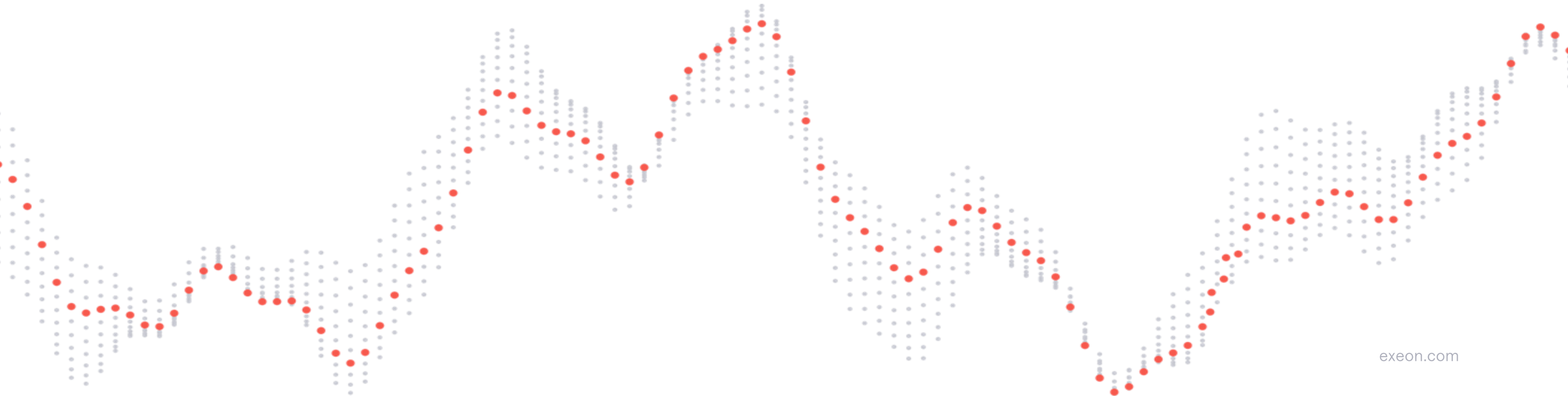
exeon

# OT Security Compliance Guide

## Wie NIS2, IEC 62443 und KRITIS in konkrete OT Security Controls umgesetzt werden

Ein Leitfaden für das produzierende Gewerbe, das Gesundheitswesen, die Versorgungswirtschaft und weitere kritische Branchen



EXECUTIVE SUMMARY

# OT Security gewinnt auch für den Verwaltungsrat an Bedeutung

NIS2, IEC 62443 und KRITIS verändern die Welt der industriellen Cybersecurity.

Drei regulatorische Entwicklungen prägen die industrielle Cybersecurity:

- **NIS2** erweitert das verpflichtende Cybersecurity Risk Management auf kritische und besonders wichtige Sektoren.
- **IEC 62443** hat sich als führendes Framework für die Absicherung industrieller Automatisierungs- und Steuerungssysteme etabliert.
- **KRITIS und branchenspezifische Vorgaben** verlangen zunehmend nachweisbare Resilienz, kontinuierliches Monitoring und Incident Reporting.


Obwohl sich diese Frameworks in ihrem Geltungsbereich unterscheiden, verfolgen sie dasselbe Ziel: **kontinuierliche Sichtbarkeit und eine schnelle Erkennung von Cyberbedrohungen in Operational Technology.**

WER IST BETROFFEN?

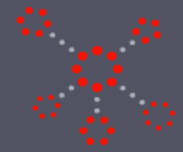
# Wer muss handeln?

OT-Security-Anforderungen betreffen immer mehr industrielle Organisationen, nicht nur die klassische "kritische Infrastruktur“.

**Operational Technology (OT)** bildet das Herzstück moderner industrieller Abläufe. Automatisierte Produktionslinien, pharmazeutische Fertigung, vernetzte Medizingeräte und kritische Infrastruktur sind zunehmend auf digitale Vernetzung angewiesen, um effizient und resilient zu funktionieren.

Mit den Cyberbedrohungen entwickeln sich auch die regulatorischen Erwartungen weiter. **NIS2** weitet die Cybersecurity-Pflichten auf zahlreiche Sektoren aus, **IEC 62443** bietet ein strukturiertes Framework für industrielle Steuerungssysteme und nationale Vorgaben wie **KRITIS** legen zusätzliches Gewicht auf den Schutz systemrelevanter Dienstleistungen.

