fernao | Use Case

Optimized IT security and audit control

Splunk as the key to IT resilience for a global bank

Our client, an international bank with around 2,500 employees, was faced with the task of taking its IT security strategy to a new level. Although Splunk was already being used successfully in IT operations, the increasing threat situation and strict regulatory requirements made an expansion necessary. The goal was to implement Splunk as a comprehensive SIEM system to better detect and analyze security incidents. In addition, a solution for the audit-proof traceability of changes in the IT environment had to be created to comply with audit requirements.

Our solution

As part of the project, Splunk Enterprise Security (ES) was implemented as a SIEM solution, supplemented by the integration of a version control system using GitLab. The bank benefited from a holistic approach:

- **Proof of Concept:** First, a customized proof of concept for Splunk Enterprise Security was developed and validated to meet the bank's specific requirements.
- **Data source connection:** Relevant data sources from the IT infrastructure were connected to obtain a complete picture of the system landscape.
- **Asset and identity management:** Assets and identities were integrated into the Splunk environment for more accurate threat analysis.
- **Installation and configuration:** Splunk Enterprise Security was installed and configured to best suit the bank's needs.
- **Version control:** The introduction of GitLab created seamless tracking and revision security for changes in the IT environment.
- **Training and workshops:** Employees were trained in the use of Splunk ES to exploit the full potential of the solution.

Results

With the introduction of Splunk, our customer was not only able to ensure compliance with regulatory requirements such as PCI DSS, but also significantly improve service quality and security.

- **Improved transaction monitoring:** Splunk enables real-time monitoring of transactions, allowing potential anomalies to be detected and resolved early.
- **Higher service quality:** Application monitoring ensures fewer outages and faster troubleshooting, increasing customer satisfaction.
- **More efficient security processes:** Thanks to the centralized SIEM solution, threats can be identified more swiftly and response times have been significantly reduced.
- **Scalable infrastructure:** The Splunk architecture is flexible and ready to grow with the future needs of the business.
- **Targeted reporting:** Decision makers receive detailed reports and dashboards that facilitate operational and strategic decisions.

A robust, powerful and future-proof solution has been implemented that has significantly increased not only the security but also the efficiency of the company.

Quick Facts

- International bank
- > 2,500 employees

Solutions

SIEM
Splunk

fernao group GmbH
info@fernao.com

Headquarter
Albin-Köbis-Str. 5
51147 Köln
www.fernao.com