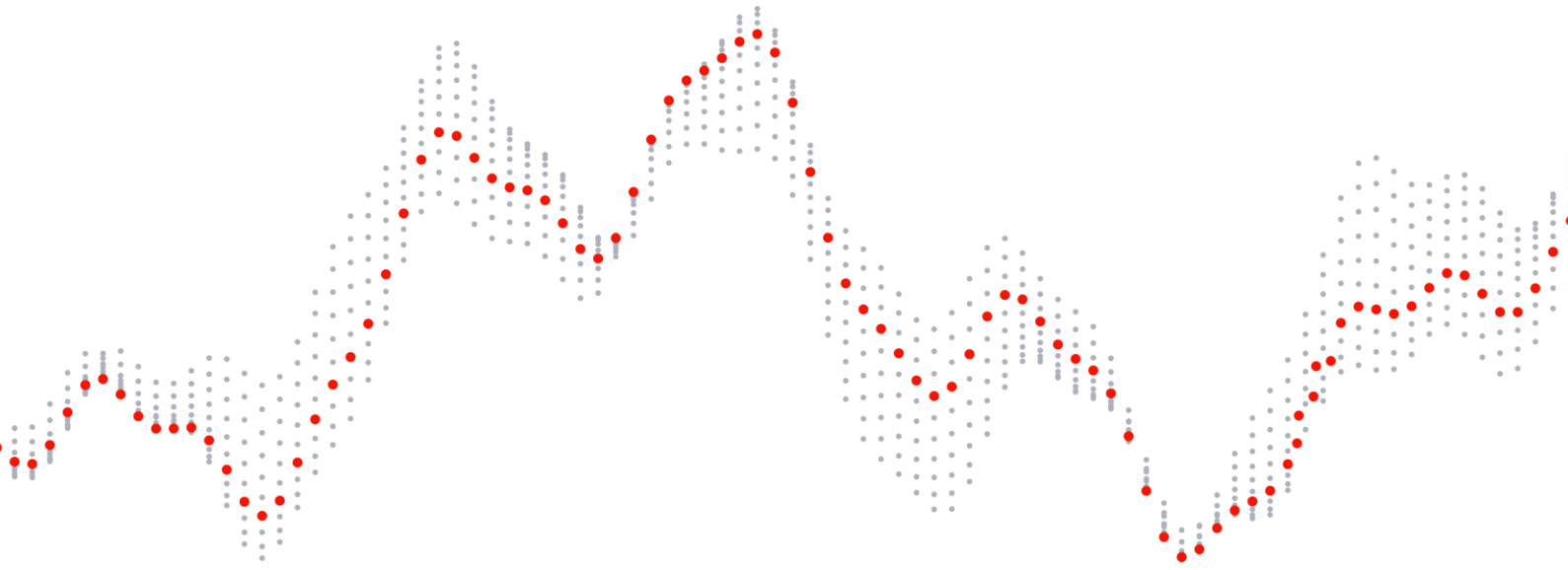
WHITE PAPER

OT Security Without the Overhead

From Compliance Obligation to Operational Resilience

How to close the OT visibility gap, validate segmentation, and operationalize OT security without adding SIEM complexity.



exeon

exeon.com

Table of Contents

Executive Summary 03

1. The Compliance Paradox: Protecting What You Cannot See 06

2. Why OT Security Projects Die in the Planning Phase 09

3. The Lightweight Approach: 90% Visibility in Weeks 12

4. Why OT Security Tools Still Need Operational Context 15

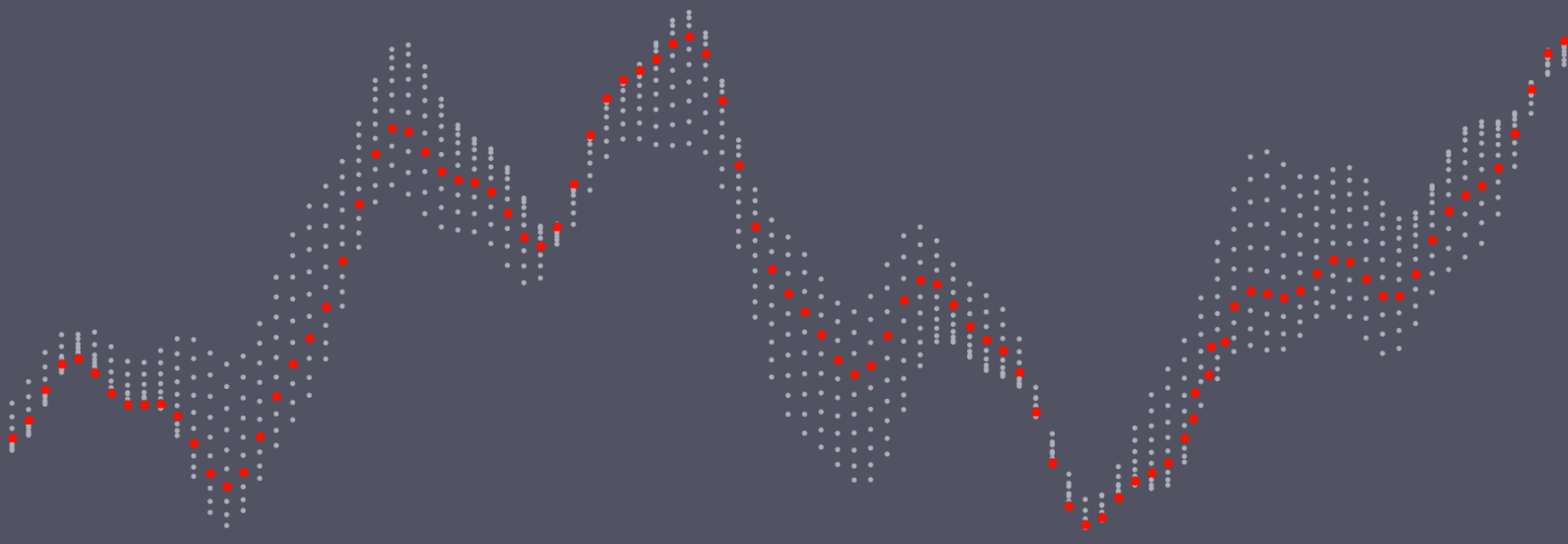
5. Firewall Rules That Lie: Continuous Segmentation Validation 18

6. Who Pushes the Button? OT Incident Response in Practice 21

7. From Compliance to Real Resilience 25

Checklist: Can You Prove OT Resilience? 29

Executive Summary



EXECUTIVE SUMMARY

Operational technology has quietly become one of the most exposed and least understood parts of modern organizations. The systems that run production lines, energy grids, water treatment, hospital infrastructure, and transport networks were designed for availability and longevity, not for a world of converged IT/OT networks, remote maintenance, and regulatory scrutiny.

Today, those same organizations are being asked a question they often cannot answer: Can you prove your OT environment is monitored and segmented? Regulations such as NIS2 and KRITIS increasingly demand evidence of continuous monitoring, asset visibility, and incident readiness. Yet most organizations still lack a reliable inventory of what is actually running in their OT networks, let alone how those systems communicate.

