VIEW POINT

ICS VULNERABILITY TRENDS AND STRATEGIC INSIGHTS

Abstract

Industrial Control System (ICS) vulnerabilities are rising sharply, with 2024 marking a 38% increase in CVE disclosures and continued growth projected for 2025. Despite improved scoring accuracy, remediation gaps persist—over one-quarter of advisories lacked patches, and many offered no mitigations. Deep-layer assets (Purdue Levels 0–2) account for most vulnerabilities, while perimeter exposure remains a critical entry point. Infosys C&A IoT & OT recommends OT-centric strategies: prioritizing critical flaws via the "Now / Next / Never" model, enforcing segmentation, managing third-party risks, and adopting compensating controls. Proactive vulnerability management and supply chain transparency will be essential to safeguard ICS environments amid accelerating OT-IT convergence.

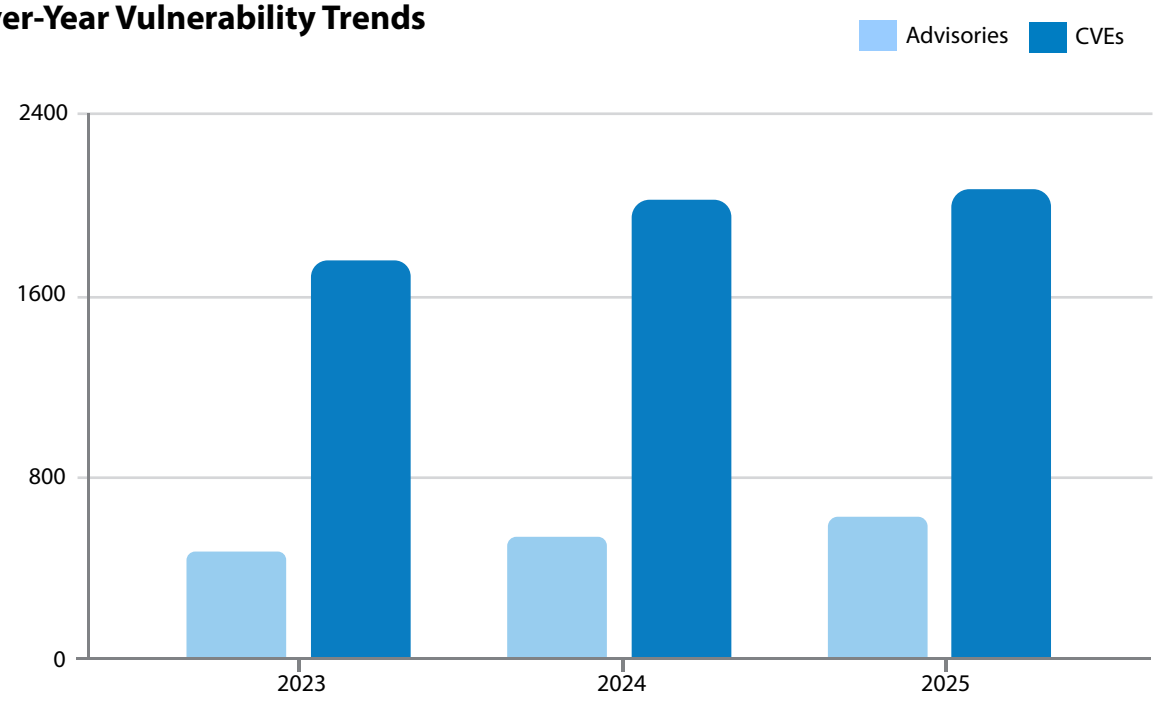
Infosys®
Navigate your next

Introduction:

In 2024, Infosys C&A IoT&OT team observed continued growth in industrial control system (ICS) vulnerabilities and evolving threat patterns. This reflects ongoing maturation of ICS security programs even as connectivity expands. Key takeaways: many disclosures lacked fixes or mitigations, adversaries increasingly target Internet-exposed devices, and highly exploitable vulnerabilities (especially with public exploits) demand urgent action. Below we summarize the data and offer strategic guidance for OT leadership and security teams.

