

7 Questions Manufacturing Leaders Should Ask Before Choosing an OT Security Operations Model

A practical decision guide for evaluating internal SOC extension, technology-only, MDR/MSS, and managed OT SOC models.



In This Guide

- The Four Operating Models
- 7 Questions to Guide Your OT Security Decision
- Operating-Model Assessment Worksheet
- Validate Before You Decide
- Final Readiness Checklist
- Determining the Right OT Security Approach

Manufacturing organizations rarely start an OT security decision with a blank sheet of paper. They may already have an enterprise SOC, invested OT monitoring technology, an MDR or MSS provider, or be weighing a dedicated managed OT SOC as connected plants and remote access expand.

This guide focuses on the operating model decision behind those technology and provider choices. It examines what each approach requires and how it affects security coverage, internal staffing, technology investment, production risk, scalability, and accountability.

The real question is: which operating model can deliver the OT security capability the organization needs while remaining sustainable across its manufacturing environment?

This guide provides seven questions to help manufacturing leaders evaluate four common approaches which are Internal SOC Extension, Technology-Only, MDR/MSS, and Managed OT SOC. The objective is to determine which approach best fits the organization's OT environment, internal capabilities, risk tolerance, and operational requirements.



The Four Operating Models

Each approach delivers OT security differently and places different demands on your organization.

How it works

What the model requires

	Internal SOC Extension Existing IT SOC expands into OT.	OT Expertise Additional Analyst Capability OT-specific Processes Production Coordination
	Technology-Only Technology provides visibility/detection while internal teams respond.	Internal 24/7 response capability OT Expertise Ownership of Investigation
	MDR / MSS Third party provides monitoring and response.	Clear Integration With Plant Operations Sufficient Ot-Specific Capability From The Provider
	Managed OT SOC Dedicated OT-focused security operations capability.	Defined Collaboration With Internal Security Operations Teams Specialized OT Capability Supplied As Part Of The Model.

The right choice depends less on what a model promises on paper and more on whether the organization can supply what that model requires.

7 Questions to Guide Your OT Security Decision

1. How much OT security expertise do we actually have in-house?

Having an experienced IT security team does not automatically mean having OT security expertise. OT environments carry long asset lifecycles, legacy technologies, specialized protocols, safety considerations, and production dependencies that change how security events must be interpreted and handled.

The question is whether existing personnel have the OT-specific knowledge to distinguish meaningful security activity from normal industrial behavior and to understand the operational consequences of taking action.

Ask:

- Do our security analysts understand the OT environment they are monitoring?
- Can they interpret industrial protocols and asset behavior?
- Do they understand which systems are operationally or safety critical?
- Do we have enough OT expertise across all shifts, not just during business hours?
- How will that expertise be maintained as the environment changes?

Decision signal

If the capability depends on a small number of OT specialists, determine whether the chosen model can provide sustainable coverage rather than relying on individual expertise.

2. Can our current SOC monitor and investigate OT environments effectively?

Adding OT data to a security platform does not necessarily make an organization capable of operating an OT security function. Visibility is only useful when someone can interpret what it means.

An enterprise SOC may already have SIEM, SOAR, EDR, threat intelligence, and established incident-response processes. But OT introduces different asset types, communication patterns, operational dependencies, and response constraints. The question is whether the existing SOC can turn OT telemetry into informed decisions.

Ask:

- Can our SOC distinguish normal industrial activity from suspicious behavior?
- Can analysts investigate OT alerts in their production context?
- Do existing workflows account for OT asset criticality?
- Can the SOC coordinate effectively with plant engineering and operations?
- What additional training, staffing, tooling, or processes would be required?

Decision signal

If the organization can collect OT telemetry but lacks the capability to consistently investigate it, technology alone will not close the operational gap.

3. What happens when an OT threat is detected outside normal IT operating hours?

A security model should be evaluated against the moment it is most likely to be tested: when an incident occurs and the right people are not immediately available.

Manufacturing operations often extend beyond the hours covered by corporate security teams. A model that works during a weekday pilot may look very different during an active incident overnight or on a weekend.

Ask:

- Who receives and triages OT alerts outside business hours?
- Who has the authority to escalate an OT incident?
- Who can engage in plant engineering or operations?
- What happens when an alert requires immediate investigation?
- Is coverage genuinely aligned with plant operating requirements, or does it depend on business-hours staffing with after-hours escalation?

Decision signal

Look beyond a “24/7” label. Determine whether the people responsible for OT detection, investigation, escalation, and response are actually available when the plant needs them.

4. How much OT-specific technology do we need to buy, integrate, and maintain?

Technology is only one component of an operating model. An organization choosing an internal or technology-led approach may need to account for deployment, integration, tuning, maintenance, analyst workflows, training, and ongoing administration, not simply the initial purchase.

Ask:

- What OT visibility and detection technologies are required?
- Who will deploy and maintain them across plants?
- Who will tune detections and investigate alerts?
- How will OT data integrate with existing security operations?
- What staffing and training costs sit alongside the technology investment?
- Which responsibilities remain internal after implementation?

