



PRUDENT

AI-Powered OT SOC for Manufacturing

Building Continuous Visibility, Threat Detection
and Cyber Resilience Across Industrial Operations

Manufacturing environments are becoming increasingly connected. Production systems, industrial control systems, engineering workstations, connected devices, remote access technologies, enterprise applications and cloud platforms now exchange data across what were once clearly separated environments.

This transformation improves visibility, automation, and operational efficiency. It also changes the security equation.

As Information Technology (IT) and Operational Technology (OT) converge, a compromise that begins with a corporate identity, endpoint or application can potentially move toward systems responsible for production processes. At the same time, OT environments continue to operate with legacy assets, specialized protocols, long equipment lifecycles and strict availability requirements.

This makes **manufacturing OT security** fundamentally different from conventional enterprise cybersecurity.

The objective is no longer limited to identifying whether an asset is vulnerable. Security teams need continuous visibility into industrial environments, the ability to understand whether activity is normal for a production process, and the capability to investigate and respond without disrupting safety or operations.

That is where an **OT Security Operations Center (OT SOC)** becomes strategically important. An OT SOC brings together OT visibility, industrial threat detection, threat intelligence, security analytics, incident investigation and response through a model designed around the realities of industrial operations. With AI and automation increasingly integrated into security operations, organizations can further improve alert prioritization, anomaly detection and analyst efficiency.

This guide examines the changing manufacturing threat landscape, the IT/OT visibility gap, the security requirements across manufacturing environments, the architecture of an OT SOC, and the role of managed services such as **SOC-as-a-Service** and **MDR for OT security**.



Manufacturing Threat Landscape

Why OT security has become an operational priority

Manufacturing organizations are no longer operating isolated production environments. Industrial networks increasingly connect with enterprise IT, Industrial Internet of Things (IIoT) platforms, cloud analytics, remote maintenance systems and third-party technologies. These connections create valuable operational capabilities, but they also expand the number of pathways through which attackers can access industrial environments.

The threat is particularly significant because an OT incident can have consequences beyond data loss.

A successful attack may affect production availability, equipment reliability, product quality, safety, supply chain continuity or the ability of plant personnel to operate critical processes. The business impact can therefore extend from cybersecurity into operations.

Common threat scenarios include ransomware moving from enterprise networks into plant environments, compromised remote access, credential abuse, malicious or unauthorized changes to engineering systems, exploitation of vulnerable legacy assets, and supply chain compromise.

The challenge is not simply more attacks. It is a more interconnected risk.

Traditional IT security programs are generally designed around endpoints, users, applications, networks and data. "OT environments introduce another dimension".

the physical process:

A security event involving a PLC, HMI, SCADA server or industrial network cannot always be evaluated only from a cybersecurity perspective. Analysts also need to understand whether the activity corresponds to a legitimate engineering action, scheduled maintenance activity, a process change or potentially malicious behavior.

This is why operational technology threat analysis services require a different level of context.

An effective approach must connect security telemetry with asset criticality, communication patterns, industrial processes and operational conditions.

From monitoring to industrial threat detection

"Manufacturers increasingly need security operations that can answer questions such as"

- Which assets are communicating across the OT environment?
- Is the communication expected for that asset and process?
- Has a device suddenly changed its normal behavior?
- Is a remote connection legitimate?
- Which alerts represent genuine operational risk?
- Could an incident in IT affect OT operations?

These questions form the foundation of modern OT security services.

The objective is not simply to generate more alerts. It is to identify meaningful threats earlier, understand their operational significance and support a response that protects both cybersecurity and business continuity.

The IT/OT Visibility Gap

One of the biggest barriers to effective **OT cybersecurity services** is incomplete visibility. Manufacturing organizations may have security technologies deployed across enterprise IT, endpoints, networks and cloud environments while still having limited understanding of what is happening inside production networks.

OT environments often contain a mixture of PLCs, RTUs, DCS platforms, HMIs, SCADA systems, engineering workstations, sensors, industrial switches and other specialized technologies. Many assets may have long operational lifecycles and may not support conventional security controls. Some systems cannot be patched frequently. Some use proprietary or industrial protocols. Others were designed primarily for reliability and availability rather than security monitoring.

