IBM QRadar SIEM

全方位合规审计解决方案建议书

目 录

摘要

我们对您的目标的理解

日益增加的合规要求，海量的告警日志，但是真正的威胁确实在发生吗？为保证信息安全，满足合规、审计要求，类似您这样的企业都在寻找一种 SIEM 解决方案，实现如下目标：

- 能够对数据库进行审计而不影响数据的性能；
- 能够帮助企业满足等保、PCI、ISO27001、SOX 等合规和审计要求；
- 能够收集和保存海量的日志并且从海量的日志和内外部安全信息中及时发现潜在威胁、正在发生的威胁以及如何满足事后调查分析。

IBM 解决方案

QRadar SIEM（安全信息和事件管理）提供完整的可视性和可操作的洞察力，协助企业保护自身网络和 IT 资产，远离花样繁多的各类威胁，并满足当前及未来严格的合规性要求。它可以做到：

- 实时收集基础架构、应用、数据库、身份认证、安全产品的日志以及网络流量、漏洞信息、资产信息；
- 内制丰富的关联分析模型，实时告警真正的安全威胁；
- 丰富的合规报表和统计报表，对企业内部安全状态一目了然；
- 操作简单、直观，丰富的搜索和分析视角，支持全文检索所需安全信息；
- 快速的部署能力，更好更快的确保企业信息安全；
- 深层次数据库审计，不影响数据库性能。

QRadar SIEM 将会为您带来如下价值：

- 单一界面自动完成合规审计报告，大大节省审计时间；
- 更加迅速地检测安全违规和风险，实时告警入侵行为；

- 多线索分析提高安全检测的准确性，减少“误报”；
- 实时检测潜在内部资料窃取、欺诈或恶意活动；
- 降低 SIEM/日志管理解决方案的成本并降低日常运维工作量。

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。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PCI.ISO27001法规遵循要求。

为什么选择 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。

第1章　我们对您的目标的理解

1.1 信息安全令人堪忧

近年来，网络技术的飞速发展给人们的工作和生活带来极大便利，同时，网络蠕虫、木马、间谍软件等技术与僵尸网络结合在一起，利用网络及信息系统的诸多漏洞，给互联网安全造成了严重的威胁，让我们回顾一下 2012 年发生的重大网络安全事件：

- 2012 年 1 月中旬前后,赛门铁克两款企业级产品源代码被盗。
- 2012 年 4 月底 VMware 确定关于 ESX Hypervisor 的源代码已经泄露。
- 2012 年 3 月，Anonymous 威胁干掉整个互联网。
- 2012 年 8 月，维基解密表示，自己的网站遭受到了持续的 DDOS(拒绝服务)黑客攻击，导致网站在一周多的时间里反应迟缓或无法登录。
- 2012 年 5 月，一种破坏力巨大的全新电脑蠕虫病毒"火焰"(Flame)被发现，这种病毒正在中东地区大范围传播。
- 2012 年 8 月，继最复杂病毒 Flame 曝光之后，卡巴斯基实验室又曝光类似 Flame 病毒的 Gauss 病毒。
- 2012 年 7 月，DNSChanger 恶意软件肆虐，仅仅在不到几小时时间内，多达 30 万台电脑和 Mac 无法上网。
- 2012 年 1 月，亚马逊旗下美国电子商务网站 Zappos 遭到黑客网络攻击，2400 万用户的电子邮件和密码等信息被窃取。
- 2012 年 3 月，信用卡支付中介机构美国"全球支付"公司确认，未授权者 3 月初进入它的系统并可能窃取一些信用卡账户信息。此次遭"大规模"盗取，波及账户数量暂时无法确定，评估数量从数以万计至超过 1000 万。
- 2012 年 10 月，黑客团伙 Team GhostShell 在推特上宣布，该组织入侵了全球百所大学的服务器，共窃取了近 12 万账户信息。
- 2012 年 10 月，据业内人士微博爆料，京东商城充值系统于 2012 年 10 月 30 日晚 22 点 30 分左右出现重大漏洞，用户可以用京东积分无限制充值 Q 币和话费。