> **This creates a paradox at the heart of OT security: organizations are obligated to protect, segment, and audit systems, they cannot fully see.**

The conventional response – large deployments of firewalls, ZTNA, and other security controls – is often slow, expensive, and operationally disruptive. Many traditional IT security approaches, such as sensor placements and endpoint agents, are not feasible in OT environments due to legacy systems, vendor restrictions, and operational requirements. As a result, many projects stall in the planning phase and never deliver the visibility they promised. This paper argues for a different sequence: visibility first, lightweight and passive, followed by continuous validation of segmentation and a clear, pre-agreed plan for who acts when an incident hits the plant floor.

Even organizations that have invested in OT security platforms often face a second challenge: operationalization. OT security alerts remain fragmented across tools, OT engineers lack a central place to analyze security information, and SOC teams often lack OT context. Traditional SIEMs can be too expensive, too complex, or unsuitable for OT environments. The missing layer is not another OT sensor, but a practical way to consolidate, contextualize, and act on OT security data.

The goal is not perfection. It is resilience you can demonstrate, starting in weeks, not years.

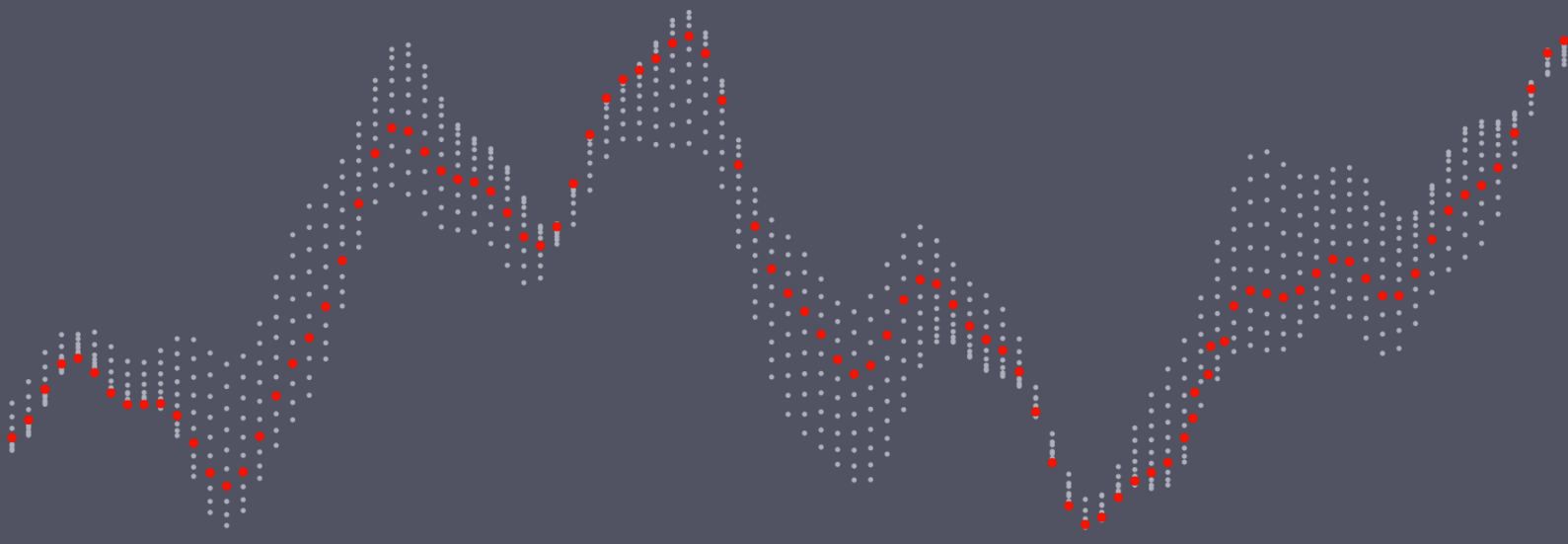
THE NEW BASELINE

The question is no longer "Do you have security controls?“ It is "Can you prove they work – across systems you can actually see?"

01

SECTION 01

The Compliance Paradox: Protecting What You Cannot See



Regulators have moved decisively

NIS2 extends cybersecurity obligations across a far wider set of essential and important entities. KRITIS rules in Germany and equivalent national frameworks impose monitoring and reporting duties on critical-infrastructure operators. DORA brings operational resilience and incident-reporting requirements to the financial sector and its providers. The common thread is evidence: organizations must now demonstrate, not merely assert, that their environments are monitored and that incidents can be detected and reported within tight timeframes.

NIS2 **KRITIS** **DORA**

This is where many OT environments fail before they begin. You cannot report on an asset you have never inventoried. You cannot demonstrate segmentation between zones you have never mapped. You cannot meet a 24-hour incident-notification deadline if you have no baseline of normal behavior to compare against. Compliance assumes a level of visibility that, in practice, most OT environments simply do not have.

Why OT Is Not IT

The instinct of many security teams is to apply the IT security playbook to OT. It rarely survives contact with the plant floor. OT environments have characteristics that make traditional approaches risky or impossible:

- **You often cannot patch.** Many systems run legacy operating systems, certified configurations, or vendor-locked software where a patch voids support or requires recertification.

- **You often cannot scan.** Active scanning and authenticated probes can crash fragile OT systems.
- **You cannot tolerate downtime.** A production line, a substation, or a hospital system cannot simply be taken offline for a security project. Availability is the overriding priority.
- **Lifecycles are measured in decades.** Equipment installed twenty years ago may still be in service, with no security features and no realistic replacement path.

These constraints are not excuses; they are engineering realities. Any credible OT security approach has to start by respecting them rather than fighting them.

> **KEY QUESTION FOR CISOS**
>
> **Could you prove today:**
>
> - What assets exist?
> - How they communicate?
> - Whether segmentation is working?
> - What happened during an incident?

