SDS
Software Diversified Services

7 Critical Mainframe Security Blind Spots

Costing Banks Millions in 2025

$4.88M	**61%**	**$10.4T**	**$2M**
Average Breach Cost (IBM 2024)	Infrastructure Leaders Use Mainframe Data	US Card Transaction Volume	SOX Compliance Costs (Large Banks)

1 **Unmonitored RACF Administrative Access** CRITICAL

RACF administrators have ultimate access, yet most banks can't see when these priviliged accounts are accessed, modified, or misused.

2 **Invisible CICS Transaction Monitoring** HIGH

CICS processes millions of real-time banking transactions, but traditional SIEM can't parse transaction logs or detect suspicious patterns.

3 **DB2 Database Access Gaps** CRITICAL

Your Db2 databases contain customer financial records and account balances, yet database access logs often go unmonitored.

4 **Batch Job Security Oversight** HIGH

Nightly batch jobs handle interest calculations and regulatory reporting, but most bands don't monitor job submissions or outputs.

5 **JCL Modification Blind Spots** MEDIUM

Job Control Language modifications can redirect data outputs or bypass security controls, yet changes often go undetected.

6 **TSO/ISPF Session Monitoring Gaps** HIGH

Direct mainframe access sessions provide insider threat vectors, but session activities often go unlogged or unmonitored.

7 **Cross-Platform Correlation Failure** CRITICAL

Even banks with mainframe logging typically can't correlate events with network intrusions, creating incomplete threat pictures.

The Solution: VitalSigns SIEM Agent for z/OS - VSA

Eliminate these blind spots with real-time mainframe security monitoring, automated compliance reporting, and comprehensive threat detection.

Learn More About VSA

Software Diversified Services - www.sdsusa.com