从总行、分行延伸至信用卡中心

IBM Qradar 助某银行打造自主可控的安全架构

客户情况：

某股份制商业银行始终坚持以创新为本，探索现代商业银行建设之路，为客户提供专业特色的现代金融服务。

深深印刻在 DNA 中的自主开发能力，使其在银行业安全之役中同样并不局限于标准化安全工具，而是寻求灵活的、可定制化的安全解决方案。

客户利益：

- 2015年，该银行通过部署 IBM QRadar SIEM，自主构建了基于日志和 QRadar flow 实时关联分析的安全运营中心(SOC)：
  - 对总行与分行各平台的网络流量、设备日志进行集中化收集与便捷化管理
  - 建立符合银行信息安全管理要求的总行和分行事件关联分析规则，对网络安全日志、网络抓包等信息进行基础性的关联分析和统计模式的基线分析，并实现信息安全事件和潜在威胁的警告，提高阻断效率
  - 建立符合内外部监管、银行信息安全管理要求和信息安全技术分析需要的实时可视化和报表

- 2019年，该银行又继续采用 IBM QRadar SIEM 和 QRadar Network Insight 部署到其信用卡中心
  - 与总行运营同一个总控台，进行联动分析，同一套产品可降低运营和维护成本
  - 使用 IBM Qradar Network Insight 进行流量全数据包分析，实现网络流量深度洞察
  - 实现风险可视化，定期汇报与总结平台检测到的安全事件次数及处理历史，体现安全团队的价值

IBM 安全优势：高度易用与可定制化

- IBM Qradar 连续十一年在 Gartner 魔力象限 SIEM 领域被评为领导者，深耕银行业多年，打造了多起成功案例。
- 安全可视化是 Qradar 的“看家本领”之一，面对高级持续性威胁与内部人员威胁等，Qradar 可以实时地捕获日志事件和网络流数据，并减少海量活动带来的“噪音”，以更短的时间实现威胁的清晰可视化，以更高的准确性了解真正的威胁。
- 良好的易用性，借助自然语言，易理解易上手，降低专业性，提高使用度
- 高度定制化，模板多样，支持基于默认规则的按需修改，灵活度高

IBM Security

IBM

IBM Guardium

从源头守护台湾某银行数据库安全

客户情况：

面对愈发严格的合规要求，银行业作为数据安全领域的“排头兵”，往往直面更严峻的挑战。台湾某大型商业银行业务网络众多，营业范围包括存款、贷款、信用卡、债券与股票投资、汇兑、证券、期货、保险、信托等。

- 数据库审计管理系统设备老旧，逾期待换
- 设备处理不当造成审计记录缺失，也无法有效监控数据访问者
- 重要数据遍布内部各类数据库与数据环境，审计无法全面涵盖

客户利益：

部署IBM Guardium，使得该银行无需修改数据库环境，也无需改变原有网络的任何设定，快速实现弹性扩充，基本可支持覆盖全行数据库，打造安全“铜墙铁壁”，满足合规要求——

- 监控本行含有个人信息的重要数据库服务器存取行为，以符合主管机关与法规要求
- 具备负载平衡与高可用性功能，数据库审计服务持续不中断
- 整合各应用程序使用者帐号，有效透视数据库存取行为，防止内部人员不当使用
- 利用分析机制找出异常使用行为，化被动为主动，降低资料外泄风险
- 建立完整的审计日志备份机制，并依业务需求产出审计报表，以供内外部查核使用

IBM 安全优势： S-TAP架构升级+弹性扩充

IBM Guardium采用高效稳定且对数据库主机效能影响最小的探针侧录架构（S-TAP），是在兼顾审计完整性与不影响网络架构下的数据库审计最佳解决方案，实现审计完整、负载平衡与高可用性，把控数据使用者存储、读取等行为，并可进行关联分析，从源头守护数据库安全。

	S-TAP 收集方式	SPAN Port 收集方式
收集完整性	可完整收集本机与与网络的数据	本机端数据无法收集 加密过的数据无法收集 网络噪声太多会影响，网络封包掉失问题
安全性	审计数据在收集，传输与储存过程中，皆有加密处理，安全无疑虑	无加密处理，接上 SPAN Port 可取得机敏数据，造成信息泄露
监控差异	本机或网络对数据库的存取皆可监控	仅对网络上数据库存取进行监控，对加密或主机端无法监控
网络影响	因为在主机端已将数据整理完毕，无需浪费太多网络资源传输数据	SPAN Port 会造成转换设备负载加重
数据库主机运作	Guardium 探针宕机不会影响主机，同时若网络断线，探针会将数据暂存在缓存当中	审计数据收集主机宕机不会影响数据库
回传数据屏蔽	是	否
高可用性	S-TAP 可将收录数据指派至多台收集器	无
导入冲击	几乎没有影响	对既有信息架构影响较大，尤其是网络
扩充性	易于扩充	扩充复杂度较高