- 2012 年 12 月，微软公司的 IE 浏览器出现巨大漏洞，黑客利用这个漏洞可以跟踪记录用户的鼠标移动轨迹，从而盗取用户使用虚拟键盘时输入的各种数据。

- 目前，1.98 亿 Android 设备拥有者的内存卡处于危险境地，用户信息有可能因恶意链接或者恶意程序被删除干净。

1.2 审计、合规要求越发严格

为加强信息科技风险管理，行业监管机构发布了更加严格的法规。众多的审计要求需要有统一的安全措施来应对。例如：

- 银监会制定的**银行业金融机构信息科技风险管理指引**（修订版）第二十七条规定：银行业金融机构应制定一系列策略和流程，控制所有生产系统的**活动日志**，以支持有效的审计、安全论证分析和**预防欺诈**。

- 公安部、国家保密局、国家密码管理委员会办公室、国务院信息化工作办公室发布的**信息安全等级保护标准，其中“安全审计**（G3）”指明：

a) 审计范围应覆盖到**服务器和重要客户端上的每个操作系统用户和数据库用户**；

b) 审计内容应包括重要**用户行为、系统资源的异常使用和重要系统命令的使用**等系统内重要的安全相关事件；

c) 审计记录应包括事件的日期、时间、类型、主体标识、客体标识和结果等；

1.3 面临的挑战

为保证信息安全，满足合规、审计要求，你或许正疲于应对如下这些棘手的问题：

- 近期遭遇过审计合规问题以及安全漏洞问题；
- 依赖手工收集用于合规报告及审计的数据；
- 无法快速发现安全漏洞和异常行为；
- 无法诊断来自企业内部的窃取、欺诈及恶意行为；
- 无法监控社交媒体和移动行为以避免数据安全风险；
- 无法在虚拟化、云环境下监控网络活动；
- 现有的日志管理或 SIEM（安全信息和事件管理）解决方案不够灵活，无法扩展；

- 在出现安全漏洞之后无法进行有效的取证；
- 网络和安全设备配置错误导致产生风险。

1.4 目标理解

类似您这样的企业都在寻找一种 SIEM（安全信息和事件管理）解决方案，实现如下目标：

- 能够对数据库进行审计而不影响数据的性能；
- 能够帮助企业满足等保、PCI、ISO27001、SOX 等合规和审计要求；
- 能够收集和保存海量的日志并且从海量的日志和内外部安全信息中及时发现潜在威胁、正在发生的威胁以及如何满足事后调查分析。

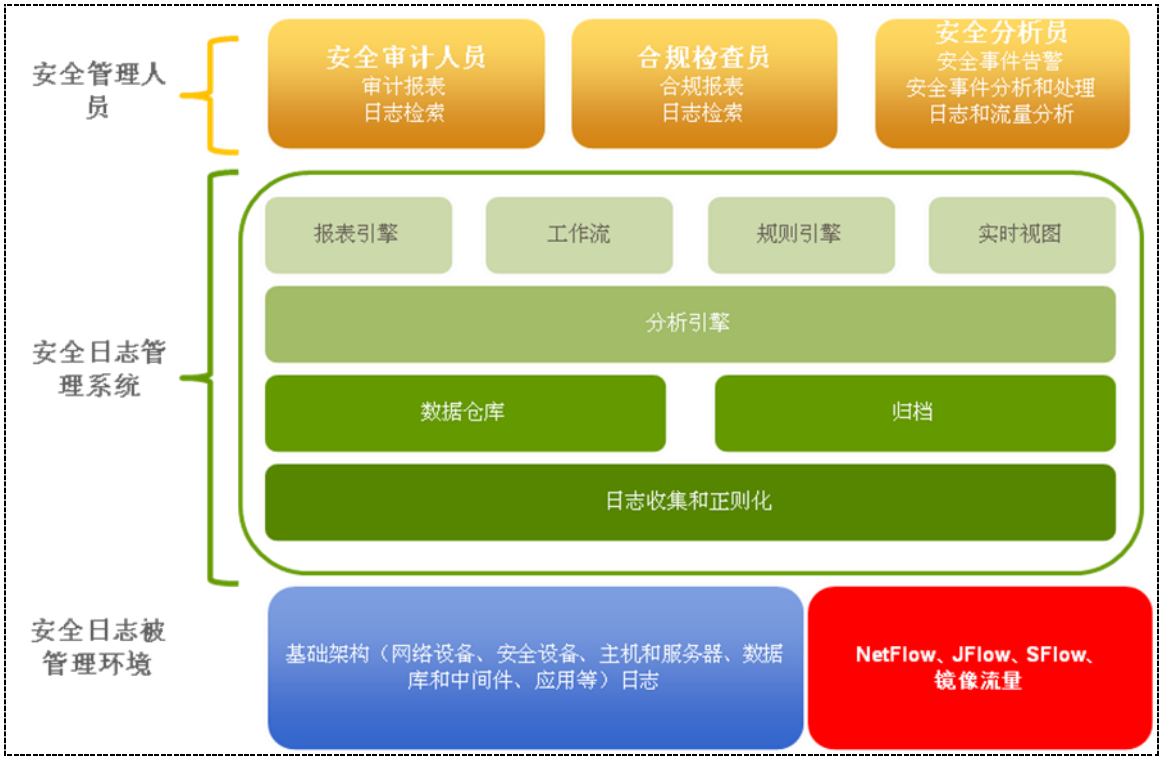
IBM QRadar SIEM 提供的解决方案可让安全专业人员获取必要的可见性，从而协助其更加有效的保护自身的网络和 IT 资产，远离日益加剧的高级威胁环境，并满足当前及未来严格的合规性要求。

