OT SOLUTION BRIEF

Secure Critical Infrastructure with a Compliant, On-Prem OT Detection Architecture

How European critical infrastructure operators achieve complete OT visibility, comply with evolving regulations, and protect operational environments without compromising data sovereignty.

Typical Situation

Critical infrastructure operators face increasing cybersecurity obligations while operating highly distributed OT environments with isolated networks, legacy systems, and strict operational requirements. Traditional OT IDS/NIDS solutions often struggle to provide cost-efficient visibility across highly distributed OT environments. Architectures relying on extensive sensor deployments can become complex and expensive to scale, especially across multiple substations, network segments, and isolated environments.

Customer Challenges

Regulatory Compliance

Meet attack detection requirements requirements (**SzA**), **NIS2**, **IEC 62443, 62443,** and **KRITIS** obligations.

Complete OT Visibility

Monitor distributed substations, segmented networks, and isolated environments **without creating blind spots**.

Secure & Scalable Deployment

Protect critical environments while integrating with existing **SOC, SIEM,** and operational processes.

Exeon OT Security Solution

Rather than replacing existing OT security investments, Exeon **complements existing IDS, DPI, and SIEM solutions** with metadata-based Network Detection & Response. By combining **Exeon.NDR** with targeted Deep Packet Inspection, organizations achieve **complete OT visibility** while reducing the need for additional sensors and enabling a scalable, cost-efficient architecture.

Solution Highlights

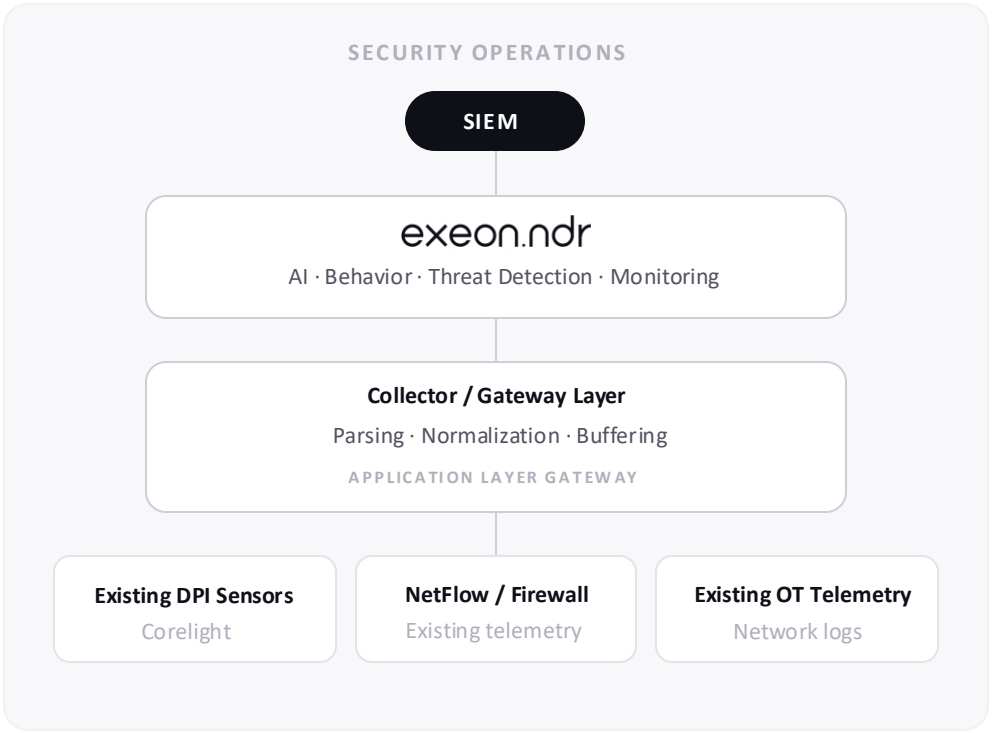
- Combined **Exeon.NDR + Deep Packet Inspection** for complete OT visibility
- Cost-efficient architecture by leveraging existing sensors and security investments
- Flexible deployment (Cloud · Self-Hosted / On-Prem)
- Seamless **SIEM integration** and open architecture
- **Data sovereignty** by design
- Scalable rollout across distributed OT environments

CUSTOMER OUTCOME · EXAMPLE IMPLEMENTATION

Large European electricity distribution operator

- Required OT transparency achieved
- Rollout started with critical network segments
- Operational value within weeks
- Integrated into existing SIEM
- Architecture prepared for phased expansion

Solution Architecture



DEPLOYMENT OPTIONS

On-Prem / Self-Hosted

Full data sovereignty within your own infrastructure.

Cloud

Fast rollout, operated and updated by Exeon.

Four Architecture Principles

1 Distributed Collection

Leverage existing OT telemetry and DPI investments while minimizing the deployment of additional sensors.

2 Secure Data Transfer

Collector Nodes normalize and enrich telemetry from existing OT monitoring solutions before securely forwarding only the required data.

3 Central Analytics

Exeon.NDR correlates network flows with existing Deep Packet Inspection to provide high-fidelity OT threat detection.

4 Existing SOC Integration

Alerts feed directly into existing SIEM and operational workflows.

Why this Architecture?

- Supports highly distributed OT infrastructures
- Extends existing IDS/DPI investments instead of replacing them
- Reduces sensor footprint and overall deployment costs
- Enables phased rollout
- Supports Cloud and Self-Hosted / On-Prem deployments
- Preserves data sovereignty

Book an OT Architecture Assessment

contact@exeon.com · +41 44 500 77 21