IBM Security

IBM

某银行联手IBM i2，加强战力重击洗钱不法行为

可视化分析明察秋毫，蛛丝马迹无所遁形

客户情况：

自2007年中国正式加入FATF后，国家反洗钱监管力度不断提升，2019年仍是反洗钱监管大年，监管机构频频打出更快更强的“拳风”，反洗钱决心可见一斑。某银行也在不断探索大数据、机器学习、人工智能及可视化等创新技术在反洗钱领域的应用。

- 正在使用的产品来自非安全专业厂商，不稳定的存储甚至一度导致日志遗失
- 正在使用的安全产品要求按数据交易量收费，成本将高至10万美元
- 人手极度短缺，并且缺少熟练的安全分析师，快速精准的安全分析难免“捉襟见肘”

客户利益：

- IBM i2 与该银行的业务场景紧密结合，分析员可以在导入客户账户明细等数据后，通过数据过滤和分析形成多种布局方式（如网络布局，层次布局，时间比例布局等），运用可视化分析深入探查可疑账户之间的交易关系、资金流向、交易路径、交易规律及趋势等。
- 独具慧眼“看清”海量数据，最强大脑充分解析账户关联，IBM i2 助力该银行从繁杂的数据中快捷找到多账户之间的资金往来关系，发现隐藏在账户数据中的高级威胁洞察，为下一步行动夯实基础；同时，IBM i2降低了该银行反洗钱调查的误报率，提高分析工作的有效性，全面提升洗钱风险管控水平。

IBM 安全优势：将数据转变为关键情报

不同于一些部署复杂的重型软件，IBM i2 是一种桌面型操作工具，简单易上手的操作背后蕴含着非同凡响的动能：

- 强大的展现能力

将结构化数据快速进行可视化展现，支持10万个节点展现零卡顿

- 丰富的可视化类型

13种布局图之间按需转换，从多个角度查看数据间的关系

- 多样的可视化分析

包括可视化查询、链接分析、路径分析、群集分析、社会网络分析等分析算法与分析工具

IBM Security

IBM 携手某大型制造企业集团打造态势感知平台

客户情况：

某大型制造集团业务规模庞大，安全工具却散乱复杂，数字化技术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

IBM携手某大型食品与饮料零售商

构建由浅入深、拾级而上的安全旅程

客户情况：

某大型食品与饮料零售商目前存在如下安全管理“瓶颈”：

- 正在使用的产品来自非安全专业厂商，不稳定的存储甚至一度导致日志遗失
- 正在使用的安全产品要求按数据交易量收费，成本将高至10万美元
- 人手极度短缺，并且缺少熟练的安全分析师，快速精准的安全分析难免“捉襟见肘”

客户利益：

IBM QRadar Data Store 使得该零售商可一次性购买，7万美元即可带来无限量存储，低于继续使用当时安全厂商所预计的10万美元。每个Data Store节点的数据容量不再受限，无限量设备的日志收集和存储轻而易举，真正适用于呈指数型增长的客户数据。

QRadar作为一个智能化 SIEM 平台，能使该零售商在收集安全数据后将安全数据关联起来，让安全分析师“事前体检，事中联动，事后反馈优化”，透过按风险优先级排序的单一界面视图，了解活动性威胁。

从最初的QRadar Data Store起步，发展到QRadar SIEM，逐渐跟随IBM安全旅程一步步升级到QRadar Advisor with Watson的典型案例。

IBM Security

IBM 安全优势：
由浅入深、拾级而上的安全旅程

IBM打造了循序渐进的两个阶段，多个IBM安全软件之间协同作用，深刻展示集成的重要性：

- 阶段1：IBM QRadar Data Store构建最具性价比的日志数据湖，无限量存储内部审计所需的日志，满足合规性需求
- 阶段2：使用IBM QRadar SIEM进一步实现用例开发和调整分析；IBM帮助客户认识到在符合内部合规性的同时也必须提高对外部高级威胁的警觉性，加强对敏感数据的保护，而由AI赋能的IBM QRadar Advisor with Watson将加快安全问题发现与调查进程，解决专业安全分析师短缺的问题。
- IBM QRadar Advisor with Watson由AI赋能，真正释放认知安全的力量，能学习与理解大量非结构化数据，并将其与结构化数据相关联以发掘新洞察，可以连接其他技术未发现的隐藏数据点以准确地识别威胁，并通过丰富的威胁调查和实时情报来正确识别恶意活动——“智能、快速、准确”三连招帮助该公司解决分析人手短缺的问题，迅速自信地响应威胁、抵御网络攻击。

