Qradar 2100
中小企业集中日志管理系统

日益增加的合规要求如何满足？海量的告警日志，但是真正的威胁在发生吗？

用户面临的挑战:

- 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 Qradar 2100集中日志管理系统，可以获得:

- 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;
- 高达每秒1000条日志收集能力，以及每分钟50000条网络流量(Flow)信息
- 自动收集、自动日志源识别，自动关联分析和Root Cause告警
- 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;

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;
- 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。其具备高可用性、易於扩展、易於部署和使用的特性，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