Q1Labs.com

Q1Labs
Total Security Intelligence

金融业安全智能

金融机构是黑客攻击、有组织的犯罪和网络犯罪的主要目标，不断上升的攻击复杂性及攻击次数展现了犯罪分子发现和利用漏洞的强大能力。因此，即使是防御最完善的防御网络也会不断被渗透。这些机构不仅身处计算机安全战役的最前线，而且也是目前受管制最严格的行业之一。

银行和保险公司等提供金融服务的机构面临着保护客户金融信息、满足内部要求和法规要求的严峻挑战。

金融机构面前的具体挑战包括：

- *信息超载* - 网络和安全团队每天要收集数以百万计的网络和安全日志，可能导致遗漏威胁、数据窃取，从而造成无法承受的运营支出。
- *合规性审计* - 实施内部安全策略，同时满足现有和新增法规的审计和管制要求，例如 格雷姆-里奇-比利雷法案 (GLBA)、萨班斯-奥克斯利法案(SOX)、联邦金融机构检查委员会(FFIEC)、支付卡行业数据安全标准 (PCI DSS) 和 国防财务和会计服务 (DFAS)。

  隐私和安全性违规的货币成本不仅仅限于合规性惩罚，比如在银行业违规中，还包括卡片补发费用。
- *网络威胁* - 对于网络和安全团队来说，保护金融服务基础架构（包括客户账户信息在内）免受内部威胁和新型复杂威胁的侵害是一项艰巨的任务。

  金融服务部门仍然是全球第二受关注的行业，大多数州的法规都存在这样的要求：如果有理由相信客户私人数据已泄露，则必须将情况告知相应个人（Verizon Business 2009 年数据泄露研究）。

挑战

您能否承担得起商业客户群流失 25% 的代价？

Ponemon Institute/Guardian 开展的一次调查表明，在线银行欺诈的增加让银行面临客户流失的代价，这次调查发现，有 55% 的企业在过去 12 个月中曾是欺诈犯罪的受害者，而 40% 的中小企业会在发生欺诈事件后更换银行。

解决方案

QRadar

金融服务机构

QRadar 凭借集成化、异构化的安全智能方法，提供以智能实时行为分析加强的安全监控和合规性验证，为金融机构提供其整个机构网络中的系统、应用程序和用户的行为概要。

Q1 Labs 金融服务业客户利用 QRadar 解决如下网络安全管理挑战：

- 跨多种不同安全性技术和供应商的日志聚合和分析
- 内外威胁管理中的威胁监控和事故检测，包括信息安全和内部人员威胁监控
- 根据 GLBA、SOX、PCI DSS 等法规要求开展的合规性审计、报告和验证计划

S1 Corporation 在评估 QRadar 时给出了这样的评价：

“使用 QRadar 的优势无穷无尽。该系统不仅附带一套预装的日志管理功能，而且具有高度灵活、易于编程的特点，让我们不仅能修改现有规则，还能轻松利用规则向导创建新规则。”

QRadar 提供了业内智能化、集成化、自动化程度最高的安全管理解决方案，成功应对了金融机构的这些挑战。

- *智能化：*通过监控更多数据、提供更为先进的分析技术，QRadar 即可检测到往往被遗漏的威胁，提供其他解决方案无法匹敌的网络和应用程序活动可见性。
- *集成化：*将来自安全日志、网络流分析、应用程序层、IAM 解决方案和基于资产的漏洞评估的信息关联到单独一个综合性管理解决方案之中。
- *自动化：*易于部署和管理的 QRadar 能自动化安全性和网络设备发现，同时自动化策略功能。QRadar 基于设备的架构和嵌入式数据库消除了妨碍传统 SIEM 和日志管理解决方案部署和长期支持的过高复杂性和成本。

Q1 Labs 的 QRadar 安全信息和事件管理 (SIEM) 解决方案专门构建用于将日志管理与 SIEM 集成在单独一个解决方案之中，在不影响 SIEM “智能” 的同时支持海量日志管理。因此，产品购买、部署和运营成本都远远低于其他 “单点式产品” 解决方案。