ICS Vulnerability Statistics (2023-2025)

Year-Over-Year Vulnerability Trends



Rising Numbers: In 2024, the total number of Common Vulnerabilities and Exposures (CVEs) published reached 40,009, marking a significant 38% increase from the 28,818 CVEs recorded in 2023. This surge underscores the growing complexity of cybersecurity threats and the expanding efforts in vulnerability identification and disclosure. Looking ahead, projections for 2025-2026 estimate that between 48,675 and 58,956 new CVEs will be published, indicating a potential year-over-year increase ranging from approximately 21.6% to 47.4% compared to 2024. This anticipated growth reflects the continued expansion of the digital landscape and the increasing emphasis on proactive cybersecurity measures. The upward trend in CVE disclosures is expected to persist, driven by factors such as the integration of operational technology (OT) assets into IT networks and improved vulnerability reporting practices by vendors.

Patch and Mitigation Gaps: In 2024, approximately 26% of Industrial Control Systems (ICS) advisories lacked an available vendor patch, and 18% offered no mitigation guidance, leaving many asset owners without immediate solutions to address identified vulnerabilities. This situation underscores the persistent challenges in securing operational technology (OT) environments, where applying patches can be constrained by factors such as the need to maintain continuous operations and the potential risks associated with system downtime.

To address these gaps, the Infosys C&A IoT&OT team developed and published workarounds for a number of cases where no official patches were available. Additionally, they provided alternative mitigation strategies in scenarios where applying official patches was impractical, such as when patches could lead to unacceptable downtime. This approach, often referred to as implementing "compensating controls," is critical in OT settings where traditional patch management practices may not be feasible.

Looking ahead of 2026, the trend of advisories lacking immediate remediation options is expected to continue. This projection is based on the increasing complexity of OT systems and the ongoing integration of OT assets into IT networks, which can introduce new vulnerabilities and complicate patch management processes. As a result, the development and implementation of compensating controls will remain a vital strategy for managing security risks in OT environments.

OT Vulnerability Management Challenges

Operational Requirements

OT environments must remain operational for safety and production purposes, limiting patching windows.

Patching Limitations

26% of advisories had no patch at publication, and 18% offered no mitigation guidance.

Alternative Solutions

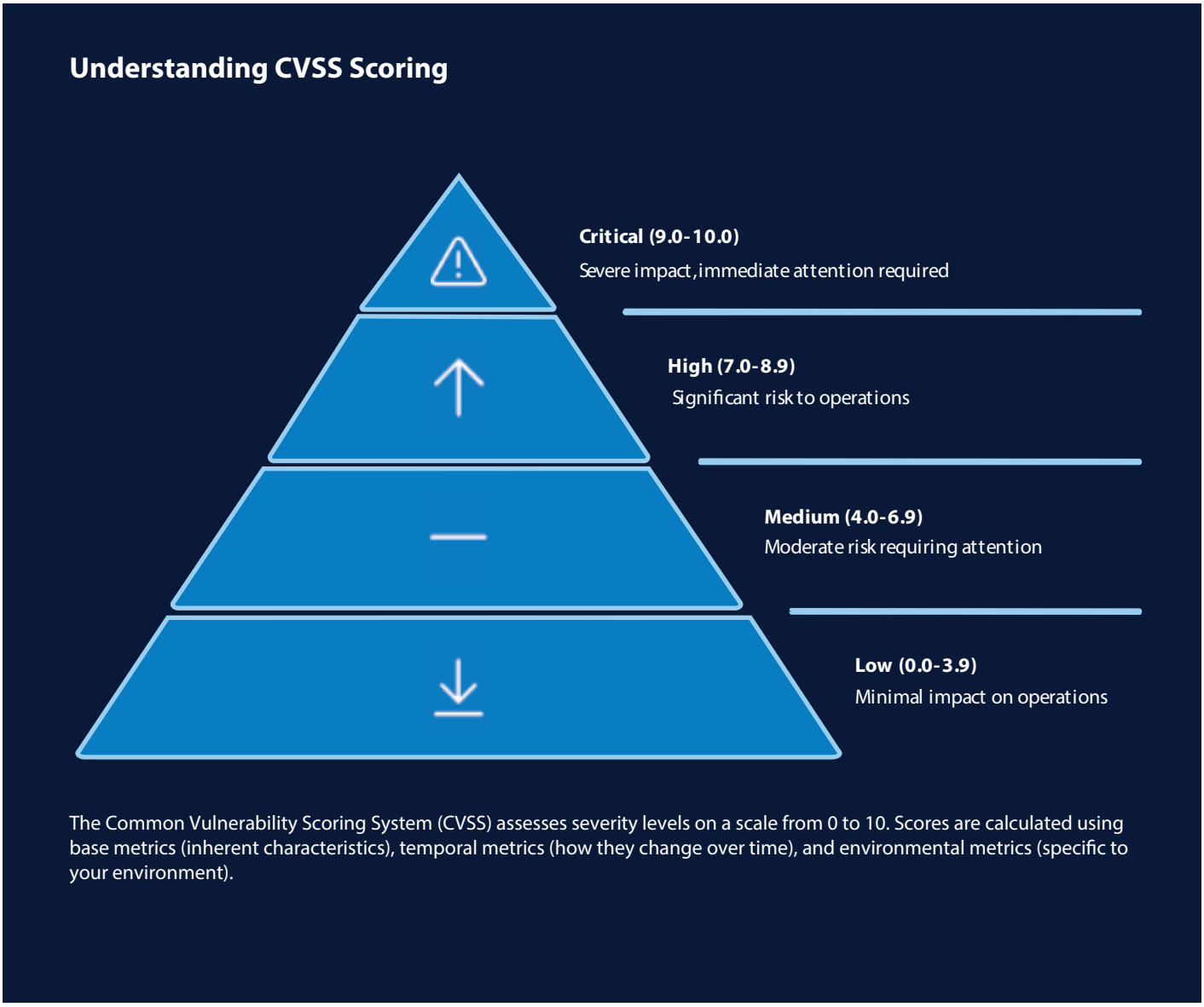
Dregos provided mitigations for 47% of unpatched vulnerabilities and alternatives for many patched systems.

