An IDC Spotlight, sponsored by Y Cyber
June 2026

Building the OT SOC: 5 Steps to Secure Industrial Operations



Joel Stradling
Senior Research Director
European Security, IDC

IDC

SPOTLIGHT

Sponsored by: Y Cyber

Building the OT SOC: 5 Steps to Secure Industrial Operations

June 2026

Written by Joel Stradling, Senior Research Director, European Security

Introduction

European industrial organizations face increasing cyber risk as IT and OT environments converge. Though greater connectivity improves operational efficiency, it also expands the attack surface and exposes production systems to safety and continuity threats.

Many industrial environments were not designed with cybersecurity as a core requirement. Legacy systems, proprietary protocols, and limited visibility complicate monitoring and response. Traditional IT security operations center (SOC) models, when applied directly to plant environments, will not account for these challenges.

Organizations with industrial operations will require a security operations model that is adapted to OT realities: one that integrates operational context, safety considerations, and production priorities within a mature SOC framework.

AT A GLANCE

KEY TAKEAWAYS

- Traditional IT-centric SOC models do not adequately address the operational, safety, and visibility constraints of industrial environments, requiring more context-aware detection and response approaches.
- An OT-native SOC model combines asset intelligence, operational risk alignment, and converged IT/OT processes while preserving industrial-specific response logic.
- Skills shortages, legacy complexity, and regulatory pressure are accelerating the shift toward centralized, scalable OT SOC models capable of supporting industrial resilience across European enterprises.

Benefits: Why an OT-native SOC model matters

An OT-native SOC model aligns detection and response with the constraints of industrial environments. The approach minimizes the risk that cybersecurity actions, such as password changes or altering policy, inadvertently disrupt production, affect industrial physical systems, or introduce physical safety hazards. In industrial settings, maintaining safe and stable process operations is paramount. A way to achieve this is by ensuring security decisions consider process stability, control logic, and real-time operational conditions. Correlating cyber events with asset criticality enables decision-making based on operational risk rather than technical severity alone. An additional benefit of the OT-native SOC is far tighter coordination between cybersecurity and engineering functions, which enables more consistent, context-aware incident response across industrial sites.

Trends: The European industrial security context

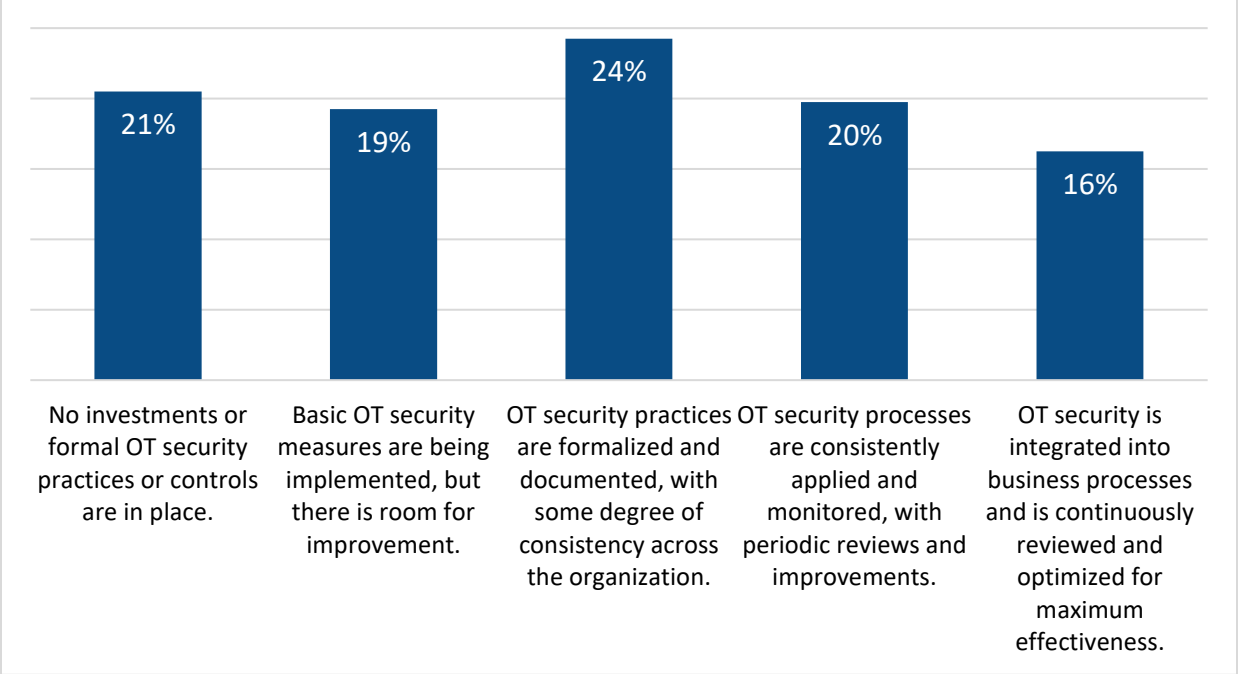
Most industrial organizations have progressed in integrating IT and OT, gaining benefits for operational management. However, there can be a side effect: IT/OT convergence can raise cyber risk. The risk is compounded by Industry 5.0 initiatives, the adoption of Industrial Internet of Things (IIoT) technologies, and the increasing use of edge computing. Increased connectivity to enterprise networks, cloud platforms, and third parties improves efficiency, but it also expands the attack surface.