独一无二的智能遥测集成

检测最复杂的金融服务基础架构威胁

利用跨系统、安全设备和网络的全面可见性，QRadar 将业界领先的事件关联应用于事件数据，包括行为分析和智能应用上下文（网络架构、系统配置文件、身份信息和第三方安全智能来源）。

QRadar 还利用客户路由/交换基础架构或分布式收集器中的本机流量来源，收集所有网络流量活动的详尽历史记录，从而对组织的整个网络进行调查。

这种独一无二的事件信息和流量活动集成在攻击发生之前提供了完善的威胁上下文，并在事后全面取证，从而轻松、准确、全面地响应意外事件、评估影响。

日志管理

除了深入理解网络安全性、设备配置和应用程序行为之外，QRadar 还提供了证实合规性的审计跟踪记录，同时支持访问历史日志数据。日志管理是 SOX 合规性的重要基础，组织需要收集、存储和报告有关事件日志的信息，并证明自身实施了足够的控制。

QRadar 提供了集成化存储以及有助确保所收集信息完整性的特性。除了日志收集、存储和搜索等重要日志管理功能之外，QRadar 还以先进的方法，通过集成化、实时的事件关联、威胁检测和合规性报告与审计利用收集到的全部信息。

威胁和欺诈管理

欺诈是一个大难题，仅在美国就造成了每年超过 2 千亿美元的损失。

当今的犯罪分子不再是处境贫寒的可怜虫。他们头脑缜密、思路清晰，不断随着企业技术的发展完善自身的犯罪手段，而网络犯罪有着被抓获、起诉的可能性极低的特点，风险回报极高，因此对他们有着极大的吸引力。

无论欺诈具体属于哪种类型，都有必要认识到，欺诈可以通过多种方法实现，包括网络钓鱼、瞒报、入侵数据库等。这些数据违规不仅会造成严重的安全性和法规风险，还会因数据泄露给金融服务企业造成负面宣传，造成灾难性的后果。您必须保护最宝贵的资产——客户的信任。

QRadar 可以检测对系统和数据的未经授权的访问，保证敏感客户信息免于被窃，免受来自内部或外部来源的其他侵害。为了检测更加复杂的网络威胁，QRadar 利用全部可用网络活动数据（包括分散在不同网络和安全解决方案与运营团队之间的信息）来发现和跟踪可疑行为。

QRadar 广泛的可见性提供了必要的网络监督能力，支持检测当今最为危险的 IT 威胁，提供排列了优先级、便于管理的一组安全威胁以及修复具体情况所需的信息。为了迅速识别内部误用，QRadar 可以集成客户的身份和访问管理 (IAM) 解决方案，分析这些数据源来开发资产用户身份和行为以及漏洞状态的全面视图，而仅凭 IAM 解决方案是无法获得这些信息的。

许多金融服务机构据为某些应用程序或其业务的某些部分实施了欺诈检测能力。QRadar 最大的价值莫过于将这些解决方案提供的智能与整个企业基础架构内收集到的更广泛的数据关联起来的能力。这将给安全专家提供更完整的视图，降低运营复杂性。

合规性管理

QRadar 为金融服务机构提供了透明度、可问责性和可度量性，这对于成功满足法规要求极为关键。QRadar 以独一无二的方式关联和集成全部监督源，从而为运营人员提供更加准确的数据（透明度）、为意外事件响应经理提供更细粒度的取证能力（可问责性）、为审计人员提供更加完善的报告（可度量性）。此外，QRadar 附带数千种报表和规则模板，包括 SOX、GLBA、FFIEC、DFAS 和 PCI 行业合规性法规所要求的具体报表和规则。

