RIVERSAFE

CASE STUDY

THE CHALLENGE

A large African bank required a modern, cloud-hosted security monitoring capability to enhance visibility across its technology estate and strengthen threat detection and response.

The objectives were to:

- **Centralise** log management
- Enable near **real-time** threat detection
- Improve **behavioural analytics** capabilities
- Establish structured **incident investigation** and response workflows
- Ensure the solution aligned with operational and **regulatory expectations**

The bank required not only deployment of the platform, but tailored configuration to ensure it delivered meaningful security outcomes.

THE SCOPE

RiverSafe was engaged to remotely deploy and configure a cloud-based SIEM and behavioural analytics solution, including:

- **ANOMALY-BASED DETECTION OF FINANCIAL FRAUD**
- **DATA INGESTION AND STORAGE CAPABILITY**
- **ADVANCED ANALYTICS AND DETECTION FUNCTIONALITY**
- **CASE MANAGEMENT AND INCIDENT RESPONSE WORKFLOWS**

The project was delivered over approximately 45 days, structured into phased deployment, configuration, validation and documentation activities.

Clear governance and coordination were maintained throughout, with defined responsibilities for infrastructure readiness, access provisioning and internal change management.

WHAT WE DELIVERED

ANOMALY BEHAVIOUR DETECTION & USE CASE ENABLEMENT

Configured the solution to detect attempts of financial fraud, insider threats, privilege misuse, suspicious logins, and potential data exfiltration, with analytics tuned for accuracy and reduced noise.

Outcome: Enhanced financial fraud and cyber threat detection with higher signal quality and fewer alerts.

DETECTION & USE CASE ENABLEMENT

Configured the solution to detect malware, ransomware, phishing, insider threats, privilege misuse, suspicious logins, and potential data exfiltration, with analytics tuned for accuracy and reduced noise.

Outcome: Enhanced threat detection with higher signal quality and fewer false alerts.

LOG SOURCE INTEGRATION

Configured the SaaS environment for **secure log ingestion**, **detection validation**, **analytics tuning**, and **operational health** monitoring.

Outcome: Platform aligned to the bank's monitoring priorities and risk profile.

OPERATIONAL READINESS

Produced **structured technical documentation** covering platform operation, configuration, maintenance, and knowledge transfer, alongside validation of system health, log accuracy, and detection effectiveness.

Outcome: Supported ongoing operations and ensured platform readiness at closeout.

DEPLOYMENT & CONFIGURATION

Onboarded multiple enterprise and security log sources across transaction gateways, core banking systems, identity, infrastructure, cloud, endpoint, and network, validating each for accurate ingestion and effective correlation

Outcome: Broad, reliable visibility across the bank's technology estate.

OVERALL OUTCOMES

- **CENTRALISED VISIBILITY ACROSS KEY SYSTEMS**
- **BEHAVIOUR-DRIVEN THREAT DETECTION**
- **STRUCTURED INCIDENT INVESTIGATION WORKFLOWS**
- **IMPROVED MONITORING CONSISTENCY**

The environment was configured and validated to align with the organisation's security objectives, with documentation in place to support continued operational management.

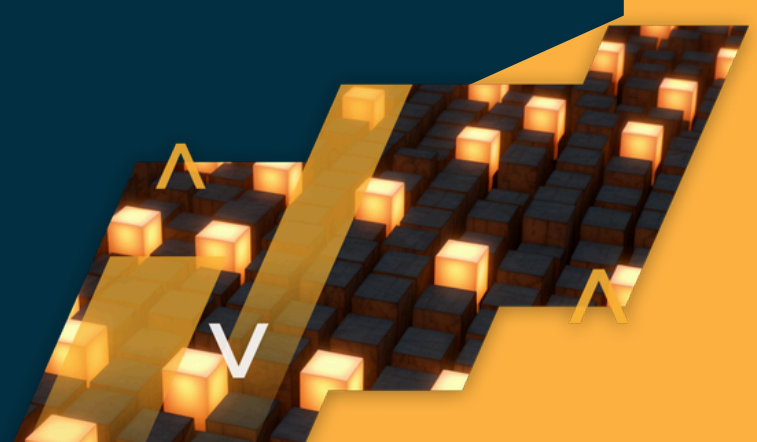
ABOUT RIVERSAFE

RiverSafe brings deep expertise across leading SIEM and security analytics platforms, combined with real-world experience in SOC operations, cloud transformation, and security engineering.

If you are modernising your monitoring capability, centralising visibility, or strengthening threat detection across a complex estate, we can help you move from platform deployment to proven outcomes.

Let's discuss how we can support your security objectives.

Get in touch >



www.riversafe.co.uk