.2.3 全面的设备支持，捕捉全部网络事件

QRadar Log Manager 从广泛的网络和安全设备收集数据，这些设备包括路由器和交换机、防火墙、虚拟专用网(vpn)、入侵检测/预防系统(IDS / IPS)、防病毒软件、主机和服务器、数据库、邮件和 Web 应用、定制设备和专有应用程序。

事件的收集通过一个 Device Support Module 接口来完成，一个先进的、两种级别的标准化分类被用于为来自不同日志源的类似事件指派通用条目。一个定制的规则引擎实时处理每个进入事件，指派严重性、可信度和关联属性，通过电子邮件通知、仪表板通告或通过将事件添加到类似活动的参考集做进一步监控而触发一个适当的响应。

2.2.4 部署可拓展的设备，扩大覆盖范围

QRadar Log Manager 设备基础架构配置范围，包括从集所有功能与一体的硬件或者软件解决方案，到使用一个集中控制台和任意数量的分布式事件处理器和事件收集设备的企业架构。QRadar Log Manager 可以轻松地拓展，在一个单一的、统一的数据库结构里，每秒支持成百上千的事件。

每个 QRadar Log Manager 设备可提供高达 16TB 的容錯存储，用于事件日志的归档并支持广泛的日志文件的完整性检查，其中包括防止篡改日志档案的 NIST Log Management Standard SHA-x (1-256)哈希表。分布式的架构使得存储容量可扩充至多大数百 TB。特制的嵌入式数据库可以进行自维护，不仅使用方便，而且可以降低整体拥有成本。

管理员可以基于粒状原则建立数据保留期限，以满足特定的内部要求或法规。可自定义的事件索引功能通过允许使用任何数据库字段来优化性能，并报告识别使用和磁盘空间消耗的特征。QRadar Log Manager 还压缩旧有的数据，以进一步延长保留期。

2.2.5 减轻当前及未来的安全负担

QRadar Log Manager 拥有超过 2000 个开箱即用的规则与报表，让组织机构能够轻松达成审计与报告需要，满足从 PCI 到 HIPAA，再到 GLBA 的合规要求。针对安全响应团队的自动化报警功能可帮助实现实时的政策执行。

组织机构可以运用 QRadar Log Manager 来帮助提升他们的安全意识，同时也帮助他们发现以往在嘈杂的网络活动中丢失的可疑事件。作为 IBM QRadar Security Intelligence Platform 的一部分，通过简单的证书升级，QRadar Log Manager 提供一个从日志管理到完整 SIEM 方案的无缝迁移途径，这样可以简化从安全事件管理到完善的安全智能的过程。

2.2.6 建立高可用、具备容灾能力的安全系统

添加 QRadar 高可用方案选项，能够帮助组织机构实现系统间的自动故障切换及完整的磁盘同步功能——该功能通常要通过昂贵的、手动实施的软件和储存解决方案才具备。通过高级的即插即用设备，用户通过可以轻松部署高可用数据存储和分析。

QRadar 容灾设备提供一种方法——镜像到第二个相同的 QRadar 部署设备备份，保护收集的所有日志源数据。

2.3 推荐产品-QRadar 2100

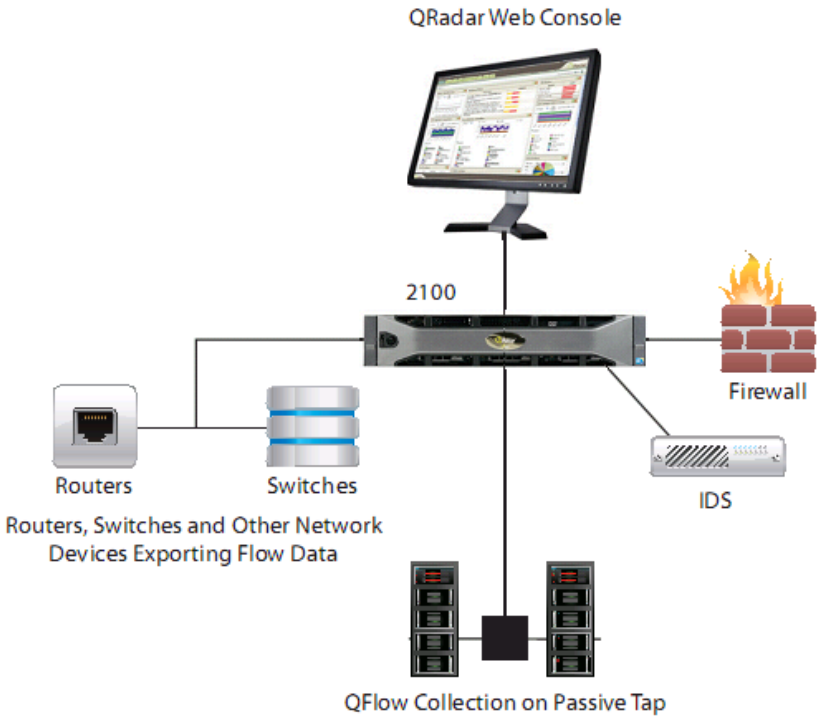
QRadar 2100 All-In-One Appliance（一体化设备）：