第2章　QRadar SIEM 全方位合规审计方案介绍

2.1 方案简述

QRadar SIEM 是 IBM 的 SIEM 产品，它提供了 SIM（安全信息管理）和 SEM 安全事件管理能力。

QRadar SIEM 提供完整的可视性和可操作的洞察力，协助企业保护自身网络和 IT 资产，远离花样繁多的各类威胁，并满足当前及未来严格的合规性要求。它包括实时日志、流量、漏洞、资产配置文件和外部威胁相关的数据，可以识别威胁并确定事件优先级。它实现了对每天高达数十亿的事件的分布式采集，通过网络流量分析以获取深度的应用洞察，分布式数据架构支持大规模的可伸缩性并减少用户部署解决方案的付出。先进的威胁检测功能既减少了误报数，又可以检测到的其他解决方案漏掉的威胁。数以百计的预定义报告、相关规则和仪表板视图减少了为确保合规性所做的努力，并为安全和网络专业人员以及企业高管提供对洞察。



QRadar SIEM 解决方案示意图

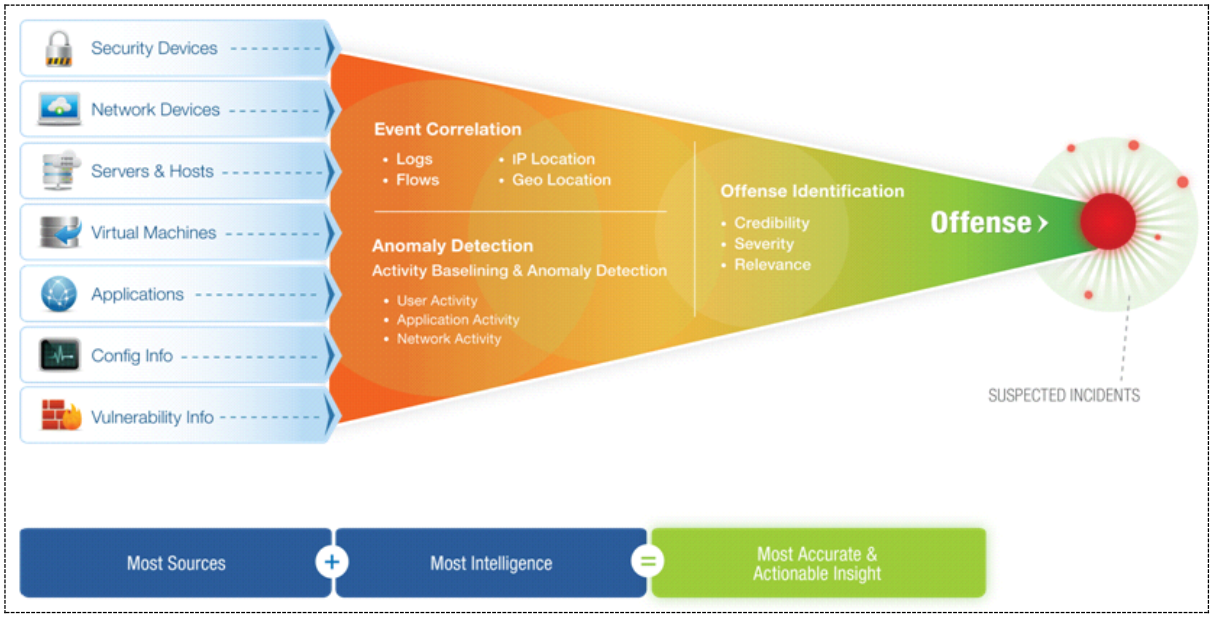
QRadar SIEM 是构建于高度灵活的 QRadar 安全智能平台之上的新一代解决方案，能随企业共同成长，扩展支持不断发展的基础架构，并为企业内的多个群体提供统一的用户体验。QRadar SIEM 集日志管理、高级威胁检测和策略感知的合规管理功能于一身，让企业从这种紧密集成的解决方案中受益，进而快速轻松地实现企业安全智能。