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

IBM Security SOC Consulting Service

为某银行量身定做 企业级SOC 战略规划

客户情况：

无论是出于内部对数字生态战略的安全保障要求、日益严峻的安全大环境、愈加严格的外部监管要求，还是来自同业安全建设的压力，某大型商业银行都需要继续升级现有的安全运营能力。

SOC一直在不断进化以满足当前和未来的安全运营需求，具备认知功能的网络安全以及混合银行各类风险的融合SOC是未来趋势。该银行决意把握这个趋势，构建一个具有前瞻性、可持续演进、自适应网络威胁态势感知的数字安全运营中心。

2018年，为应对安全与合规的双重挑战，该银行选择与IBM的合作，通过部署 IBM QRadar SIEM解决方案，打下良好的 SOC（安全运营中心）基础。

客户利益：

IBM Security为该银行评估、规划和设计数字安全运营中心（SOC）以及支撑该中心的整体安全体系，帮助该银行快速实现SOC的基本功能，并为该银行打造成为银行业内重要的安全托管服务（MSS）提供者的规划。IBM为该银行打造了量身定做的 SOC 战略规划：

SOC所使用的SIEM和SOAR安全事件管理平台 / SOC团队 (有经验的分析员和安全专家) / 安全相关报告和看板 / 用于处理安全事件的各SOC流程 / 威胁智能分析（AI）和大数据分析能力 / 监控，响应/提升安全事件相关能力 / 集中化的安全事件聚合（知识库，用例库）/ 特定技术或者工具支持 / MSS服务目录及相关架构 / MSS运营团队人员组成和数量配置 / 各项服务SLA / 绩效管理KPI /成本管理，计费模式

规划后的企业级 SOC 将成为该银行的风险融合中心，运用演绎推理和自我学习能力，全面应对科技安全风险、重要业务风险，对整个银行环境进行安全防御；同时，它将在未来5年内为该银行及其集团子公司与金融云租户提供安全服务，也为数字生态相关合作伙伴提供专业的安全托管服务，安全护卫该银行业务的长远发展。

IBM Security

为安全运营保驾护航，IBM Security咨询服务实力“亮剑”

作为业界唯一一家既提供SOC安全咨询又提供SOC关键技术平台的厂商，IBM在SOC规划建设和安全运营方面是当之无愧的领跑者：

- 丰富的全球行业经验：数以千计推动客户安全转型的成功案例，尤其在银行业的风险融合中心领域； 成功建设90多个客户SOC，在自己的 SOC 中每天管理的安全日志超过350亿条
- 完整的安全系统：超过100家安全厂商采用和支持 IBM 开放式安全免疫平台；20项战略收购，在12个细分市场上提供领先方案
- 领先的 AI 智能分析和大数据分析能力：业务领先的安全分析平台，跨各领域的全新人工智能；已在网络安全语言方面成功训练了 Watson
- 全球金牌智囊团：优秀的SOC规划建设能力与实施经验；标准化的实施方法以及全球客户的定制能力

IBM

IBM 安全打通物联安全通路助力某电力供应商实现 OT 安全规划与评估

客户情况：

客户希望为其580,000个用户提供更明细的电力消费信息，以帮助他们优化能源使用，从而助力民众采取适当的措施来节约能源。因而其将在 2020至2025年逐步实现智能电表的部署。而对于智能电表基础架构（AMI）的部署而言，其需要一套能够识别、保护、检测和响应网络安全风险和威胁的 安全解决方案，补足IT与OT安全、物联设备与IT基础设施之间的安全鸿沟。

客户利益：

面向物联网安全的全生命周期安全评估服务：

守护智能电表基础架构的设计和部署安全，保障 IOT 架构稳定支持对公民和企业的供电。

确保重大公用事业资产和客户信息的全面保护，预防未来增长的恶意网络攻击。

计划从 2020 年 4 月到 2025 年为客户部署智能电表。该计划将在未来 6 年内按地区分阶段实施。

为 580,000 个客户提供更多的消费明细，帮助他们优化能源使用，进而采取适当的措施来节约能源。促进高效的电表到现金活动及电网运营。

IBM Security

为何选择 IBM

信息安全领域的全球领先实践

- 全球最大的企业网络安全提供商
- 12 个安全市场细分领域的领导者
- 拥有 8,000 多名安全运营人员
- 20 多家安全领域企业并购
- 每天监控 700 亿次以上的安全事件

AMI 安全方面的丰富经验

- 我们曾在全球范围内进行过许多类似评估：成熟度和风险评估
- 我们曾为能源和公用事业开展过多个项目
- 我们的团队拥有多项认证，包括 62443、GICSP、GXPN 等

OT 架构的独特模拟工具

- 发现复杂架构中的所有攻击路径并模拟攻击的横向移动
- 发现最可能的攻击路径
- 恶意软件如何在网络中传播（攻击范围）
- 了解架构是否可以检测到每个攻击步骤和场景
- 最佳补救措施（假设分析）

IBM