Unabhängig davon, ob der Handlungsdruck aus Regulierung, Kundenanforderungen oder operativen Risiken entsteht, sollten Betreiber von OT-Umgebungen prüfen, welche Vorgaben für sie gelten und welche Fähigkeiten sie für mehr Cyberresilienz benötigen.



OT-UMGEBUNGEN

**Fertigungs-industrie**

**Gesundheits-wesen**

**Kritische Infrastruktur**

↓

**Steigende Cybersecurity-Anforderungen**

WER IST BETROFFEN?

# Typische OT-Umgebungen

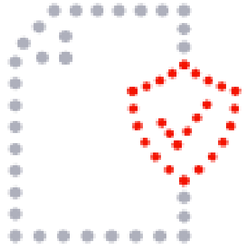
| Branche | Typische OT-Umgebung | Relevante Vorgaben und Frameworks |
|---|---|---|
| **Fertigungsindustrie (einschliesslich Automobilindustrie, Maschinenbau, Elektronik, Lebensmittel- und Getränkeindustrie, Chemie und Pharmazie)** | Produktionslinien, PLCs, SCADA, DCS, Robotik, MES | NIS2, IEC 62443 |
| **Gesundheitswesen** | Medizingeräte, Laborsysteme, bildgebende Systeme, Gebäudemanagement | NIS2, KRITIS, IEC 62443 (in ausgewählten Umgebungen) |
| **Kritische Infrastruktur** | Energieerzeugung und -verteilung, Utilities und weitere systemrelevante operative Umgebungen | NIS2, KRITIS, IEC 62443 |

ÜBER DEN FORMALEN RAHMEN HINAUS

Viele Industrieunternehmen implementieren diese Security-Fähigkeiten unabhängig vom formalen Geltungsbereich. Sie stärken damit ihre operative Resilienz, erfüllen Kundenerwartungen und reduzieren Risiken in ihrer Wertschöpfungskette.

# Unterschiedliche Vorgaben, gemeinsame Security-Anforderungen

Diese Cybersecurity-Fähigkeiten braucht jede OT-Organisation.



Organisationen behandeln **NIS2, IEC 62443** und **KRITIS** häufig als separate Compliance-Initiativen. In der Praxis führen sie jedoch zu denselben zentralen Security-Anforderungen. Dabei schreiben sie keine bestimmten Technologien zur Anwendung vor, sondern definieren Kapazitäten. Diese sollen es Organisationen ermöglichen kontinuierliche Sichtbarkeit zu schaffen, Bedrohungen zu erkennen, auf Vorfälle zu reagieren und so ihre operative Resilienz zu stärken.

Die folgende Übersicht ordnet diese gemeinsamen Anforderungen den drei Frameworks zu. Diese gemeinsamen Anforderungen bilden den roten Faden dieses Guides und dienen als Grundlage für die nachfolgende Einordnung technischer Sicherheitsmassnahmen und der Rolle von **Network Detection and Response (NDR)**.

GEMEINSAME SECURITY-ANFORDERUNGEN

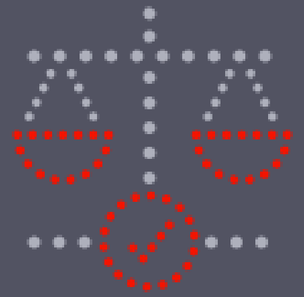
# Anforderungen über die drei Frameworks hinweg

Legende: ✓ explizite Anforderung △ indirekte oder unterstützende Anforderung

| Security-Anforderung | NIS2 | IEC 62443 | KRITIS | Warum das wichtig ist |
|---|---|---|---|---|
| **Asset Visibility** | ✓ | ✓ | ✓ | Wissen, was verbunden ist |
| **Kontinuierliches Monitoring** | ✓ | ✓ | ✓ | Bedrohungen früh erkennen |
| **Threat Detection** | ✓ | ✓ | ✓ | Dwell Time reduzieren |
| **Validierung der Netzwerksegmentierung** | △ | ✓ | △ | Laterale Bewegung verhindern |
| **Incident Response** | ✓ | ✓ | ✓ | Operative Störungen minimieren |
| **Incident Reporting** | ✓ | △ | ✓ | Regulatorische Anforderungen erfüllen |
| **Nachweise & Logging** | ✓ | ✓ | ✓ | Auditierbarkeit sicherstellen |

VON DER RICHTLINIE ZU DEN SECURITY CONTROLS

# Regulatorische Anforderungen in konkrete OT-Security-Massnahmen übersetzen



Regulatorische Vorgaben definieren, was Organisationen erreichen müssen, nicht wie diese technisch realisiert werden müssen. Security Teams müssen rechtliche Anforderungen und Frameworks deshalb in konkrete Kontrollstellen übersetzen, die Cyberrisiken reduzieren und Compliance unterstützen.