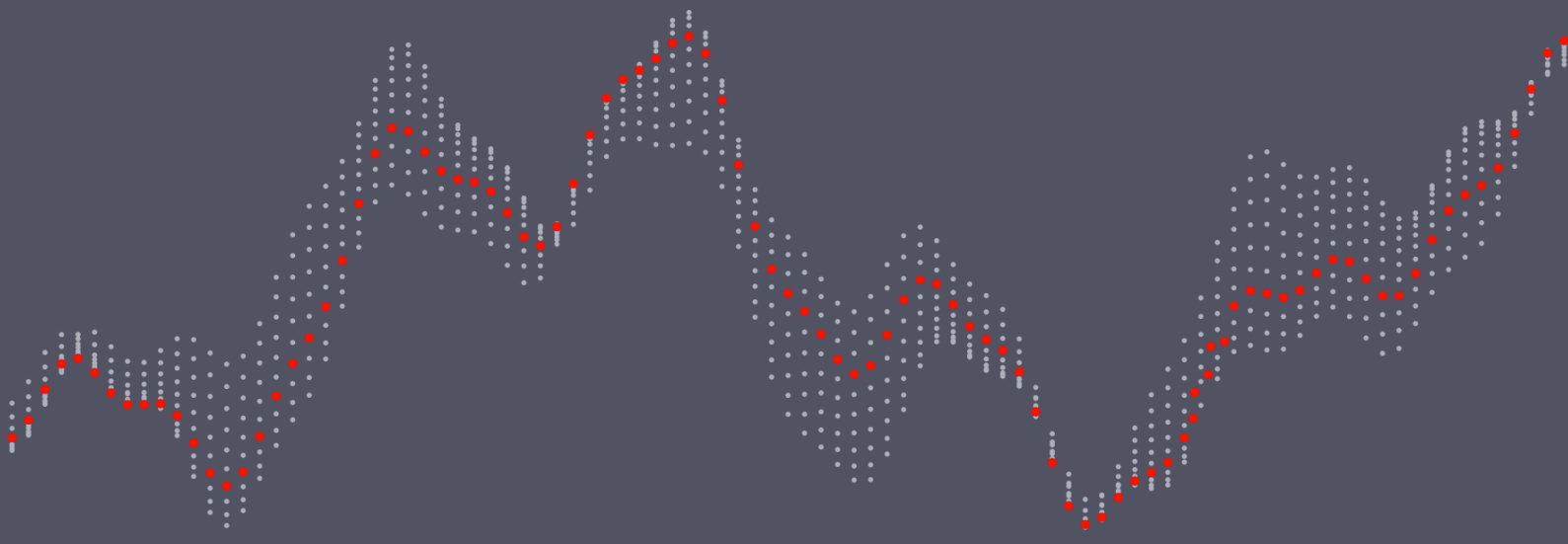
The Reporting Gap

Regulatory reporting requires a baseline. To report a deviation, an anomaly, or an incident, you need to know what normal looks like. Without a map of assets and communication paths, an OT operator confronted with a regulator's question – what happened, when, to which systems, and how did you contain it – is left reconstructing the answer after the fact, under pressure, from incomplete data. The baseline must exist before the incident, not after.

02

SECTION 02

Why OT Security Projects Die in the Planning Phase



SECTION 02

A familiar pattern

Ask almost any OT security leader about their last major initiative and a familiar pattern emerges. The project is scoped ambitiously: full sensor coverage, firewalls at every zone boundary, ZTNA for remote access, agents where they can be deployed. The business case targets near-total coverage. And then the project meets reality.

Sensor-heavy deployments require hardware procurement, network changes, change advisory board approvals, maintenance windows, vendor coordination, and careful testing to avoid disrupting production. Each of these steps takes time, and in OT, each change carries operational risk that must be justified and scheduled. Months pass. Budgets are consumed by planning and integration before any visibility is delivered. Priorities shift. The project that promised 98% coverage in eighteen months is quietly still in planning at month twelve.

KEY INSIGHT

In OT security, perfect is the enemy of good. 80% visibility today is worth more than 98% visibility that never arrives.

The Cost of Waiting

While the comprehensive project stalls, the environment remains largely unmonitored. Shadow OT – unmanaged devices, forgotten remote-access paths, contractor laptops, undocumented connections – continues to accumulate. The blind spots that motivated the project in the first place persist for the entire duration of the planning phase. The pursuit of completeness has, paradoxically, left the organization less secure for longer.

There is a better sequence. Rather than treating visibility as the end-state of a long deployment, treat it as the first, fast, low-risk step – and let what you learn shape the heavier investments that follow.

Start seeing first. Invest second.

TRADITIONAL OT SECURITY PROJECT TIMELINE

Planning	Procurement	Deployment	Integration

✓ Visibility

VISIBILITY-FIRST APPROACH

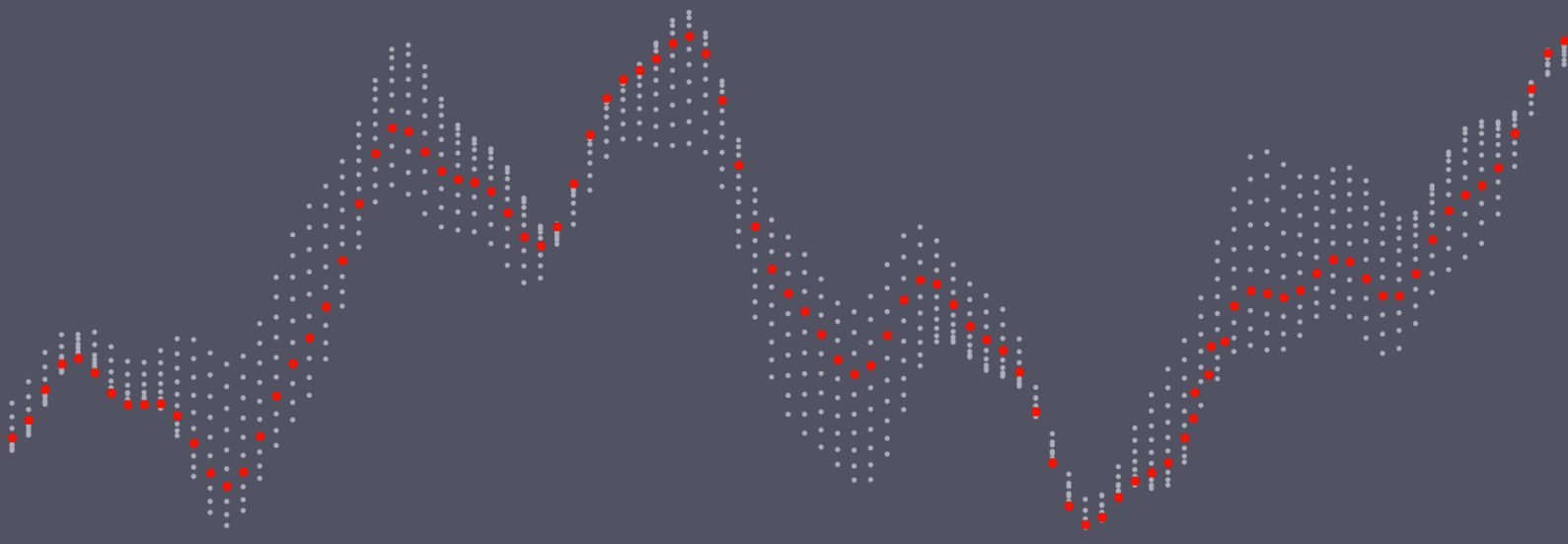
Passive Visibility	Asset Inventory	Segmentation Validation	Targeted Security Investments

✓ Visibility

03

SECTION 03

The Lightweight Approach: 90% Visibility in Weeks



Passive visibility changes the economics

Passive visibility changes the economics of OT security. Instead of deploying intrusive agents or active scanners, organizations can leverage the network telemetry they already have – from firewalls, switches, and existing security infrastructure – to build a comprehensive picture of OT assets and communication flows. By relying on existing data sources rather than introducing new infrastructure, deployment is faster, simpler, and far less disruptive. Nothing is injected into the OT network, resulting in no production impact and effectively zero downtime risk.

From that passively collected metadata, a remarkably complete picture emerges, often within days:

- **Asset inventory:** The devices actually communicating on the network, including ones no spreadsheet ever recorded.
- **Communication flows:** Which systems talk to which, over what protocols, and across which network zones.
- **Shadow OT:** Unmanaged and unexpected assets and connections surface immediately, including remote-access paths that bypass intended controls.
- **Anomalies:** Once a behavioral baseline exists, deviations – new connections, unusual volumes, unexpected external communication – can be detected.

