fernao | Use Case

Big data meets cyber defense

How an automotive supplier established Splunk as the basis for Big Data Services and uses it as a central service platform.

Our customer, a leading global automotive supplier with over 400,000 employees, was faced with the task of establishing a central platform for big data services within the group. The goal was to use Splunk Enterprise as the basis for IT operations, IT security, digitalization and business analytics. At the same time, services from the group's own IoT cloud were to be provided to end customers. The platform not only had to meet the company's high security requirements but also offer a globally scalable architecture. An additional challenge was the integration of this solution into the Cyber Defense Center (CDC), which serves as a global security authority.

Our solution

To overcome the challenges, a complex, multi-layered Splunk architecture was set up. Splunk was established as a central service that supports all divisions within the group. Both IT operations and IT security applications were integrated, including performance monitoring, SAP monitoring and the basis for a global SOC.

- **Global log management infrastructure:** Developing a centralized approach to securely collect and manage log data in a multi-tier and multi-cluster environment.
- **Cyber Defense Center:** Planning and implementation of a Splunk Enterprise Security environment as a foundation for cyber defense.
- **IoT Integration:** Development of Splunk-based IoT services for end customers.
- **Automation:** Implementation of an internal marketplace for the automated rollout of Splunk instances using Docker technology.
- **Training:** Development and delivery of internal training to ensure optimal use of Splunk.

Results

The implementation of the Splunk platform provided our client with a consolidated and scalable solution for big data, IT operations and cyber defense. The key benefits include:

- **Transparency and efficiency:** Worldwide monitoring of security-relevant systems and IT processes.
- **Increased security:** Optimized security monitoring through the integration of Splunk Enterprise Security into the Cyber Defense Center.
- **Future-proofing:** Flexibility and scalability to support the global digitalization and IoT strategy.

With the new infrastructure, our customer was able to increase operational security, improve service quality and create a central basis for innovative IT and security projects.

Quick Facts

- automotive supplier
- 400,000 employees

Solutions

Splunk

fernao group GmbH
info@fernao.com

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