Critical Infrastructure Success Story

One IT/OT View, Full OT Coverage: Energy Operator Strengthens Security Operations and Compliance with Exeon.NDR

About the Company

ENERGY SECTOR · GERMANY · DISTRIBUTION SYSTEM OPERATOR (KRITIS)

A state-owned electricity distribution system operator running one of Germany's major metropolitan grids - connection, operation, expansion and metering. As a designated KRITIS operator, it supplies households, hospitals, public authorities and industry; a grid outage would hit public life and the economy immediately.

10,000s km
of power lines in operation

Top tier
among Germany's largest urban distribution grids

Dozens
of substations and network nodes

2,000+
employees across the service area

Initial situation & challenges

Legally required to operate an attack-detection system (SzA) across a highly distributed grid, under tight budget constraints, and after an earlier open-source trial fell short of the requirement.

CHALLENGE 01

Meet the legal SzA requirement

Attack detection is a compliance obligation under the EnWG IT-Sicherheitskatalog, with NIS2 and the KRITIS-Dachgesetz raising the stakes.

CHALLENGE 02

Achieve full OT visibility across a distributed grid

Near-complete transparency over devices and communication in every relevant OT segment, spread across dozens of sites.

CHALLENGE 03

Extend existing investments across the grid

DPI delivered valuable insight, but sensor-only coverage across every segment was not economically viable.

The solution

Exeon.NDR combined with sensor-based Deep Packet Inspection, deployed fully on-prem/air-gapped on the operator's own infrastructure. The rollout ran in phases, starting with the most critical network segments.

Outcomes & benefits

~2 weeks
to realized value after technical installation

One IT/OT view
across OT segments and relevant IT-to-OT communication paths

On budget
full coverage delivered within the given cost frame

- **Unified security operations** - OT activity and relevant IT-to-OT communication paths available in one operational view.
- **Greater value from existing investments** - DPI, network telemetry and the existing SIEM complemented rather than replaced.
- **Compliance-ready evidence** - reporting and documentation supported the operator's SzA obligations.
- **Fast time to value** - actionable monitoring available approximately two weeks after technical installation.
- **Scalable coverage -** phased licensing and targeted sensor use extended monitoring across the distributed grid within budget.
- **Data sovereignty preserved** - the solution operated fully on the organization's own air-gapped infrastructure.

Contact us

contact@exeon.com
exeon.com
+41 44 500 77 21