Executive Summary

Threat detection with AI-based behaviour analysis

The workbench on the 30th of September, featuring Philipp Lachberger (Head Presales & Deployment, Head Information Security @ Exeon) and Torsten Schwarz (Managing Consultant @ amasol), focused on the capabilities and benefits of Exeon.NDR for AI-based behavioral threat detection.

Exeon.NDR is a modern Network Detection & Response (NDR) solution that leverages AI-driven behavioral analytics to identify hidden attack patterns, close blind spots, and reduce manual workload for SOC teams – an ideal fit for today's complex IT security architectures.

In daily operations, security teams often face the same challenge: despite a wide array of tools and complex security infrastructures, attacks are still detected too late. Are critical threats overlooked due to blind spots? Are hidden attack patterns escaping traditional detection? Or is the lack of automation putting too much strain on security analysts?

This is exactly where Exeon.NDR provides value ...

Combining network visibility and anomaly detection with metadata

Why traditional tools fall short: many organizations use security tools that cannot detect modern, multi-stage attack scenarios. Blind spots remain, and automation is often insufficient.

How AI-based behavioral analysis helps: By continuously monitoring network traffic and learning what "normal" looks like, AI models can identify deviations that point to malicious behavior. This enables early detection of attacks that bypass signature-based or rule-based tools.

Practical use with Exeon.NDR: Exeon's NDR solution analyzes log and network data without requiring invasive hardware. This makes deployment faster and helps organizations gain visibility into encrypted and internal traffic where attackers often hide.

Operational benefits:

- Significant reduction of false positives compared to rule-based systems.
- Faster detection and response thanks to automated correlation of anomalies.
- Relief for security teams, who spend less time on manual investigation.
- Integration into existing SOC workflows, strengthening overall resilience.

Real-world applications: Case examples showed how Exeon.NDR uncovers lateral movement, data exfiltration, and insider threats that would otherwise remain invisible.

The workbench confirmed amasol's role as an integration partner: helping organizations connect innovative solutions like Exeon.NDR with their IT security landscape, thereby raising both detection quality and operational efficiency.

Watch on-demand

Watch the recording on-demand to see Exeon.NDR in action, or contact amasol to explore how AI-driven network detection can strengthen your security posture. .

amasol events

We cordially invite you to participate in future workbenches, where we will present practical solutions, new features, and best practices together with our technology partners. Stay informed: Sign up for our newsletter so you don't miss any invitations.

Future events: You can find an overview of all upcoming workbenches and events on our website at any time.

We look forward to your participation and the opportunity to exchange ideas!

amasol HQ | Claudius-Keller-Str. 3 B | 81669 Munich | Germany | www.amasol.com