



QRadar+Guardium 全面的集中审计解决方案

日益增加的合规要求如何满足？海量的告警日志，都是真正的威胁在发生吗？

用户面临的挑战：

- 如何能够对数据库进行审计而不影响数据的性能？
- 如何满足等保、PCI,ISO27001、SOX等合规和审计要求？
- 如何收集和保存海量的日志？
- 如何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。

如果我们通过IBM关键技术和手段：

- 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。

将会为用户带来如下价值：

- 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、风险管理和网路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。

如有相关问题可以咨询IBM服务热线：800-810-1818转5339