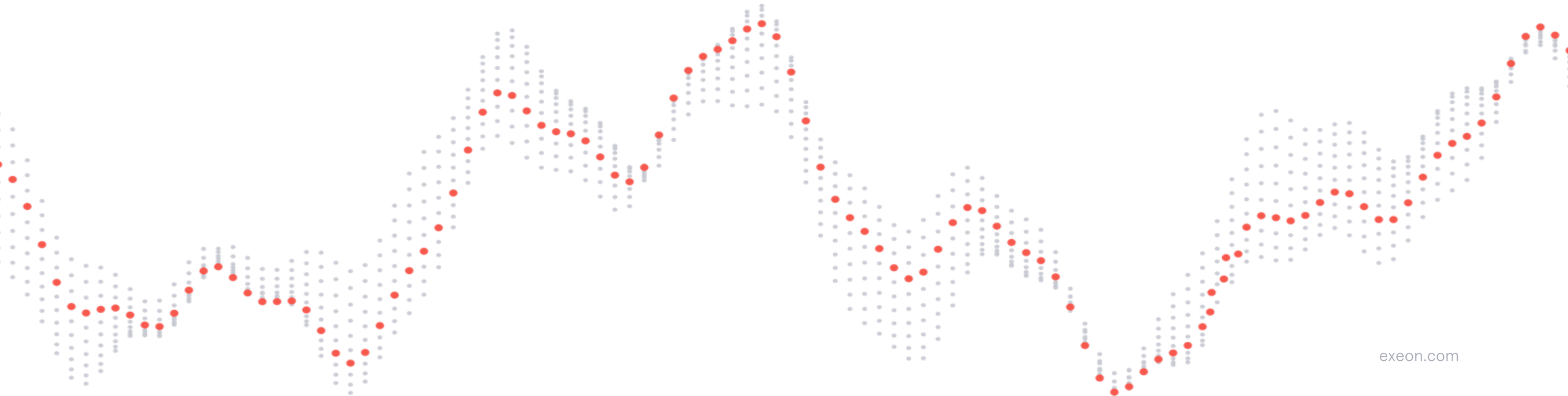
exeon

OT Security Compliance Guide

How NIS2, IEC 62443, and KRITIS translate into practical OT security controls

A practical guide for Manufacturing, Healthcare, Utilities, and other critical industries



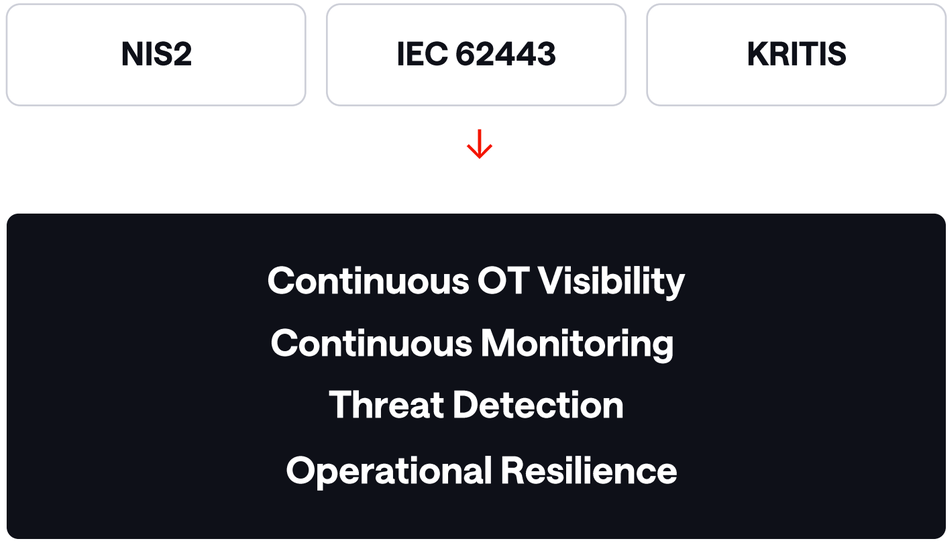
EXECUTIVE SUMMARY

Why OT security has become a board-level issue

How NIS2, IEC 62443, and KRITIS are reshaping industrial cybersecurity.

Three regulatory developments are reshaping industrial cybersecurity:

- **NIS2** expands mandatory cybersecurity risk management across critical and essential sectors.
- **IEC 62443** has become the leading framework for securing industrial automation and control systems.
- **KRITIS / sector-specific regulations** increasingly require demonstrable resilience, continuous monitoring, and incident reporting.



