Industry: Finance & Banking

Action Plan: Tackling Advanced Threats

As financial institutions continue to digitize their operations, they need to strengthen their IT security to combat the growing number of cyber-attacks that pose significant financial and operational risks, especially given their systemic importance to society.

Organizations face cyber threats from nation-state actors and specialized criminal groups, such as LockBit, QakBot, Grandoreiro, and Emotet, which use sophisticated techniques, such as ransomware and advanced persistent threats (APT) campaigns.

According to the IBM/Ponemon Institute, the average total cost of data breaches in 2023 was $4.45 million, while the finance industry averaged $5.90 million.

In 2023, companies in Germany lost a total of 205.9 billion EUR to cybercrime (Statista).

Can your company afford to risk similar losses?

Do You Encounter Common Security Challenges as Many Financial Organizations Do?

- Growing attack surfaces due to new technologies.
- Increasing complexity of cyber security within multi-cloud environments.
- Protecting the most sensitive data stored via air-gapped networks.
- Resource intensive and mandatory requirements due to compliance like DORA.
- Being & staying ready to protect digital assets and wallets from breaches.
- Handling growing security challenges and benefiting from chances posed by AI.

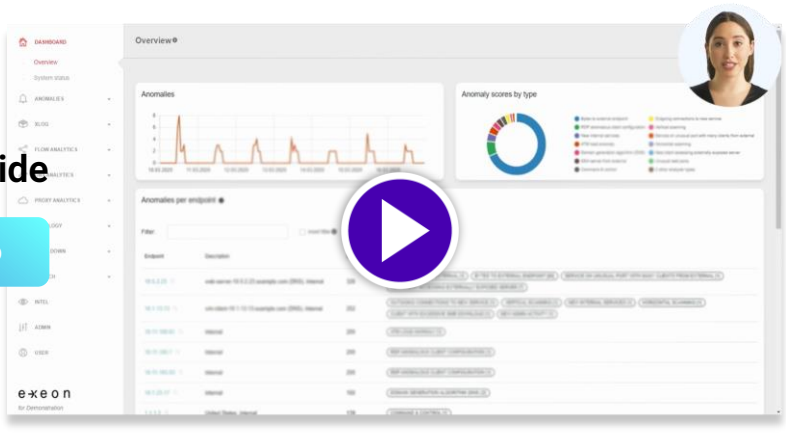
4-6 Mio. EUR Average Data Breach Cost, 2023

Top 7 Serious Threats to Watch Out For:

1. **Ransomware:** Encrypts data and extorts ransom, severely disrupting operations and compliance, with significant financial and reputational impact.
2. **Social engineering attacks:** Phishing tricks employees into revealing confidential information, leading to compromised accounts and data theft.
3. **Exploits and zero-day attacks:** Exploit unknown software vulnerabilities to bypass security measures via supply-chain, causing severe breaches and financial losses.
4. **Banking trojans:** Steal confidential information from online banking systems, using techniques like form-grabbing and code injection.
5. **DDoS attacks:** Overloading network resources disrupts financial services, causing significant downtime and financial losses.
6. **Advanced Persistent Threats:** State-sponsored entities conduct prolonged espionage, targeting high-value financial organizations for sensitive data.
7. **OT:** Attackers manipulate, e.g., ATMs by using malware to infect and manipulate the network.

Monitoring ATM Machines Worldwide

Watch the Demo Video



exeon
Smart Cyber Security.

Rapid detection, damage limitation, and root cause analysis are crucial in mitigating unavoidable cyber-attacks. Trends emphasize detection, response, and compliance with regulations like DORA. Key steps include continuous monitoring, robust response plans, and mandatory reporting to strengthen IT security and operational resilience.

Rapid Detection

- **Strengthen Incident Response:** Regularly update incident response plans with detailed threat data and risk-scores to ensure rapid containment and remediation.
- **Security Solutions Adoption:** Implement EDR, NDR, and SIEM solutions to monitor and secure IT/OT infrastructure.

Damage Limitation

- **Third-Party Risk Management:** Identify and mitigate security vulnerabilities in third-party services to prevent supply chain attacks.
- **Zero Trust:** Implement strict access- and traffic-controls rejecting inherent network trust to protect data and minimize insider threats.

Root Cause Analysis

- **Security Audits and Penetration Tests:** Regularly conduct security audits and penetration tests to identify and eliminate network vulnerabilities.

Your 6 Steps to Cyber Resilience

1. **Define clear security classifications.** First things first: introduce clear security classifications for all IT assets based on sensitivity, access rights and business relevance. This is essential to understand the risk potential of possible anomalies and help prioritize.

2. **Determine if you can continuously monitor data flow within your network to detect even unknown anomalies promptly.** Threat actors always leave communication traces in your network. You don't necessarily need hardware to detect threats early and develop incident response plans for swift, effective action. If you struggle to detect anomalies, consider exploring AI-enabled threat detection tools to identify abnormal network communication.

3. **Identify if you have blind spots and possibly offer threat actors a hideout.** Automate your asset discovery and implement tools to continuously inventory all IT assets, including those in cloud and hybrid environments, to ensure comprehensive visibility and management of your infrastructure.

4. **Understand your compliance requirements and ability to ensure consistent reporting.** Only continuous and full monitoring ensures compliance with regulations like DORA. If you are not compliant, consider threat detection and response solutions that help you correct compliance deviations in real time to document events, record countermeasures and enable reporting for all IT assets.

5. **Evaluate your security team's workload** realistically to understand if they can spot the most relevant threats promptly. Too much noise – if this is the answer, then start considering the integration of AI to enhance threat detection and response by utilizing predictive analytics and automated intelligence. This will help your team focus.

6. **If you are using SIEM, then start enhancing detection further.** Improve SIEM detection capabilities by mitigating false positives and inadequate detection through real-time monitoring and analysis of network traffic.

Act now – get your detailed version of the action plan.

Get your copy

Use Case

PostFinance, one of the leading financial institutions for private customers in Switzerland, already followed these essential steps and improved cyber resilience significantly:

- Systemically important financial institution in Switzerland
- Fulfills all of the special regulations regarding data security and confidentiality
- Highly integrates Network Detection and Response as multi-layered protection of sensitive and business relevant systems
- ExeonTrace, with its open and future-proof architecture, allows this without hardware sensors and with full control over all data flows.

"PostFinance has chosen ExeonTrace because of its open and future-proof architecture.
Not needing any hardware sensors and being able to control data flows, we didn't have to make any significant changes to our existing infrastructure.
We are also convinced by the cooperation with the competent and technically outstanding Exeon team."

— **Head IT Security, PostFinance**

PostFinance

exeon
Smart Cyber Security.

Exeon Analytics AG
contact@exeon.com
exeon.com

Grubenstrasse 12
8045 Zurich
Switzerland

LinkedIn
YouTube