2.2 方案功能及特性

QRadar 的新一代 SIEM 解决方案是业内智能化、集成化和自动化程度最高的 SIEM 解决方案。促使 QRadar SIEM 脱颖而出的重要因素是其无与伦比的平台架构，该平台架构能够实现：

- 全包式统一化部署及更加有效的运营管理
- 分布式关联，每天对数十亿日志和记录进行监控
- 单一日志归档功能，确保实现无缝报告和全面搜索
- 集中命令和控制，降低安全管理解决方案购置成本并提高 IT 效率
- 高级威胁和安全事件检测，既能减少误报数，又能检测其他解决方案遗漏的威胁
- 以合规为核心的工作流程，确保提供最佳 IT 实践，为合规举措提供支持
- 分布式设备架构，扩展后可对所有企业网络进行日志管理

2.2.1 全方位智能化和可见性



QRadar SIEM 通过上下文分析 & 关联分析——安全智能（QRadar SIEM 从大量馈送中捕获相关数据，使用已有和客户定义规则将其缩减为可管理的攻击行为列表）

第一代 SIEM 旨在监控传统安全遥测运行状况，减少通过规则和数据关联收集到可疑安全事件子集的数据。SIEM 的这种传统方法能够对服务器、主机和安全系统实施监控，但缺乏从所有可能来源收集数据的能力，也无法有效区分真实威胁和虚假警报。

- 作为业内唯一一项自主设计，提供新一代 SIEM 优势的 SIEM 解决方案，QRadar SIEM 大幅扩展了网络活动、虚拟活动、用户活动及应用程序活动的可见性，为网络安全专业人员实现了无以伦比的智能化，使其能够侦测其整个网络内的各种潜在攻击源。

- QRadar 会关联网络活动环境内的安全和网络基础架构日志数据，以便检测其他产品遗漏的事件并正确区分事件优先级。

- 全面智能化还包括对攻击之前、期间、之后进行全方位的影响分析。第一代 SIEM 技术能够在发生攻击时提供评估值，但在事件发生前剖析攻击者和目标（以便更好地划定优先级并做出响应）方面的能力有限。同时，在意识到检测事件后进行充分取证的能力也极其有限。由于 Qradar 的新一代 SIEM 充分考虑了行为和上下文，因而能够全面提供攻击发生之前、期间、之后的值。这意味着它能够实现更加有效的安全分析、高级检测和全面取证。

