

Manufacturing OT SOC Use Case

From OT Security Alerts to Production-Aware Investigation and Response

An illustrative scenario, built from typical elements of a manufacturing OT investigation, showing how a production-aware SOC reasons through an alert, weighing evidence, context, and operational risk before deciding how to respond.



The Manufacturing OT Environment

Where security meets the production floor

Engineering workstations exist to keep production running. Engineers use them to configure, maintain, troubleshoot, and monitor the PLCs, HMIs, and other systems supporting the line.

That access is necessary. It also means an unusual event involving an engineering workstation raises a question about the production environment, not just the endpoint.

Consider a large manufacturing plant operating multiple production lines with:



PLCs
controlling industrial processes



Engineering workstations
used for configuration & maintenance



Historian
systems storing process data



HMIs
providing operator visibility and control



MES
supporting manufacturing operations

IT and OT networks are segmented, but controlled connectivity remains necessary for engineering and maintenance work.

That connectivity is what makes a single unusual connection hard to read at a glance.

It could be an engineer's ordinary Tuesday, or the earliest sign of something else.

For the SOC, the significance of a security event depends on what that device connects to, what those systems support, and what is happening in production when the event occurs.

An Alert from the Production Floor

An unusual connection on an active production line

The SOC receives an alert for anomalous communication from an engineering workstation. The destination is a network segment containing PLCs on an active production line.

Network telemetry shows an unexpected communication pattern with an industrial asset. The protocol and destination are associated with the OT environment.

The alert doesn't establish why communication occurred. First, the evidence is inconclusive.



What the SOC sees	What it could mean
Engineering workstation communicating with an OT asset	Authorized engineering activity
Unexpected communication pattern	Configuration or maintenance change
New or unusual OT connection	Compromised workstation
Communication extending toward production systems	Potential lateral movement

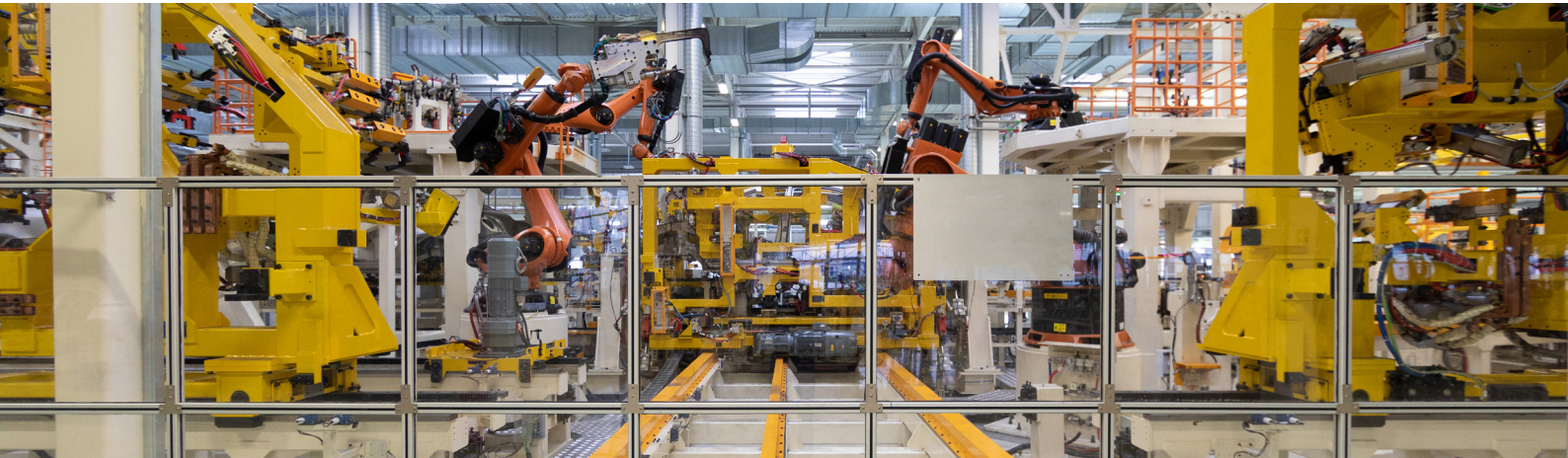
The workstation has legitimate access to the production environment. The alert can't be classified from the connection alone.

A workstation with standing access to doing something unusual isn't automatically a red flag. Engineers make undocumented changes often enough that this alone means little.

At the same time, a compromised workstation would look, at this stage, exactly like an engineer doing unscheduled work.



The alert establishes a signal. The investigation has to establish what that signal means.



The Blind Spot Between **Detection** and **Context**

The five questions that separate a detection from a decision

An IT-centric SOC may see the workstation, its network activity, the destination, protocol, and timing. What it may not see is the context behind those signals.

The Analyst Needs To Know

- 01 **What is the destination?**
A PLC? HMI? Server? Network device?
- 02 **What does it support?**
Which production process or operational function depends on it?
- 03 **Is the communication expected?**
Has this workstation communicated with the asset before, under similar conditions?
- 04 **What was happening at the time?**
Was there scheduled maintenance, troubleshooting, or engineering work?
- 05 **What happens if access is restricted?**
Could containment affect an active production process?

