Syteca

Case Study

A European Bank Mitigates Third-Party Admin Risks with Syteca

The challenge

A European bank needed third-party service providers to administer some of their databases. As a large organization operating in the global market, the bank wanted to protect sensitive financial data, end customers' personal information, and other critical IT assets from unauthorized access.

The bank's security department decided to implement an advanced security system for administrator access control. Additionally, they needed all user sessions of third-party providers to be monitored for security compliance and logged to enable post-audit activities.

Bank representatives considered several possible solutions and decided to go with Syteca. To reduce the attack surface, Syteca's team suggested solving the customer's problem by installing a bastion host running the Syteca client application.

The customer

Industry: Banking

Location: Europe

Market: Global

Must comply with:
PCI DSS, SWIFT CSP, GDPR

Pending issues: Secure third-party admin access to databases and monitor admin activity with sensitive data.

Customer's requests

- Limit access of third-party administrators to the bank's IT infrastructure
- Monitor administrators' actions with sensitive assets
- Mitigate data security risks by responding to suspicious activity
- Conduct audits to analyze third-party activity

Customer's need	Achieved results	Our offering
Limit and secure third-party access to sensitive data	Reduced attack surface due to strict access limitation	Continuous monitoring of employee and third-party' activity
Monitor activity of third-party admins	Complete live view of third parties' actions in the bank's infrastructure	Monitoring of third-party user activity
	Differentiating activity of third-party admins using shared accounts	Secondary user authentication
Mitigate data security risks	Real-time notifications on specified events	Customizable rule-based alerts
	Automated blocking of suspicious users, processes, and applications	Robust incident response capabilities
Conduct audits and investigations	Detailed, immutable evidence for internal security audits and forensic investigations	Recording of user sessions
		Rich reporting capabilities
		Exporting monitored user sessions in a protected format

Additionally, Syteca's rich user activity monitoring and privileged access management capabilities helped the customer meet the requirements of industry-specific IT security standards.

The result

Deploying Syteca enabled our customer to:

- Reduce the attack surface due to strict access limitations
- Differentiate activity of third-party administrators using shared accounts
- Get a complete live view of what third parties do in the bank's IT infrastructure
- Receive real-time notifications about cybersecurity events and specified admin actions
- Automatically block the activity of suspicious users, processes, and applications
- Get detailed, immutable evidence for internal security audits and forensic investigations

With Syteca's support team being available 24/7, deployment of and further work with the platform went smoothly and without any complications.

How we did it

By deploying Syteca, the customer managed to significantly reduce the risks posed by third-party administrators' access to the bank's systems. With Syteca, our customer now has all the means to:

Limit access of third-party administrators to the bank's IT infrastructure

Our team helped the customer deploy a bastion host with Syteca's client application. By installing all the tools needed for database administration on the bastion host, the customer secured and limited access to the bank's internal infrastructure to a single point, significantly minimizing the potential attack surface. The bank's security officers can now monitor and control administrators connecting to the bastion server via RDP.

Monitor administrators' actions with sensitive assets

The customer monitors the activity of third-party administrators and watches all their real-time actions in a convenient YouTube-like player. Security officers can also track various metadata such as opened applications, executed commands, and typed keystrokes. With Syteca's secondary authentication functionality, the customer has gained full visibility into administrators' shared accounts and can distinguish the activity of each third-party user.

Mitigate data security risks by responding to suspicious activity

With the help of customizable rule-based alerts, our customer receives real-time notifications about specified actions of third-party administrators and cybersecurity events on the server. After receiving a notification, the bank's security officers can check a third-party user session in real time and immediately disrupt their activity if they find it suspicious or dangerous. Alternatively, the customer's security officers can configure Syteca to automatically terminate a user's session or initiated process.

Conduct audits to analyze third-party activity

The bank collects cybersecurity evidence by recording all admins' user sessions in an indexed video format. Having an abundant collection of Syteca's customizable reporting capabilities, the customer conducts regular internal security audits. Additionally, the bank's security team can export user sessions to cybersecurity investigators. The file containing an exported session is immutable, ensuring the integrity of the investigation data.

After over 10 years of close cooperation, our customer is still happy with the quality of third-party access management and monitoring as well as the level of support provided by Syteca.