CASE STUDY

IBM i Session Monitoring & User Activity Record with Capture

Asian Financial Services Organization *Anonymized | Confidential*

Client Profile

Industry	Financial Services
Region	Asia-Pacific
Environment	IBM i — 5 LPARs supporting customer services, transaction processing, financial operations, and regulatory reporting
Security Scope	User Activity Monitoring, Session Recording, Insider Threat Detection, and Compliance Support
Assessment Type	Security Monitoring & Operational Visibility Initiative

The Challenge

The organization managed highly sensitive financial and customer information within its IBM i environment. As cybersecurity threats evolved and regulatory expectations increased, management required greater visibility into user activities occurring on critical systems.

Limited Visibility into User Actions

Although user authentication and audit logging were in place, security teams often lacked sufficient context to understand exactly what actions users performed during IBM i sessions. Including:

- Difficulty investigating suspicious user activities
- Limited visibility into privileged user operations
- Time-consuming forensic investigations
- Inability to easily reconstruct user sessions
- Increased challenges identifying insider threats

Security teams required a more effective method to monitor and review user activities across critical IBM i applications.

Regulatory and Governance Requirements

Internal auditors and compliance teams required stronger monitoring controls for sensitive systems and privileged accounts. Key concerns included:

• Demonstrating oversight of privileged users

- Supporting internal investigations
- Improving accountability for sensitive operations
- Maintaining detailed records of user activities
- Strengthening compliance with financial sector regulations

The organization sought a solution capable of capturing and replaying user activities while providing comprehensive monitoring capabilities.

Solution Deployed

Raz-Lee deployed the following iSecurity module across the IBM i environment:

iSecurity Capture

Implemented advanced session monitoring and activity recording for IBM i users. Capabilities included:

- Recording of user sessions and activities
- Monitoring of privileged and high-risk users
- Detailed playback of user actions for investigations
- Improved visibility into operational activities
- Support for forensic analysis and incident response
- Centralized review of user behavior
- Enhanced monitoring of sensitive business processes

The implementation provided security and compliance teams with a clear view of activities occurring across the IBM i environment.

Results

- Improved visibility into user and administrator activities
- Accelerated security investigations and incident response
- Enhanced monitoring of privileged accounts
- Strengthened insider threat detection capabilities
- Improved audit readiness and compliance support
- Increased accountability for critical business operations
- Reduced time required to reconstruct security events
- Deployment completed without disruption to production operations

The organization significantly improved its ability to monitor, investigate, and validate user activities while strengthening security governance across its IBM i infrastructure

Key QSA Feedback

> *"Traditional logs tell us what happened, but not always how it happened. Capture gave us the ability to see and replay user activities in context, dramatically improving investigations, compliance reviews, and oversight of privileged users. It has become an essential component of our IBM i monitoring strategy."*

— Head of Cybersecurity Operations (paraphrased)