Industry: Finance and Banking

Use Case: Bank in Germany

The bank has 120 employees, total assets of 25 billion euros, and 80 branches across Germany and Central Europe.

As a medium-sized institution in the German banking sector, it faces specific challenges in terms of IT security and **compliance**. It must comply with BaFin's regulations, the BSI and KRITIS regulations, and the **DORA directive**'s requirements.

The complex IT infrastructure, the company's digitalization projects, and the networking of locations increase the attack surface for cyber threats, with financial institutions being particularly attractive targets for cybercriminals anyway due to the sensitive financial data they hold.

Spring 2023 should not be repeated

Digitalization opens new opportunities for banks and insurance companies but also makes them more vulnerable to cyber threats that endanger data security and the availability of services. With DORA, the EU has introduced a regulation that obliges financial service providers to strengthen their IT security measures and build operational resilience against attacks.

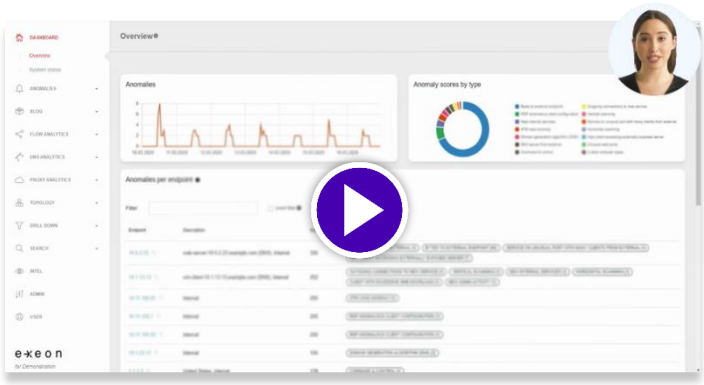
A major challenge for financial service providers is reconciling data protection, smooth operations, and compliance with regulatory requirements. In particular, implementing DORA requirements requires banks to coordinate workflows between operational IT processes and cyber security measures.

In spring 2023, the bank was the target of a complex cyberattack. The attack began with a phishing campaign aimed at stealing access data from employees. An attacker gained access to the internal network and began exfiltrating sensitive data and spreading malware. As a result, the company wanted to strengthen its existing security systems (firewall, EDR, etc.) and therefore took a closer look at network monitoring and network security.

From the outset, it was important to the bank that a European solution was introduced and that the GDPR requirements were taken into account through the possibility of hosting the security product on-premises and air-gapped, as opposed to cloud-only products, in order to ensure the protection of personal data (data privacy).

Monitor ATM machines worldwide

Watch the demo video



exeon
Smart Cyber Security.

Challenges from DORA and hacker threats

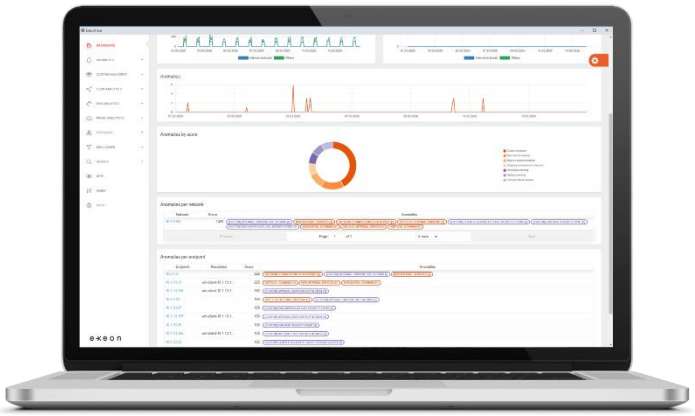
DORA requires financial service providers to identify and minimize IT risks, implement effective incident management to respond quickly to cyberattacks, and implement technical and organizational cybersecurity measures. In addition, continuous reporting of security incidents and their consequences to the supervisory authorities must be possible at all times.
Non-compliance with DORA can lead to considerable financial and reputational damage for financial service providers.