This is where a purely IT-trained investigation tends to stall. The tooling can confirm a connection that happened and describe it in technical terms.

What it typically can't say is whether that destination is safety-critical, or whether the line is mid-batch right now.

Without those five answers, the SOC has visibility into the event but only a partial view of its risk.

Treat every OT-adjacent alert as routine, and a real intrusion moves undetected. Treat everyone as a crisis, and plant operations lose confidence in the SOC's judgment.



For the broader operational assessment that should inform OT security monitoring and response, see the [Manufacturing OT Security Operations Checklist](#).



Understanding the Environment Behind the Alert

Connecting the Asset to Its Operational Role

The gap exposed by the alert isn't a lack of security telemetry. It's the absence of enough OT and production context at the point of investigation.

The SOC needs to connect the alert to:

Dimension	Question it answers
Asset	What is it and what does it do?
Zone	Where does it sit within the OT environment?
Behavior	Is the communication expected?
Activity	What else was happening around the alert?
Production	What operational dependency could be affected?

Building that picture isn't simply collecting more logs. It requires a working model of the OT environment.

That model needs to cover which assets exist, what they do, who normally touches them, and what happens downstream if they're disrupted.

It also needs to be usable mid-investigation, not reconstructed from scratch once an alert fires.

With that model in place, the analyst's task shifts from whether a connection looks unusual, to whether it's a risk, what it affects, and what response fits.

Production-Aware Investigation

Bringing Security, Asset, and Production Evidence Together

Establish the baseline

The analyst checks whether the workstation has previously talked to this destination, under similar conditions.

Timing matters, too. Does the connection line up with a shift change, a scheduled diagnostic, a known maintenance window?

An unusual connection is a reason to investigate. It isn't proof of malicious activity on its own.

Build the timeline

The investigation expands beyond the original connection. The analyst reviews network activity, endpoint activity, authentication events, and related alerts.

Recent engineering or maintenance records get checked too. The goal is to see whether the connection stands alone or fits a broader sequence.

An unexpected connection during an approved change tells a different story than the same connection alongside unusual endpoint activity.

Determine what changed

The analyst asks what specifically changed, when it changed, and who or what initiated it.

The investigation looks for evidence supporting three possibilities: authorized engineering work, an unexpected configuration change, or movement toward production systems.

Put the alert in production context

The destination is an industrial asset supporting a production process, not just another network address.

A connection to a non-critical system carries different stakes than activity touching a PLC controlling a safety-relevant process.

The analyst weighs four things together:

Layer	What it captures
Security evidence	What happened, and how suspicious is it?
Asset context	Which industrial systems are involved?
Production context	What process depends on them?
Response context	What action reduces risk without unnecessary operational consequences?



Production-aware investigation connects the security event to the environment it could affect, before the response decision gets made.

Responding the Right Way

The investigation can't confidently attribute the activity to authorized engineering work. The SOC now evaluates the appropriate response.

Dimension	When it fits
Monitor	Evidence remains ambiguous and the assessed risk allows further observation
Escalate	OT engineering or plant operations need to validate activity or its implications
Contain	Evidence indicates enough risk to justify restricting the affected access

The workstation connects to an active production environment. Because of that, the SOC coordinates with OT engineering and plant operations before acting.

This isn't a procedural courtesy. It changes what safe containment actually looks like.

Isolating a workstation abruptly mid-process can leave a controller in an unpredictable state. Coordinating first lets plant engineering confirm the safest way to cut access.

The objective is to contain the suspicious activity while avoiding unnecessary disruption to the line.

The affected path is contained under established plant procedures. The SOC keeps monitoring in case the initial containment didn't fully close the exposure.

The decision point isn't whether to isolate the workstation. It's choosing the response that reduces risk without treating every OT alert as a reason to stop production.

For manufacturing security leaders evaluating their OT security operating model, start with these [7 questions for choosing the right OT security model].

From Investigation to Action

What the SOC Establishes

The suspicious activity is investigated and contained without unnecessarily interrupting the affected production process.

The SOC establishes:

- What happened
- Which assets were involved
- What the activity meant in context
- Which operational stakeholders needed to be involved
- What response was taken



That record matters beyond the immediate incident. It gives plant engineering and security teams a shared reference for the next similar alert.

Over time, that shared history is what lets a SOC calibrate its judgment to a specific plant's environment.

The immediate outcome is containment. The longer-term value is a more informed understanding of how security events get interpreted and handled at that plant.

A Production-Aware Approach to OT Security

How Prudent Supports Investigation and Response

Manufacturing security operations need to connect suspicious activity with the industrial systems and production processes it could affect.

Prudent's OT MDR/MSS approach brings together:

Capability	What it enables
OT-aware detection	Identify abnormal activity within industrial environments
Contextual investigation	Connect alerts with relevant asset, network, and activity context
Production-aware analysis	Assess the operational relevance of a security event
Coordinated response	Bring security, OT engineering, and plant stakeholders into the decision
Risk-calibrated action	Align response with both security and operational considerations

For manufacturing organizations, this changes what an OT SOC is actually being asked to do.

It isn't just watching for intrusions. It's making judgment calls, incident by incident, about what a signal means for that specific plant.



Detect the signal. Understand the environment. Investigate the risk. Respond with production in context.

Talk to an OT Security Expert