可问责性：提供谁在何时执行了哪些操作的信息

透明度：提供有关安全控制、业务应用程序和受保护资产的可见性

可度量性：有关企业或组织内风险的指标和报告

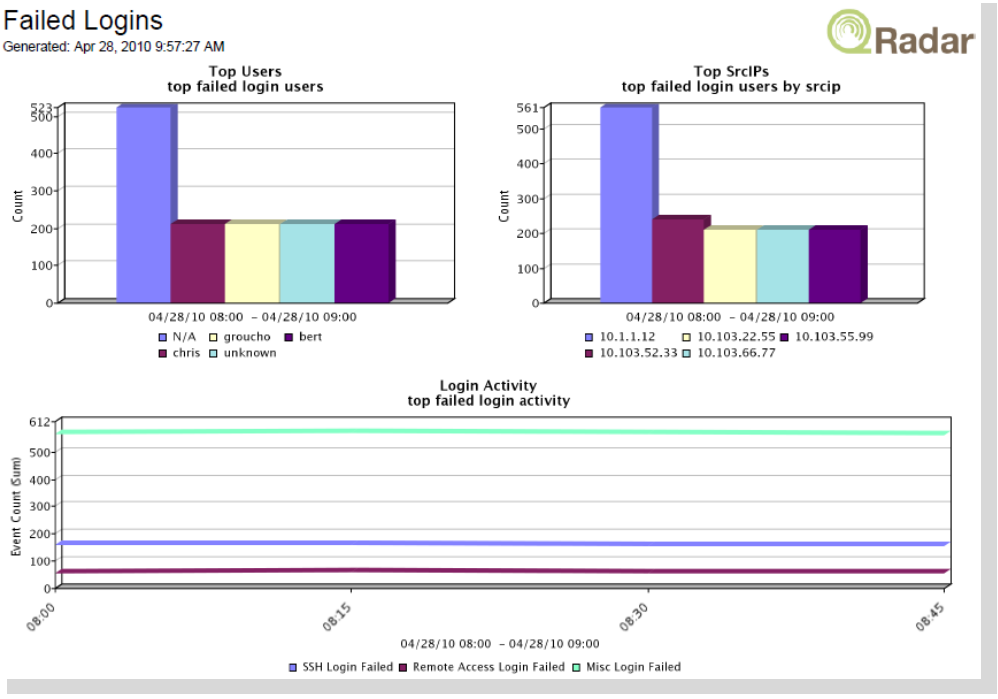
QRadar 满足了 SOX 的许多要求，例如（SOX 合规性规则要求）：

- SOX 要求（第 302 (a)(4)(C) 和 (D) 条 - 登录/注销监控）：用户对系统的访问必须记录在案并加以监控，确定是否存在滥用现象。

  QRadar 提供：

  - 开箱即用、可定制的访问和身份验证规则，支持轻松检测存在威胁或无效的访问尝试。
  - 对所有日志数据和网络通信的深入取证监测视图，支持监控/审计与一次访问攻击有关的所有活动。
  - 通过日志分析执行文件完整性监控和通知。
  - 访问审计跟踪记录的备份和存档。

SOX 合规性报表样例



QRadar
Integrated Solution

- 自动发现
- 基于设备的架构
- 数以百计的预定义规则
- 数以千计的预定义报表

自动化部署能力

优化大规模运营的效率

对于希望通过自动化资源密集型安全性和合规性计划（SOX、GLBA、PCI 等）来确保合规性、掌控成本、管理重要人员的金融服务机构来说，提供针对网络攻击、违规、欺诈和内部人员威胁的保护的需求比以往更为紧迫。

QRadar 的自动化设备发现和数据收集能缩短价值创造进程，持续以被动和主动方式识别和分析资产，从而根据服务、漏洞、系统和身份的变化调优安全性系统。这种安全管理的自动更新让误报现象有所减少，支持精准识别威胁，并按相关性、严重性和整体影响进行优先排序。

QRadar 的自动化能力包括：

- 自动发现，提供持续监测和分析法规合规性要求保密和评估的新资产（例如，服务器）的能力，减少运营工作量，确保受影响设备/服务的准确威胁识别。
- QRadar 基于设备的架构提供了紧密集成的高可用性，我们在各设备中内嵌可扩展数据库，因而不再需要部署和维护成本高昂的外部关系数据库。
- 数以百计的预定义规则可检测主要威胁，例如机器人感染、数据泄露和合规性违规。
- 超过 3500 种预定义报表提供了组织所有层面的可见性，支持金融服务合规性计划（所有规则和报表均免费提供给 Q1 Labs 客户，包括定期更新）。
- 威胁监控，包括自动更新第三方威胁数据源（包括黑名单网络、应用程序检测和地理位置数据），同时集成 IAM，支持更好地识别和解决威胁。