While these frameworks differ in scope, they converge on one objective: **Continuous visibility and rapid detection of cyber threats affecting operational technology.**

WHO IS AFFECTED?

Who Needs to Act?

OT cybersecurity requirements are expanding across industrial organizations – not just traditional critical infrastructure.

Operational Technology (OT) is at the heart of modern industrial operations. From automated production lines and pharmaceutical manufacturing to connected medical devices and critical infrastructure, these environments increasingly rely on digital connectivity to maintain efficiency and resilience.

As cyber threats continue to evolve, so do regulatory expectations. **NIS2** broadens cybersecurity obligations across many sectors, **IEC 62443** provides a structured framework for securing industrial control systems, and national regulations such as **KRITIS** place additional emphasis on protecting essential services.

Whether driven by regulation, customer requirements, or operational risk, organizations operating OT environments should assess how these requirements apply to their business and establish the capabilities needed to strengthen cyber resilience.

OT ENVIRONMENTS

Manufacturing

Healthcare

Critical Infrastructure

↓

Increasing Cybersecurity Expectations

WHO IS AFFECTED?

Typical OT Environments

Industry	Typical OT Environment	Primary Regulatory / Framework Drivers
Manufacturing (incl. Automotive, Machinery, Electronics, Food & Beverage, Chemicals and Pharmaceuticals)	Production lines, PLCs, SCADA, DCS, robotics, MES	NIS2, IEC 62443
Healthcare	Medical devices, laboratory systems, imaging equipment, building management systems	NIS2, KRITIS, IEC 62443 (selected environments)
Critical Infrastructure	Energy generation & distribution, utilities, and other essential operational environments	NIS2, KRITIS, IEC 62443

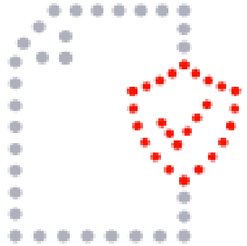
BEYOND FORMAL SCOPE

Many industrial organizations implement these security capabilities regardless of formal regulatory scope – to strengthen operational resilience, satisfy customer expectations, and reduce supply chain risk.

COMMON SECURITY REQUIREMENTS

Different Regulations - Common Security Requirements

The cybersecurity capabilities every OT organization needs.



Organizations often approach **NIS2, IEC 62443,** and **KRITIS** as separate compliance initiatives. In practice, however, they converge on a common set of operational security requirements. Rather than prescribing specific technologies, they define the security capabilities organizations must establish to achieve continuous visibility, detect threats, respond to incidents, and strengthen operational resilience.

The following overview maps these common security requirements across the three frameworks and provides the foundation for understanding where technologies such as **Network Detection & Response (NDR)** can help organizations meet their operational and compliance objectives.

COMMON SECURITY REQUIREMENTS

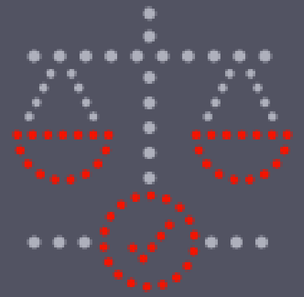
Requirements Across the Three Frameworks

Legend: ✓ Explicit requirement △ Indirect / supporting requirement

Security Requirement	NIS2	IEC 62443	KRITIS	Why It Matters
Asset visibility	✓	✓	✓	Know what is connected
Continuous monitoring	✓	✓	✓	Detect threats early
Threat detection	✓	✓	✓	Reduce dwell time
Network segmentation validation	△	✓	△	Prevent lateral movement
Incident response	✓	✓	✓	Minimize operational disruption
Incident reporting	✓	△	✓	Regulatory compliance
Evidence & logging	✓	✓	✓	Auditability

FROM REGULATION TO SECURITY CONTROLS

Translating regulatory requirements into practical OT security measures.



Regulations define what organizations must achieve, not how to implement it. Security teams are therefore responsible for translating legal and framework requirements into practical technical controls that reduce cyber risk and support compliance.

The following examples illustrate how key OT-related requirements from NIS2, IEC 62443, and KRITIS translate into operational security capabilities, and where Network Detection & Response (NDR) contributes to meeting those objectives.

