fernao | Use Case

Compliance under control

Monitoring highly privileged users (HPU) in financial institutions with Splunk

Our customer, a nationwide financial institution with around 8,500 employees, was faced with the task of implementing new regulatory requirements. These included the monitoring of highly privileged users (HPU) across the entire IT infrastructure. The existing Splunk SIEM solution had to be expanded to include specific functions in order to meet the strict compliance guidelines.
The translation of the regulatory requirements into technically feasible use cases, the collection of HPU-relevant data and the development of a system for risk-based alerting were particularly challenging. In addition, the integration of the monitoring functions for over 100 applications and the coordination of several IT service providers and application manufacturers posed a major challenge.

Our solution

As a trusted advisor, fernao magellan supported the financial institution in the design and implementation of a customized solution:

- **Regulatory advice:** Formulation of technical requirements based on HPU monitoring guidelines.
- **Data analysis:** Elicitation of HPU rights at operating system, database and middleware level.
- **Use case development:** Derivation of over 200 specific security use cases from the collected data.
- **Implementation:** Implementation of the use cases in Splunk with risk-based alerting and visual preparation using dashboards.
- **Test framework:** Establishment of a framework for continuous testing of the use cases.
- **Project coordination:** Steering of stakeholder meetings and continuous consulting during the entire project duration.

Results

With the extended Splunk SIEM solution, the financial institution was able to fully meet the regulatory requirements for monitoring highly privileged users.

- **Compliance security:** Proven and audited compliance with industry-specific requirements, averting the threat of penalties.
- **Increased efficiency:** Reduction of compliance efforts through automated monitoring processes.
- **Increased security:** Effective protection against internal threats through targeted monitoring and alerting.
- **Scalable solution:** A future-proof system with over 200 implemented use cases that can be flexibly expanded.

Thanks to the expertise and comprehensive support of fernao magellan, a reliable and efficient monitoring solution has been developed that meets current and future requirements.

Quick Facts

- financial sector
- 8,500 employees

Solutions

SIEM
Splunk

fernao group GmbH
info@fernao.com

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