Syteca

Case Study

Strengthening Privileged Access Security for a Leading Bank in the GCC

Customer profile

A leading bank in the GCC operating mission-critical Oracle databases on Oracle Linux to support core banking systems. Multiple DBAs and system administrators access the database servers daily to manage performance, security, and availability of financial data.

Challenges

As a highly regulated financial institution, the bank required strict control and visibility over privileged access to its Oracle database servers.

Native database auditing did not provide full visibility into OS-level terminal activity performed via SSH. Administrators could log in to the Oracle Linux servers and execute powerful CLI commands that could:

- Modify or delete sensitive financial records
- Change database configurations
- Impact core banking availability
- Create compliance and operational risks

Additionally, multiple administrators often accessed the servers simultaneously. The bank needed:

- Complete recording of all terminal sessions
- Command-level visibility
- Login and logout tracking
- Real-time alerts for critical commands
- Monitoring of multiple concurrent sessions
- Focused oversight of privileged users only

The solution: Syteca terminal session monitoring

Syteca deployed its **Terminal Agent** on the Oracle Linux servers hosting the bank's Oracle databases, enabling full privileged session monitoring.

Complete session recording & audit trail

Syteca provided end-to-end visibility into administrator activity, including:

- Full terminal session recording
- Detailed command history tracking
- User login and logout time monitoring
- Session duration tracking
- Execution timestamps for every command
- Searchable audit logs for fast investigations

Every SSH session became fully traceable and securely stored, ensuring accountability for all privileged activities.

Real-time detection of critical commands

Custom alert policies were configured to detect high-risk commands such as:

- DROP
- DELETE
- ALTER
- Other predefined administrative commands

When executed, Syteca immediately captures the activity and generates alerts, enabling proactive risk mitigation before significant damage can occur.

Focused monitoring with user filtering

To reduce noise and improve investigative accuracy, monitoring policies were configured to:

- Target administrator-level accounts
- Exclude read-only users

This ensured security teams focused only on high-risk privileged activity.

Monitoring multiple concurrent sessions

With Syteca's **terminal-based licensing model**, a single terminal agent can monitor multiple simultaneous SSH sessions.

For this bank:

- More than five concurrent administrator sessions were monitored from a single agent
- No additional deployment complexity
- Optimized licensing and operational efficiency

Results & business impact

- ✓ 100% visibility of vendor activities
- ✓ Complete session recording with command history
- ✓ Accurate login/logout tracking for compliance audits
- ✓ Real-time detection of destructive commands
- ✓ Monitoring of 5+ concurrent administrator sessions
- ✓ Reduced insider threat and operational risk
- ✓ Improved regulatory readiness and audit confidence

Conclusion

By implementing Syteca's Terminal Session Monitoring, the bank achieved full control and accountability over privileged database server access. With complete session recording, command-level visibility, concurrent session monitoring, and intelligent alerting, Syteca delivered a scalable and compliance-ready solution for securing critical financial infrastructure.