Industry: Manufacturing

Use Case: Mechanical Engineering Firm

A mechanical engineering company of approx. 10,000 employees and several production sites in Europe and Asia faces the challenge of meeting national and EU compliance requirements according to **NIS2** and the Machinery Regulation.

Additionally, it faces a changing cyber threat landscape and exposure, in particular, **the integration of Operational Technology (OT)** and Industrial Internet of Things (IIoT) significantly increases the industry's vulnerability to cyber threats.

Robust cyber security to reduce production downtime and ensure compliance

As part of the country's now critical infrastructure, the company is committed to further improving its cyber security and resilience to IT risks. The points of particular attention from NIS2 include identifying and minimizing IT and cyber security risks, implementing an efficient incident management system, and being able to concisely report security incidents to the relevant authorities. The company aims to implement suitable measures quickly and effectively in order to avoid damage caused by production downtime, data or knowledge leakage, reputational damage, and fines to national authorities, even in the event of an increasing threat situation.

The "EU Machinery Regulation", which will be binding from 2027, also aims to increase cybersecurity in mechanical engineering and requires machine manufacturers to ensure that all machine products "have a robust security architecture that is protected against cyberattacks". This applies, in particular, to networked machines and production systems that regularly communicate with external networks.

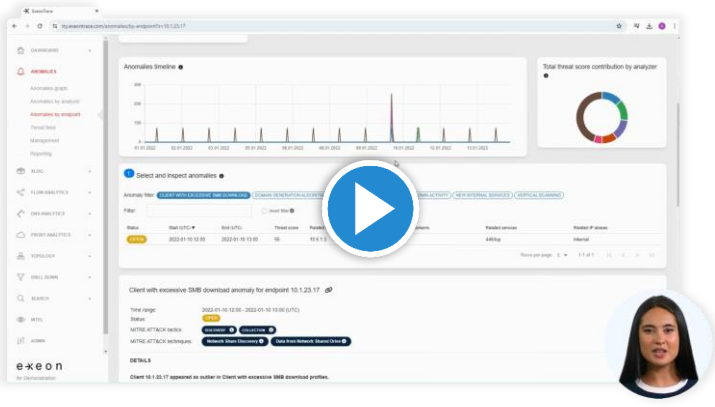
Machine manufacturers must also ensure that all new machines meet cybersecurity requirements right from the development phase and are designed to withstand unauthorized access.

Global business, global production, global risk

Due to the increasing networking of production sites and the digitalization of machines and processes, companies are already facing a significant increase in cyber risks. Attacks on industrial control systems (ICS) via IT, IIOT, and OT systems can disrupt production and jeopardize sensitive design, customer, or patent data. At the end of 2022, the company was already the target of a ransomware attack: after a long undetected entry via a phishing email, production data was encrypted, and the control of the production machines was paralyzed. The IT team was only able to react with a delay at this point due to a lack of visibility, isolate the affected systems, and stop the spread of the malware at a late stage.

Detecting advanced threats in OT

Watch the demo video



exeon
Smart Cyber Security.

It took almost five working days before the production data was restored and operations could be resumed. Operations came to a standstill, which led to delivery problems and a subsequent loss of sales.

The challenges: ICS, APTs, NIS2,...

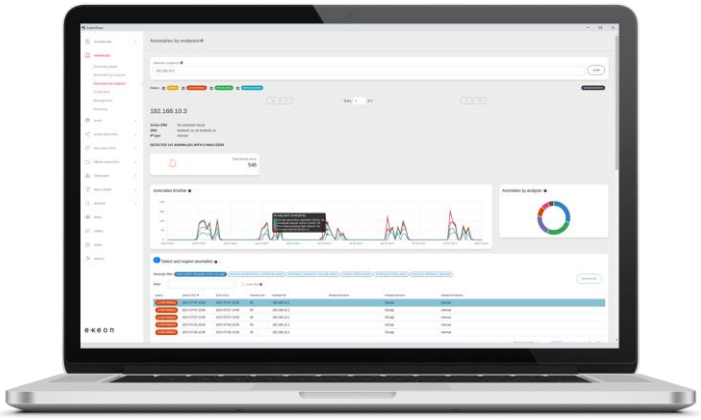
With the new ExeonTrace solution in the—internally operated—SOC, the manufacturer wants to meet the requirements of the NIS2 directive for continuous network monitoring, faster response to incidents, and better transparency and reporting "in the event of an incident" and be better prepared for future threats. In addition, the company's security team is relieved of routine tasks such as tracking false positives.

Protecting against supply chain threats and Zero-Day exploits

The security technology used is designed to combine preventive and reactive approaches to detect and stop cyberattacks without disrupting ongoing operations. Ransomware, Advanced Persistent Threats (APTs), and insider attacks are to be detected and contained at an early stage thanks to comprehensive network transparency. In addition, threats to the company from the hardware and software supply chain or zero-day exploits, i.e., previously unknown threats outside the perimeter, are to be warded off. The implementation should be carried out in such a way that the data protection regulations in accordance with the GDPR are complied with, which is why the company considered the on-premise version of the solution.

