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

13年“真爱”长跑，践行持续发展之路

IBM 携手某大型车企共建 IAM 平台

客户情况：

某大型车企曾在身份与访问管理之路上面临一连串“路障”：

- 如何有效管理 HRMS, ERP, OA, MAIL, SDA 等几十种应用的身份
- 如何管理数以十万计的员工、经销商与供应商等用户，并能即时查看这些用户的活动登录、认证等行为，如何进行密码管理
- 如何快速实现多因子认证
- 如何和 兄弟集团公司，供应商系统实现联邦 SSO（单点登录）

客户利益：

13年的时间，IBM IAM 已稳步发展为该大型车企的核心管理平台之一，为内部其他业务系统提供集中的认证、授权、身份生命周期管理和 SSO 等服务；为该大型车企提供身份主数据平台，在防范内部威胁的同时释放业务价值；为其他安全态势感知等平台提供身份依据。

- 内外部审计均无短板
  - 集中管理与访问控制，报表完整，十几年来在身份管理与 SSO 方面基本零纰漏
- 助力标准化流程
  - 对新系统、软件进行评估，进行集中化、标准化管理，方便后续管理，保护现有投资的同时节省成本
- 为业务保驾护航
  - 应用系统可直接接入 IAM 系统，无需增加防火墙、负载均衡器或进行网络调整
  - 集中式进行拦截、管理、认证等工作，减少守护用户凭证与访问权限的复杂性和成本，提高身份管理的效率
  - 登录方式从密码逐步演进至工卡、手机登录，建立以用户为核心的身份管理模式，提高终端用户在各种环境下工作效率

IBM Security

IBM 安全优势：稳定发挥十三年

- IBM IAM 连续十年在 Gartner 魔力象限 IAM 领域被评为领导者
- 作为业内功能最为完整的 IAM 平台，服务的全球客户超过 1000 家，为客户提供高质量的身份管理、单点登录、授权管理、联邦认证、双因素认证等服务
- 自 2006年起，某大型车企携手 IBM 深耕 IAM 平台建设，13年时间里彼此充分信任，志同道合，稳扎稳打，逐年迭代建立起 IAM 坚实的基础平台，标准化规范与框架，为该车企现有和未来企业应用提供了坚实基础

IBM

守护“塔尖上的安全”

IBM QRadar “入驻”某芯片公司

客户情况：

纵观该芯片公司的安全环境，CISO需要提升整体安全运维的水平，实现对安全事件检测和响应的智能化、标准化和自动化，当务之急在于扭转以下形势——

- 缺乏整体安全态势感知的能力，在进行形势研判和决策支持时，无法获得全面的、多维度的安全情报
- 缺乏专业的信息安全人员，面对每天大量的安全事件，无法进行甄别和响应
- 现有安全基础设施仅能够满足单领域防御的需求，面对高级威胁场景，无法进行集成化，关联化、智能化分析

客户利益：

该芯片公司选择携手 IBM，从 IBM安全免疫力体检开始，先评估自身安全免疫力，再一步步细化安全路线。IBM安全免疫力体检旨在通过简单、快速、易于实施的方式，帮助企业发现潜在安全威胁，了解自身安全建设等级，从而有的放矢地提升整体安全运维水平。

该芯片公司快速启动体检，两个星期后 IBM QRadar 即发现了一系列安全威胁：

- 暴力破解，PA防火墙存在大量账号暴力破解尝试
- 僵尸网络连接，内部主机连接国外僵尸网络控制中心
- 漏洞利用，外部恶意IP对内部主机的漏洞利用行为
- 访问大量国外FTP地址，内部主机疑似被挂马
- 明文FTP应用，安全合规性疑似遭到破坏
- 内部数据泄露风险

IBM Security

IBM 安全优势：
为客户制定稳打稳扎的安全运维建设路线

通过快速启动体检，两个星期后 IBM QRadar 即发现了一系列安全威胁。根据体检结果，该芯片公司迅速启动立项工作，与 IBM 共同制定了稳扎稳打的安全运维建设路线：

- 阶段1：SIEM平台第一期，主抓风险可视化
- 阶段2：SIEM平台第二期，主抓 EPS 扩容，增加流量 FPM License, 特别关注未知风险的检测，内部横向移动等风险
- 阶段3：主抓 SOAR 平台建设、个案管理建设等
- 通过快速启动体检，两个星期后 IBM QRadar 即发现了一系列安全威胁。根据体检结果，该芯片公司迅速启动立项工作，与IBM共同制定了稳扎稳打的安全运维建设路线：

- 作为业内功能最为完整的 SOC 平台，IBM QRadar SIEM 可帮助该芯片公司集中管理和分析日志和网络流数据，整合安全设备日志、网络流量、资产信息与漏洞信息等，检测网络异常行为与威胁情报，通过专业智能的分析模型降低对安全人员专业水平的依赖度，并兼顾企业合规与安全需求，最终提升整体安全运营水平。

IBM