OT asset owners face unique challenges when addressing vulnerabilities. Unlike IT environments, they can't immediately apply patches due to operational requirements. Even when patches exist, they may not fix inherent flaws or may require unacceptable downtime.

CVSS Accuracy: In 2024, approximately 22% of Industrial Control Systems (ICS) advisories were identified as having inaccurate Common Vulnerability Scoring System (CVSS) scores. This marks a notable improvement from previous years, reflecting enhanced precision in vulnerability assessments.

The Infosys C&A IoT&OT team has proactively re-evaluated some CVSS vector within the ICS context to ensure that scoring aligns with the operational impact. Accurate scoring is critical: underestimating a vulnerability's severity can lead to inaction, while overestimating can result in unnecessary allocation of limited OT maintenance resources. To address this, the team supplements CVSS assessments with OT-specific factors such as the likelihood of exposure and potential safety impacts, providing a more comprehensive risk ranking.

Looking ahead to 2026, the trend of improving CVSS accuracy is expected to continue, driven by the adoption of CVSS version 4.0, which offers enhanced metrics for evaluating vulnerabilities in OT environments. This progression underscores the industry's commitment to refining risk assessment methodologies to better protect critical infrastructure.



CVSS Scoring and OT Mitigations

In 2025, only 22% of ICS advisories required corrections to vendor-assigned CVSS scores—a significant improvement compared to previous years, signaling enhanced vendor maturity in vulnerability scoring. This trend is expected to continue into 2026 with broader adoption of CVSS v4.0, which introduces more context-aware metrics suited for OT environments.

Despite this improvement, CVSS should be treated as just one input among many in risk prioritization. Infosys C&A IoT&OT team recommends ranking vulnerabilities using operationally relevant factors such as:

- Ease of exploitation in the actual ICS environment
- Impact on critical control functions
- Availability of network-based vs. local exploit vectors

For instance, a high CVSS vulnerability that requires physical access may be less urgent than a medium-severity vulnerability with available remote exploit code. Given the strict maintenance constraints in OT, these compensating controls—like enabling vulnerable services or segmenting network traffic—enable timely risk reduction without waiting for official patches. Heading into 2026, OT asset owners should continue to demand ICS-specific mitigation advice from vendors and be prepared to implement tailored interim solutions to sustain safe operations.

