

Case Study

Offensive security testing helps elevate cloud security, reduce risks and cut costs.

Industry:

- ▶ Financial Services

Brief Company Description:

- ▶ A leading UK-based financial institution known for its comprehensive range of services, including personal and business banking, mortgages, loans and digital banking solutions.
- ▶ **Area of Focus:** Security Testing



BUSINESS CHALLENGE

Our client, a leading bank, had security challenges in the cloud landscape as it strived to safeguard customer data and maintain regulatory compliance.

With the migration of some parts of critical financial systems to Azure Cloud infrastructure, the bank focuses on addressing issues like data protection, threat detection, and secure access management and continuous monitoring.



KEY INITIATIVES

Using a Red Teaming approach, we focused testing on their Aure Cloud security posture from an attacker with zero knowledge.

This included:

- Identity & Access Management
- data storage security
- access and credential management
- virtual machine security
- Azure firewall configuration
- Azure Function and Logic App security
- container security
- encryption and third-party integrations



RESULTS

Our report identified a number of high severity findings including complete compromise of the Azure Domain. These findings included poor password management and insecure default configurations.

We recommended changes to the cloud infrastructure and established a continuous processes (including configuration management) to address the findings and reduce the likelihood of vulnerabilities arising in the future.