90%

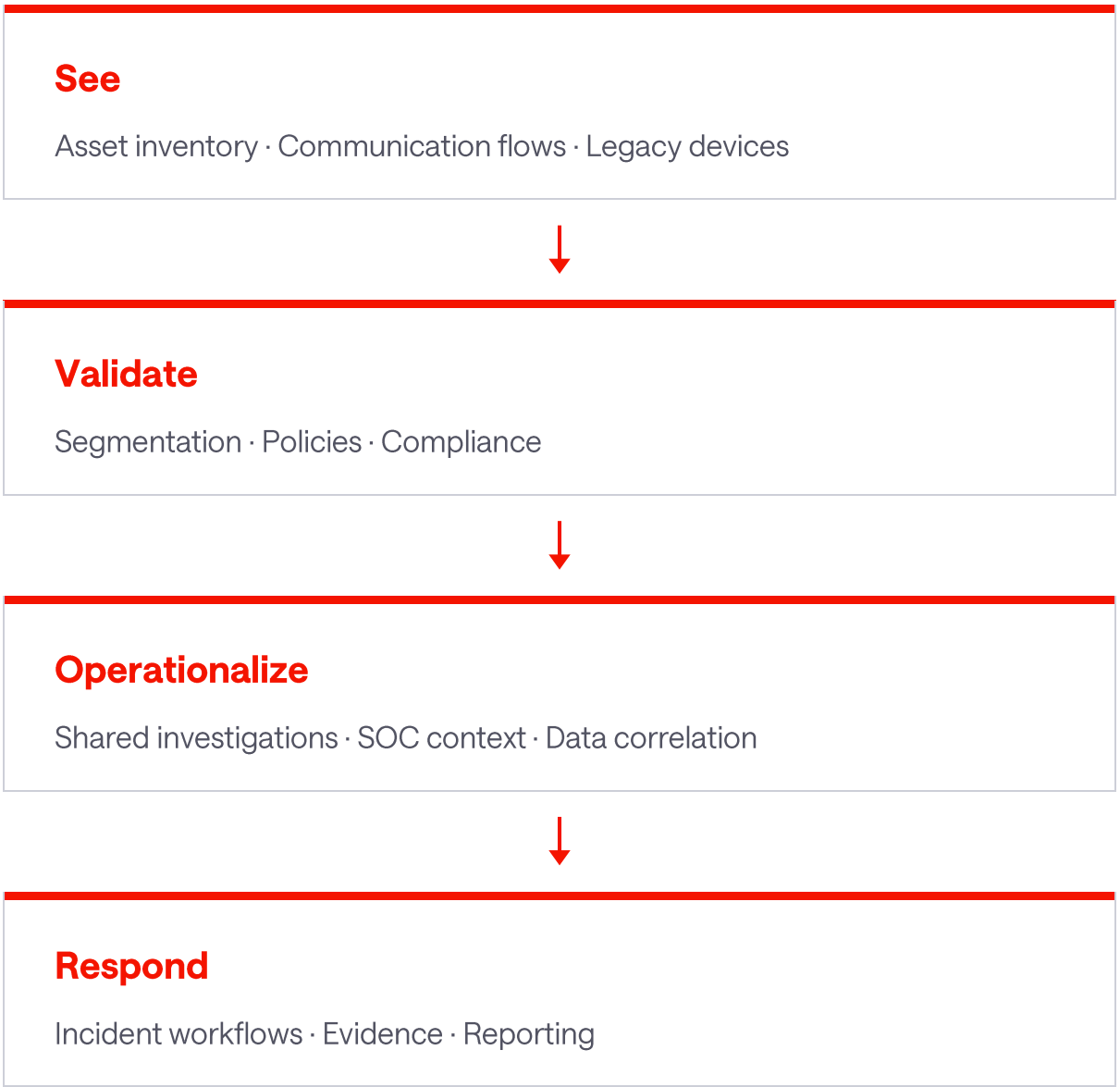
VISIBILITY IN ~2 WEEKS

This is the practical meaning of "90% in two weeks." Instead of waiting months for a perfect deployment, organizations can start reducing risk immediately and expand their security capabilities step by step, investing where visibility indicates the greatest impact.

Visibility as the Foundation, Not the Finish Line

Passive visibility is not a replacement for segmentation, access control, or incident response. It is the foundation that makes all of them achievable and verifiable. You segment based on the communication flows you can now see. You write access policies informed by the dependencies you have actually observed. You detect incidents against a baseline that finally exists. Each subsequent control becomes faster to plan and easier to justify because it is grounded in evidence rather than assumption.

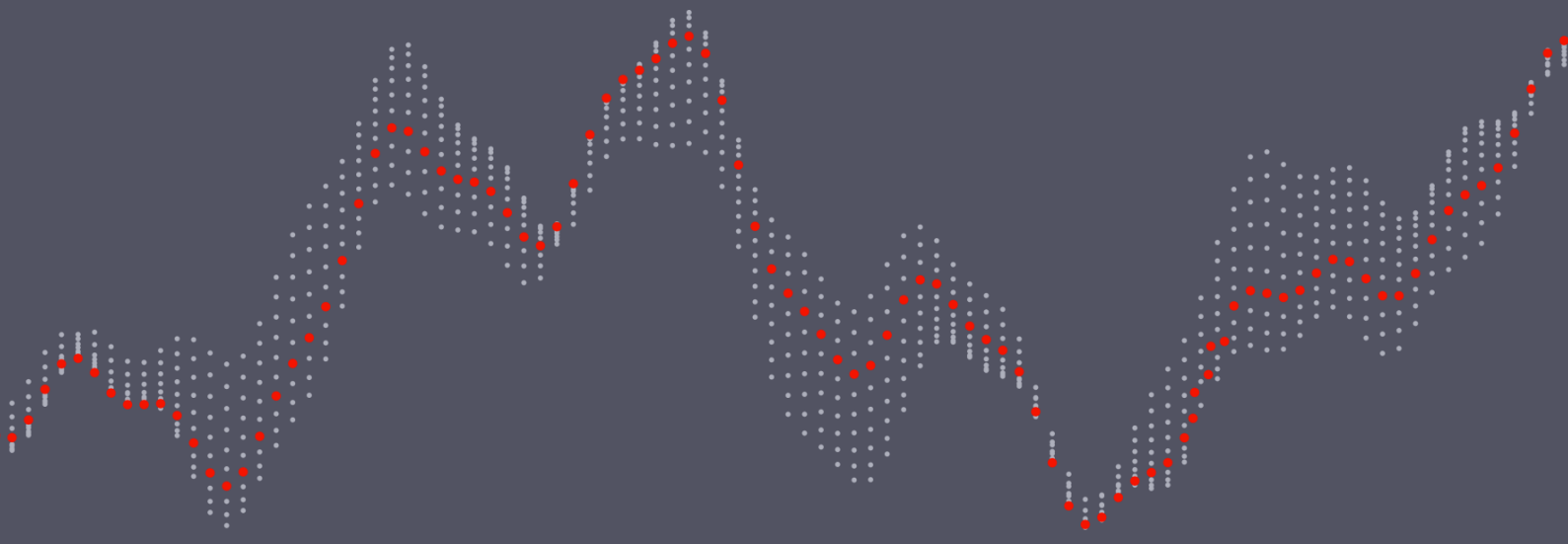
OT Security Maturity Journey



04

SECTION 04

Why OT Security Tools Still Need Operational Context



Neither side has the complete picture

Many organizations have already invested in OT security platforms to improve visibility into industrial assets, protocols, and anomalies. These solutions provide valuable insights and are an essential part of a modern OT security architecture.