Industrial processes are tightly linked across sites and supply chains, meaning a cyber incident can directly affect production continuity and safety, and cyber risk in OT environments is closely tied to operational resilience.

At the same time, organizations face structural constraints, including insufficient OT cybersecurity skills and many environments relying on legacy systems with limited native security capabilities.

Figure 1 shows that OT security maturity remains uneven, with fewer than one in five organizations reporting full integration into business processes. This variable maturity makes it difficult to apply traditional IT-centric security models directly to industrial environments, driving the need for the OT-native SOC.

FIGURE 1: OT security maturity in Europe



Source: IDC Europe's *Security Technologies and Strategies Survey*, 2025

Why the IT SOC model does not translate to OT

Traditional IT SOC models are designed for environments where visibility is standardized, assets are homogeneous, and response actions have limited or no physical consequences. Industrial environments operate under fundamentally different technical and operational constraints. Many businesses feed OT data into the SOC, but interpreting cyber events is typically through an IT lens, creating gaps.

- **Visibility gap**. Many OT environments rely on legacy programmable logic controllers (PLCs), distributed control system (DCS), and control systems that were not designed for continuous security monitoring. The use of proprietary protocols, limited endpoint instrumentation, and passive monitoring requirements constrain the availability and granularity of telemetry. Even when IT SOCs ingest OT data, detection models developed for enterprise IT cannot be directly applied to industrial processes without adaptation.
- **Response constraints**. In IT environments, isolating a system or blocking traffic is often a routine containment measure. In OT environments, such actions can interrupt production or introduce safety risks. False positives may therefore have physical consequences, and strict operational and maintenance schedules often limit intervention windows. Effective security responses must therefore be carefully coordinated with engineering teams and a deep understanding of process dependencies.
- **Data diversity**. Industrial security operations require correlation across multiple data types, including traditional IT logs, OT network traffic, control system events, physical process telemetry, badge access systems, and environmental signals. Interpreting alerts requires operational context that goes beyond traditional IT monitoring practices.

Applying a traditional IT SOC model directly to OT environments, or extending it without adopting an OT-native approach, can introduce operational friction, increase the likelihood of inappropriate response actions, and leave residual risk unaddressed. Effective OT security operations require a dedicated model that accounts for industrial visibility limitations, response constraints, and the critical importance of maintaining safe, stable production processes.

Five steps to building an OT SOC for industrial resilience

The following five steps outline a structured approach to establishing an OT SOC model that supports cybersecurity objectives while reinforcing industrial resilience.