2.2.2 集成平台，提供单控制台安全性及无与伦比的可扩展性

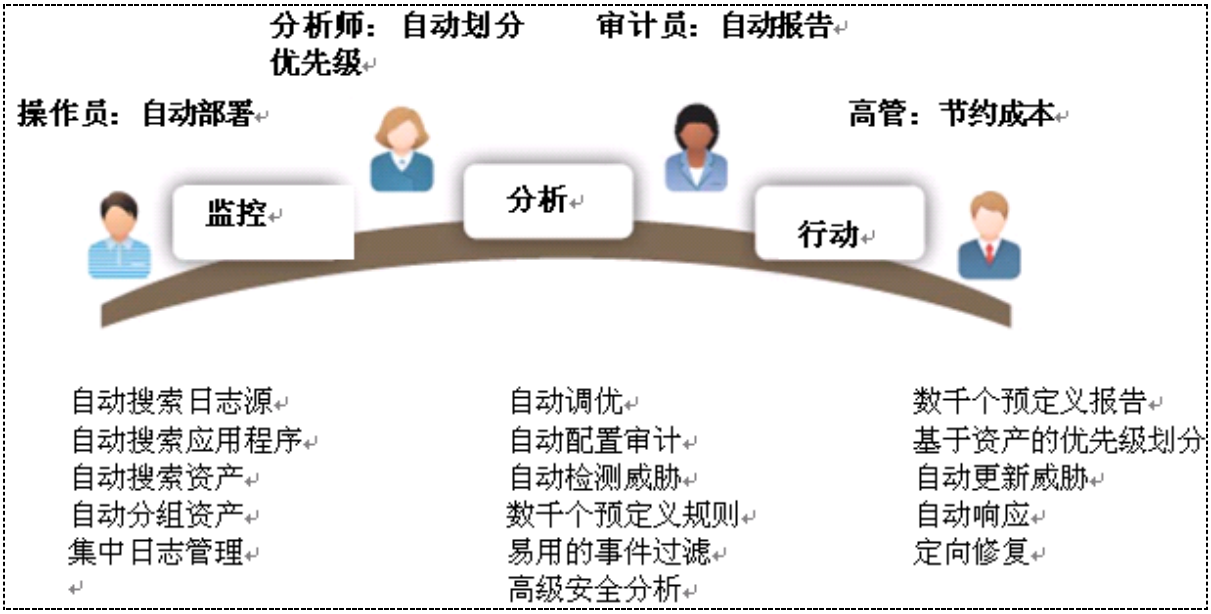
第一代 SIEM 解决方案依靠组合多项产品，尝试将它们作为一项 SIEM 解决方案进行部署。得到的细分解决方案不必要地比较复杂、难以管理甚至难以扩展。更重要的是，经过过滤的选择性数据关联、日志重复、多个用户界面、非统一报告和搜索会限制您的网络保护能力。

QRadar 新一代 SIEM 采用全自主化设计，作为完善的集成解决方案运行。与市场上的其他产品（需要集成多种不同产品和接口）不同，QRadar 提供的解决方案无论存在何种规模要求，均为所有安全智能任务（从搜索和过滤到报告和响应）提供通用平台和用户界面，不必再像使用第一代 SIEM 时不得不在智能化和简易性之间做出艰难抉择。

2.2.3 自动化，可让您更加有效地开展监控、分析和行动

在未实现自动化之前，您需要依赖供应商花费大量的时间和精力配置解决方案的正常运营。他们甚至需要在考虑优化解决方案运营之前思考这一点。与第一代 SIEM 解决方案不同，QRadar 的新一代 SIEM 将为客户自动完成各流程，从搜索日志源到分析应用程序和资产。只需进行极少的定制，即可提供规则和构造块等宝贵的开箱即用内容。

此外，此内容（包括第三方情报来源内容）将每周自动更新。其中还纳入了成千上万与您的特定角色、设备合规法规及垂直行业相关的自带报告。企业现在可以借助 QRadar SIEM 更加有效地监控、分析和实现市场上最强大的自动部署、自动优先级划分、自动报告及高效的 SIEM。



异构设备支持：

由于能够为企业网络内部署的几乎每一家领先供应商提供的 450 多种产品提供支持，QRadar SIEM 能够跨越一系列广泛的系统（包括网络解决方案、安全解决方案、服务器、主机、操作系统和应用程序）执行收集、分析和关联。此外，QRadar SIEM 还能轻松扩展，以支持专有应用程序和新兴系统。QRadar SIEM 支持 F5、Cisco、Juniper、Nortel、Checkpoint、Oracle、Sun、Enterasys、Symantec、ISS/IBM、McAfee、Sourcefire、RSA 等设备。

2.3 方案价值

QRadar SIEM 将会为您带来如下价值：

- 单一界面自动完成合规审计报告，大大节省审计时间；

- 更加迅速地检测安全违规和风险，实时告警入侵行为；
- 多线索分析提高安全检测的准确性，减少“误报”；
- 实时检测潜在内部资料窃取、欺诈或恶意活动；
- 降低 SIEM/日志管理解决方案的成本并降低日常运维工作量。

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 SIEM 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。我们的客户还包括一些最主要的美国联邦政府部门，其中有美国宇航局、美国陆军和美国海军等。

IBM 拥有世界上规模最大的安全研发和交付机构，每天监控 130 多个国家超过 130 亿个安全事件，并持有 3,000 多项安全专利。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。