Yet visibility alone does not make OT security operational.

Security information is often distributed across multiple platforms: OT IDS, firewalls, switches, remote access solutions, and existing IT security tools. Each provides part of the picture, but none provides the complete operational context needed to investigate incidents, validate controls, or support security operations.

The result is a familiar challenge: OT teams understand the production environment, while SOC teams understand cyber threats. Both have valuable information, but neither has the complete picture.

> **KEY QUESTION FOR SOC TEAMS**
>
> **Can your SOC investigate an OT incident without asking the OT team to manually reconstruct what happened?**

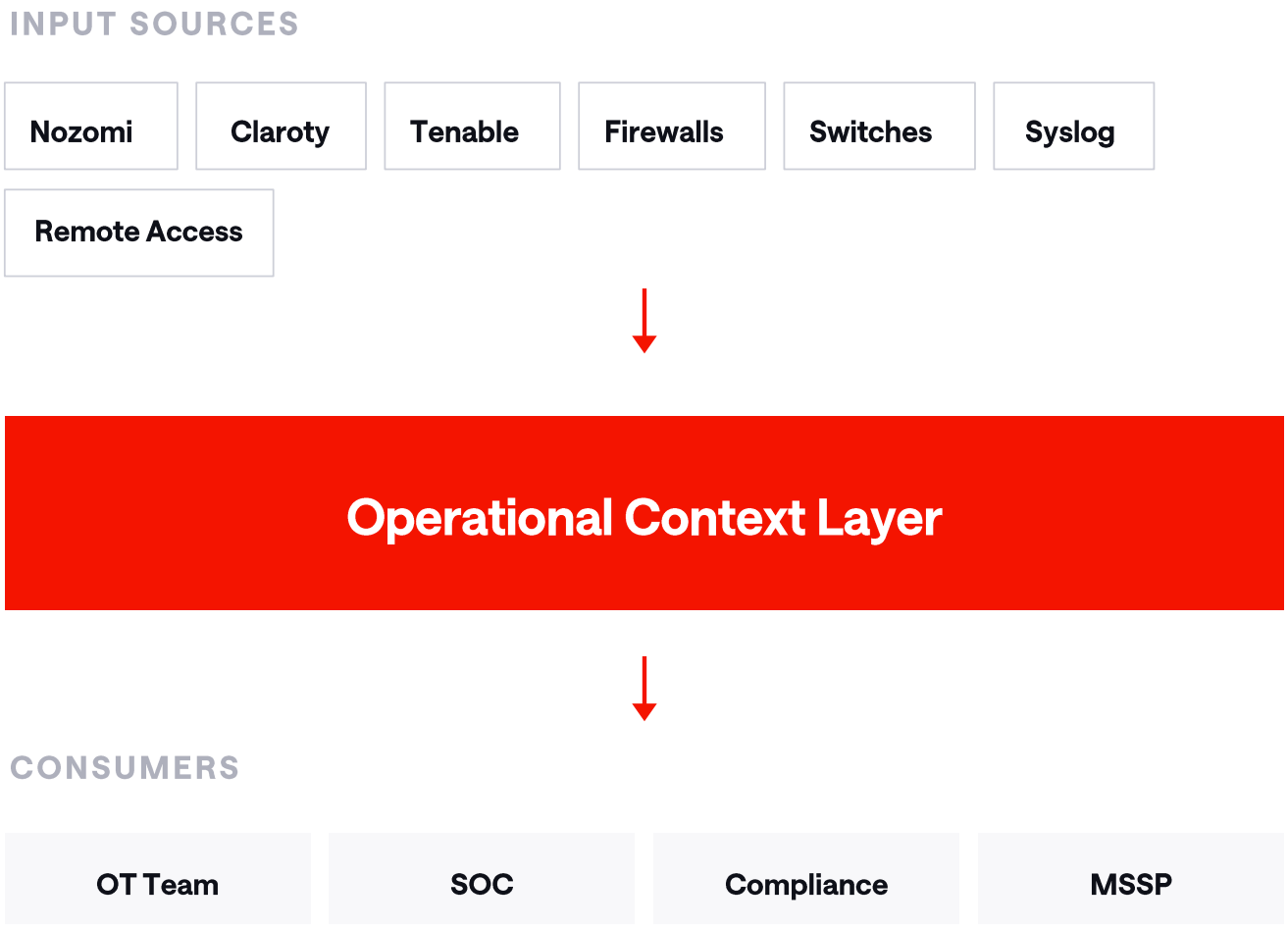
Beyond Detection

A common response is to introduce a SIEM. In many OT environments, however, traditional SIEM platforms prove difficult to justify. They can be expensive to operate, complex to maintain and are often designed around IT-centric workflows rather than the realities of industrial operations.

Operational resilience requires something different: not another monitoring platform, but a way to consolidate existing security information, correlate events across IT and OT, and provide the context needed for investigations and compliance.

> **The objective is not to replace OT security solutions.**
> **It is to help organizations get more value from the ones they already have.**