QRadar 2100 是整合了 QRadar 强大的 SIEM（安全信息和事件管理）、日志管理、内置的网络行为监控功能和特性的一体化设备。QRadar 2100 是专门为中小企业提供的，在单一设备上实现的 QRadar SIEM 方案。它提供了一个易于快速部署的集成的安全解决方案。QRadar 2100 直观的用户界面，配置非常简单，您可以在数分钟内完成 QRadar 2100 一体化设备的部署，并就此开启你的网络安全之旅。

QRadar 2100 包括 QRadar QFlow Collector 的一个内置版本，提供第七层网络流量和深度应用可视性，以便侦测高级威胁和法庭取证。此外，分布式的 QFlow Collector 也可以通过与 QRadar 2100 配合实现更广泛的网络可视性。

QRadar 2100 特性：

- 实现全面 SIEM 方案的交钥匙设备，包括所有功能（收集、存储、索引、相关性、攻击管理、分析和报告）
- 每秒钟支持 1000 个事件
- 每分钟支持多达 50000 个双向数据流
- 包括 on-board 50Mbps QRadar QFlow Collector，通过被动连接界面或 SPAN 端口采集
- 支持 750 个日志源（设备），可扩展到成千上万个日志源。
- 包括 1.5TB 可用于长期数据保留的 on-board 存储
- 为典型部署提供一年的事件和数据流存储
- 支持光纤通道，可以同 SAN 环境整合
- 10/100/1000 BASE-T 连接用于监控
- 10/100/1000 BASE-T 管理
- 双冗余电源（自适应）
- 内置硬件 RAID10 实现操作系统和存储的可高用和冗余
- 可选的集成 HA 的交钥匙设备



图：QRadar 2100 部署方案示例

2.4 更高级的可选产品

QRadar 3100/3105 All-In-One and Console Appliances

QRadar 3100/3105 面向各种规模的组织机构及企业交付 QRadar SIEM 解决方案。它是那些在未来需要额外的网络活动和事件监控能力的成长型企业的理想选择。它们也是那些地域分散、需要企业级扩展能力的大型企业的基础平台。

QRadar 3124 All-In-One and Console Appliances

QRadar 3124 为大型分布式企业交付 QRadar SIEM 解决方案，比如那些运行安全和网络运营中心（SOC 和 NOC）的企业。

第3章　成功案例

客户名称：台湾财团法人联合信用卡处理中心

客户背景： 一九七九年五月，银行与信托公司合资成立「联合签帐卡处理中心」并于一九八八年九月正式更名为「财团法人联合信用卡处理中心」。主要业务范围包括：

- 信用卡清算中心及授权转接中心
- 提供参加机构信用卡共用资讯系统
- 办理U Card联合信用卡品牌授权及赞助会员机构取得VISA、MasterCard及JCB等三种国际信用卡品牌授权
- 接受参加机构委托发卡作业服务

客户问题：

- 安全事件与日俱增，攻击手法越来越高明，法规遵从要求日益严格，使用者与设备数量不断增加，资料威胁与外泄成为企业的一大挑战。
- 提供安全资讯与事件管理平台(SIEM)及事件流程管理系统，协助资讯人员适时进行资讯安全事件应变，追踪处理，加强资讯安全监控防护机制。
- 提供各种原始事件(Raw data)的保存与检视功能，并提供法规遵从报表，包含 ISO27001、PCI (DSS)等。

解决方案：

利用 QRadar 搭建安全信息与事件管理平台(SIEM)，结合事件流程管理系统来监控现有设备。藉由该管理平台，监控人员可即时监控资讯安全信息，侦测中心之网路环境、主机、系统设备与网际网路所产生的状态，并适时进行资讯安全事件应变、追踪处理等处置回应并提供咨询建议。

客户收益：

- 结合安全事件分析与管理、日志管理、风险管理和网路行为分析为一体的高价值、符合成本效益的产品。
- QRadar 具备高可用性、易于扩展、易于部署和使用的特性，可快速实现价值。
- 能立即满足作业面之需求与法规遵循要求。

第4章　为什么选择 IBM

IBM QRadar 解决方案开创先河、自成一派，成千上万的客户依靠 QRadar 进行安全与合规管理。QRadar 被世界各地的医疗保健机构、能源公司、零售机构、电力公司、金融机构、政府机构及高校广为采用。我们的客户还包括美国联邦政府一些最主要的部门，其中有美国宇航局、美国陆军和美国海军等。

IBM 拥有全球最广泛的安全研究、开发和交付组织，其中包括 10 安全运营中心、9 个 IBM 研究中心、11 个软件安全开发实验室和分布在美国、欧洲和亚太地区高级安全研究所。

IBM 解决方案帮助组织机构减少其安全漏洞，并更加关注于引领成功的战略行动。IBM Security 可提供最先进的集成式企业安全产品和服务组合之一。该组合由世界知名的 IBM X-Force® 研发团队提供支持，提供充足的安全智能，以身份和访问管理、数据库安全、应用程序开发、风险管理、端点管理、网络安全及其他各方面的解决方案，帮助企业全面保障其人员、基础架构、数据和应用程序的安全。这些解决方案可帮助企业有效管理风险，并针对移动设备、云平台、社交媒体及其他企业业务架构实施集成式安全解决方案。

此外，IBM Global Financing 可以帮助您以最经济高效和最具策略性的方式获得您企业所需的软件功能。 我们将与符合信用要求的客户合作以定制最适合其业务与发展目标的融资解决方案，实现高效的现金管理，并降低其总拥有成本。 IBM Global Financing 可为您的重要 IT 投资筹措资金并推动业务向前迈进。