QRadar 支持金融服务网络中部署的近 200 种产品（几乎涵盖了每一家领先供应商），包括 Cisco、Juniper、Nortel、Checkpoint、Oracle、Sun、Enterasys、Symantec、ISS/IBM、McAfee、Sourcefire、RSA 等供应商的设备，提供跨各种系统的收集、分析和关联，包括联网解决方案、安全性解决方案、服务器、主机、操作系统和应用程序。此外 QRadar 解决方案可轻松扩展，以支持专有应用程序和新系统。

QRadar 实践

众多 QRadar 金融服务业部署的成果

某大型地区性银行在美国西部的 10 个州设有超过 500 处分行，这家银行利用 QRadar 集中监控其安全基础架构，包括防火墙、VPN 和漏洞扫描器。

某财富杂志百强保险公司在全企业范围内利用 QRadar，集中化日志管理，提供新型网络威胁保护，并提供针对 SOX、GLBA 和 PCI 的安全控制。

某全球最大的商品市场证券交易所利用 QRadar 实现企业级日志管理，集中管理网络威胁，并实现了与 SOX 相关的安全性控制。

某领先金融和支付服务公司拥有超过 3,000 家客户，包括美国排名前十五位的银行中的三家银行在内，该公司在短短一天内就完成了 QRadar 的部署。QRadar 让他们的整个基础架构得以安全运行，还帮助其满足了 SOX、GLBA、PCI DSS、FFIEC 和 HIPAA 的合规性要求。

“我们希望客户对我们有信心，相信我们能妥善保护他们的个人信息，QRadar 让我们能实现这样的目标。” Regulus Group 的技术运营官 Jeff Dalton 说，*“此外，我们选择 Q1 Labs 而非其他主要竞争厂商的原因在于，他们提供了最完善的安全智能和最出色的客户支持。”*

客户示例

Q1 Labs 的金融服务业安装客户群包括 ING Direct、Sungard、Zions Bancorporation、North Carolina State Employees Credit Union、S1 Corporation、Liberty Bank、West Coast Bank、La Roche and Co、State Auto Insurance 等公司。

结束语

对于提供金融服务的机构（包括银行和保险公司在内）而言，有效的 IT 安全性计划至关重要。改进整体 IT 安全性的动机涉及方方面面，包括运营改进和合规性，但一切都指向一个最终目标：保护关键基础架构资产和敏感客户信息。

过去，企业投资采用多种单点式解决方案，试图缓解特定的 IT 风险。将来，组织需要设法利用现有资产，综合利用这些解决方案已经提供的信息，发挥其价值。

Q1 Labs 的 QRadar 为组织提供了通过一种集成化的网络安全管理方法加强整体 IT 安全性、满足特定法规要求的特性，在日志管理、威胁管理和合规性管理提供了独一无二、独具优势的价值。

Q1 Labs

Total Security Intelligence

890 Winter Street
Suite 230
Waltham, MA 02451 USA

电话：781.250.5800
传真：781.250.5880
电子邮件：
info@Q1Labs.com
Web: Q1Labs.com
HCB 410

Q1 Labs 是高价值、高成本效益的安全信息和事件管理 (SIEM) 产品的全球供应商。QRadar 安全智能平台是这家公司大力发展的旗舰产品，它在一种整体安全智能解决方案内集成了过去支离破碎的功能，包括日志管理、网络行为分析和安全性事件管理。QRadar 为用户提供了了解网络、数据中心和应用程序状况的重要可见性，从而帮助其更好地保护 IT 资产、满足法规要求。Q1 Labs 的客户包括医疗保健提供商、能源机构、零售机构、公共事业企业、金融机构、政府机构和大学院校等。