Connecting what already exists

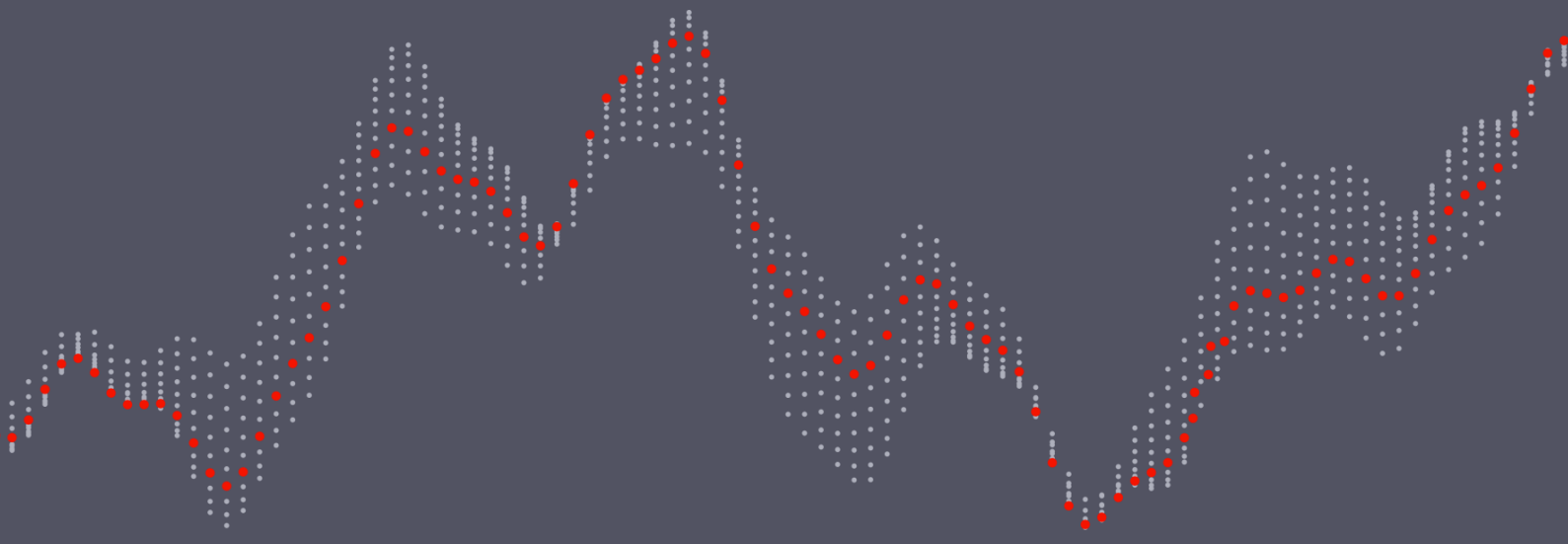


Existing tools generate valuable information. Operational resilience comes from connecting it.

05

SECTION 05

Firewall Rules That Lie: Continuous Segmentation Validation



Segmentation drift

Segmentation is the backbone of OT security architecture: the principle behind the Purdue model, zone-and-conduit designs, and most regulatory expectations. But segmentation has a quiet failure mode: it degrades over time. A firewall rule added for a temporary maintenance window is never removed. An "any-any" rule is created under deadline pressure and forgotten. A new system is connected without updating the policy. The documented architecture and the actual traffic slowly diverge.

This is segmentation drift, and it is dangerous precisely because it is invisible. The network diagram on the wall still shows a clean separation between zones. The reality on the wire tells a different story. An annual audit catches a snapshot; it cannot catch the eleven months of drift in between.

> **A firewall rule describes what is permitted. Network metadata reveals what is actually happening. The gap between them is your risk.**

From Point-in-Time to Continuous

The same passive visibility that builds the asset inventory can continuously validate segmentation. By comparing observed communication flows against intended policy, an organization can answer – at any moment, not just at audit time – whether traffic is crossing zone boundaries it should not, whether prohibited protocols are in use, and whether the segmentation that exists on paper exists in practice. Continuous validation turns segmentation from a static design document into a living, monitored control.

Who Is Allowed to Change What?

Segmentation drift is not only a technical problem; it is a governance one. In most organizations, responsibility for OT network changes is split across teams with different priorities. OT operations owns uptime and the production process. IT security owns the policy and the threat model. Compliance owns the audit trail and the regulatory relationship. When these groups operate without a shared, current view of the network, changes are made in good faith that nonetheless undermine the overall security posture.

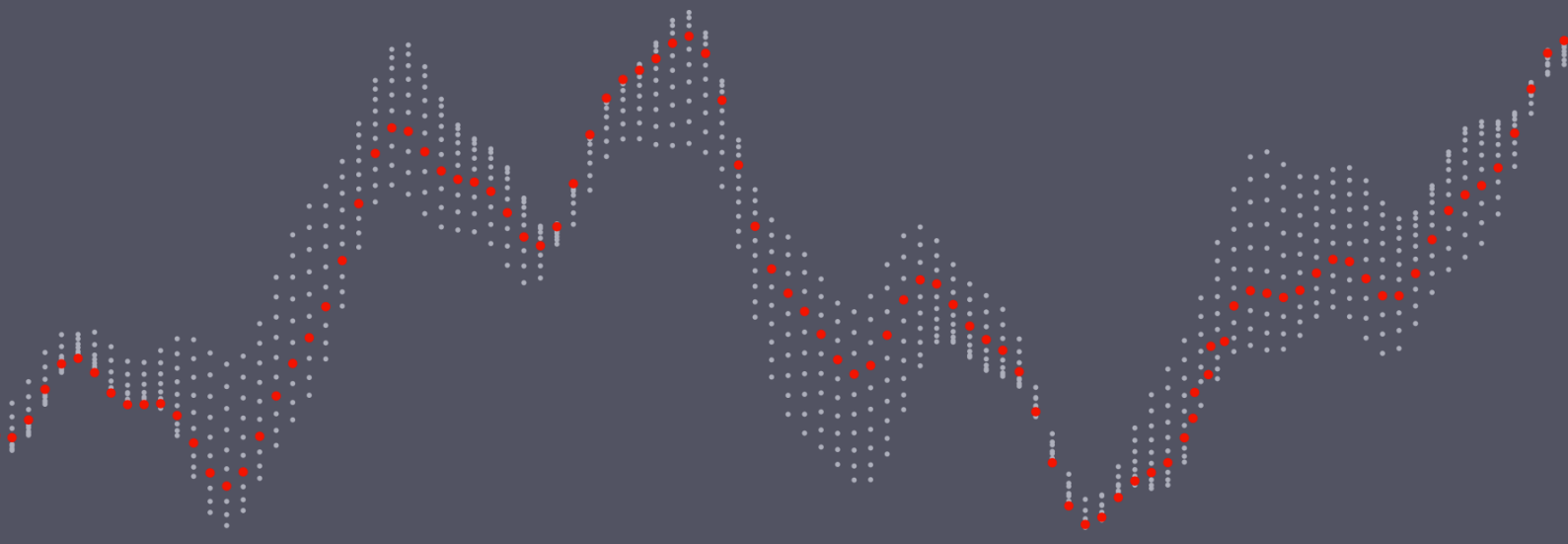
Continuous validation gives all three groups the same source of truth. It makes change visible, attributable, and reviewable, so that the question "who changed what, and was it allowed?" has an answer that does not depend on memory or goodwill.

TEAM	PRIMARY CONCERN	WHAT THEY NEED FROM VALIDATION
OT Operations	Uptime and process continuity	Assurance that changes will not disrupt production
IT Security	Threat model and policy enforcement	Evidence that policy matches reality, continuously
Compliance / Risk	Audit trail and regulatory readiness	Demonstrable, time-stamped proof of control effectiveness

06

SECTION 06

Who Pushes the Button? OT Incident Response in Practice



The containment decision

Every OT security incident eventually reaches a critical operational decision: how can the incident be contained without creating greater operational risk? Unlike in IT, simply isolating an affected system is often not possible. Production dependencies, safety requirements, and supply chain connections may require systems to remain available, even during an investigation. The right course of action depends on the process, the operational context, and the business impact: knowledge that resides with operations, not the SOC.

In OT, the containment decision is not purely a security decision. It is an operational and safety decision that security cannot make alone.

The Hybrid Playbook

Effective OT incident response is inherently hybrid. OT teams understand the physical process, the dependencies, and the safe states. IT security teams understand forensics, threat behavior, and containment technique. Neither can respond well without the other. The organizations that handle OT incidents effectively are the ones that have agreed – in advance, in writing – how the two will work together: who is consulted, who decides, and under what conditions production continuity overrides containment or vice versa.

