Manufacturing Sector Cybersecurity

INTELLIGENCE-DRIVEN CYBER DEFENSE STRATEGY 2025

From board members to practitioners, there should be alignment on your cybersecurity needs. Only measuring cybersecurity controls against frameworks, regulations, or risk scores ultimately hinders this alignment.

Move beyond compliance frameworks to threat-focused cybersecurity that addresses real adversary behaviors and protects what matters most.

STEP 1 Identify Intelligence-Driven Threat Scenarios

STEP 2 Deploy Critical Security Controls

STEP 3 Prioritize Industrial Sites

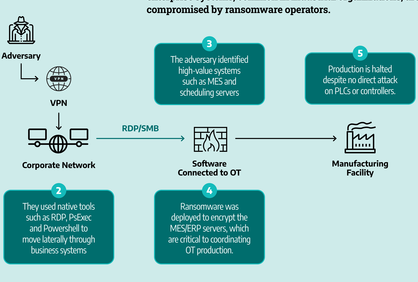
STEP 4 Gain Security Investment Alignment

Step 1: Identify Intelligence-Driven Threat Scenarios

Identifying industry-specific threat scenarios can enable an organization to understand the adversaries targeting network protocols and systems in operational technology (OT) environments.

Ransomware Attack with OT Impacts

Ransomware campaigns continue to wreak havoc on manufacturing, with 1171 attacks targeting manufacturers alone in 2024. Though often treated as an IT problem, ransomware that encrypts enterprise systems like MES (Manufacturing Execution Systems) and ERP (Enterprise Resource Planning) platforms can cripple OT production lines – even without accessing the OT networks directly.



In the 2019 attack on Norsk Hydro, ransomware encrypted MES and ERP systems, disrupting aluminum production and forcing facilities into manual fallback procedures. In 2024, the food and beverage manufacturer Stoli Group faced severe operational disruption, supply chain impacts, and delayed recovery timelines – they ultimately filed for bankruptcy. These attacks highlight the cascading impacts when key enterprise systems, common in industrial organizations, are compromised by ransomware operators.

Step 2: Deploy Critical Security Controls

What security measures are most critical against the threat?

Applying SANS 5 Critical Controls for World-Class OT Cybersecurity can mitigate threats like ransomware targeting MES and ERP platforms. Each control addresses specific aspects of cybersecurity readiness and resilience.

1 Incident Response for ICS

Develop cross-functional playbooks that include fallback procedures for MES/ERP outages. Simulate ransomware scenarios involving business systems that support OT operations. Coordinate response between IT and OT teams to ensure production continuity.

2 Defensible Architecture

Segment MES/ERP systems from OT and IT networks with firewall and access controls. Apply network zoning and restrict lateral movement using industrial DMZs and access gateways. Disable direct access to MES from external or untrusted networks.

3 ICS Network Visibility & Monitoring

Use protocol-aware detection to identify abnormal traffic between IT and OT. Monitor lateral movement protocols like RDP and SMB. Alert on unusual patterns and software changes in MES/ERP systems.

4 Secure Remote Access

Enforce MFA and least privilege access for all remote connections. Log and review all access to MES/ERP systems. Regularly audit and restrict VPN, RDP, and third-party access pathways used in business side-operations.

5 Risk-Based Vulnerability Management

Prioritize patching of systems interfacing with OT. Where patching isn't feasible, apply compensating controls like whitelisting and user role restrictions. Maintain up-to-date asset inventories and baselines to quickly access exposure.

Step 3: Prioritize Industrial Sites

Where are you most at risk from the threat?

Map exposed sites with direct or indirect access from business networks.

Identify facilities using remote access or shared engineering workstations.

Focus on high-consequence environments.

Step 4: Gain Security Investment Alignment

What should you do and why now?

Justify investments with real threat scenarios and known adversary activity.

Use threat intelligence to show business risk, not just technical risk.

Align controls to adversary behavior, not just compliance frameworks.

GLOBAL CYBERSECURITY REGULATION DRIVERS

NERC CIP | NIS2 | AESCSF | OTCC | CCOP

ADDITIONAL MANUFACTURING SECTOR THREAT SCENARIOS

Bx BAUXITE

METHOD: Exploitation of vulnerable internet-facing firewall

TARGET: Opportunistic manufacturing

IMPACT: Potential reconnaissance; pathway for future OT disruption

ATTACK PATH

- Internet-facing firewall appliances
- Vulnerability exploited
- Pathway to actions on objectives

Ka KAMACITE

METHOD: Phishing and credential theft

TARGET: Manufacturing sector

IMPACT: Conducts reconnaissance, supports follow-on OT compromise

ATTACK PATH

- Phishing
- Remote Access
- Lateral movement to OT with native/ commodity tools

Gr GRAPHITE

METHOD: Spearphishing and malicious documents to deliver malware

TARGET: Defense manufacturing

IMPACT: Credential harvesting

ATTACK PATH

- Phishing email delivers malicious documents
- Downloads malware enabling backdoor
- Harvests credentials
- Gains access to files tied to OT systems

Want Deep Insights Into These Threats?

Explore detailed threat group profiles, real-world attack scenarios, and electric sector risk trends in the 2025 Dragos OT/ICS Cybersecurity Report, our 8th Annual Year in Review.

DOWNLOAD REPORT

Dragos delivers complete industrial cybersecurity for electric utilities, from real-time OT detection to in-depth threat intelligence and expert-led threat hunting and response services. Let's work together to reduce risk, stop adversaries, and safeguard operations across your OT network. Dragos.com.

DRAGOS