CASE STUDY

IBM i EDR Visibility & Threat Response

European Banking Institution *Anonymized | Confidential*

Client Profile

Industry	Banking
Region	Europe
Environment	IBM i — 4 LPARs supporting core banking, transactions, and customer services
Security Scope	Endpoint Detection & Response (EDR) Visibility for IBM i
Assessment Type	Internal Cybersecurity Modernization & Security Operations Integration

The Challenge

The client's Security Operations Center (SOC) had enterprise-grade EDR coverage across Windows, Linux, and cloud infrastructure, but the IBM i environment remained a visibility gap within the organization's cybersecurity monitoring framework. As IBM i systems hosted critical banking applications and sensitive financial data, the absence of IBM i-native monitoring and response capabilities created operational and compliance concerns.

Security Visibility Gap

Traditional EDR platforms deployed within the organization could not provide:

- Real-time monitoring of IBM i user activity, Detection of suspicious command execution
- Visibility into privileged operations
- Tracking of unauthorized access attempts
- Correlation of IBM i events within the centralized SOC environment

The SOC lacked actionable IBM i telemetry required for modern threat detection workflows.

Threat Detection & Response

The organization required the ability to:

- Detect abnormal or unauthorized IBM i activity in real time, Identify privilege escalation attempts
- Monitor sensitive object and configuration changes
- Trigger automated alerts and response procedures
- Integrate IBM i security events into enterprise SIEM workflows

Without IBM i-native event intelligence, the security team could not achieve consistent detection and response coverage across the enterprise.

Compliance & Operational Requirements

The solution needed to:

- Operate natively on IBM i, Require no application modifications

- Integrate with the bank's centralized SIEM platform
- Support rapid deployment across multiple LPARs
- Minimize operational impact on production banking systems

Solution Deployed

Raz-Lee deployed the following iSecurity modules across all IBM i partitions::

iSecurity Audit

Implemented centralized real-time monitoring and auditing of IBM i security events.

Capabilities included:

- Monitoring of user sign-ons and authentication activity
- Tracking of command execution and privileged operations
- File and object access monitoring
- Detection of security policy violations
- Real-time alerting for suspicious or unauthorized behavior

The solution provided detailed IBM i activity visibility required by the SOC and security teams.

iSecurity Action

Implemented automated incident response and policy enforcement capabilities.This allowed the organization to introduce active threat response capabilities within the IBM i environment.

iSecurity SIEM

Integrated IBM i security events into the bank's centralized SIEM platform.The implementation enabled IBM i to become fully visible within the organization's enterprise cybersecurity operations.

Results

- Achieved enterprise-level EDR visibility for IBM i environments
- Integrated IBM i events into centralized SOC monitoring and SIEM correlation
- Improved detection of suspicious user and privileged activity
- Reduced incident response time through automated alerting and actions
- Eliminated IBM i visibility gaps within enterprise security operations
- Deployment completed without application changes or production disruption

The organization significantly strengthened its IBM i security monitoring and response capabilities while aligning IBM i systems with enterprise cybersecurity standards.

Key QSA Feedback

> *"For years, IBM i operated outside the visibility scope of our enterprise EDR and SOC processes. Raz-Lee enabled us to integrate IBM i into our centralized detection and response strategy with real-time monitoring, actionable alerts, and SIEM correlation."*

— Head of Cybersecurity Operations (paraphrased)