In many organizations, this collaboration is difficult to achieve. Security operations are often handled by a centralized or external SOC that receives alerts but lacks the OT context needed to assess operational impact. At the same time, OT engineers understand the affected systems but rarely work within SOC processes or investigation tools. This disconnect slows investigations, complicates decision-making, and creates uncertainty at the moments when rapid, coordinated action is most critical.

A Shared Operational Picture

Effective collaboration also requires a shared source of truth. When OT security information is fragmented across multiple platforms, every investigation begins by collecting data from different teams and tools before meaningful analysis can even begin. Providing OT operations, security teams, and external SOC providers with the same operational context helps reduce investigation time, improve decision-making, and ensure that regulatory reporting is based on consistent information rather than manual reconstruction.

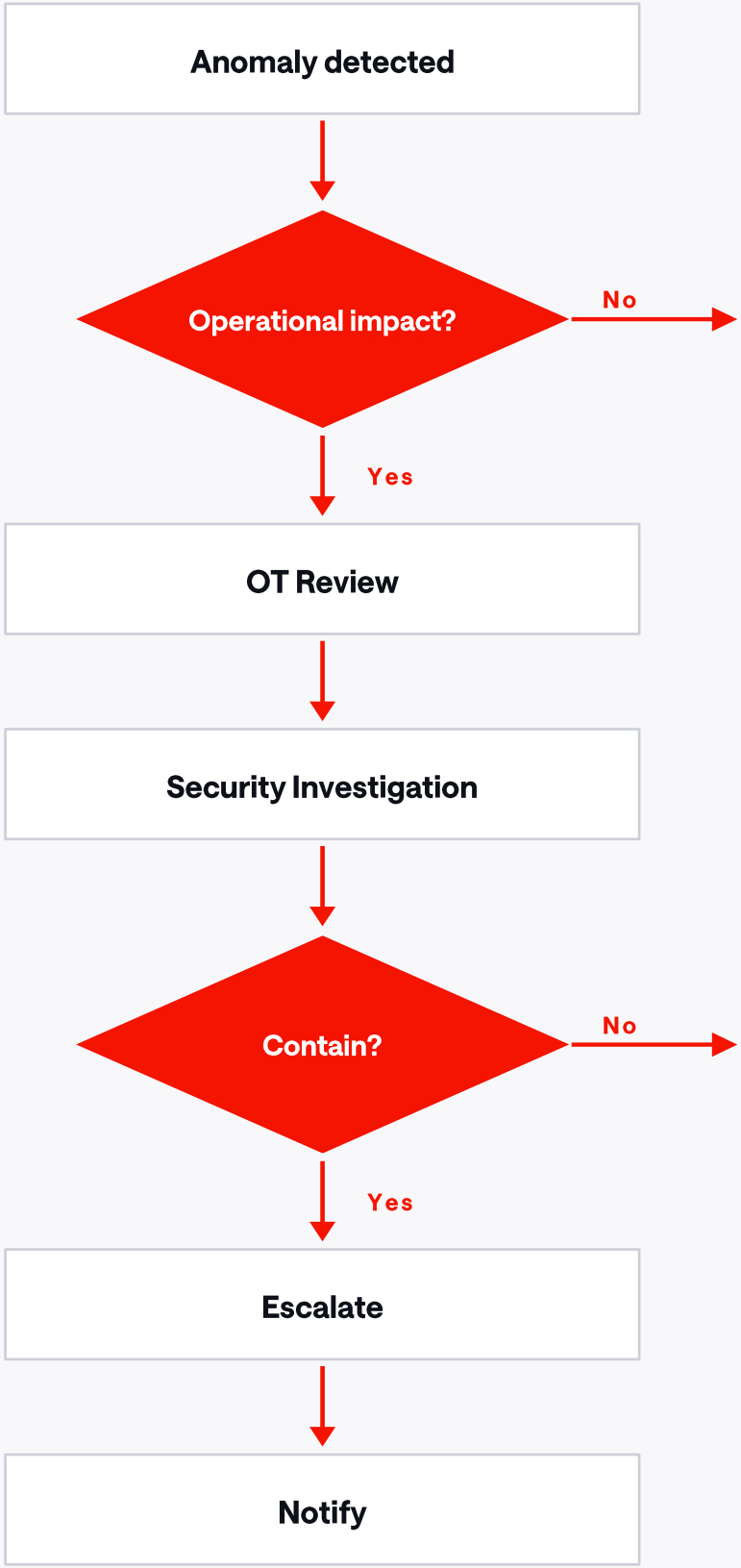
A Clear Escalation Path

Alongside the playbook, incident response needs an unambiguous escalation chain so that the right people are engaged at the right moment, and regulatory clocks are met:

1. Operations detects or is alerted to an anomaly and assesses the immediate operational and safety impact.
2. Security is engaged to investigate, characterize the threat and advise on containment options.
3. OT and security jointly determine the operational consequences before containment actions are taken.
4. Management is brought in for decisions that carry significant operational, safety or business consequences.
5. Regulators are notified within the timeframes mandated by NIS2, KRITIS, or sector rules, which is only possible if the preceding steps produced a clear record.

None of this works without the visibility foundation. An escalation path is only as effective as the information flowing through it. The team that can see assets, communication flows, and anomalies can characterize an incident quickly and escalate with confidence. Without that shared context, even well-defined incident response processes become slower, less coordinated, and more difficult to execute.

INCIDENT DECISION FLOW



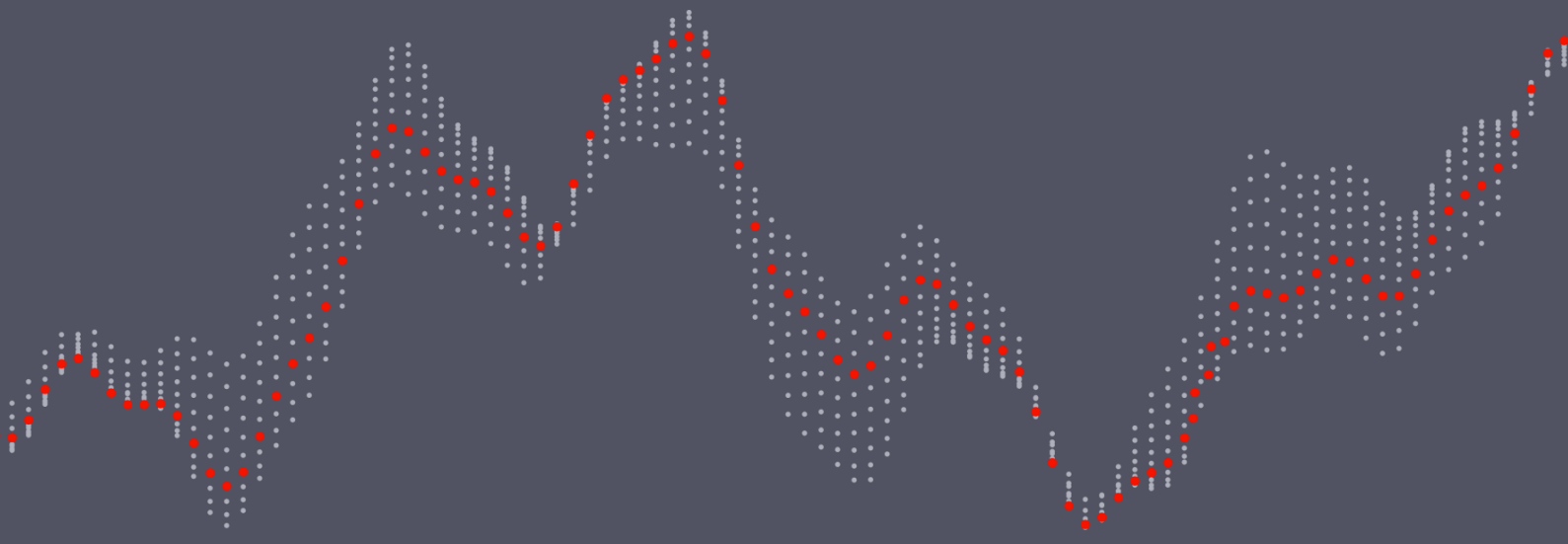
In OT environments, containment is not purely a security decision.

