CONSIST PROJECT REFERENCE

Security for bank operations – a case for Splunk

The story in brief

From simple payment flows to foreign trade financing to risk hedging on the currency or interest sides, companies expect their bank to offer a model of these services that is fast and available at all times.

The background of any bank's business is therefore a complex landscape of IT systems and processes, for example aggregating, processing, and reporting figures for risk management and controlling, or using special algorithms for trading. The result is a data hype for which integrity, availability and security must be guaranteed at all times, day and night – Big Data for Big Business.

These massive data streams run the risk of being misdirected, tapped, or incorrectly handled at many different points. Banks are therefore faced with the task of overseeing each and every system access using specific monitoring.

Within the financial sector, Consist has just completed a customer project involving the installation of the central security information and event management system (SIEM) required – a system that cannot be manipulated and that can operate in real time. All user processes, even for privileged users, are thus securely versioned and integrated into everyday banking processes based on the latest security requirements from the ECB and BaFin.

The smooth handling of the project by certified Consist specialists impressed everyone involved. All steps along the way, from consulting to implementation, to the transition to Managed Services by Consist, were implemented on time and within budget.

The task

- Monitoring of privileged users/ admins
- Replacement of heterogeneous security systems using central security information management

The challenge

- Special feature: more than 40 heterogeneous systems with very high protection requirements were involved, including SAP, and all had to be integrated and monitored
- Establishment of a central current standard system, that can be extended with new applications at any time
- Implementation of a non-manipulable, real-time notification system

The solution with Consist

- Proof of Concept
- Project team with internal specialists (project leader and application support) and external specialists from Consist (certified Splunk and security consultants)
- Consulting and support in the areas of architecture, system design, and operation
- Setup and commissioning of a standard system, including embedding into development, test, and production migration processes typical for the customer (for example using staging)

Functionality of the SIEM

- Efficient standard connection with flexible customizing based on the Splunk Enterprise Platform and Splunk Enterprise Security
- Integration of specialized banking applications, both purchased and custom-designed (including SAP)
- Alert and documentation function

Particular strengths of Consist

- Extensive Big Data and mainframe expertise
- Certified Splunk specialists
- Methodology of agile software development
- Completion of project on time and within budget
- Smooth transition to application management using Managed Services

Customer advantages

- Risk minimization by subjecting high-privilege users to monitoring as well and through
- Detecting inside threats
- Version-safe, non-manipulable security system that acts in real time
- Compliance with BSI, ECB, and BaFin security requirements

CONSIST
Business Information Technology

We do IT for you.

Your contact:
Joscha Sternadel
sternadel@consist.de
+49 431 3993-775
Consist Software Solutions GmbH
Christianspries 4, 24159 Kiel, Germany
www.consist.de