Perimeter vs. Deep Network Exposure (Purdue Model)

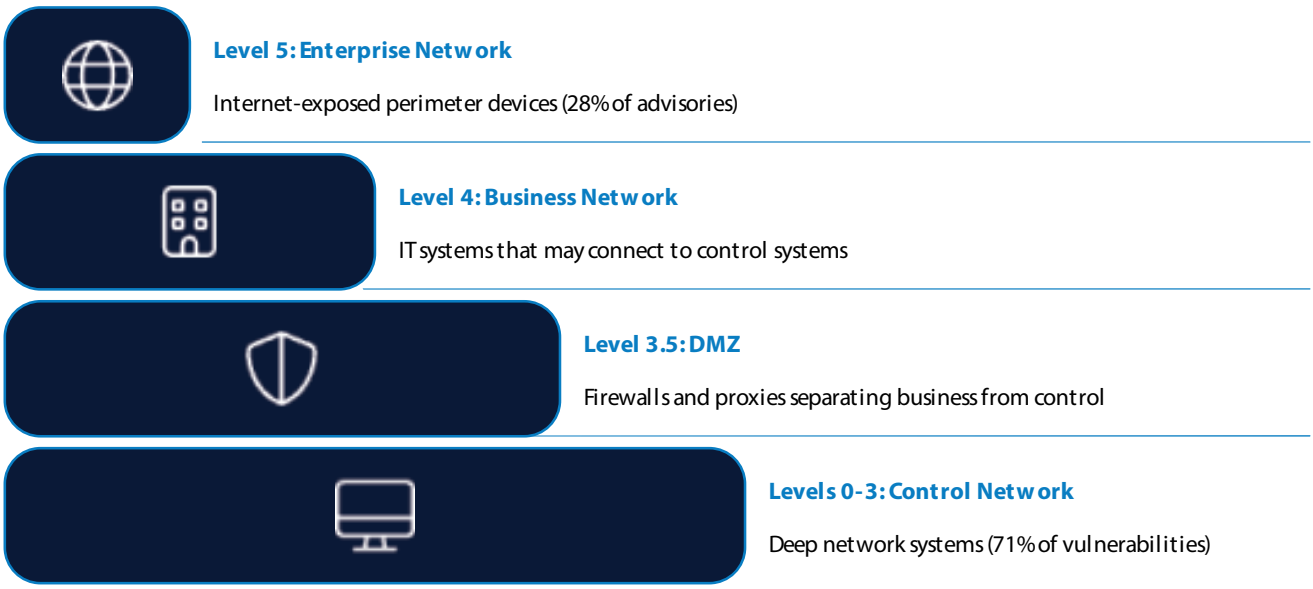
Vulnerability Exposure by Purdue Model Level (2024–2026 Trends)

In 2024, the Infosys C&A IoT&OT team observed ICS vulnerabilities based on their location within the Purdue model. The analysis revealed:

- 28% of ICS advisories involved Purdue Level 5 assets — such as Internet- or DMZ-facing devices like firewalls, VPN gateways, and externally exposed servers.
- 71% of vulnerabilities were located in Purdue Levels 0–2, near the physical process layer, which includes PLCs, RTUs, and HMIs.
- This distribution highlights two critical and contrasting risks:
- The high share of deep-level vulnerabilities (71%) underscores the potential for direct process disruption, including loss of view or control over industrial operations.
- The significant perimeter exposure (28%) reflects persistent adversary interest in public-facing or lightly segmented assets. Throughout 2024, attackers exploited legacy vulnerabilities (e.g., in Ivanti and SonicWall firewall appliances) to gain initial access into ICS environments.

Looking ahead to 2026, these trends are expected to persist — or intensify — as more OT systems connect to IT networks and cloud services, increasing both deep and edge exposure.

The Purdue Model for ICS Security



Strategic Response: Zoning and Hardening

To mitigate these threats, segmentation remains foundational. We recommend:

- Enforcing strict network zoning: **separate Level 5 systems from Levels 3** and below using DMZs and hardened jump hosts.
- Isolating Levels 0–2 from business networks to prevent lateral movement from compromised enterprise assets.
- Allowing only essential communication protocols, preferably via tightly controlled jump servers.
- Moving device management interfaces off public LANs and into **secure VPN tunnels**.
- Promptly patching and hardening perimeter devices by:
  - Disabling unused accounts
  - Enforcing strong authentication
  - Monitoring continuously for anomalies

In summary, **every Internet-facing OT asset is a potential entry point**. As such, proactive segmentation and edge device security will remain high priorities for 2025 and beyond.

"Now / Next / Never" Vulnerability Prioritization (2024–2026 Trends)

To efficiently manage ICS vulnerabilities, the Infosys C&A IoT&OT team applies a "Now / Next / Never" triage model—designed to align technical urgency with operational feasibility in OT environments. The 2024 data breakdown reinforces its value:

- **Now (6%)** – These are high-risk vulnerabilities that are:
  - Remotely exploitable without authentication or with easily bypassed controls
  - Often tied to public proof-of-concept exploits or are under active exploitation
  - Directly impact critical ICS assets (e.g. unauthenticated RCE on a PLC or HMI)

These vulnerabilities represent only 6% of the total, but demand immediate response—patching, isolation, or compensating controls should be applied without delay.