Step 1. Industrial asset intelligence and passive visibility

An OT SOC requires accurate and continuous visibility into industrial assets. Many environments lack a reliable inventory of PLCs, human-machine interfaces (HMIs), engineering workstations, and network components. Continuous asset discovery provides the foundation for monitoring.

Monitoring should understand industrial protocols. Industrial communications differ from traditional IT traffic and require contextual interpretation based on device behavior and process activity. In addition to asset and network visibility, it is critical to incorporate visibility over key physical process parameters such as pressure, temperature, flow rates, and system states. These parameters provide essential context for determining whether a cyber event is influencing the process's physical and dynamic behavior.

Visibility mechanisms should remain non-intrusive. Passive inspection techniques are essential in environments where active scanning may disrupt operations or interfere with control processes.

OT telemetry, including both cyber and physical data, should be integrated into the broader SOC framework to provide a unified view while preserving industrial context.

Step 2. Operational risk alignment

An OT SOC should move beyond a compliance-driven approach and focus on operational risk. While regulatory alignment remains important, detection and response priorities must reflect the potential impact on production continuity, safety, and business operations.

Cyber events should be evaluated in relation to asset criticality and their role within industrial processes. This enables security teams to distinguish between events with limited operational significance and those that could disrupt core production functions.

Monitoring strategies should reflect system criticality. Assets supporting safety-critical or high-value production processes require enhanced scrutiny.

Safety considerations must be embedded into cyber-incident handling. Response actions should account for how systems interact with physical processes and must follow controlled change procedures. Close coordination with engineering and operations is essential to ensure decisions are both technically sound and operationally feasible.

Step 3. OT-centric detection and validation

Detection engineering in OT environments must incorporate both cyber indicators and process-aware logic. Traditional IT cyber protection is poorly suited to connecting dots when deviations in industrial process behavior are, in fact, the key indicators of initial cyber compromise.

Frameworks such as MITRE ATT&CK for ICS provide a useful foundation for aligning detection with known industrial attack techniques, including unauthorized remote access, control logic manipulation, and lateral movement across segmented networks.

Critically, effective detection in OT environments should be based on rules that link anomalies in network or system behavior to deviations in variables such as pressure, temperature, or process states.

More advanced approaches can model the industrial process as a multidimensional state vector, combining cyber telemetry and physical measurements. Machine learning algorithms can then be applied to detect deviations from expected process behavior.

Validation remains essential. Detection use cases and correlation models should be tested in controlled environments before deployment. Poorly tuned rules or models can generate false positives with potential operational consequences.

Step 4. Unified IT/OT security operations

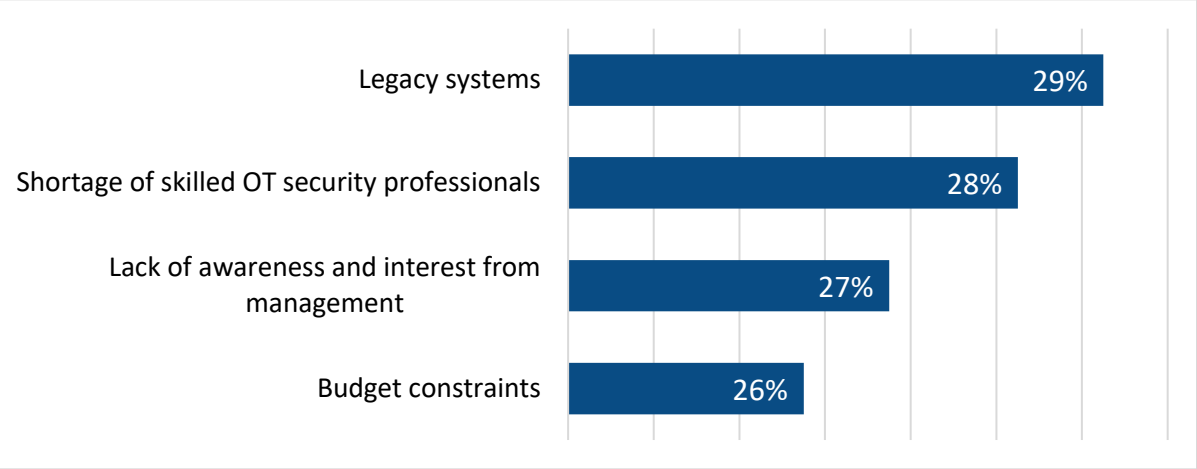
IT and OT environments need to be managed together. A unified service model supports shared governance, tooling, and reporting while maintaining domain-specific processes.

