Atumcell

Cutting Through the Hype: A Pragmatic Guide to OT Cybersecurity in 2025

Contact

David E. Williams, CEO

d@atumcell.com

(617) 671-8810

atumcell.com

February 2025

Introduction

Operational technology (OT) is the hardware and software that controls physical processes in manufacturing, energy, transportation, and utilities. While IT manages data and communications, OT monitors and controls industrial equipment, from power grids to assembly lines. Historically, OT systems operated in isolated environments, but digitization and connectivity have introduced cybersecurity threats that these systems were never designed to handle.

Beginning an OT cyber security journey can feel overwhelming. Experts are few and far between, and the landscape is filled with buzzwords and confusing advice. This guide lays out a straightforward roadmap to help make tangible progress in a reasonable timeframe.

Step 1

Start with Asset Mapping

Why This Matters: The first step to effective OT cybersecurity is understanding what assets you have. A complete inventory of devices, networks, and control systems is needed to implement an effective security program. Asset mapping provides the foundational knowledge required for segmentation, vulnerability management, and incident response.

Organizations often skip this step and find themselves struggling to apply security measures that don't align with their actual infrastructure, leading to wasted resources, ineffective protections, and a false sense of security.

OT asset mapping is non-trivial. Traditional IT asset mapping tools such as Nmap can overwhelm OT systems that are designed for much more limited bandwidth. If you're not careful, asset mapping itself can cause operational disruptions and system failures.

What to Do:

- Deploy OT-specific asset discovery tools such as AtumScan Industrial. These tools use OT protocols such as Modbus to safely capture details including device types and firmware versions.
- Map the relationship of assets to one another, following the Purdue model.
- Use the asset map to form the backbone for all subsequent cybersecurity efforts.

Step 2

Adopt Basic Cyber Hygiene

Why This Matters: Many OT cybersecurity incidents result from basic lapses. Unchanged default credentials provide an easy entry point for attackers, while shared accounts make it difficult to track and manage user activities. Unlike IT environments, where identity management solutions are more common, OT environments frequently lack proper authentication controls, leading to heightened exposure. Strengthening authentication measures is one of the most impactful steps an organization can take to enhance security and mitigate threats.

These steps align with compliance frameworks such as IEC 62443, NIST 800-82, and NERC CIP. Achieving compliance with relevant industry standards can also improve your cybersecurity posture.

What to Do:

- Segregate IT and OT networks to limit attack pathways.
- Eliminate default passwords and enforce password management policies.
- Restrict the use of shared accounts; implement individual user authentication where possible.
- Enforce strong authentication mechanisms, such as multi-factor authentication, tailored to OT environments where legacy systems may pose integration challenges.
- Regularly update software and firmware to address known vulnerabilities, ensuring updates are tested in a controlled environment to avoid operational disruptions.

Step 3

Build Awareness of OT-Specific CVEs

Why This Matters: The growing catalog of OT-specific Common Vulnerabilities and Exposures (CVEs) provides warnings about the threats your environment faces. Unlike IT CVEs, OT-specific CVEs often target industrial control systems (ICS) or programmable logic controllers (PLCs), which can disrupt physical processes.

For example, the Privilege Escalation Vulnerability CVE-2024-31485 for Siemens power automation equipment is akin to giving a hotel guest a master key that can open all rooms, not just their own.

However, the explanatory information in OT-CVE bulletins is often very sparse, making it difficult to determine severity and impact. Atumcell is addressing these deficiencies with an initiative to better characterize the most important vulnerabilities and publish intrusion detection rules to recognize and counter them.

What to Do:

- Regularly monitor OT-specific CVEs through platforms like CISA ICS-CERT, MITRE ATT&CK for ICS, or vendor advisories.
- Map relevant CVEs to your asset inventory to determine potential impact and prioritize remediation.
- Develop intrusion detection rules tailored to your specific OT assets and configurations, or partner with OT security providers like Atumcell.

Step 4

Adopt the Hacker's Perspective

Why This Matters: Compliance-driven approaches are often detached from real world threats. Adopting a hacker's perspective is more helpful in identifying the most likely attack paths. An auditor might check for documented policies, patch management schedules, and access control lists. Meanwhile, a hacker will seek out an exposed engineering workstation connected to both IT and OT networks, using it as a pivot point to gain deeper access.

Skilled penetration testers emulate adversaries to identify such vulnerabilities. However, OT penetration testing is highly specialized and requires careful planning to avoid disruption.

What to Do:

- Engage experienced OT penetration testers who understand the nuances of industrial systems.
- Vet providers by assessing their expertise with OT protocols, ICS components, and safety controls.
- Scope and plan testing to minimize operational risks while delivering pragmatic insights.
- Consider Red Team exercises to simulate a real-world attack and strengthen your incident response capabilities.

Step 5

Address Legacy Systems Strategically

Why This Matters: Legacy systems are ubiquitous in OT environments, and while their vulnerabilities are well-documented, upgrading or replacing them can be prohibitively expensive and disruptive. For example, a legacy distributed control system (DCS) in a refinery might be integral to operations but lack modern security features.

What to Do:

- Prioritize upgrades for systems that present the highest risk, such as those exposed to external networks.
- For systems that cannot be replaced, implement compensating controls including network segmentation, strict access controls, and regular vulnerability scanning.
- Use a cybersecurity roadmap to build a business case for modernization. Demonstrating how outdated systems increase risk to operations and profitability can justify investments in upgrades.

Step 6

Tackle Supply Chain Risks

Why This Matters: Supply chain cybersecurity is increasingly important, but it's difficult to manage if your own systems are insecure. Internal protections must come first.

What to Do:

- Begin by securing your internal OT environment.
- Extend these practices to your supply chain by applying the same principles, such as penetration testing and adopting a hacker's perspective.
- Establish minimum cybersecurity standards for suppliers and use contractual obligations to enforce accountability.
- Encourage suppliers to align with frameworks such as NIST Cyber Supply Chain Risk Management (C-SCRM).

Step 7

Adjust to the Changing Cyberinsurance Landscape

Why This Matters: As cyberinsurance providers narrow their coverage and impose stricter requirements, organizations can no longer rely on insurance as a safety net. In some cases, investing in cybersecurity and resilience may yield greater returns than paying premiums.

What to Do:

- Evaluate whether insurance premiums would be better invested in hardening your systems and improving resilience.
- Harden your systems to meet or exceed insurance standards.
- Use penetration testing, vulnerability management, and compliance with recognized frameworks to demonstrate proactive risk reduction, which may help in negotiations with insurers.

Conclusion

Practical Progress Starts Here

Cut through the hype by focusing on foundational actions that deliver real security outcomes. Start with asset mapping, implement basic hygiene, stay current with OT vulnerabilities, and think like a hacker. Then move on to address legacy systems, the supply chain, and cyber insurance. Doing so will foster a resilient OT environment for the long-term.

For expert guidance and tools designed to make OT cybersecurity practical and effective, contact Atumcell CEO, David Williams today.

d@atumcell.com
(617) 671-8810
atumcell.com