Decision signal

Compare the full operating burden — not just technology cost — including staffing, expertise, integration, maintenance, training, and ongoing ownership.

5. Can the model scale across plants, sites, and increasingly connected OT environments?

A model that works for one plant is not necessarily a model that works for an enterprise. Manufacturing organizations often operate plants with different equipment generations, network architectures, production processes, and security maturity levels.

A scalable operating model must accommodate differences between plants without multiplying security complexity, staffing requirements, or operational overhead.

Ask:

- Can the model be extended consistently across multiple plants?
- How much additional staffing is required as sites are added?
- Can the approach accommodate different OT architectures and asset inventories?
- Does each new site require significant redesign or specialist effort?
- How will the model support increasing connectivity between OT, IT, cloud, and remote environments?

Decision signal

Evaluate scalability based on the operating model, not simply whether the technology can technically be deployed at another site.

6. Who determines whether a security action is operationally acceptable?

OT security decisions do not happen in isolation from production. When a security action could affect operations, the operating model must define who has authority to assess and approve that action - a distinct question from who owns the security function overall.

Actions that are routine in IT, such as isolating a system, stopping a process, or blocking communication, can have very different consequences in a manufacturing environment.

Process safety determinations belong with the appropriate operational and engineering functions, with security teams contributing rather than holding sole authority. The operating model needs to make clear who is involved before an action that could affect production or safety-critical systems is taken.

Ask:

- Are plant engineering and operations involved before actions that could affect production or safety-critical systems?
- Are response procedures designed specifically for OT?
- Can the security team distinguish between containment options based on operational impact?
- What happens when security urgency conflicts with production continuity?
- Is there a documented, joint sign-off process for high-impact actions?

Decision signal

A mature model does not treat production constraints as an obstacle to security. It incorporates them into detection, investigation, escalation, and response.

7. Who is accountable across the Security Lifecycle?

This is the question that most exposes the real difference between operating models.

Technology can generate alerts. Providers can monitor them. Internal teams can own response. Plant engineering can control operational systems. But if ownership is unclear, an incident can move between teams without anyone having clear responsibility for the outcome.



Ask:

- Who owns initial detection and alert triage?
- Who investigates suspicious OT activity?
- Who decides when an event becomes an incident?
- Who coordinates with plant operations and engineering?
- Who has authority to recommend or initiate containment?
- Who owns post-incident improvement?
- Which responsibilities remain internal even when monitoring is outsourced?

Decision signal

The more telling measure of a model is what it leaves the organization responsible for, beyond what it simply provides.

Operating-Model Assessment Worksheet

Rate how much of each capability the operating model provides, rather than how desirable the model is.

1 = Significant internal capability required **2 = Mostly internal capability required** **3 = Shared capability**
4 = Mostly provided by the model **5 = Capability largely provided by the model required**

Dimension	Internal SOC Extension	Technology-Only	MDR / MSS	Managed OT SOC
 OT Visibility				
 Detection & Response				
 OT Expertise				
 Operational Impact				
 Scalability				
 Accountability				

The strongest operating model is the one whose capability requirements and accountability structure match the organization's actual ability to operate them.

Validate Before You Decide

Five questions to test whether the model will work in practice.

A successful OT security model needs to remain effective after deployment — across changing production environments, new connected assets, personnel changes, and real incidents. Before committing, make sure the organization can answer each of these clearly

- 01 **Who sees the event?** Is there reliable OT visibility and continuous monitoring?
- 02 **Who understands the event?** Can someone interpret the activity in its production context?
- 03 **Who decides what happens next?** Are escalation and response responsibilities explicit?
- 04 **Who can act safely?** Are the right operational and engineering functions involved in that call?
- 05 **Who owns improvement?** Does someone remain accountable for reducing recurring risk?

If those answers depend on assumptions, informal escalation, or a small number of individuals, the operating model may not be sustainable.

Final Readiness Checklist

Seven conditions that should be resolved before finalizing the decision.

- ☐ OT expertise requirements are clearly defined.
- ☐ OT monitoring and investigation ownership is established.
- ☐ Required coverage aligns with plant operating requirements.
- ☐ Technology and operating costs are understood.
- ☐ Multi-site scalability has been tested.
- ☐ Production-safe response responsibilities are defined.
- ☐ End-to-end accountability is assigned.

If any of these remain unresolved, the operating-model decision is not ready to be finalized.

Determining the Right OT Security Approach

The right OT security operating model comes down to whether the organization can sustain the expertise, coverage, response capability, operational coordination, scalability, and accountability required to protect its manufacturing environment. Deploying another tool or outsourcing another function does not settle that decision on its own.

If the organization discovers gaps in OT expertise, continuous coverage, production-aware response, or the internal resources to sustain the function, an externally supported operating model may warrant further evaluation.

Find the OT Security Model That Fits Your Environment

Explore where internal capability ends and specialized OT security support can close the gap.

[Talk to an OT Security Specialist](#)