FROM REGULATION TO SECURITY CONTROLS

Requirement, Interpretation, Contribution

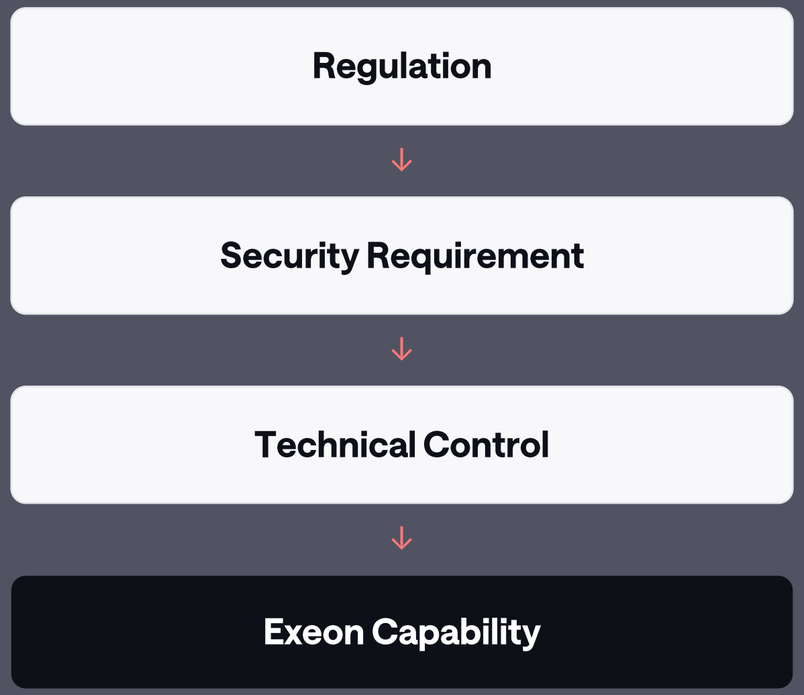
Regulatory Requirement (official wording*)	Technical Interpretation	How Exeon.NDR Contributes
NIS2, Article 21: “Policies and procedures to assess the effectiveness of cybersecurity risk-management measures.”	Organizations require continuous visibility and evidence to validate that security controls are operating effectively.	Continuous monitoring, historical network evidence and detection metrics support validation and audit readiness.
NIS2, Article 21: “Incident handling.”	Rapid detection, investigation and containment of cyber incidents.	Detects anomalous network behavior, lateral movement and provides investigation context to accelerate incident response.
NIS2, Article 21: “Security in network and information systems acquisition, development and maintenance.”	Security controls must continuously protect operational environments, not only during deployment but throughout their lifecycle.	Continuously monitors network communications to identify suspicious or unauthorized activity across IT and OT environments.
IEC 62443-3-3: “Monitor system activity for detection of cybersecurity events.”	Passive monitoring of industrial communications and operational anomalies.	Behavior-based monitoring without requiring endpoint agents or active scanning.
IEC 62443-3-3: “Detect malicious or unauthorized communications.”	Identify abnormal communication patterns, unauthorized devices and policy violations.	Detects unusual East-West traffic, new assets, beaconing and lateral movement.
BSI KRITIS / IT Security Act: “Operators must implement appropriate organizational and technical measures to avoid disruptions to critical services.”	Organizations need continuous visibility into operational environments to identify threats before they impact availability.	Provides continuous network visibility and early threat detection to support operational resilience.

*Wording shortened for readability. Refer to the official sources for the complete legal text.

KEY TAKEAWAY

Across **NIS2, IEC 62443, and KRITIS,** the emphasis is remarkably consistent: organizations must continuously monitor their environments, detect malicious activity, investigate incidents, and demonstrate that appropriate security measures are effective. While the regulations define these objectives, technologies such as **Network Detection & Response** provide the operational visibility and threat detection capabilities needed to support them.

THE GOLDEN THREAD



WHAT THIS MEANS FOR SECURITY TEAMS

Implementing OT Security in Practice

How security teams can address modern compliance requirements through continuous visibility and threat detection.

While regulations define the outcomes organizations must achieve, security teams are responsible for implementing the technical controls that make those outcomes possible. For OT environments, this means establishing continuous visibility, detecting abnormal behavior without disrupting operations, and providing the evidence needed to demonstrate resilience during audits or incidents. The following sections outline the core capabilities that underpin modern OT security.