Financial institutions process highly sensitive and regulated data. They must, therefore, ensure that they comply with data protection requirements and are constantly targeted by hackers from all over the world. Attacks that disrupt business operations, damage data, or expose confidential information, e.g., cyberattacks such as **ransomware**, insider threats, **Advanced Persistent Threats (APTs)**, and **DDoS attacks**, must therefore be monitored and prevented.

Easy as Pie: Implementation of NDR in the existing IT infrastructure

1. POC: Concrete security threats and scenarios

ExeonTrace was the most successful solution in the bank's "beauty contest" for the detection of tested use cases (Red Teaming/Proof of Concept). These included Lateral Movement, Domain Generation Algorithms, Hidden DNS Channels, and Command and Control Channels.



It was particularly important for the customer that multiple locations were supported by a 360° view of their network. The bank's **SOC team** loved the intuitive navigation of ExeonTrace through current and historical log data for complete transparency in a single dashboard.

2. Easy Implementation

The bank uses a heterogeneous IT infrastructure with different locations and cloud services, which increases the complexity of the network. The integration of ExeonTrace into the bank's IT landscape began with a detailed analysis of the current infrastructure and a review of the network architecture in order to meet the bank's specific requirements and integrate it into existing security solutions such as firewalls and **SIEM**: ExeonTrace is to monitor all network segments at the company, i.e., internal and external networks and also interfaces to third-party providers and cloud applications.
Once implemented, ExeonTrace collects and analyzes network metadata that is exported from the entire IT, cloud and OT infrastructure.

This includes information such as IP addresses, ports, protocols, data transfer rates, and connection times. ExeonTrace uses graph databases to reduce storage requirements by storing data in the form of nodes and edges. This structure enables efficient storage and retrieval of highly networked data, as relationships are mapped directly and without additional indexes. Since ExeonTrace does not mirror complete network packets, but only analyzes metadata, the amount of processed data is additionally reduced. The metadata obtained is compared with highly developed trained and untrained AI algorithms for potential threats. The integration into the existing systems worked seamlessly and is easily scalable as ExeonTrace can work without hardware appliances, can be integrated into the bank's existing security and IT management systems and, for example, firewall logs can be integrated into Exeon's communication monitoring.

Meeting the challenges of DORA and cybercrime: ExeonTrace at work!

ExeonTrace offers complete transparency in the bank's highly virtualized IT infrastructure. With the help of AI and behavioral analysis, known and new attacks can be better detected and responded to more quickly. ExeonTrace analyzes communication patterns and alerts in the event of anomalies. Examples of threats that are identified and managed with NDR are APTs (long-term cyberattacks that aim to remain undetected), insider threats, ransomware, DDoS attacks, **zero-day exploits** (the system recognizes early signs of ransomware attacks, e.g., unusual data movements or ransomware activity in the network). The ability to identify unknown attacks, immediate response mechanisms, and improved reporting also support DORA requirements. Compared to firewalls and EDRs, NDR offers a network-centric approach that also detects threats that are not directly visible on the end devices and protects areas where no sensors or agents can be installed, for example for monitoring industry-specific assets such as ATMs and other OT.