It is an operational and safety-critical decision that security teams cannot make alone.

07

SECTION 07

From Compliance to Real Resilience



A resilience-first sequence

The throughline of this paper is a reordering of priorities. For years, OT security has been approached as a deployment problem: a question of which sensors, firewalls, and agents to install. That framing leads to long projects, high costs, and stalled initiatives, while the underlying blind spots persist. A resilience-first approach inverts the sequence:

See first. Establish broad, passive visibility into assets and communication flows in weeks, with no production impact.

Validate continuously. Compare what is happening against what is permitted, so segmentation is monitored rather than assumed.

Prepare to respond. Agree on the hybrid playbook, escalation path, and shared operational picture before an incident, so OT teams, SOCs, and external providers can act from the same context rather than improvise under pressure.

Then invest deliberately. Use what visibility reveals to target heavier controls – firewalls, ZTNA, agents – where they deliver the most risk reduction.

This sequence does not abandon comprehensive controls; it earns them. It also helps organizations get more value from the tools they already have. OT security platforms, firewalls, and infrastructure telemetry all provide useful signals, but resilience depends on connecting those signals into a shared operational view that teams can investigate, validate, and retain over time.

It produces compliance evidence as a by-product of doing security well, rather than treating compliance as a separate box-ticking exercise. And it delivers something regulators, boards and operators all increasingly demand: resilience that can be demonstrated, starting now.

Resilience isn't another security product. It's the outcome of connecting visibility, validation and operations.

Where Exeon Fits

Organizations do not need to replace their existing OT security investments to improve resilience. In fact, specialized OT security platforms remain essential for capabilities such as industrial asset discovery, protocol analysis and OT-specific threat detection.

The challenge is operationalizing the information these tools produce.

Exeon complements existing OT security solutions by consolidating metadata, firewall logs, OT security alerts and infrastructure telemetry into a shared operational view. This enables OT teams, security operations and compliance stakeholders to investigate incidents with greater context, continuously validate segmentation, retain historical evidence and demonstrate operational resilience.

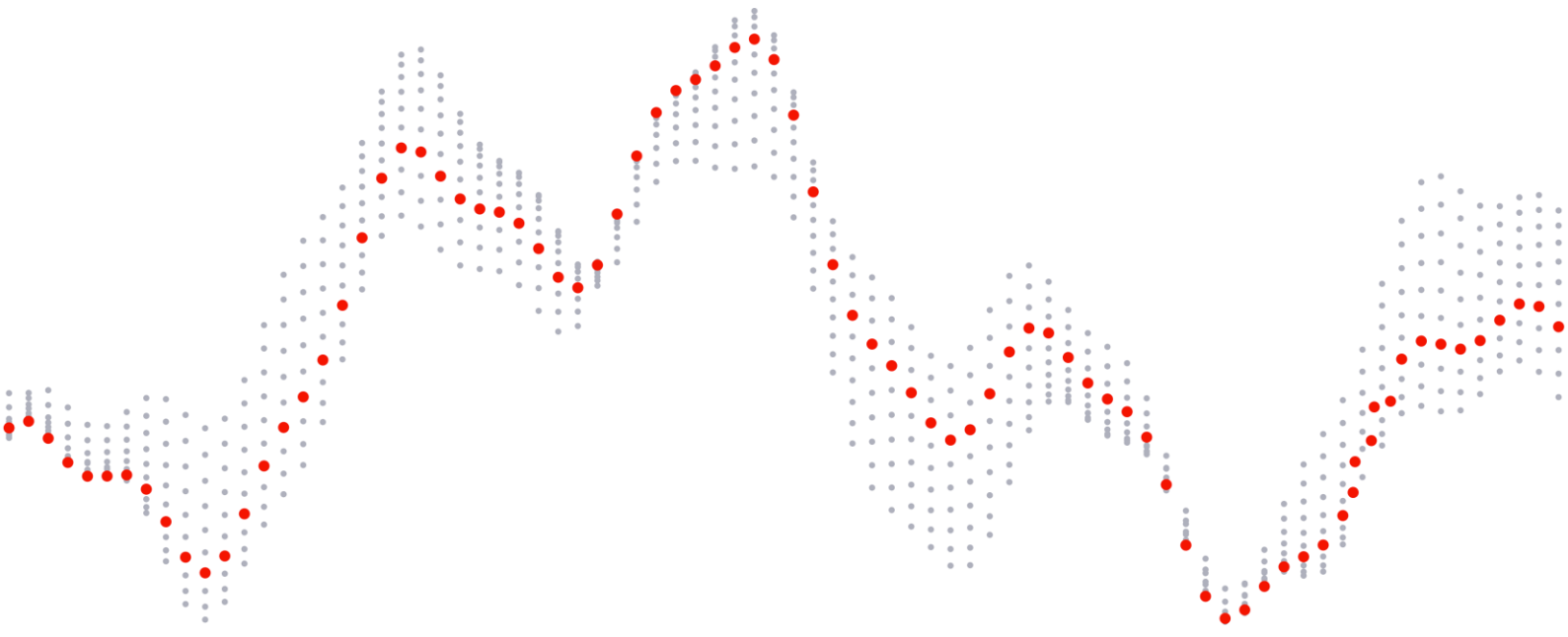
Rather than adding another isolated security platform, Exeon helps organizations connect the information they already have, extend OT visibility into existing security operations, and maximize the value of their existing OT security investments.

The result is a practical, vendor-independent approach to operationalizing OT security: strengthening visibility, collaboration, and resilience while respecting the operational realities of industrial environments.

CHECKLIST

Can You Prove OT Resilience?

- Do you know every communicating OT asset?
- Can you identify unmanaged or legacy devices?
- Can you continuously validate segmentation?
- Can your SOC investigate OT incidents?
- Is OT security information consolidated?
- Can you reconstruct an incident six months later?
- Can you provide evidence for NIS2 or IEC 62443 audits?
- Are OT and IT teams working from the same operational picture?
- Can external SOC providers understand OT alerts?
- Can you start improving visibility without disrupting production?

exeon

exeon.com