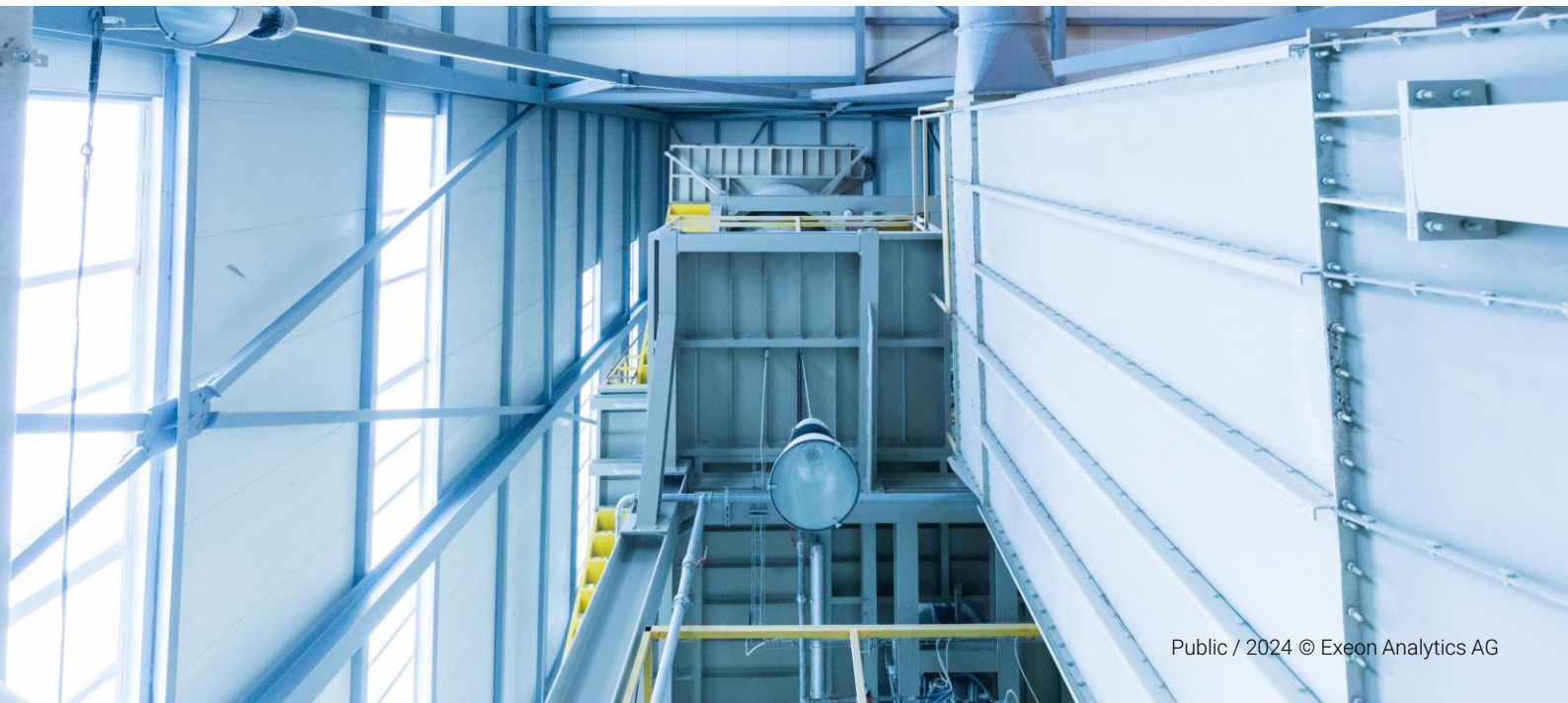
Implementation of ExeonTrace

The machine manufacturer's complex infrastructure, consisting of IT and OT systems, required a thorough analysis of the network architecture to ensure seamless



integration. In addition, the existing security stack was integrated with EDR, SIEM, and firewalls. ExeonTrace monitors all assets across all network segments, including internal IT networks, industrial control systems (ICS), production environments, and external connections to third-party providers, via communication protocols. This ensures complete coverage and consistent monitoring of all critical systems.

Since the rollout, ExeonTrace has continuously monitored all network segments, including internal, external, and production networks, in real-time using metadata such as IP addresses, ports, communication protocols, and transmission rates. The metadata is analyzed using AI-based algorithms to quickly detect unusual communication patterns and potential (even novel) threats to CC channels and reduce the false positive and false negative rate of events. ExeonTrace uses advanced behavioral analysis and machine learning to create a baseline of normal network traffic. Deviations, such as sudden data transfers to external IPs or unusual login attempts, are flagged as anomalies and reported immediately. If an incident is detected, measures can be initiated immediately, such as the isolation of affected systems, the dynamic adjustment of network rules, or the blocking of suspicious IP addresses.