As a result, simply extending an existing IT monitoring model into the plant may leave important gaps.

Why conventional visibility is not enough

A manufacturing SOC may receive thousands of events from enterprise systems, yet still lack the telemetry necessary to understand what is happening at the operational layer. This creates several challenges.



Asset visibility gaps

make it difficult to maintain an accurate picture of what is connected to the environment.



Context gaps

make it harder for analysts to distinguish normal industrial activity from suspicious behavior.



Skill gaps

arise when cybersecurity analysts lack experience with industrial processes, OT protocols and operational constraints.



Response gaps

occur when generic IT playbooks are applied to environments where a poorly timed response can affect production.

These challenges explain why OT **cybersecurity** cannot be answered simply by describing another layer of network protection.

OT cybersecurity is the practice of protecting the systems, networks, devices and processes that support physical and industrial operations while maintaining their availability, integrity and safety.

Bridging IT and OT without treating them as identical

IT and OT security need to work together, but they do not necessarily need identical controls or response procedures.

A modern security model should provide

- **Shared visibility** across relevant IT and OT activity.
- **Logical separation** that limits unnecessary exposure between environments.
- **OT-aware monitoring** that understands industrial protocols and asset behavior.
- **Risk-based prioritization** that considers asset criticality and operational impact.
- **Defined response procedures** involving security, engineering, plant and vendor stakeholders.

This is the foundation for an OT SOC that can operate as a central security capability while respecting the realities of distributed manufacturing environments.

OT Security Across “Five Manufacturing Segments”

The need for OT security is common across manufacturing, but the risk profile is not identical from one production environment to another.

Different manufacturing segments operate different combinations of industrial control systems, automation technologies, connected equipment, process environments and third-party ecosystems.



Automotive and Mobility Manufacturing

Automotive plants depend heavily on connected production lines, robotics, programmable controllers, industrial networks and engineering systems.

Security priorities include protecting production continuity, controlling remote access, securing interconnected manufacturing equipment and detecting unusual activity across highly automated production environments.



Pharmaceuticals and Life Sciences Manufacturing

Pharmaceutical manufacturing places strong emphasis on process integrity, product quality and controlled production environments.

Cybersecurity must therefore protect the systems supporting production processes while maintaining traceability, availability and reliable operations. Unauthorized changes to control environments can create consequences that extend beyond conventional IT risk.



Chemicals and Process Manufacturing

Chemical manufacturing relies on process control systems where changes to operating parameters can have significant operational and safety implications.

OT security programs need strong visibility into control networks, engineering activity, asset behavior and communication patterns, supported by response procedures that account for process safety.



Food, Beverage and Consumer Manufacturing

Highly distributed facilities and connected production equipment can create a broad attack surface across plants and supply chains.

Organizations need scalable approaches to industrial OT cybersecurity services that can maintain consistent visibility and security operations across multiple sites while accounting for differences in equipment and plant architecture.



Discrete and Industrial Manufacturing

Discrete manufacturing environments often combine multiple production lines, automation platforms, industrial endpoints and engineering systems from different vendors.

Security teams must be able to identify assets, understand communication relationships and detect abnormal behavior without interfering with production processes.

A common requirement across every segment

“Although the technologies differ, the fundamental requirement remains the same”

Manufacturers need continuous awareness of what is happening across their operational environment and the ability to determine which activity represents genuine risk. That requires more than periodic assessment.

It requires an operating capability that combines **OT security services, continuous monitoring, industrial threat detection, threat analysis and response.**

What a Modern OT SOC Needs to Deliver

An OT SOC should not be viewed simply as a room of analysts watching security dashboards.

It is an operating capability that brings people, processes, technology and industrial context together to continuously protect operational environments.

A mature OT SOC should support five connected outcomes.

1. Continuous OT Visibility

The first requirement is an accurate understanding of the environment.

This includes asset discovery, network visibility, communication mapping and awareness of systems across the industrial environment.

Passive monitoring is particularly important because security visibility needs to be established without unnecessarily affecting production.

2. Industrial Threat Detection

OT security monitoring must identify both known threats and deviations from expected industrial behavior.