01

Continuous Monitoring

02

Network Visibility

03

Network Segmentation & Policy Validation

04

Threat Detection & Incident Investigation

01 Continuous Monitoring

Regulations increasingly expect organizations to maintain ongoing awareness of their operational environments rather than relying on periodic assessments or reactive investigations. Continuous monitoring enables security teams to detect threats early, measure the effectiveness of security controls, and provide evidence of compliance.

OPERATIONAL CHALLENGE

Many OT assets cannot run endpoint agents or tolerate active security scanning, leaving large parts of the environment invisible to traditional security tools.

WHAT ORGANIZATIONS NEED

Passive, continuous monitoring of network communications across IT and OT environments.

HOW EXEON.NDR CONTRIBUTES

- Agentless deployment
- Passive network monitoring
- Continuous visibility across hybrid IT/OT environments

02 Network Visibility

Understanding which assets communicate, how they communicate, and whether those communications are expected is fundamental to protecting industrial environments. Without comprehensive visibility, organizations cannot effectively identify unmanaged assets, unauthorized connections, or emerging threats.

OPERATIONAL CHALLENGE

Industrial networks often evolve over many years, creating undocumented devices, legacy systems, and hidden communication paths.

WHAT ORGANIZATIONS NEED

Comprehensive visibility into assets, network flows, and communication patterns.

HOW EXEON.NDR CONTRIBUTES

- Automatic asset discovery
- Communication mapping
- Network flow analytics

03 Network Segmentation & Policy Validation

Standards such as **IEC 62443** promote network segmentation to reduce the impact of cyber incidents. However, segmentation is only effective if organizations continuously verify that communication between zones follows the intended security policy.

OPERATIONAL CHALLENGE

Firewall rules, temporary maintenance access, and infrastructure changes often introduce unintended communication paths.

WHAT ORGANIZATIONS NEED

Continuous validation of network segmentation and communication policies.

HOW EXEON.NDR CONTRIBUTES

- East-West traffic visibility
- Detection of unauthorized communication
- Network relationship analysis

04 Threat Detection & Incident Investigation

Modern attackers increasingly exploit trusted access, move laterally across environments, and blend into legitimate network activity. Detecting these behaviors early is essential to minimize operational disruption and support timely incident reporting.

OPERATIONAL CHALLENGE

Traditional signature-based tools often struggle to identify novel or behavior-based attacks within OT environments.

WHAT ORGANIZATIONS NEED

Behavioral detection combined with rapid investigation capabilities.

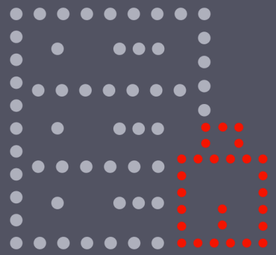
HOW EXEON.NDR CONTRIBUTES

- Behavioral anomaly detection
- Lateral movement detection
- Command-and-control detection
- Historical investigation and forensic evidence

WHERE NDR HELPS

Why Modern NDR Is Well Suited for OT Security

Comparing traditional monitoring approaches with modern, metadata-driven **Network Detection & Response** for industrial environments.



OT environments require continuous visibility and threat detection without disrupting industrial processes. However, not every security technology is equally suited for operational networks. Traditional SIEM platforms depend on the quality of available log sources, whereas many first-generation NDR solutions rely on dedicated sensors and packet inspection, which can increase deployment complexity.

Modern NDR takes a different approach by leveraging existing network telemetry, behavioral analytics, and AI-driven detection to deliver comprehensive visibility with minimal operational impact.

WHERE NDR HELPS

Comparing Monitoring Approaches for OT

Legend: ✓ Strong capability △ Available depending on implementation — Limited

Security Requirement	Generic SIEM	Traditional NDR (Sensor-Based)	Exeon.NDR (Metadata-Driven)
Continuous network visibility	Depends on available log sources	✓ Network traffic visibility	✓ Flow- and metadata-based visibility across IT & OT
Passive deployment	✓	△ Often requires additional sensors or TAP/SPAN infrastructure	✓ Uses existing telemetry (NetFlow, IPFIX, firewall, DNS, cloud metadata)
OT-safe monitoring	Depends on data sources	△ May require packet inspection infrastructure	✓ Agentless, passive monitoring without impacting industrial systems
Behavior-based threat detection	△ Rule-based correlation	△ Often signature-focused	✓ ML-based behavioral analytics and anomaly detection
Lateral movement detection	— Limited	✓	✓ Advanced behavioral detection across hybrid environments
Encrypted traffic visibility	— Limited	△ Payload inspection becomes ineffective	✓ Metadata analysis independent of payload encryption
Scalability across distributed OT	Depends on log architecture	△ Additional sensors increase complexity	✓ Lightweight architecture leveraging existing infrastructure
Compliance evidence & investigations	Depends on retained logs	✓	✓ Historical network evidence, investigation workflows and audit support