The option of whitelisting and identifying particularly high-risk subnets using risk-based alerting in ExeonTrace enables even more targeted alerting and makes work in SOC even easier. All security-relevant information and network activities are visualized in a central dashboard. This enables the security team to monitor threats in real-time, see the entire network status at a glance, and take immediate action. Activities can be detected at an early stage, the security team can quickly isolate affected devices and protect production processes from potential attacks.
ExeonTrace is operated entirely on-premises at the company, which means that all data remains within the company's secure infrastructure. This meets the requirements of both the GDPR and the NIS2 directive and ensures maximum control over sensitive production and company data.

The impact of NDR

This comprehensive security solution protects the machine builder's production process without disrupting it and enables proactive defense against cyberattacks, increasing operational resilience and confidence in security measures. ExeonTrace detects unusual network activity such as unexpected data transfers to external IP addresses and suspicious login attempts on production systems at an early stage. The rapid response capabilities allow the security team to contain potentially serious incidents in time, isolate infected systems faster, stop the spread of malware, and restore encrypted data from backups so that production does not have to be interrupted. The incident response time required by NIS2, among others, can thus be drastically reduced. Improved traceability has significantly increased the efficiency of the security team, resulting in sustainably higher security and less downtime.

The use of improved AI algorithms has reduced the number of false alarms by 50%, further increasing the efficiency of the security team.

In addition, all potential security incidents can now be fully documented and submitted in reports to the relevant authorities, meeting the compliance requirements of the NIS2 directive within 12 hours. ExeonTrace also enabled full traceability of all malicious activity, providing 100% traceability of infection paths and threat origins.

ExeonTrace reduces the company's SIEM data volume by filtering out irrelevant information, correlating events, and aggregating and compressing similar incidents before they are forwarded. As a result, only security-relevant and optimized data is processed in the SIEM, which significantly reduces the overall load. Since ExeonTrace transfers data to the SIEM in an optimized format, the amount of data is further reduced.

Other manufacturers who trust ExeonTrace:

WIN GD

trafag sensors controls

Allianz für Cyber-Sicherheit

CYBERSECURITY MADE IN EUROPE

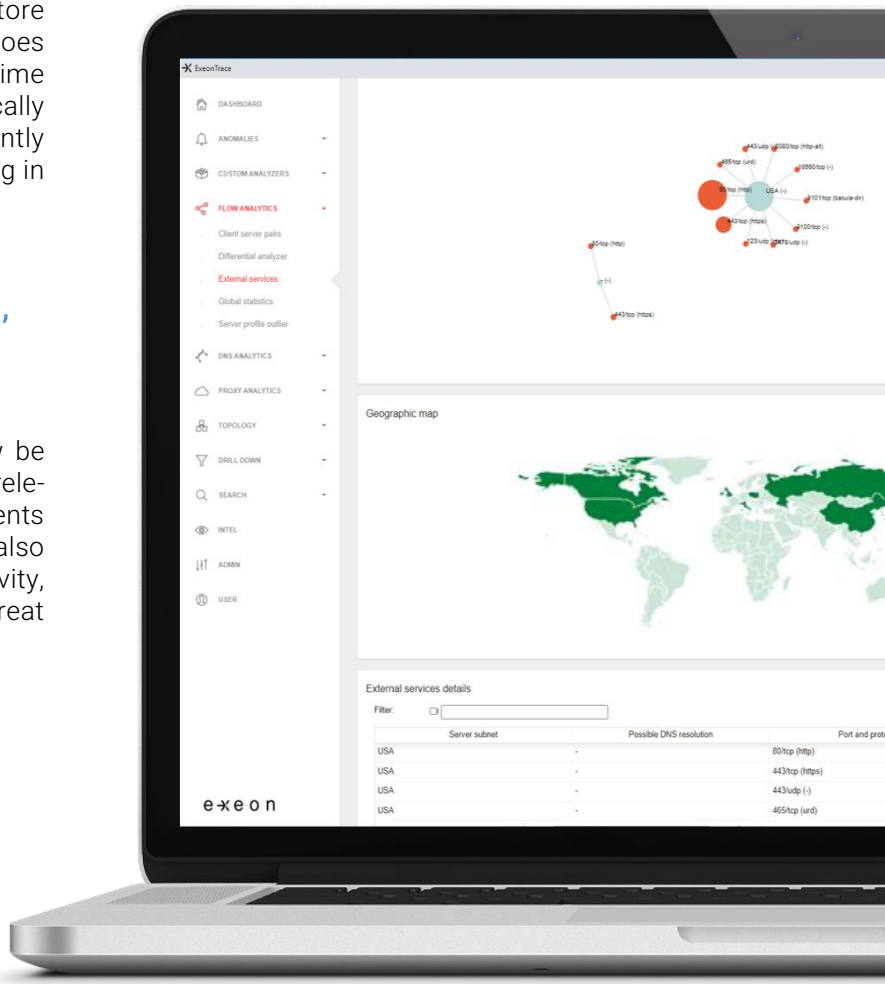
ATTESTA ISO 27001 CERTIFIED

Exeon Analytics AG
contact@exeon.com
exeon.com

Grubenstrasse 12
8045 Zürich
Switzerland

LinkedIn

YouTube



exeon
Smart Cyber Security.