This can include suspicious remote access, unauthorized communication, unusual protocol activity, abnormal device behavior and indicators associated with known OT attack techniques. AI and machine learning can strengthen this capability by establishing behavioral baselines and highlighting anomalies that may otherwise be difficult to identify through static rules alone.

3. Contextual Alert Prioritization

A security alert is not automatically a business-critical incident.

An OT SOC must determine the relevance of an event by considering the affected asset, its operational role, the production process, historical behavior and the potential impact of the activity.

This is where AI-assisted analysis can help analysts reduce noise, correlate related events and focus attention on higher-risk activity.

4. OT-Specific Investigation and Response

Response procedures must account for operational constraints.

Generic IT playbooks may recommend isolation or shutdown actions that are inappropriate for a production environment. OT response therefore requires defined escalation paths, site contacts, engineering involvement, vendor coordination and controlled containment procedures.

The objective is to contain threats while protecting operational continuity and safety.

5. Continuous Improvement

An effective OT SOC should learn from every investigation.

Detection rules, playbooks, threat intelligence, asset context and response procedures need to be continuously refined based on new threats, operational changes and lessons from incidents.

This creates a shift from reactive monitoring toward measurable security maturity.

What are the best practices for OT security?

At a foundational level, strong OT security practices include accurate asset visibility, network segmentation, passive monitoring, vulnerability management, industrial threat intelligence, OT-aware detection, defined incident response procedures and continuous coordination between IT security and plant operations.

These practices provide the foundation. The OT SOC turns them into a continuous operating model.

OT SOC Architecture Connecting the Plant to Security Operations

An effective OT SOC architecture must create visibility without compromising the environment it is designed to protect.

The architecture typically connects plant-level systems, industrial network monitoring, security controls, centralized analytics and response workflows through carefully controlled data flows.

At the plant level, OT environments may include field devices, sensors and actuators, PLCs, RTUs, DCS systems, HMIs, SCADA platforms and engineering workstations.

These systems connect through industrial networks and controlled zones into higher operational and enterprise layers.

A secure architecture begins with segmentation

Network segmentation helps limit unnecessary communication between enterprise and operational environments and restricts the ability of an attacker to move laterally.

Firewalls, industrial DMZs, controlled conduits and access policies can be used to establish defined communication paths.

Visibility is established through OT-aware telemetry

Industrial IDS, network monitoring tools and passive discovery technologies can observe communications without actively interacting with sensitive production devices.

Telemetry can then be normalized and forwarded to the security operations environment for correlation and analysis.

Analytics add operational context

“A modern architecture can combine”

- **Industrial IDS and network monitoring** for OT-specific visibility.
- **SIEM capabilities** for centralized correlation and investigation.
- **Threat intelligence** for known industrial threats and indicators.
- **AI and behavioral analytics** for anomaly detection and prioritization.
- **SOAR and workflow automation** for controlled response processes.

Asset and vulnerability information for understanding the criticality and exposure of affected systems.

This architecture allows security operations teams to move beyond isolated alerts and understand relationships between assets, events and potential attack paths.

AI becomes an operational force multiplier

AI should not replace OT expertise or autonomous decision-making where operational safety is involved.

Its value is in helping security teams process more information effectively.

AI can support alert triage, event correlation, anomaly detection, investigation assistance, threat prioritization and playbook recommendations. It can also help analysts connect historical activity with current events to accelerate root cause analysis.

This is particularly valuable in environments where specialist OT security talent is limited. The result is a security architecture designed not simply to observe manufacturing environments, but to create continuous, contextual and actionable visibility.

Managed OT Security SOC-as-a-Service and OT MDR

Not every manufacturing organization has the resources, specialist skills or operating model required to establish a fully dedicated OT SOC internally.

Distributed plants, multiple technology vendors, long equipment lifecycles and shortages of OT cybersecurity specialists can make internal capability difficult to build and sustain. This is where managed security models become valuable.

SOC-as-a-Service

SOC as a Service provides organizations with access to security monitoring, analytics, investigation and response capabilities without requiring them to build every element internally.