Incidents should follow a common life cycle, enabling consistent escalation, tracking, and communication across domains. Information sharing enhances visibility and reduces duplication of effort during investigations.

However, response procedures must remain differentiated. IT-centric containment actions cannot be applied directly to OT systems without evaluating their impact on physical processes and production stability.

As highlighted in Figure 2, structural challenges (e.g., limited OT cybersecurity expertise and legacy system complexity) reinforce the need for centralized, scalable, and context-aware operating models.

FIGURE 2 Primary barriers to implementing OT security measures



Source: IDC Europe's *Security Technologies and Strategies Survey*, 2025

Step 5. Scaling the OT SOC with automation and AI

As monitoring capabilities expand, manual analysis becomes increasingly unsustainable. Automation plays a key role in improving correlation, prioritization, and operational consistency.

In environments with low signal-to-noise ratios, structured prioritization mechanisms help focus analyst attention on events with real operational impact. Guided investigation workflows support consistent triage, particularly where OT-specific expertise is limited.

The integration of AI and machine learning techniques further enhances detection capabilities, particularly when applied to combined cyber-physical datasets. By analyzing both network activity and process variables, these techniques can identify subtle deviations in system behavior that may indicate emerging threats or process anomalies.

Documented playbooks, correlation rules, and analytical models reduce dependency on individual expertise and support repeatable operations. However, automation must be carefully designed to respect industrial constraints, ensuring that all actions align with production requirements and approved change management processes.

Vendor profile

Y Cyber operates as part of HWG Sababa, a European cybersecurity services provider with established SOC infrastructure and industrial security capabilities. The company supports industrial and regulated-sector organizations seeking to integrate operational technology monitoring into broader security operations frameworks.

Y Cyber's service model includes managed detection and response, OT-focused monitoring, industrial assessments, incident response, and advisory services aligned with established industrial security frameworks, built on its HyperSOC™ SOC-as-a-Service platform. Its client base includes enterprises operating complex and distributed environments where production continuity and regulatory alignment are strategic priorities.

The company operates a 24 x 7 security operations capability designed to monitor both IT and OT environments within a unified framework. The operational model follows a tiered structure, combining real-time monitoring and triage with deeper investigation, threat analysis, and coordinated remediation processes. This structure is intended to provide centralized oversight while supporting domain-specific escalation paths.

Within industrial environments, Y Cyber emphasizes asset visibility, protocol-aware monitoring, and context-driven incident handling. Its OT SOC capability is designed to collect and analyze telemetry from industrial systems and correlate it with enterprise security data. This approach aims to provide cross-domain visibility while preserving operational context.

Y Cyber also supports organizations through OT security assessments, onboarding of industrial components into monitored environments, and structured validation of detection logic before production deployment. These services are positioned to address the visibility gaps and response constraints commonly found in plant environments.

Y Cyber is headquartered in Europe (Italy) and operates globally, with offices across Europe, the Middle East, and Central Asia, supporting OT customers in multiple countries worldwide. It serves organizations subject to evolving regulatory requirements and sector-specific security frameworks. Its positioning emphasizes combining centralized SOC processes with OT-specific expertise to support industrial resilience. Y Cyber's model aligns with the broader industry's shift toward converged yet operationally aware security operations. Its integration of industrial telemetry, structured incident workflows, and scalable monitoring enables the company to support enterprises in strengthening their cybersecurity oversight across IT and OT domains without compromising production realities.

