exeon

OT SOLUTION BRIEF

Kritische Infrastruktur absichern mit Compliance – treuer On-Prem-Sicherheitsarchitektur

Mit Exeon.NDR können europäische Betreiber kritischer Infrastruktur die vollständige Übersicht über ihre OT-Systemen gewinnen, Compliance mit immerwandelnden Regularien wahren und ihre operativen Systeme schützen ohne dabei die Hoheit über ihre eigenen Daten zu gefährden.

Die Ausgangslage

Betreiber kritischer Infrastruktur stehen wachsenden Cybersicherheitspflichten gegenüber, die sie auf ihre hochgradig verteilte OT-Umgebung mit isolierten Netzwerken, Legacy-Systemen und unter strengen betrieblichen Anforderungen anwenden müssen. Herkömmliche OT-IDS/NIDS-Lösungen haben oft Schwierigkeiten, einen kosteneffizienten Überblick über stark verteilte OT-Umgebungen hinweg bereitzustellen. Sicherheitsarchitekturen, die auf umfangreichen Sensor-Deployments beruhen, können komplex und teuer werden, wenn sie skaliert angewendet werden sollen – insbesondere über mehrere Umspannwerke, Netzsegmente und isolierte Umgebungen.

Herausforderungen der Kunden

Rechtliche Compliance

Erfüllung der Anforderungen zur Angriffserkennung **(SzA), NIS2, IEC 62443** und **KRITIS**-Pflichten

Vollständige OT-Transparenz

Überwachung verteilter Umspannwerke, segmentierter Netzwerke und isolierter Umgebungen, **ohne Blindflecken zu erzeugen**

Schnelles & skalierbares Deployment

Schnelles Deployment mit schmalem Footprint, der bestehende SIEM- und SOC-Infrastruktur nutzt, um den Wert innerhalb der **Budgetgrenzen** zu maximieren

Die Exeon OT-Sicherheitslösung

Exeon.NDR ergänzt **vorhandene IDS-, DPI- und SIEM-Lösungen** um metadatenbasierte Network Detection & Response. Durch die Kombination von **Exeon.NDRs** Metadatenanalyse mit gezielter Deep Packet Inspection erreichen Organisationen **vollständige OT-Transparenz**. Dies reduziert gleichzeitig den Bedarf an zusätzlichen Sensoren und ermöglicht eine skalierbare, kosteneffiziente Sicherheitsarchitektur.

Lösungs-Highlights

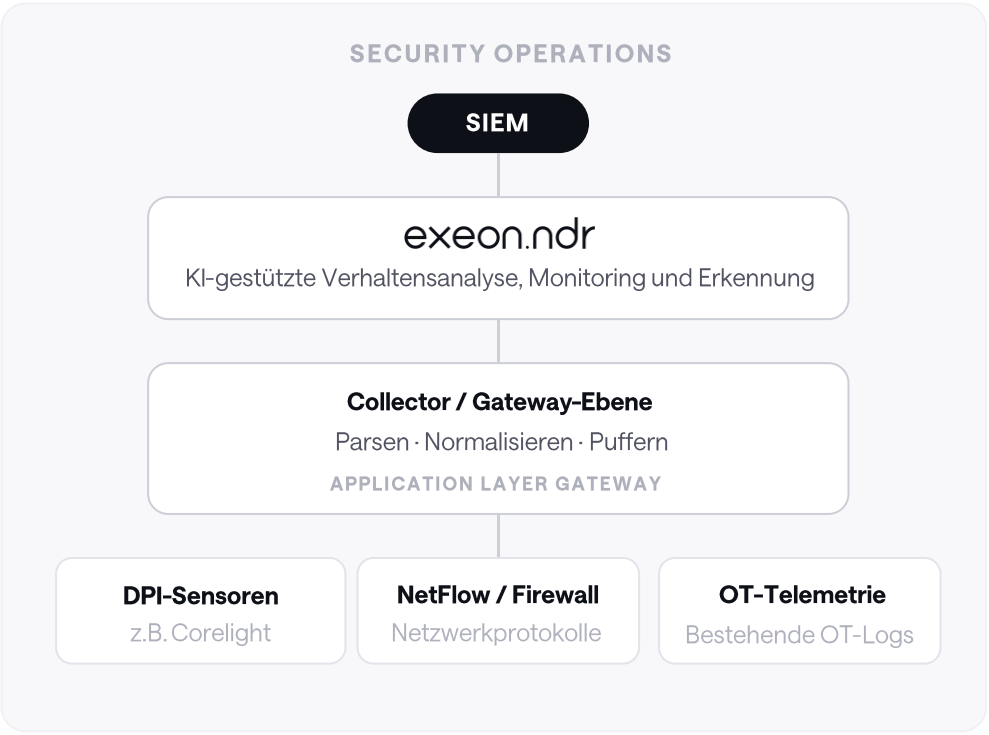
- Kombination aus **Exeon.NDR + Deep Packet Inspection** liefert vollständige OT-Transparenz
- **Kosteneffiziente Sicherheitsarchitektur**, die bestehende Sensoren und Telemetriedaten nutzt und Ihre Sicherheitsinvestitionen schützt
- **Flexibles Deployment** (Cloud oder Self-Hosted / On-Prem)
- Nahtlose **SIEM-Integration** und offene Architektur
- **Datensouveränität** per Design
- **Skalierbarer** Rollout über verteilte OT-Umgebung

KUNDENERGEBNIS · BEISPIELIMPLEMENTIERUNG

Grosser europäischer Stromverteilnetzbetreiber

- Geforderte OT-Transparenz erreicht
- Rollout gestartet mit kritischen Netzsegmenten
- Operativer Mehrwert innerhalb von Wochen
- In bestehendes SIEM integriert
- Architektur für eine phasenweise Erweiterung vorbereitet

Lösungsarchitektur



BEREITSTELLUNGSOPTIONEN

On-Prem / Self-Hosted

Vollständige Datensouveränität: Alle Daten verbleiben innerhalb Ihrer eigenen Infrastruktur

Cloud

Schneller Rollout, betrieben und aktualisiert durch Cloud-Partner

Vier Architekturprinzipien

1

Verteilte Erfassung

Nutzung bestehender OT-Telemetrie- und DPI-Investitionen bei gleichzeitiger Minimierung zusätzlich notwendiger Sensoren

2

Sichere Datenübertragung

Collector-Nodes normalisieren und reichern Telemetrie mit Erkenntnissen aus bestehenden OT-Monitoring-Lösungen an, bevor sie ausschliesslich die erforderlichen Daten sicher weiterleiten

3

Zentrale Analytik

Exeon.NDR korreliert IP-Datenverkehr mit bestehender Deep Packet Inspection, um eine OT-Bedrohungserkennung mit hoher Genauigkeit zu ermöglichen

4

Integration mit bestehenden Security Operations

Alarme fliessen direkt in bestehende SIEM- und operative Workflows ein

Weshalb genau diese Sicherheitsarchitektur?

- Unterstützt hochgradig verteilte OT-Infrastrukturen
- Erweitert bestehende IDS/DPI-Investitionen, anstatt sie zu ersetzen
- Reduziert den Sensor-Footprint und die gesamten Bereitstellungskosten
- Phasenweiser Rollout
- Unterstützt Cloud- und Self-Hosted-/On-Prem-Deployment
- Wahrt die Datensouveränität

Buchen Sie ein OT-Sicherheits-Assessment contact@exeon.com · +41 44 500 77 21