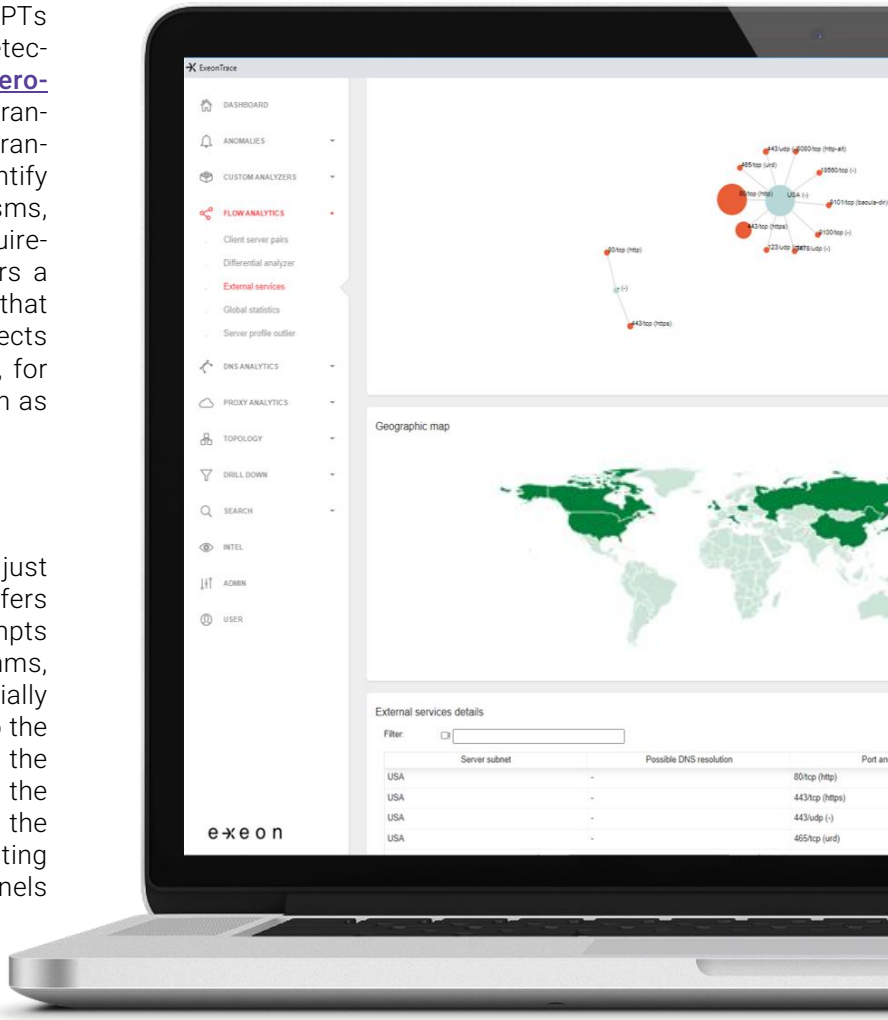
The concrete impact of NDR

ExeonTrace detected unusual network activity after just a short learning phase, such as increased data transfers to unknown IP addresses and unusual login attempts outside of normal working hours. Using AI algorithms, ExeonTrace identifies these activities as potentially malicious and generates alerts that are forwarded to the bank's security team. It is now possible to isolate the affected systems and block infected devices from the network and suspicious IP addresses to prevent the spread of malware through lateral movement, disrupting communication from Command-and-Control Channels (C&C Channels).

Other irregular activities have been whitelisted in advance with the SOC team and will no longer trigger alerts as a result. By detecting and responding quickly, the bank can minimize potential damage, while the intelligent algorithms and whitelisting reduce the number of false alerts and, thus, the workload of the bank's security team.

For the SOC team, “monitoring network traffic for unusual activity to detect and report cyberattacks early”, as required by DORA guidelines, has now been highly automated from time-consuming and error-prone manual monitoring. The security team uses ExeonTrace's comprehensive incident management capabilities to analyze and document incidents, with all steps logged to ensure complete traceability The detailed logging and reporting of communications on the network enables the bank to meet the regulatory reporting requirements of DORA.

As ExeonTrace does not use packet mirroring and does not process data in a public cloud, all sensitive information remains within the bank's secure environment. The processed user data is anonymized by hashing the personal information, which increases the protection of customer privacy and supports compliance with GDPR guidelines.



The ability to run ExeonTrace in a fully isolated (air-gapped) environment provides additional protection from external threats and ensures that no data leaves the bank's secure network.

The decisive result

The success of the ExeonTrace implementation was measured after 6 months using various KPIs, including the number of threats detected, response time, reduction of false positives through the use of advanced algorithms, DORA readiness, fulfillment of other cyber-security and compliance regulations for the financial industry, and satisfaction and reduced workloads of the bank's IT and security teams with ExeonTrace.

Allianz für Cyber-Sicherheit

CYBERSECURITY™ MADE IN EUROPE

ATTESTA ISO 27001 CERTIFIED

Exeon Analytics AG
contact@exeon.com
exeon.com

Grubenstrasse 12
8045 Zürich
Switzerland

LinkedIn
YouTube