Challenges

The managed detection and response (MDR) and OT SOC markets are becoming more competitive as global providers and regional specialists expand into converged IT/OT monitoring. This increases competitive pressure, particularly in Europe, where regulatory requirements are accelerating demand for industrial cybersecurity services.

Pricing pressure is also emerging as enterprises compare managed SOC offerings based on cost, automation, and service levels. Providers must balance operational efficiency with continued investment in detection engineering and domain expertise.

Scaling OT-specific talent remains a structural constraint. Industrial cybersecurity skills are limited, and maintaining expertise in control systems while expanding services is not easy.

As IT and OT monitoring models converge, providers must ensure industrial expertise is not diluted. While unified SOC models can improve efficiency, industrial environments still require detection and response approaches adapted to production constraints.

Conclusion

Industrial cybersecurity cannot rely solely on traditional IT security models. OT environments operate under different constraints, where detection and response decisions can directly affect production and safety. This requires monitoring and response approaches that account for the industrial context.

At the same time, IT and OT security are becoming more closely integrated. While this can improve visibility and efficiency, it should not come at the expense of industrial specificity. Detection, escalation, and response processes must remain adapted to plant environments.

Providers that combine OT expertise with mature SOC capabilities are well-positioned to support industrial organizations. The ability to integrate asset visibility, detection, and scalable operations will increasingly differentiate providers in the OT SOC market.

Y Cyber's approach reflects this direction, with a focus on converged, yet OT-aware, security operations aligned with the needs of industrial environments.

About the analyst



Joel Stradling, *Research Director, European Security*

As senior research director for IDC's European Security practice, Joel Stradling leads the content and analyst team for tracking the European security segment. His main focus areas include zero-trust network architecture (ZTNA), managed security services, and cyber risk and resiliency. Stradling has 22 years of experience as a cybersecurity analyst, international managed enterprise networks, and IT services. He is a regular speaker at major industry conferences about security and privacy, digital trust, and managed security services in B2B enterprise services. Joel is a well-known and highly regarded expert in the industry, offering insight and advice to C-level executives on security technology competitive landscapes and evolving security market segments, including managed security services, ZTNA, cloud security, risk and compliance, endpoint, identity and access management, IT/OT security, secure IoT and 5G, and secure operations.

MESSAGE FROM THE SPONSOR

As industrial environments become increasingly interconnected, cybersecurity requirements are evolving beyond traditional IT-centric approaches. Organizations operating in OT and critical infrastructure contexts require security operations models that account for production constraints, safety considerations, and limited visibility across industrial assets. Y Cyber, part of the HWG Sababa Group, provides security operations capabilities designed to address these challenges. Its model integrates IT, OT, and IoT monitoring within a unified framework, combining centralized SOC processes with domain-specific expertise in industrial environments. Built on the HyperSOC™ SOC-as-a-Service platform, this approach supports continuous visibility, structured detection engineering, and validation of exposure across complex environments. This enables organizations to improve detection accuracy, align response with operational priorities, and strengthen overall resilience. Learn more about Y Cyber: https://y-cyber.com/

IDC Custom Solutions

The content in this paper was adapted from existing IDC research published on www.idc.com.

IDC Research, Inc.
One Beacon Street
Suite 33100
Boston, MA 02108, USA
T 508.872.8200
F 508.935.4015
blogs.idc.com
www.idc.com

IDC Custom Solutions produced this publication. The opinion, analysis, and research results presented herein are drawn from more detailed research and analysis that IDC independently conducted and published, unless specific vendor sponsorship is noted. IDC Custom Solutions makes IDC content available in a wide range of formats for distribution by various companies. This IDC material is licensed for external use, and in no way does the use or publication of IDC research indicate IDC's endorsement of the sponsor's or licensee's products or strategies.

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications, and consumer technology markets. With more than 1,300 analysts worldwide, IDC offers global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries. IDC's analysis and insight help IT professionals, business executives, and the investment community make fact-based technology decisions and achieve their key business objectives.

©2026 IDC. Reproduction is forbidden unless authorized. All rights reserved. CCPA