第5章　附录：产品数据表

要点

- 在通用数据库和共享仪表板用户界面内集成日志管理和网络威胁保护技术
- 将数千例安全事件缩减为一份可管理的可疑攻击行为列表
- 长期检测及跟踪恶意活动，有助于揭示通常为其他安全解决方案所遗漏的高级威胁
- 借助高级功能检测内部欺诈
- 帮助超越监管要求及支持合规性
- 自动探索大多数网络日志源设备并检查网络流数据，以查找网络上的有效主机和服务器并对其分类
- 充分利用对事件和流数据的实时、基于地点及历史搜索进行分析和取证
- 从单一的一体化解决方案着手，并根据需要添加事件和流处理器设备

与以往相比，当今的网络规模更大、复杂程度更高，保护其免受恶意活动侵犯是一项永无止境的任务。企业在寻求保护其知识产权和客户身份及避免业务中断时，除监控日志和网络流量数据外，还需要充分利用高级工具，以可行方式检测这些活动。IBM® Security QRadar® SIEM 可作为小型或大型企业安全运营中心内的核心解决方案，借助多年来积累的丰富环境洞察，收集、规范化和关联可用的网络数据，所取得的成果称为安全智能。

此产品的核心为具备高扩展性的数据库，旨在捕获实时日志事件和网络流数据，揭露潜在攻击者的踪迹。QRadar SIEM 是一种企业解决方案，可整合分布在整个网络数千台设备中的日志源事件数据，以原始形式存储每个活动，然后执行即时关联活动，以区分实际威胁和误报。此外，该解决方案还可捕获第 4 层实时网络流数据，更独特的是，还可以使用深层包检查技术捕获第 7 层应用程序负载。

直观的用户界面跨所有 QRadar 系列组件共享，可帮助 IT 人员快速识别网络攻击并按级别予以补救，管理数以百计的警报和异常活动模式，大幅减少需授权进一步调查的攻击行为。

提供威胁检测和优先级划分的实时可见性

QRadar SIEM 提供跨整个 IT 基础架构的环境相关且切实可行的监控，有助于企业检测及补救通常为其他安全解决方案所遗漏的威胁。这些威胁包括应用程序的不当使用、内部欺诈，以及轻易淹没在数百万计的繁杂事件中的高级“低慢”威胁。

QRadar SIEM 收集下列信息：

- **安全事件：** 来自防火墙、虚拟专用网络、入侵检测系统和入侵预防系统等的事件
- **网络事件：** 来自交换机、路由器、服务器和主机等设备的事件
- **网络活动环境：** 来自网络和应用程序流量的第 7 层应用程序环境
- **用户或资产环境：** 来自身份及访问管理产品和漏洞扫描器的环境相关数据
- **操作系统信息：** 网络资产的供应商名称和版本号详情
- **应用程序日志：** 企业资源规划 (ERP)、工作流、应用程序数据库和管理平台等