Die folgenden Beispiele zeigen, wie zentrale OT-Anforderungen aus NIS2, IEC 62443 und KRITIS in operative Sicherheitskontrollen übertragen werden und welchen Beitrag Network Detection and Response leisten kann.

# Anforderung, Interpretation, Beitrag

| Regulatorische Anforderung (offizieller Wortlaut*) | Technische Interpretation | Beitrag von Exeon.NDR |
|---|---|---|
| **NIS2, Artikel 21:** “Konzepte und Verfahren zur Bewertung der Wirksamkeit von Risikomanagementmassnahmen im Bereich der Cybersicherheit.” | Organisationen benötigen kontinuierliche Sichtbarkeit und Nachweise, die die Wirksamkeit ihrer Security Controls validieren. | Kontinuierliches Monitoring, historische Netzwerkdaten und Detection Metrics unterstützen Validierung und Audit Readiness. |
| **NIS2, Article 21:** “Bewältigung von Sicherheitsvorfällen.” | Cybervorfälle müssen schnell erkannt, untersucht und eingedämmt werden. | Erkennt anomales Netzwerkverhalten und laterale Bewegung und liefert Untersuchungskontext für eine schnellere Incident Response. |
| **NIS2, Article 21:** “Sicherheitsmassnahmen bei Erwerb, Entwicklung und Wartung von Netz- und Informationssystemen.” | Security Controls müssen operative Umgebungen über den gesamten Lebenszyklus schützen, nicht nur bei der Implementierung. | Überwacht Netzwerkkommunikation kontinuierlich und erkennt verdächtige oder nicht autorisierte Aktivitäten in IT- und OT-Umgebungen. |
| **IEC 62443-3-3:** “Systemaktivitäten zur Erkennung von Cybersicherheitsereignissen überwachen.” | Passive Überwachung industrieller Kommunikation und operativer Anomalien. | Verhaltensbasierte Überwachung ohne Endpoint Agents oder Active Scanning. |
| **IEC 62443-3-3:** “Erkennung bösartiger oder unautorisierter Kommunikation.” | Ungewöhnliche Kommunikationsmuster, nicht autorisierte Geräte und Policy-Verstösse erkennen. | Erkennt ungewöhnlichen East-West Traffic, neue Assets, Beaconing und laterale Bewegung. |
| **BSI KRITIS / IT-Sicherheitsgesetz:** “Betreiber müssen angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen kritischer Dienstleistungen treffen.” | Organisationen brauchen kontinuierliche Sichtbarkeit in operativen Umgebungen, um Bedrohungen vor einer Beeinträchtigung der Verfügbarkeit zu vermeiden und rasch zu erkennen. | Kontinuierliche Network Visibility und frühe Threat Detection unterstützen operative Resilienz. |

*Der offizielle Wortlaut wurde für eine bessere Lesbarkeit gekürzt. Der vollständige Text ist den offiziellen Quellen zu entnehmen.

## KEY TAKEAWAY

**NIS2, IEC 62443** und **KRITIS** setzen sehr ähnliche Schwerpunkte: Organisationen müssen ihre Umgebungen kontinuierlich überwachen, bösartige Aktivitäten erkennen, Vorfälle untersuchen und die Wirksamkeit angemessener Security-Massnahmen nachweisen. Die Vorgaben definieren diese Ziele, Technologien wie **NDR** schaffen die dafür notwendige operative Sichtbarkeit und Threat Detection.

### GOLDEN THREAD

BEDEUTUNG FÜR SICHERHEITSTEAMS

# OT Security in der Praxis umsetzen

Mit kontinuierlicher Sichtbarkeit und Threat Detection moderne Compliance-Anforderungen erfüllen.

