IBM 携手某大型车企集团打造态势感知平台

客户情况：

某大型车企集团业务规模庞大，安全工具却散乱复杂，车联网在孕育无限商机的同时也带来更高的安全要求。该集团决意严守两条“网络安全车道”，合规性与安全分析“两手抓”，巩固安全防线，扫除业务发展的后顾之忧：

- 满足日志管理的合规性要求包括网络安全法、等级保护、上级主管部门相关性要求与内控要求
- 满足安全分析的要求
  - 管控整体安全风险
  - 保护车联网等重要IT资产
  - 防止违规操作与敏感数据泄露
  - 防止高级威胁，防范欺诈等恶意攻击
  - 为安全主管领导提供安全态势的综合视图和信息
  - 为安全分析人员提供统一的安全信息采集、分析、建模和处理的能力

客户利益：

凭借产品系统的智能基因，IBM QRadar打造态势感知平台，助力该集团理清散乱复杂的安全工具，把实时捕获日志流、安全警报优先排序、分析情报三者完美结合，改善安全人手有限、机能不足的现状，实现风险可视化，主动“出击”发现并解决安全问题，提升威胁保护与合规性，筑好安全堡垒，将业务价值冲锋至新高度！

- 支持日志留存6个月，满足法律法规、主管部门与内控合规性要求
- 提高了安全风险管控的能力，安全分析效率提升10倍
- 节省时间与人力成本，仅需1人监控QRadar平台以支撑安全威胁侦测

IBM Security

IBM 安全优势：智能基因

- IBM Qradar 连续十一年在 Gartner 魔力象限 SIEM 领域被评为领导者
- IBM QRadar SIEM是业内功能最为完整的SOC平台，覆盖日志管理、网络异常行为检测、威胁情报、内置的关联规则库、实时关联分析引擎、用户行为分析、漏洞管理和风险管理等
- QRadar提供了一系列高级分析和响应能力，包括用户行为分析（UBA）、实时深度包检测（QRadar Network Insights）、全包取证（QRadar Forensics）、威胁情报（IBM X-Force）、应急响应平台（Resilient）以及QRadar Advisor with Watson（认知安全），这些能力都可以转化成为客户提供增值服务的能力

IBM