减少警报数量并划分其优先级，以重点调查可能实施的攻击行为

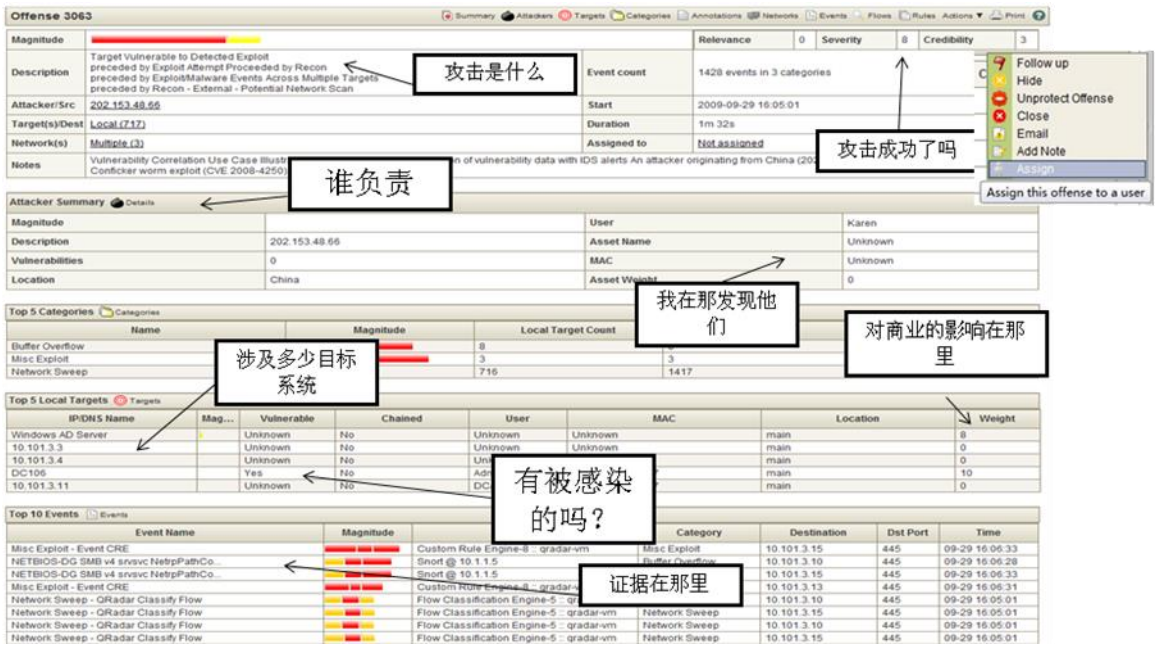
许多企业每天都会产生数百万乃至数十亿的事件，将事件数据提取至简短的攻击行为优先级列表是一项艰巨的工作。QRadar SIEM 通过跟踪所使用的应用程序、协议、服务和端口，自动探索大部分网络日志源设备并检查网络流数据，以查找网络上的有效主机和服务器（资产）并对其分类。它可以收集、存储及分析相关数据，并执行实时事件关联，以便在威胁检测及合规性报告和审计中使用。因此，可以缩减数十亿计的事件和流，并根据业务影响对其划分优先级，总结出少量可能实施的攻击行为。

因此，安全专家通常能够在安装 QRadar SIEM 的几天，而非几周内开始看到价值，并且无需聘请费用昂贵的顾问即可进行部署。借助自动发现功能、即时可用的模板以及过滤器，您无需像使用一般的 IT 运营工具那样，花费数月时间让系统熟悉贵企业的环境。该架构采用事件处理器设备、事件收集器设备、流处理器设备和中央控制台等多个模型，这些模型均可用作基于硬件的设备、仅限软件的设备或虚拟软件设备。小型安装可从单一的一体化解决方案入手，并根据需要添加事件和流处理器设备，轻松升级至控制台部署。

提高威胁管理成效的关键问题解答

安全团队需要回答下列关键问题，以充分了解其所面临的潜在威胁的性质：谁是攻击方？谁是被攻击方？攻击产生了哪些业务影响？调查应从哪些方面入手？QRadar SIEM 可以跟踪大量的事件和威胁，构建支持数据及相关信息的历史资料。攻击目标、时间点、资产值、漏洞状态、攻

击用户身份、攻击者资料、主动威胁和以往攻击记录等详细信息，均有助于向安全团队提供需要实施的智能。



图：QRadar SIEM 清晰简明的展示了安全事件最相关的信息

充分利用对事件和流数据的实时、基于地点及历史搜索进行分析和取证，能够大幅提升企业访问活动及解决事件的能力。借助易于使用的仪表板、事件序列视图、深入搜索、包级内容可见性和数以百计的预定义搜索，用户可快速汇总数据，总结和识别出异常行为及主要的活动参与者。他们还可以跨大型地区分布式环境执行联合搜索。

获取应用程序可见性及异常检测

QRadar SIEM 支持各种异常检测功能，可识别影响应用程序、主机、服务器和网络区域的行为变化。例如，QRadar SIEM 可检测应用程序或基于云的服务的非运作时间或过度使用，或者与移动平均历史资料不一致的网络活动模式，以及季节性使用模式。QRadar SIEM 了解如何识别这些每日和每周使用资料，从而帮助 IT 人员快速识别有意义的差异。

QRadar SIEM 集中式数据库将日志源事件和网络流量存储在一起，有助于将离散事件与来自相同 IP 源的双向网络流活动相关联。此外，它还可以将短时间内发生的网络流量和记录操作分组为单一数据库条目，以帮助减少存储消耗并保留许可要求。

QRadar SIEM 能够检测第 7 层的应用程序流量，可针对企业网络提供准确的分析和洞察，适用于策略、威胁和常规网络活动监控。通过添加 IBM Security QRadar QFlow 或 VFlow Collector 设备，QRadar SIEM 可监控 ERP、数据库、Skype、IP 语音 (VoIP) 和网络内社交媒体等应用程序的

