BLACK BOX

CASE STUDY
CYBER SECURITY / MANAGED SOC

Centralizing Threat Detection at a Leading Mongolian Bank with a 24/7 Managed SOC

Overview

A leading Mongolia-based bank relies on core banking platforms, digital channels, ATMs, payment infrastructure, and other critical systems to deliver secure, uninterrupted services. Rising log and alert volumes, however, were outpacing its existing monitoring processes.

Security data remained distributed across multiple technologies, limiting centralized visibility and increasing reliance on manual investigation. The bank needed a consistent way to detect threats, respond to incidents, and support compliance without adding operational complexity.

Black Box introduced a centralized security operations model built on Securonix SIEM and User and Entity Behavior Analytics (UEBA), supported by a Mongolia-based 24/7 Managed Security Operations Center (MSOC). The engagement unified monitoring, analytics, investigation, response, reporting, and continuous optimization.

Challenges

As the bank's digital environment expanded, security events grew in volume and complexity. Logs spread across separate systems prevented analysts from seeing related activity in one place, slowing correlation and making emerging threats harder to identify.

Manual, reactive monitoring increased alert fatigue and investigation effort. Without dedicated 24/7 coverage, delayed detection and containment could disrupt critical banking services.

The solution also had to integrate with a diverse technology environment without affecting service continuity. It needed to strengthen incident governance, compliance reporting, and audit readiness while scaling cost-effectively with the bank's digital operations.

AT A GLANCE

CHALLENGES

- Fragmented logs limited centralized visibility.
- Manual monitoring slowed detection, triage, and response.
- Limited resources constrained 24/7 security coverage.
- Growing compliance needs increased reporting complexity.

SOLUTIONS

- Centralized monitoring with Securonix SIEM and UEBA.
- Onboarded log sources and tuned priority use cases.
- Established a Mongolia-based 24/7 Managed Security Operations Center.
- Added continuous monitoring, investigation, response, and reporting.

RESULTS

- Achieved 100% visibility across onboarded security systems.
- Improved threat-detection capability by 80%.
- Reduced MTTD by 80% and MTTR by 75%.
- Reduced manual investigation effort by 90%.

BENEFITS

- Strengthened visibility across critical banking systems.
- Increased cyber resilience and service continuity.
- Improved compliance reporting and audit readiness.
- Created a scalable foundation for future security growth.

Solutions

Black Box assessed the bank's environment, security gaps, priority risks, and operating requirements. The resulting plan defined log sources, detection use cases, escalation paths, reporting, and governance.

Securonix SIEM centralized security telemetry, while UEBA added behavioral context to identify unusual user and entity activity. Black Box tuned priority use cases to the bank's risk profile.

A Mongolia-based 24/7 MSOC provided continuous monitoring, alert triage, threat hunting, investigation, response, reporting, and optimization without increasing internal headcount.

Delivery progressed through three controlled phases: discovery and assessment, integration and use-case tuning, and go-live with SOC transition. Testing, knowledge transfer, and readiness reviews supported a smooth move to consistent security operations.

Results

Centralized monitoring across 42 security log sources gave the bank 100% visibility across onboarded systems and a unified view for identifying, prioritizing, and investigating threats.

The platform now processes about 8.62 million security events daily. Centralized correlation, behavioral analytics, and tuned workflows reduced Mean Time to Detect (MTTD) by 80%, Mean Time to Respond (MTTR) by 75%, and manual investigation effort by 90%, allowing analysts to focus on higher-risk incidents.

The six-week transition comprised two weeks each for discovery, integration and tuning, and go-live. With ongoing Black Box MSOC support, the bank improved threat-detection capability by 80%, strengthened compliance reporting and audit readiness, and established a scalable security operations framework.

Why Black Box?

Black Box combined cybersecurity consulting, Securonix integration, and 24/7 managed security operations in one delivery model. Local engagement, structured governance, and global cybersecurity resources addressed immediate monitoring needs while advancing long-term operational maturity.

The result is a scalable, resilient foundation for regulatory obligations, business continuity, and the bank's evolving digital environment, backed by continuous monitoring and ongoing managed services support.