NIS2, IEC 62443 und KRITIS schreiben keine konkreten Technologien vor. Sie verlangen jedoch, dass Organisationen ihre OT-Umgebungen kontinuierlich überwachen, Sicherheitsvorfälle frühzeitig erkennen und ihre Sicherheitsmassnahmen nachvollziehbar belegen können.
Für Security Teams stellt sich daher weniger die Frage, ob diese Fähigkeiten benötigt werden, sondern wie sie in industriellen Umgebungen umgesetzt werden können. Die folgenden vier Fähigkeiten bilden dafür die technische Grundlage.

**01**

**Kontinuierliches Monitoring**

**02**

**Network Visibility**

**03**

**Netzwerksegmentierung und Policy-Validierung**

**04**

**Threat Detection & Incident Investigation**

# IMPLEMENTIERUNG VON OT SECURITY IN DER PRAXIS

## 01 Kontinuierliches Monitoring

Organisationen sollen ihre operativen Umgebungen kontinuierlich verstehen, statt sich auf punktuelle Assessments oder reaktive Untersuchungen zu verlassen. Kontinuierliches Monitoring hilft Securityteams dabei, Bedrohungen früh zu erkennen, die Wirksamkeit der Kontrollsysteme zu messen und Compliance-Nachweise bereitzustellen.

### OPERATIVE HERAUSFORDERUNG

Viele OT-Systeme unterstützen weder Endpoint Agents noch aktive Sicherheitsscans. Dadurch haben traditionelle Security Tools keine Einsicht in grosse Teile der Netzwerkumgebung.

### WAS ORGANISATIONEN BRAUCHEN

Passive, kontinuierliche Überwachung der Netzwerkkommunikation in IT und OT.

### BEITRAG VON EXEON.NDR

- Deployment ohne Agenten
- Passives Network Monitoring
- Kontinuierliche Sichtbarkeit in hybriden IT-/OT-Umgebungen

## 02 Network Visibility

Für den Schutz industrieller Umgebungen muss bekannt sein, welche Assets kommunizieren, wie sie kommunizieren und ob diese Kommunikation erwartungsgemäss abläuft. Ohne umfassende Sichtbarkeit lassen sich unverwaltete Assets, unerlaubte Verbindungen und neuartige Bedrohungen nicht zuverlässig erkennen.

### OPERATIVE HERAUSFORDERUNG

Industrielle Netzwerke wachsen über Jahre. Während dieses Wachstums könnten Geräte hinzugefügt werden, die nicht oder unzureichend dokumentiert sind. Systeme, die bei Erstimplementierung des Netzwerks dem neusten Stand der Technik entsprechen, werden im Laufe der Jahre zu Legacy-Systemen. Beides begünstigt die Entstehung unbekannter – damit unüberwachter – Kommunikationspfade.

### WAS ORGANISATIONEN BRAUCHEN

Umfassende Sichtbarkeit über Assets, Network Flows und Kommunikationsmuster.

### BEITRAG VON EXEON.NDR

- Automatische Asset Discovery
- Communication Mapping
- Network Flow Analytics

## 03 Netzwerksegmentierung und Policy-Validierung

Frameworks wie IEC 62443 empfehlen Netzwerksegmentierung, um die Auswirkungen von Cybervorfällen einzugrenzen . Die Segmentierung wirkt jedoch nur, wenn Organisationen kontinuierlich prüfen, ob die Kommunikation zwischen Zonen wirklich den vorgesehenen Policies entspricht.

### OPERATIVE HERAUSFORDERUNG

Firewall-Regeln, temporäre Wartungszugriffe und Änderungen an der Infrastruktur schaffen häufig unbeabsichtigte Kommunikationspfade.

### WAS ORGANISATIONEN BRAUCHEN

Kontinuierliche Validierung der Netzwerksegmentierung und der Kommunikations-Policies.

### BEITRAG VON EXEON.NDR

- Sichtbarkeit des East-West Traffic
- Erkennung unerlaubter Kommunikation
- Analyse von Netzwerkbeziehungen

## 04 Threat Detection & Incident Investigation

Moderne Angreifer missbrauchen zunehmend vertrauenswürdige Zugänge, bewegen sich dann lateral durch das umgebende Netzwerk und verbergen sich dabei in legitimer Netzwerkaktivität. Eine frühe Erkennung reduziert operative Störungen und unterstützt fristgerechtes Incident Reporting.

