ACTION FRAMEWORK · MANUFACTURING · IT/OT SECURITY

Manufacturing & IT/OT Security: What to Do Right Now

A practical action framework for manufacturing leaders and security teams — whether you engage a partner or not.

AUTHOR
Steve Weltman, CISSP

ORGANIZATION
Aletheia Security Consulting

SCOPE
3 Phases · OKRs · Frameworks

WHY THIS CAN'T WAIT

The attack surface isn't just IT anymore.

Manufacturing is now the most-attacked sector globally. Ransomware demands have doubled year-over-year. But the attack surface isn't just IT anymore — it's the factory floor. And most manufacturers have never formally examined the intersection between their IT infrastructure and their operational technology.

This guide tells you what to do — whether you engage a partner or not. It describes the processes you need, the things you should be measuring, and how to report your security posture to your board in a language they can govern with.

> **Start here. Then decide what you need help with.**

01 Get Visible

IMMEDIATE PRIORITY — DO THIS BEFORE ANYTHING ELSE

The most common OT security failure isn't a technical control gap — it's that nobody knows what's running on the plant floor. Before you can protect it, you have to see it.

Asset Discovery & Inventory

- [ ] Conduct a passive OT network scan to discover connected devices (use passive tools — active scanning can crash PLCs and controllers)
- [ ] Build an asset inventory that includes: device type, manufacturer, firmware version, IP address, physical location, last-known patch date, owner/responsible team
- [ ] Identify any OT devices that are directly internet-accessible — this is your most urgent exposure
- [ ] Map which OT systems communicate with IT systems, and how
- [ ] Document every remote access path into OT environments: vendor VPNs, remote desktop, jump servers

Network Architecture Review

- [ ] Draw your current IT/OT network topology — including every connection point between them
- [ ] Identify your IT/OT boundary(ies) — this should be explicit and documented, not assumed
- [ ] Check whether your OT zones are network-segmented from IT (if not, this is your #1 priority)
- [ ] Identify where the Purdue Model breaks down in your actual environment (it usually does)

02 Close the Biggest Gaps

30–90 DAYS — HIGH-IMPACT, LOW-DISRUPTION CONTROLS

Access Control

- [ ] Enforce multi-factor authentication on all remote access paths into OT systems — no exceptions
- [ ] Implement jump hosts / bastion servers for all vendor and contractor OT access
- [ ] Remove or disable default credentials on all OT devices (routers, switches, PLCs, HMIs)
- [ ] Audit current user accounts on OT systems — remove inactive accounts, enforce least privilege
- [ ] Establish a formal contractor access process: provisioned, time-limited, logged, deprovisioned

Segmentation

- [ ] Implement network segmentation between IT and OT environments if not already in place
- [ ] Create a DMZ for data historians and other IT/OT bridge systems — nothing should pass directly
- [ ] Restrict lateral movement: OT systems should not be able to initiate connections to IT systems
- [ ] Disable unused ports and services on all OT devices

Patching & Vulnerability Management

- [ ] Identify every unpatched critical vulnerability in your OT environment — prioritize by operational risk
- [ ] For systems that cannot be patched (legacy PLCs, old SCADA): document compensating controls
- [ ] Establish a realistic patching cadence for OT — tied to planned maintenance windows, not ad hoc
- [ ] Create a formal process for evaluating new OT vulnerabilities before they reach CISA KEV

Incident Response

- [ ] Verify your IR plan explicitly covers OT scenarios — most IT-focused IR plans don't
- [ ] Define "production shutdown" as a severity category with its own escalation path
- [ ] Document recovery procedures for each critical OT system — tested, not theoretical
- [ ] Identify your OT-specific contact list: plant engineering, automation vendors, SCADA support

03 Build Sustainable Processes

ONGOING — THE PRACTICES THAT MAKE SECURITY DURABLE

Change Management

- [ ] Implement formal change control for OT configuration changes — treat unauthorized config changes as security events
- [ ] Log all changes to PLC, DCS, and controller configurations with timestamps and operator identity
- [ ] Establish a baseline configuration for each critical OT system — and alert on deviations

Vendor & Contractor Governance

- [ ] Maintain a current list of all third parties with OT access — this list is usually longer than expected
- [ ] Define and enforce minimum security requirements for OT vendors (contractors cause ~27% of OT incidents)
- [ ] Require vendors to use managed/approved devices when accessing your OT environment — no personal laptops
- [ ] Log all vendor OT activity; review logs quarterly

OT-Specific Security Monitoring

- [ ] Deploy passive OT monitoring on your production networks (tools: Claroty, Dragos, Nozomi, Tenable OT)
- [ ] Establish baselines for normal industrial protocol traffic — alert on deviations
- [ ] Monitor IT/OT boundary points 24/7 — this is your most important detection point
- [ ] Ensure your SOC (internal or MSSP) has OT-trained analysts, not just IT security staff

Tabletop Exercises

- [ ] Run an annual tabletop exercise that includes a production shutdown scenario
- [ ] Include plant operations leadership, not just IT/security — the response is a joint function
- [ ] Test your OT-specific IR plan at least once before you need it

MONITORING & MEASUREMENT

What to watch. What deviation looks like.

