IBM Security QRadar SIEM

借助集成式调查报告系统提升威胁保护及合规性

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

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。

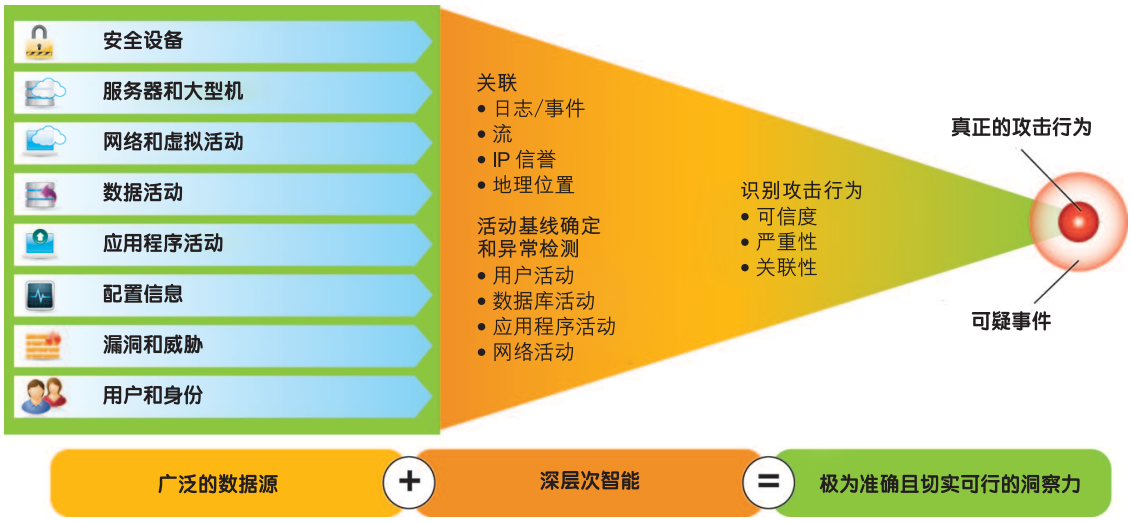
QRadar SIEM 收集下列信息：

- **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。



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。

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。

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。

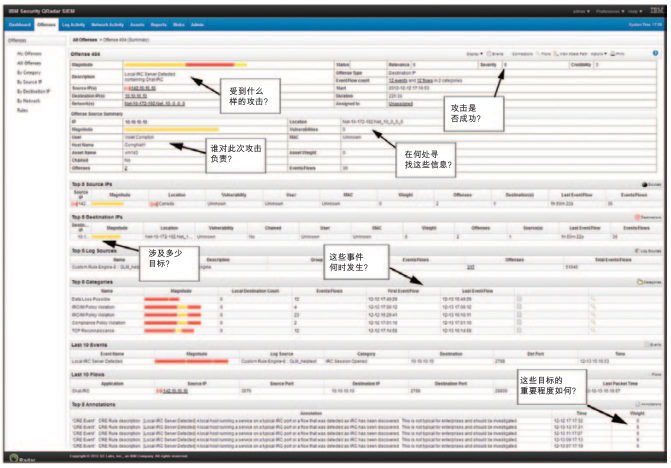
QRadar SIEM 集中式数据库将日志源事件和网络流量存储在一起，有助于将离散事件与来自相同 IP 源的双向网络流活动相关联。此外，它还可以将短时间内发生的网络流量和记录操作分组为单一数据库条目，以帮助减少存储消耗并保留许可要求。

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。



QRadar SIEM 可以挖掘出每起可疑攻击行为背后隐藏的每个细节，并能够通过整合现有规则或添加规则来以减少误报。

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。

为何选择 IBM?

IBM 拥有世界上规模最大的安全研发和交付机构。IBM 解决方案可助力企业减少其安全漏洞，并将精力更多地放在其战略计划的成功上。

如需更多信息

要了解有关 IBM Security QRadar SIEM 如何解决贵企业的威胁管理及合规性挑战，请联系 IBM 代表或 IBM 业务合作伙伴，或访问：**ibm.com**/security。

关于 IBM Security 解决方案

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。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。

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。 如需更多信息，请访问：**ibm.com**/financing

IBM Corporation
Software Group
Route 100
Somers, NY 10589

美国印制
2013 年 1 月