IBM Security 帮助英国的一家全球银行优化了安全监控流程，提升了网络威胁检测和响应能力

客户情况：

- 过去，该客户一直依赖分散、脱节的威胁检测平台来应对 **12 个孤立的安全运营中心 (SOC)**，监控信息和安全风险。结果，该银行在洞悉各个实体内的威胁时，只能获得**支离破碎的可视性**。更糟糕的是，SOC 每天只工作八小时，一周只工作五天，导致客户一周有很长一段时间处于无人监管的状态。此外，该银行**依靠数名全职员工来运营 SOC 和提供合规性报告**。因此，银行的运营成本非常高。为了解决这些问题，客户希望利用一款强大的安全解决方案来**实现 SOC 的转型**。

IBM 解决方案：

该客户分三个阶段实施 IBM 安全软件，构建集成式 SOC。

1. 在第 1 阶段，客户制定了端到端的 SOC 转型路线图。他们**开展了成熟度评估**，编制了 SOC 章程，制定了投资计划。然后，为了实现 SOC 的转型，客户实施了 IBM Security QRadar SIEM 软件来准确检测客户面临的威胁，并对威胁进行优先级排序。
2. 在第 2 阶段，该银行**将 Security QRadar SIEM 软件推广至其余的 11 个本地 SOC**，以改进智能威胁检测和响应。借此，客户消除了平台孤岛，将 SOC 集成到了**全天 24 小时运行**的连贯系统中。
3. 在第 3 阶段，为了增强 SOC 功能，客户部署了 IBM Resilient Incident Response Platform，以便**自动执行 SOC 工作流管理和事件响应流程。**

客户收益：

- 通过实施上述解决方案，该客户能够通过单一界面**获得**覆盖整个企业的**可视性**，**更高效**地检测和响应网络威胁，**降低事件的影响，不再需要全职员工**来持续监控系统，进而大幅**减少运营成本**。

客户资料：

该公司是一家总部位于英国的大型全球银行。