Continuous Monitoring — Alert On:

- **New devices** appearing on OT network segments (unauthorized asset introduction)
- **Unauthorized PLC/controller configuration changes** — any change outside a change window
- **Remote access anomalies** — off-hours access, new source IPs, access outside normal scope
- **Data transfer anomalies** — unusual volume leaving OT environments
- **Unusual protocol traffic** on industrial networks (Modbus, OPC-UA, DNP3 anomalies)
- **IT-to-OT lateral movement attempts** — any IT system probing OT addresses
- **Credential anomalies** — failed login spikes, inactive account use, service account misuse

MONTHLY REVIEW

- Open vulnerability count by severity (OT and IT separately)
- Contractor access audit — active credentials vs. active contracts
- Patch compliance rate by system category
- Anomaly alert volume trends — increasing without explanation?

QUARTERLY REVIEW

- IT/OT segmentation audit — validate controls are still in place
- Vendor security compliance check
- IR plan review and update (especially after any incident or near-miss)
- OKR/KPI report for board/executive leadership

BOARD REPORTING

OKRs for IT/OT Security Governance

The board doesn't need every metric. They need to understand the organization's direction and whether it's improving. Each OKR has measurable, time-bounded key results.

OKR 1 — Achieve Operational Visibility Across IT/OT Environments

We know what's on our plant floor and where it connects to our business systems.

KR	MEASUREMENT	TARGET
KR1	% of OT assets inventoried with known security status	**100% by [date]**
KR2	IT/OT network topology documented and validated	**Complete by [date]**
KR3	Internet-exposed OT assets	**Zero (or risk-accepted w/ compensating controls)**
KR4	Remote access paths audited and controlled	**100% covered by MFA + jump host**

OKR 2 — Reduce Exposure of Legacy and Unmanaged OT Systems

Our highest-risk OT systems have known, documented risk posture.

KR	MEASUREMENT	TARGET
KR1	Critical OT vulnerabilities open > 90 days	**< 5 (or 0 without documented control)**
KR2	OT systems with default credentials	**Zero**
KR3	Legacy systems with no patch path	**100% have compensating controls**
KR4	Unauthorized IT/OT connections	**Zero after remediation milestone**

OKR 3 — Mature OT Incident Response Capability

We can detect, respond to, and recover from an OT security incident without sustained production loss.

KR	MEASUREMENT	TARGET
KR1	OT-specific IR playbook status	**Documented and tested**
KR2	Annual OT tabletop exercise	**Completed with plant ops leadership present**
KR3	Mean Time to Detect (MTTD) anomalous OT activity	**Baselined; YoY improvement**
KR4	Documented RTO for each critical production system	**100% defined**

QUARTERLY BOARD REPORTING

KPIs to Report Every Quarter

KPI	WHY IT MATTERS
% of OT assets with known security status	Visibility is the foundation — if this isn't 100%, nothing else is reliable
# of critical/high OT vulnerabilities open	Exposure trending — is the backlog growing or shrinking?
IT/OT segmentation compliance (% sites fully segmented)	The most impactful single control — boards should know its status
Remote access audit results (# unauthorized/uncontrolled paths)	Vendor risk and remote access are the top OT attack vectors
Time since last OT IR exercise	Untested plans don't work; boards need to know this is live
# of OT security incidents or anomaly detections	Trending metric — direction matters more than absolute count
Compliance status vs. applicable framework(s)	NIST CSF 2.0 Mfg Profile, IEC 62443, CMMC Level 2 as applicable

FRAMEWORKS TO KNOW

The standards that govern OT security

NIST CSF 2.0 — **Manufacturing Profile** (released May 2025). NIST's first manufacturing-specific CSF profile. Bridges IT and OT governance. Start here for board-level reporting structure.

IEC 62443 — The international technical standard for industrial control system security. Use alongside NIST CSF — IEC 62443 is the technical implementation layer; NIST CSF is the governance layer.

NIST 800-82 — Foundational OT security guidance from NIST. Provides the technical baseline for ICS/SCADA security programs.

CMMC L2 — If you're in the U.S. defense supply chain, your OT environment is in scope. This is not optional and enforcement is active.

NIS2 — If you operate manufacturing facilities in Europe or supply EU critical infrastructure, your OT environments are now explicitly in scope.

BEFORE YOU ENGAGE A PARTNER

If you decide you need outside help, here's what to know.

1. **Start with a risk assessment, not a tool.** Any reputable partner should want to understand your environment before recommending anything. If the first conversation is about a product, move on.
2. **OT and IT security are different disciplines.** Active scanning tools that work fine on IT networks can crash PLCs and halt production. Insist that your partners know the difference.
3. **The ISERA is designed for this.** Aletheia Security's Information Security Enterprise Risk Assessment spans IT and OT, runs perception gap analysis between your technical and operations teams, and produces a prioritized roadmap — not a 47-item findings list.
4. **Ask about IEC 62443 fluency.** This is the OT practitioner's litmus test. If a security partner can't speak to zone/conduit architecture and security levels, they're an IT firm with an OT slide deck.

Information Security Enterprise Risk Assessment (ISERA)

Framework-agnostic — satisfies NIST CSF 2.0 Mfg Profile, IEC 62443 alignment, CMMC, and HIPAA risk requirements simultaneously. 30 business days. No tools sold. No findings list. A real picture of where you stand.

NIST CSF 2.0 · IEC 62443 · NIST 800-82 · CMMC 2.0 · HIPAA · NIS2

Ready to talk? sweltman@aletheiasecurity.com · aletheiasecurity.com