WHERE NDR HELPS

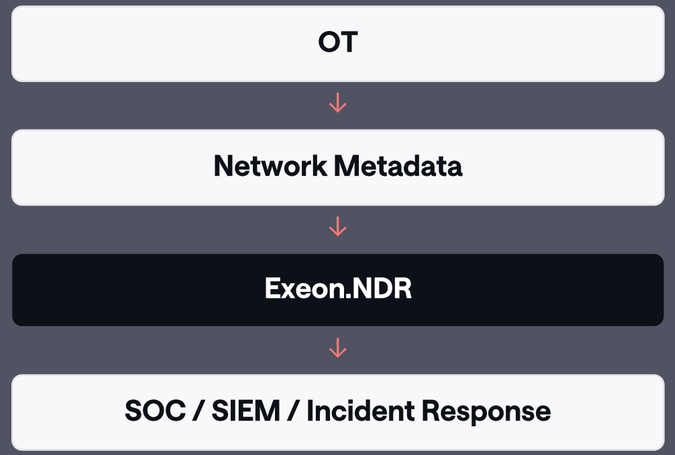
Modern OT security is less about collecting more data and more about extracting better security insights from existing telemetry.

By combining passive deployment, behavioral analytics, and metadata-based detection, modern NDR enables organizations to improve visibility, strengthen threat detection, and support compliance objectives without introducing additional operational complexity.

POSITIONING

Modern NDR complements, not replaces, existing firewalls, SIEM, and EDR.

ARCHITECTURE DIAGRAM



WHAT EXEON DOES NOT COVER

Technology Is One Part of OT Compliance

Building resilient OT security requires people, processes, and technology working together.

NIS2, IEC 62443, and **KRITIS** define security objectives, not specific technologies. Achieving compliance, therefore, requires organizations to combine governance, operational processes, and appropriate technical controls.

Network Detection & Response (NDR) plays a critical role by providing continuous visibility, behavioral threat detection, and investigation capabilities. However, it complements rather than replaces broader security and compliance activities. Understanding this distinction helps organizations build an effective and sustainable **OT security strategy**.

Where Exeon.NDR Fits

Exeon.NDR strengthens...	Organizations should complement with...
Continuous network visibility across IT and OT	Asset inventory and configuration management
Behavior-based threat detection and anomaly detection	Risk management and cybersecurity governance
Detection of lateral movement and suspicious communications	Network segmentation, firewall policies and access control
Historical investigation and forensic evidence	Incident response procedures and regulatory reporting
Continuous monitoring supporting audit readiness	Compliance management and security awareness
Open integration into existing security ecosystems	SIEM, IAM, EDR, vulnerability management and other complementary controls

KEY TAKEAWAY

No single technology delivers compliance on its own. Organizations achieve resilient OT security by combining governance, operational processes, and modern detection capabilities. Exeon.NDR strengthens the technology pillar by providing continuous visibility, behavioral analytics, and investigation capabilities needed to support regulatory objectives and operational resilience.

Technology provides the visibility and evidence needed for compliance - but resilient OT security is achieved by combining people, processes, and technology into a single security program.

OT Compliance

People

- Security awareness
- Roles & responsibilities
- Skills

Process

- Risk management
- Incident response
- Compliance management
- Governance

Technology

- Continuous visibility
- Behavioral detection
- Investigation
- Evidence
- Integration

Exeon's Contribution

- Continuous monitoring
- Threat detection
- Investigation
- Audit evidence
- Open integrations

