

Short introduction to Exeon.NDR



Smart Network Detection & Response

The Exeon.NDR Network Detection & Response (NDR) platform is the smart way to **strengthen cybersecurity**.

Powerful Machine Learning (ML) and proven algorithms provide complete visibility across the entire network, automatically detect suspicious behavior and support the respective security team to efficiently assess and combat early-stage cyber threats.



Exeon.NDR offers **holistic visibility** into IT/IoT/OT network communications to identify and respond to cyber threats quickly and effectively

Exeon.NDR leverages and augments the existing cybersecurity infrastructure (firewalls, SIEM etc.) and completely runs within your network or cloud (full data control)

As it relies on the **analysis of network log data**, Exeon.NDR is not affected by encrypted network traffic Exeon.NDR can be virtually deployed, is compatible with leading network device vendors and easily integrable into the existing cybersecurity infrastructure

Exeon.NDR is specialised in **protecting cloud**, on-premise or hybrid network environments

Exeon is a Swiss vendor, based on more than a decade of academic research at a leading European technical university (ETH Zurich)



Trusted by



PostFinance

Schweizerische Eidgenossenschaft Confédération suisse Confederazione Svizzera Confederaziun svizra













How Exeon.NDR works

Light-weight network log data

Log data from firewalls, virtual and physical switches (e.g., NetFlow, IPFIX), DNS servers, secure web gateways, and cloud platforms such as Azure, Google Cloud, and AWS.

Exeon.NDR algorithms

Full representation of IT activities

Data is stored in a graph database, enabling a 100x reduction compared to the original input volume.



Used for

Visibility

An intuitive GUI with dedicated visualizations for network traffic, enabling fast and interactive drilldowns.

Anomaly detection

Uses supervised and unsupervised ML models, expert use cases, threat correlation, and supports integration of additional log sources.

Response

Graphical representation of security incidents, incident prioritization, and automated alerting and response via API triggers.



The alarm system for your network

Immediate detection of cyber threats such as advanced persistent threats (APTs), ransomware, supply chain attacks, or data leaks from exposed, insecure systems. Powerful detection, even for threats that span multiple data sources.

Network data flows easily understood

With unique and intuitive visualizations, large and complex networks can be instantly monitored and easily understood. Incidents are detected early, and the IT, IoT & OT security posture is strengthened without disrupting ongoing, critical business processes.

Efficient investigation of security incidents

Security alerts can be handled faster and better by immediately displaying all relevant information. Our algorithms **minimize false** alarms and automatically prioritize incidents by threat level. Security teams save crucial time in security operations and reduce workload.

Interested to learn more?

exeon +

Exeon Analytics AG

exeon.com

+41 44 500 77 21

contact@exeon.com



Gregor Erismann

Co-CEO

+41787970509

gregor.erismann@exeon.com