### OPERATIVE HERAUSFORDERUNG

Traditionelle signaturbasierte Tools erkennen neuartige oder verhaltensbasierte Angriffe in OT-Umgebungen oft nur unzureichend.

### WAS ORGANISATIONEN BRAUCHEN

Verhaltensbasierte Erkennung kombiniert mit schnellen Investigation-Fähigkeiten.

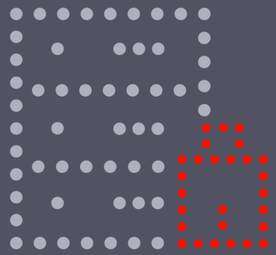
### BEITRAG VON EXEON.NDR

- Verhaltensbasierte Anomalieerkennung
- Erkennung lateraler Bewegung
- Command-and-Control Detection
- Historische Untersuchungen und forensische Nachweise

WO NDR UNTERSTÜTZT

# Warum sich modernes NDR für OT Security eignet

Der Vergleich zwischen traditionellem Monitoring und metadatenbasiertem NDR für industrielle Umgebungen



OT-Umgebungen brauchen kontinuierliche Sichtbarkeit und Threat Detection, die die industriellen Prozesse nicht beeinträchtigen. Nicht jede Security-Technologie ist dafür gleich gut geeignet. Klassische SIEM-Plattformen hängen von Qualität und Umfang der verfügbaren Logquellen ab. Viele NDR-Lösungen der ersten Generation benötigen dagegen dedizierte Sensoren und Packet Inspection, was die Implementierung komplizierter gestaltet.

Modernes NDR nutzt bestehende Netzwerk-Telemetrie als Datenbasis. Diese Informationen werden mithilfe von Verhaltensanalysen und KI-gestützten Erkennungsverfahren ausgewertet, um bekannte und unbekannte Bedrohungen zu identifizieren. Dadurch entsteht umfassende Sichtbarkeit mit minimalen Auswirkungen auf den Betrieb.

WO NDR UNTERSTÜTZT

# Vergleich von Überwachungsansätzen für OT

Legende: ✓ starke Fähigkeit △ abhängig von der Implementierung verfügbar — eigenschränkt

| Security-Anforderung | Generisches SIEM | Traditionelles, sensorbasiertes NDR | Exeon.NDR metadatabasiert |
|---|---|---|---|
| **Kontinuierliche Network Visibility** | Abhängig von verfügbaren Logquellen | ✓ Sichtbarkeit des Network Traffic | ✓ Flow- und metadata-basierte Sichtbarkeit in IT und OT |
| **Passive Implementierung** | ✓ | △ Benötigt häufig zusätzliche Sensoren oder TAP-/SPAN-Infrastruktur | ✓ Nutzt vorhandene Telemetrie wie NetFlow, IPFIX, Firewall-, DNS- und Cloud-Metadaten |
| **OT-sicheres Monitoring** | Abhängig von den Datenquellen | △ Kann Infrastruktur für Packet Inspection erfordern | ✓ Agentless, passiv und ohne Beeinträchtigung industrieller Systeme |
| **Verhaltensbasierte Threat Detection** | △ Regelbasierte Korrelation | △ Häufig signaturorientiert | ✓ ML-basierte Verhaltensanalyse und Anomalieerkennung |
| **Erkennung lateraler Bewegung** | — Begrenzter Kontext | ✓ | ✓ Erweiterte verhaltensbasierte Erkennung in hybriden Umgebungen |
| **Sichtbarkeit in verschlüsseltem Traffic** | — Eingeschränkt | △ Payload Inspection verliert an Wirksamkeit | ✓ Metadatenanalyse unabhängig von der Payload-Verschlüsselung |
| **Skalierbarkeit in verteilter OT** | Abhängig von der Logarchitektur | △ Zusätzliche Sensoren erhöhen die Komplexität | ✓ Schmalgehaltene Architektur auf Basis vorhandener Infrastruktur |
| **Compliance-Nachweise und Untersuchungen** | Abhängig von gespeicherten Logs | ✓ | ✓ Historische Netzwerkdaten, Investigation Workflows und Audit-Unterstützung |