Exeon.NDR

INDUSTRY PERSPECTIVES

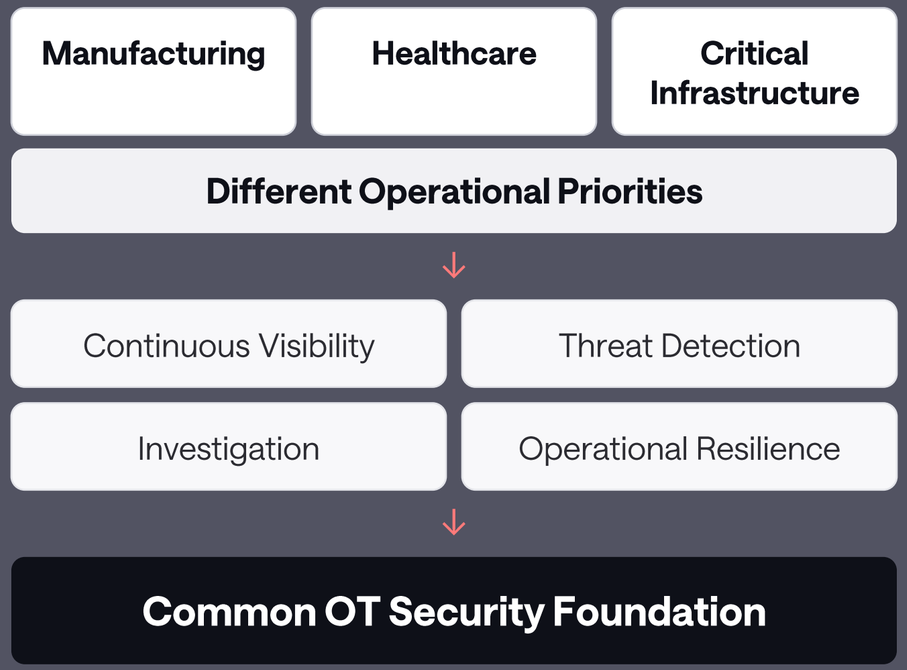
One Foundation - Different OT Environments

Operational priorities differ - but the security capabilities needed to protect industrial operations remain remarkably consistent.

A production facility focuses on maintaining uninterrupted operations. A pharmaceutical manufacturer prioritizes product integrity and regulatory compliance. Hospitals must ensure patient safety, while operators of critical infrastructure are responsible for delivering essential services.

Although these environments differ significantly in their operational priorities, technologies, and risk profiles, the cybersecurity capabilities they require are fundamentally the same. Organizations need continuous visibility into network activity, the ability to detect abnormal behavior early, and the evidence required to investigate incidents and demonstrate resilience.

Building these capabilities creates a flexible security foundation that supports multiple industries while adapting to evolving threats and regulatory requirements.



INDUSTRY PERSPECTIVES

OT Priorities Across Industries

Industry	Operational Priority	Core Security Focus
Manufacturing (including Automotive, Machinery, Electronics, Food & Beverage, Chemicals and Pharmaceuticals)	Production continuity, product quality and intellectual property protection	Detect lateral movement, validate segmentation, monitor industrial communications and remote access
Healthcare	Patient safety and uninterrupted clinical operations	Protect connected medical devices, gain visibility into legacy environments and detect abnormal behavior without disrupting operations
Critical Infrastructure	Availability and resilience of essential services	Continuously monitor distributed OT environments, detect threats early and support rapid incident response

INDUSTRY PERSPECTIVES

The Common Security Foundation

Regardless of industry, resilient OT security depends on the ability to:

- Maintain continuous visibility across industrial networks
- Detect abnormal and malicious behavior early
- Investigate incidents using historical network evidence
- Support operational resilience through timely detection and response
- Demonstrate the effectiveness of security controls during audits and incident reporting

KEY TAKEAWAY

Operational priorities may differ, but resilient OT security always starts with the same foundation: visibility, detection, and operational awareness. Organizations that establish these core capabilities are better prepared for evolving regulations, emerging threats, and the increasing convergence of IT and OT.

The objective isn't to build a different security architecture for every industry. It's to establish core security capabilities that can be consistently applied across OT environments and mapped to evolving regulatory requirements.

