identify and eleminate real security incidents

Managed SIEM with IBM QRadar for the Oldenburgische Landesbank

ConSecur
[security and consulting]

Differentiate precisely incidents from permitted access

The Oldenburgische Landesbank (OLB) layed the managment of its information security in the hands of ConSecur GmbH.
ConSecur analysts precisely distinguish security incidents from legitimate events from 10,000 events per second. Identified security incidents trigger a defined chain of actions in the bank´ s IT department via the ticket system, so that escalation can take place quickly and in a structures manner. The prioritization of incidents allows the bank to respondto security incidents in realt time, reducing the impact of threats within its critical infrastructure.

Frank Feldmann, IT security and data protection officer at the OLB: "We have created a structure with which we can clearly identify and eleminate real security incidents. The processes in Managed SIEM (Security Informaiton and Event Management) are coordinated so efficiently that our IT department and ConSecur work hard hand in hand.

analysts differentiate between security incidents andunauthorized access from 10,000 events per second

Initial situation

The bank, which has been created in 2018 through the merger of OLB and the Bremer Kreditbank, worked with a management tool that logged and saved all incidents of the devices, endpoints and applications connected to the network.

All of the data has been made available to Frank Feldmann, IT security and data protection officer at the OLB and his team in a simple PDF report covering several thousand pages.

This legacy system was not designed for the correlation of the collected data and the precise detection and prioritization of security incidents.

With the merger, building a SIEM that detects and prioritizes security incidents became more urgent. OLB was looking for an external partne, who is able to design a new SIEM solution from scratch within a short period of time, who has the manpower for permanent operation and work closely with the in-house IT department. " If we want to successfully implement a SIEM, we need the human ressources to do so.

With these requirements, the OLB sought the conversation with the ConSecur GmbH.

„We have created a structure with which we can clearly identify and elminate realt security incidents."

„For us it quickly became clear to us that ConSecur was a component partner for the construction and having a SIEM running."

FRANK FELDMANN, IT security and data protection officer at the OLB AG.

Proof of Concept (PoC) – SIEM-piloting within 15 days

The requirements for the new SIEM to be designed were the rapid provision of an operational SIEM, the scabality of the solution, which grew with the bank and operational management by specialized teams.

After analyzing these requirements, ConSecur submitted the proposal to OLB to set up a SIEM with security monitoring as a pilot project and to demonstrate the performance of the SIEM live during operation. IBM QRadar Security Information and Event Management (SIEM) helps security teams accurately identify and prioritize security threats. The market-leading tool reliably detects IT security incidents and thus minimizes the risk of security threats to the corporate network.

„With the SIEM pilot, we were able to simulate in an environment adapted to the OLB how the SIEM will be structured and how security monitoring will work with our analysts in practice, " according to Jens Wübker, sales manager at ConSecur GmbH.

Within 15 days, ConSecur presented an operational managed SIEM solution that was adapted to the OLB and that

- the architecture of the SIEM solution (products, licences, processes, roles),
- individual use cases to be monitored (risk scenarios),
- the recommended SIEM tool QRadar and IBM as well as
- a working team of professional security analysts and incident management

contains.

The proof of concept convinced Frank Feldmann and his team to commission ConSecur GmbH to set up a SIEM. "It quickly became clear to us that with ConSecur we had a competent partner for setting up and running a SIEM."

„We were enthusiastic about the focused cooperation with OLB. The rapid commission of the SIEM succeeded because everyone pulled together with the common goal in mind."

STEPHAN ILIC, CDC MANAGER OF CONSECUR GMBH

> *„IBM QRadar is a very rapidly deployable solution and our number one choice to keep security incidents reliable and thus the to recognize the risk of security threats for corporate networks.“*

**JENS WÜBKER,
SALES MANAGER OF
CONSECUR GMBH**

SIEM-implementation within a week – reduction in licence costs

The implementation of the SIEM should take place in shortest possible time. Within a week, ConSecur set up the SIEM readyf for operation, connecting 800 log sources such as firewall, servers, switches and bank specific applications and integrating them into the monitoring.

Due to these newly connected log sources, however, the number of incidents (events) per second increased unexpectedly, so that ConSecur advised an adjustment of the licensing. OLB has already been using IBM QRadar with licensing based on events per second and followed ConSecur´ s recommendation to switch to licensing based on virtual servers. This has been achieved by using IBM Cloud Pak for Security.

IBM Cloud Pak for Security also enables any expansion from a SIEM solutionto a comprehensive SOC solutions while reusing existing security tools and simplifying holistic security analyses.

ConSecur security analysts identify and prioritize security threats 24/7 and generate tickets in the ticket system if security incidents occur. These tickets are forwarded with a corresponding priorization of the employees of the OLB IT department, who initiate countermeasures.

Conclusion – leading, goal- oriented implementation

The Oldenburgische Landesbank has a scalable SIEM solution checking security events within the critical infrastructure promptly and appropriately.

After the piloting and the rapid provision of the SIEM, the analysts at ConSecur GmbH took over the day-to-day operations with Managed SIEM.

„I really liked how ConSecur implemented the project management in a responsible and goal-oriented manner“, according to Frank Feldmann.

ConSecur

[security and consulting]

ConSecur GmbH
Nödiker Straße 118
49716 Meppen

TEL.: +49 5931 9224-0
info@ConSecur.de
www.ConSecur.de