## WO NDR UNTERSTÜTZT

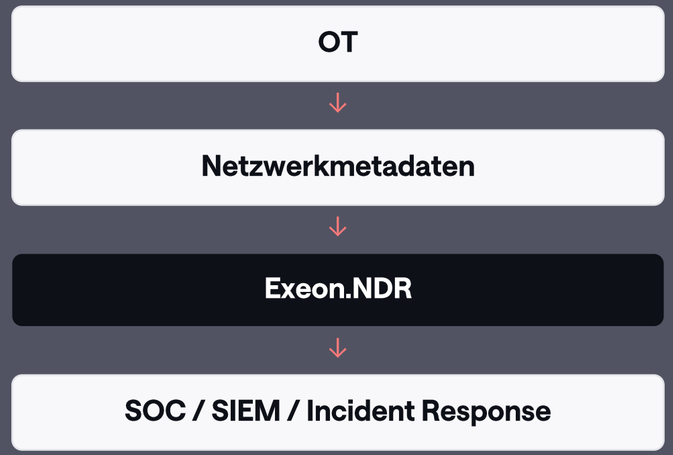
**Moderne OT-Security versucht nicht immer mehr Daten zu sammeln, sondern aus vorhandener Telemetrie bessere Security-Insights zu gewinnen.**

Durch die Kombination aus passive Monitoring, Verhaltensanalyse und metadata-basierter Erkennung verbessert modernes NDR die Sichtbarkeit und Threat Detection und unterstützt Compliance-Ziele, ohne zusätzliche operative Komplexität einzuführen.

### POSITIONIERUNG

**Modernes NDR ergänzt bestehende Firewalls, SIEM- und EDR-Systeme, es ersetzt sie nicht.**

### ARCHITEKTURVISUAL



WAS EXEON NICHT ABDECKT

# Technologie ist nur ein Teil von OT Compliance

Resiliente OT Security verbindet Menschen, Prozesse und Technologie

**NIS2, IEC 62443** und **KRITIS** definieren Security-Ziele, nicht bestimmte Technologien. Compliance erfordert deshalb eine Kombination aus Governance, operativen Prozessen und geeigneten technischen Kontrollen.

**Network Detection and Response** spielt dabei eine wichtige Rolle. Es stellt kontinuierliche Sichtbarkeit, verhaltensbasierte Threat Detection und Investigations-Möglichkeiten bereit. Es kann jedoch nur ergänzend zu umfassenderen Security- und Compliance-Aktivitäten stehen, statt sie zu ersetzen. Diese Abgrenzung zu sehen hilft Organisationen, eine wirksame und nachhaltige OT-Security-Strategie aufzubauen.

## Wo Exeon.NDR ansetzt

| Exeon.NDR stärkt... | Organisationen ergänzen dies durch... |
|---|---|
| Kontinuierliche Network Visibility in IT und OT | Asset Inventory und Configuration Management |
| Verhaltensbasierte Threat Detection und Anomalieerkennung | Risk Management und Cybersecurity Governance |
| Erkennung lateraler Bewegung und verdächtiger Kommunikation | Netzwerksegmentierung, Firewall Policies und Access Control |
| Historische Untersuchungen und forensische Nachweise | Incident-Response-Prozesse und regulariengerechtes Reporting |
| Kontinuierliches Monitoring zur Unterstützung der Audit Readiness | Compliance Management und Security Awareness |
| Offene Integration in bestehende Security-Ökosysteme | SIEM, IAM, EDR, Vulnerability Management und weitere ergänzende Kontrollinstanzen. |

## KEY TAKEAWAY

Keine einzelne Technologie stellt im Alleingang Compliance sicher. Resiliente OT Security entsteht durch das Zusammenspiel von Governance, operativen Prozessen und moderner Threat-Detection-Technologie. Exeon.NDR stärkt die technologische Säule mit kontinuierlicher Sichtbarkeit, Verhaltensanalyse und Investigation-Fähigkeiten, die regulatorische Ziele und operative Resilienz unterstützen.