EVALUATE YOUR OT MONITORING STRATEGY

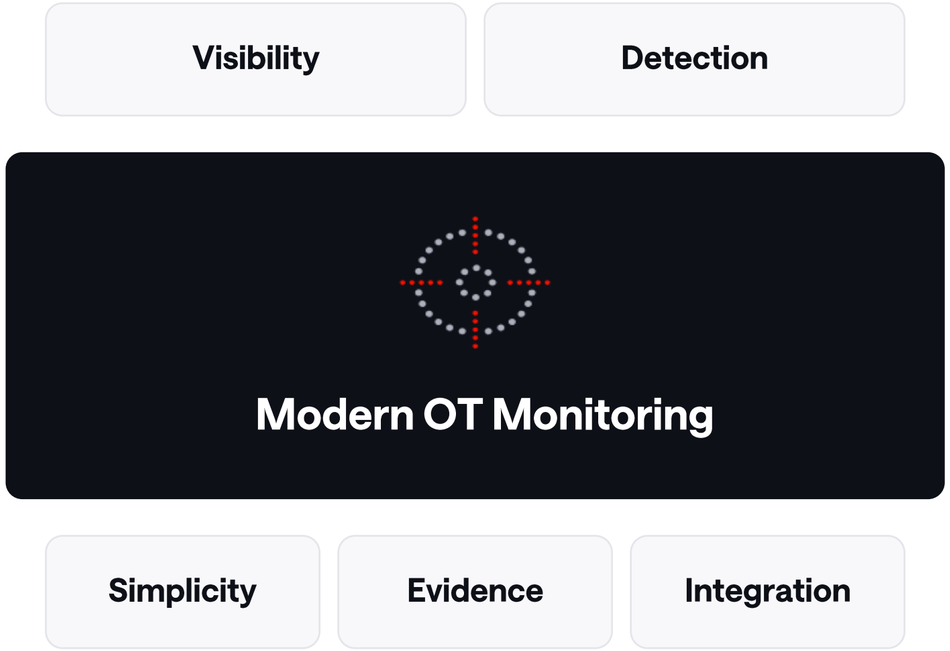
Choosing the Right OT Monitoring Approach

The right technology should strengthen both operational resilience and regulatory compliance.

The security capabilities discussed throughout this guide provide a useful framework for evaluating OT monitoring solutions. Rather than comparing products based on feature lists alone, organizations should focus on whether a solution supports the operational outcomes required by modern OT environments.

When evaluating solutions, consider whether they can deliver:

- Continuous visibility across industrial networks
- Behavior-based threat detection beyond known signatures
- Low operational impact through passive monitoring
- Support for investigations and compliance evidence
- Integration into existing security operations



KEY TAKEAWAY

The best OT monitoring solutions don't just collect data – they help organizations improve visibility, detect threats earlier, and strengthen operational resilience.

For a detailed framework, evaluation criteria, and vendor comparison questions, continue with the **Exeon NDR Evaluation Guide**.

OT COMPLIANCE QUICK CHECK

Is Your OT Environment Ready?

A quick self-assessment to identify opportunities for improving OT visibility, threat detection, and compliance readiness.

Use the following questions as a starting point to assess whether your current monitoring strategy supports the security objectives discussed throughout this guide.

OT Security Readiness Check	✓
Do you maintain continuous visibility across your OT network?	☐
Can you automatically identify new or unmanaged OT assets?	☐
Can you detect abnormal behavior and lateral movement?	☐
Can you investigate incidents using historical network evidence?	☐
Can you demonstrate continuous monitoring during an audit?	☐
Is your OT monitoring integrated into your broader SOC and incident response processes?	☐
Does your monitoring approach have minimal impact on sensitive industrial systems?	☐

What Good Looks Like

Organizations with a mature OT monitoring strategy typically have:

- Continuous, passive visibility across IT and OT
- Behavior-based threat detection
- Fast investigation capabilities
- Audit-ready evidence
- Seamless integration into existing security operations

NEXT STEPS

Whether you're preparing for NIS2, aligning with IEC 62443, or strengthening operational resilience, modern OT monitoring is a foundational capability.

YOUR PATH FROM HERE

OT Compliance Guide (this one)

↓

Self Assessment

↓

Demo / Workshop

↓

NDR Evaluation Guide

↓

Architecture Review / Demo

FURTHER RESOURCES

Continue your OT Security and Compliance Journey

Official References

The following resources provide authoritative guidance on OT cybersecurity, regulatory compliance, and industrial security best practices.

Category	Resource
Regulations & Standards	NIS2 Directive (EU 2022/2555), IEC 62443 Series, BSI KRITIS Guidance
Implementation Guidance	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

Continue Your Evaluation

Ready to assess your OT monitoring strategy? Explore the Exeon.NDR Evaluation Guide for:

- Evaluation criteria for modern NDR solutions
- OT-specific architecture considerations
- Questions to ask vendors
- Practical buyer's checklist

Download the Exeon NDR Evaluation Guide

Let's Talk

Whether you're preparing for NIS2, aligning with IEC 62443, or strengthening your OT security posture, we're happy to discuss your environment and challenges.

Get in touch. Book a meeting to discuss your situation

exeon

exeon.com