For manufacturing organizations, the model can extend beyond traditional IT monitoring by incorporating OT telemetry, industrial threat detection and OT-specific response workflows.

A managed SOC model can help organizations establish

- Continuous security monitoring
- Centralized event correlation
- Alert triage and investigation
- Threat intelligence integration
- Incident escalation
- Reporting and security visibility
- Detection and use-case tuning
- Ongoing operational support

The value is not simply outsourcing monitoring. It is extending security capability with a repeatable operating model.

MDR for OT Security

MDR for Operational Technology Security adds a more active detection and response capability.

OT MDR can combine continuous monitoring with threat investigation, threat hunting, contextual analysis and coordinated incident response.

For manufacturers, this is particularly important because the service must understand the difference between a conventional cybersecurity event and an event that may affect an industrial process.

An effective OT MDR model should therefore connect central security teams with plant personnel, engineering teams and relevant technology or equipment vendors.

Managed OT security should extend capability, not create another silo

The strongest operating models establish clear relationships between the manufacturer, its internal security organization and its service provider.

The objective is a coordinated security function where roles, escalation paths, response authority and communication procedures are defined in advance.

Choosing an OT security vendor

Manufacturers evaluating an OT security vendor, OT security company or one of the top operational technology security providers should look beyond the technology stack.

Relevant evaluation areas include



OT expertise

Understanding of industrial environments, processes and protocols.



Security operations maturity

Ability to continuously monitor, investigate and respond.



Technology integration

Ability to work across existing IT and OT security technologies.



Response capability

Defined procedures for operationally sensitive incidents.



Scalability

Ability to support multiple plants and evolving environments.



Service model

Clear responsibilities between the provider, security team, engineering teams and site operations

The right partner should function as an extension of the organization's security capability, rather than operate as a disconnected monitoring function.

OT Assessment to Continuous Security The Prudent Approach

A sustainable OT security program begins with understanding the environment before attempting to transform it.

An OT assessment provides the foundation for this process by establishing visibility into assets, architecture, security controls, operational dependencies and existing monitoring capabilities.

The goal is not simply to identify vulnerabilities.

It is to understand where security gaps intersect with operational risk.

From assessment to action

A practical OT security journey can be structured around four stages.

Assess

Establish a clear view of the OT environment, assets, connectivity, security controls, vulnerabilities, visibility gaps and operational constraints.

Prioritize

Map identified risks against asset criticality, business impact and operational exposure to determine where security improvements will create the greatest value.

Strengthen

Implement the required combination of architecture improvements, segmentation, monitoring, detection, threat intelligence, response procedures and security operations

Operate

Maintain continuous monitoring, threat detection, investigation, response and optimization through an appropriate internal, managed or hybrid operating model.

Building an OT SOC that fits the manufacturing environment

There is no single OT SOC design that works for every manufacturer.

Some organizations may require dedicated internal capabilities. Others may benefit from a hybrid model that combines internal security teams with managed services. Distributed manufacturers may require a centralized operating model capable of maintaining visibility and coordination across multiple plants.

The architecture and operating model should therefore be shaped around the organization's production environment, risk profile, technology landscape and security maturity.

Prudent's approach to OT security

Prudent approaches OT cybersecurity as an operational resilience discipline rather than a standalone technology deployment.

The focus is on connecting security visibility, industrial threat detection, security operations and response into a model that supports the realities of manufacturing.

This includes helping organizations move from fragmented visibility toward a more structured OT security capability, supported by assessment, monitoring, threat detection, managed security operations and continuous improvement.

The objective is straight forward

Know what is happening across the industrial environment. Understand what matters. Detecting meaningful threats earlier. Respond safely. Keep operations resilient.

Ready to strengthen your manufacturing OT security?

Manufacturing security cannot stop at the enterprise network.

As IT and OT become increasingly connected, organizations need security operations that understand both the cyber environment and the operational processes that depend on it.

From **OT security assessment** and industrial threat detection to **SOC-as-a-Service**, **managed SOC services** and **MDR for OT security**, the right capability can help manufacturers build continuous visibility and a more resilient security operation.

**Secure the plant.
Strengthen the operation.
Build OT resilience.**