**Technologie liefert die Sichtbarkeit und Nachweise für Compliance. Resiliente OT Security entsteht jedoch erst, wenn Menschen, Prozesse und Technologie in einem gemeinsamen Security-Programm zusammenspielen.**

**OT Compliance**

### Menschen

- Security Awareness
- Rollen und Verantwortlichkeiten
- Skills

### Prozesse

- Risk Management
- Incident Response
- Compliance Management
- Governance

### Technologie

- kontinuierliche Sichtbarkeit
- verhaltensbasierte Erkennung
- Investigation
- Nachweise
- Integration

### Beitrag von Exeon

- kontinuierliches Monitoring
- Threat Detection
- Investigation
- Audit-Nachweise
- offene Integrationen

**Exeon.NDR**

BRANCHENPERSPEKTIVEN

# Eine Grundlage für unterschiedliche OT-Umgebungen

Operative Prioritäten unterscheiden sich, die benötigten Security-Fähigkeiten sind ähnlich

Ein Produktionsbetrieb konzentriert sich auf unterbrechungsfreie Abläufe. Pharmaunternehmen priorisieren Produktintegrität und regulatorische Compliance. Spitäler müssen die Patientensicherheit gewährleisten. Betreiber kritischer Infrastruktur stellen systemrelevante Dienstleistungen sicher.

Trotz unterschiedlicher Prioritäten, Technologien und Risikoprofile benötigen diese Umgebungen dieselben grundlegenden Cybersecurity-Fähigkeiten: kontinuierliche Einsicht in Netzwerkaktivitäten, eine frühe Erkennung ungewöhnlichen Verhaltens und belastbare Nachweise für Untersuchungen und den Resilienznachweis.

Diese Fähigkeiten schaffen eine flexible Security-Grundlage, die verschiedene Branchen unterstützt und sich an neue Bedrohungen und regulatorische Anforderungen anpassen lässt.

BRANCHENPERSPEKTIVEN

# OT-Prioritäten nach Branche

| Branche | Operative Priorität | Zentraler Security-Fokus |
|---|---|---|
| **Produzierendes Gewerbe (einschliesslich Automobilindustrie, Maschinenbau, Elektronik, Lebensmittel- und Getränkeindustrie, Chemie und Pharmazie)** | Produktionskontinuität, Produktqualität und Schutz geistigen Eigentums | Laterale Bewegung erkennen, Segmentierung validieren sowie industrielle Kommunikation und Remote Access überwachen |
| **Gesundheitswesen** | Patientensicherheit und unterbrechungsfreier klinischer Betrieb | Vernetzte Medizingeräte schützen, Legacy-Umgebungen sichtbar machen und ungewöhnliches Verhalten ohne Betriebsunterbruch erkennen |
| **Kritische Infrastruktur** | Verfügbarkeit und Resilienz systemrelevanter Dienstleistungen | Verteilte OT-Umgebungen kontinuierlich überwachen, Bedrohungen früh erkennen und eine schnelle Incident Response unterstützen |

# Die gemeinsame Security-Grundlage

Resiliente OT Security erfordert branchenunabhängig:

- kontinuierliche Sichtbarkeit in industriellen Netzwerken
- frühe Erkennung von ungewöhnlichem und bösartigem Verhalten
- Untersuchung von Vorfällen anhand historischer Netzwerkdaten
- operative Resilienz durch schnelle Detection und Response
- Nachweis der Wirksamkeit von Security Controls bei Audits und Incident Reporting

**KEY TAKEAWAY**

Operative Prioritäten unterscheiden sich, resiliente OT Security beginnt jedoch immer mit derselben Grundlage: Sichtbarkeit, Erkennung und operativer Kontext. Organisationen mit diesen Fähigkeiten sind besser auf neue Vorgaben, Bedrohungen und die zunehmende Konvergenz von IT und OT vorbereitet.

**Das Ziel ist nicht eine eigene Security-Architektur für jede Branche, sondern grundlegende Fähigkeiten, die sich konsistent in unterschiedlichen OT-Umgebungen einsetzen und neuen regulatorischen Anforderungen zuordnen lassen.**

# Den richtigen OT-Monitoring-Ansatz wählen

Die richtige Technologie stärkt operative Resilienz und regulatorische Compliance

Die in diesem Guide beschriebenen Security-Fähigkeiten bieten einen Rahmen für die Evaluation von OT-Monitoring-Lösungen. Organisationen sollten Produkte nicht nur anhand von Feature-Listen vergleichen. Sie sollten prüfen, ob eine Lösung die operativen Ergebnisse unterstützt, die moderne OT-Umgebungen erfordern.