使用。其中包括了解应用程序及应用程序使用者、内容传输的分析和警报，以及与其他网络和日志活动的关联，以揭露不当数据传输及过度使用模式。虽然 QRadar SIEM 配有大量异常事件和行为检测规则，安全团队仍可借助过滤功能创建自己的规则，该功能可帮助其针对时间序列数据应用异常检测。

获得高度直观的单一控制台安全解决方案

QRadar SIEM 通过提供集中式用户界面为企业的安全运营中心提供坚实的基础，其中该界面可按职能提供基于角色的访问，同时提供一个全局视图，可用于访问实时分析、事件管理和报告。提供五个默认仪表板，分别是安全、网络活动、应用程序活动、系统监控及合规性，此外，用户还可创建及定制个人工作空间。

这些仪表板易于找出警报活动中可能标志着攻击开始的峰值。单击图表即可启动深入分析功能，能够帮助安全团队快速调查突出显示的事件或与可疑攻击相关的网络流。此外，还提供与特定角色、设备、合规性法规及垂直行业相关的数百个模板，这些模板可用于加速生成报告。

将威胁保护扩展至虚拟环境

由于虚拟服务器与物理服务器一样易受安全漏洞的影响，因此综合性的安全智能解决方案还必须包括适当的措施，以保护虚拟数据中心内的应用程序和数据。IT 专家使用 QRadar VFlow Collector 设备提升对虚拟网络内大量业务应用程序活动的可见性，并能够更好地识别这些应用程序，以进行安全监控、应用程序层行为分析和异常检测。操作人员还可获取适用于更深层次安全和策略取证的应用程序内容。

生成详细数据访问及用户活动报告以管理合规性

QRadar SIEM 可提供透明度、责任感和可衡量性，这对于企业成功达成监管要求及合规报告而言十分重要。该解决方案能够关联并集成监控反馈，为审计员生成用于报告 IT 风险的更完备的标准，以及数百个报告和规则模板，以应对行业合规性要求。

借助 QRadar SIEM 的可扩展性，企业可通过自动更新囊括新的定义、法规和最佳实践，从而高效响应合规性驱动的 IT 安全要求。此外，所有网络资产的资料可按业务职能分组，例如，受《健康保险便携性与责任法案》(HIPAA) 合规性审计管制的服务器。

该解决方案的预置仪表板、报告和规则模板设计用于下列法规和控制框架：CobiT、SOX、GLBA、NERC/FERC、FISMA、PCI DSS、HIPAA、UK GSi/GCSx 和 GPG 等。

添加高可用性及灾难恢复功能

为实现高可用性及灾难恢复功能，相同的次级系统可与 QRadar 系列所有设备进行配对。从事件处理器设备，到流处理器设备，再到一体化和控制台 SIEM 设备，用户可根据需要添加稳健性和保护，从而帮助确保持续运作。

对于寻求业务弹性的企业而言，QRadar 高可用性解决方案可提供系统之间的集成式自动故障转移和全盘同步。这些解决方案可通过功能完备的架构化即插即用型设备轻松部署，且无需使用附加的第三方故障管理产品。

对于寻求数据保护和恢复的企业而言，QRadar 灾难恢复解决方案可将主要 QRadar 系统的实时数据（例如流和事件）转发给位于单独设施中的次级并行系统。

漏洞分析

IBM Security QRadar Risk Manager 可识别网络中最重要的资产，以此完善 QRadar SIEM 的功能。当这些系统参与有潜在威胁的活动时，它可以立即生成报警。例如，企业可以扫描其网络中未安装补丁的应用程序、设备和系统，确定哪些连接至互联网，并根据每个应用程序的风险状况划分补救的优先顺序。有关详细信息，请查看 QRadar Risk Manager 数据表 。

获得综合设备支持以捕获网络事件和流

借助几乎每个领先供应商在企业网络中部署的 450 多种产品的支持，QRadar SIEM 可跨各类系统提供集成、分析和关联，其中包括联网解决方案、安全解决方案、服务器、主机、操作系统和应用程序。此外，QRadar SIEM 能够轻松进行扩展，支持 IBM 和许多其他供应商的专有应用程序和新系统。