Eine geeignete Lösung sollte Folgendes bieten:

- kontinuierliche Sichtbarkeit in industriellen Netzwerken
- verhaltensbasierte Threat Detection über bekannte Signaturen hinaus
- geringe operative Auswirkungen durch passives Monitoring
- Unterstützung von Untersuchungen und Compliance-Nachweisen
- Integration in bestehende Security Operations

**KEY TAKEAWAY**

Die besten OT-Monitoring-Lösungen sammeln nicht nur Daten. Sie verbessern die Sichtbarkeit, erkennen Bedrohungen früher und stärken die operative Resilienz.


Der **Exeon NDR Evaluation Guide** bietet einen detaillierten Rahmen mit Evaluationskriterien und Fragen für den Anbietervergleich.

OT COMPLIANCE QUICK CHECK

# Ist Ihre OT-Umgebung bereit?

Kurze Selbstbeurteilung für OT Visibility, Threat Detection und Compliance Readiness

Die folgenden Fragen helfen Ihnen dabei, zu beurteilen, ob Ihre aktuelle Monitoring-Strategie die in diesem Guide beschriebenen Security-Ziele unterstützt.

| OT Security Readiness Check | ✓ |
|---|---|
| Haben Sie kontinuierliche Sichtbarkeit in Ihrem OT-Netzwerk? | ☐ |
| Können Sie neue oder nicht verwaltete OT-Assets automatisch identifizieren? | ☐ |
| Können Sie anormales Verhalten und laterale Bewegung erkennen? | ☐ |
| Können Sie Vorfälle anhand historischer Netzwerkdaten untersuchen? | ☐ |
| Können Sie bei einem Audit kontinuierliches Monitoring nachweisen? | ☐ |
| Ist Ihr OT Monitoring in die übergeordneten SOC- und Incident-Response-Prozesse integriert? | ☐ |
| Beeinträchtigt Ihr Monitoring-Ansatz sensible industrielle Systeme nur minimal? | ☐ |

# So sieht ein guter Reifegrad aus

Organisationen mit einer ausgereiften OT-Monitoring-Strategie verfügen typischerweise über:

- kontinuierliche, passive Einsicht in IT und OT
- verhaltensbasierte Threat Detection
- schnelle Investigation-Fähigkeiten
- auditfähige Nachweise
- nahtlose Integration in bestehende Security Operations

### NÄCHSTE SCHRITTE

Ob Sie sich auf NIS2 vorbereiten, an IEC 62443 ausrichten oder Ihre operative Resilienz stärken, modernes OT Monitoring schafft eine wichtige Grundlage.

### IHR WEITERER WEG

**OT Compliance Guide (dieses Dokument)**

↓

Self Assessment

↓

Demo / Workshop

↓

NDR Evaluation Guide

↓

Architecture Review / Demo

# Setzen Sie Ihre OT-Security- und Compliance-Evaluation fort

## Offizielle Referenzen

Die folgenden Quellen bieten verlässliche Orientierung zu OT Cybersecurity, regulatorischer Compliance und Best Practices für industrielle Security.

| Kategorie | Resource |
|---|---|
| **Regulierung und Standards** | NIS2-Richtlinie (EU 2022/2555), IEC-62443-Reihe, BSI-KRITIS-Leitlinien |
| **Umsetzungshilfen** | ENISA NIS2 Resources, NIST SP 800-82 Rev. 3 (Guide to OT Security), NIST Cybersecurity Framework (CSF) 2.0 |
| **Industrial Cybersecurity** | CISA Industrial Control Systems (ICS) Guidance, MITRE ATT&CK® for ICS |

## Evaluation fortsetzen

Möchten Sie Ihre OT-Monitoring-Strategie evaluieren?
Der Exeon NDR Evaluation Guide bietet:

- Evaluationskriterien für moderne NDR-Lösungen
- OT-spezifische Überlegungen zur Architektur
- Fragen für den Anbietervergleich
- eine praxisnahe Checkliste für die Evaluation

**Exeon NDR Evaluation Guide herunterladen**

## Sprechen Sie mit uns

Ob Sie sich auf NIS2 vorbereiten, Ihre Security an IEC 62443 ausrichten oder die OT Security Posture stärken möchten, wir besprechen gerne Ihre Umgebung und Herausforderungen.

**Kontakt aufnehmen. Vereinbaren Sie einen Termin, um Ihre Ausgangslage zu besprechen.**

exeon

exeon.com