- **Next (63%)** – These are important vulnerabilities that:
  - Are remotely exploitable but require credentials or preconditions
  - Can potentially affect operations but are mitigated by segmentation and hygiene
  - Should be addressed in the standard patch cycle, post-Now items

Comprising 63% of ICS vulnerabilities in 2024, this category represents the bulk of structured remediation planning.

- **Never (31%) – These are low-impact or theoretical issues that:**

Are difficult or impractical to exploit

Typically involve local-only access, obscure vectors, or outdated hardware

Pose minimal real-world risk in properly segmented ICS environments

At 31%, these are best documented and deprioritized unless part of a larger threat chain.

Strategic Implication for 2025-2026

Attempting to address every CVE equally—"boiling the ocean"—is neither effective nor necessary in OT. By focusing scarce OT maintenance windows on "Now" threats (especially those with public PoC), this prioritization model ensures:

- Better risk reduction
- Efficient resource allocation
- Avoidance of unnecessary downtime

As threat actors increasingly exploit known vulnerabilities with low barriers to entry, this structured prioritization will remain essential for ICS defenders throughout 2025.

Triage by Risk, Not Just Severity: Instead of relying solely on generic severity scores (like CVSS), Infosys evaluated each vulnerability in the context of **operational risk.** Key questions were asked: Does this vulnerability affect a critical process (a Crown Jewel asset)? Is there known exploit activity in the wild for it? What's the likelihood of this being an attack vector versus a theoretical issue? They developed a simple three-tier model for prioritization:

Patch Now

Criteria:

Known exploits exist (e.g., CISA KEV list)

Direct exposure to untrusted networks

High-impact to safety or critical processes

Remote code execution vulnerabilities on critical assets

Examples:

CVE in a remote access gateway affecting VPN auth

Critical PLC firmware vuln allowing unauthenticated writes

Action:

Coordinated downtime, vendor patch support, full regression testing

Applied within 7–10 days

Patch Later

Criteria:

Medium severity or mitigated by compensating controls

Exploits not publicly available

Devices within segmented, monitored networks

Examples:

Engineering workstation vulnerable to local privilege escalation

ICS protocol stack flaw not exposed due to firewall controls

Action:

Scheduled during planned maintenance windows

Deferred 30–90 days with documented justification

Patch Later

Criteria:

Legacy system with no vendor support

No patch available, or patch causes system failure

Device mitigated by isolation, monitoring, and/or physical controls

Examples:

Legacy HMI running on Windows XP

Field controller only accessible via air-gapped conduit

Action:

Isolated via segmentation

Monitored with strict anomaly detection

Risk acceptance documented and signed by plant leadership

3rd Party (Supply Chain) Vulnerability Risks – 2024 to 2026 Outlook

Third-party libraries, firmware, and embedded components continue to present growing risk within ICS environments. In 2024, the Infosys C&A IoT&OT team observed a sustained increase in supply chain-related CVEs, with third-party advisories rising 8.5% year-over-year from 2022 to 2023, and further growth projected for 2025-2026.

These vulnerabilities often cascade across multiple products and vendors, making identification and remediation far more complex than traditional first-party flaws.

Notable 2024-2025 Examples:

- Palo Alto Networks' PAN-OS (CVE-2024-3400)

  Widely used in ICS edge security, PAN-OS was discovered embedded in Siemens' Rugged.com APE1808 industrial firewall. The vulnerability in PAN-OS triggered a secondary Siemens advisory after confirmed in-the-wild exploitation on ICS assets.

- cURL Open-Source Library

  A 2023 vulnerability in the ubiquitous cURL utility impacted numerous ICS products using embedded Linux. Vendors including Siemens, Schneider Electric, and Phoenix Contact issued advisories due to inherited exposure. One OEM using Fortinet/Marvell routers in their DCS stack required validation—even though they were unaffected, highlighting the detective work involved.

Strategic Risks and Recommendations:

- Each new third-party disclosure requires ICS operators to "scramble":
  - Determine which devices include the vulnerable component.
  - Assess real exploitability (e.g. is it externally reachable?).
  - Implement mitigation even when patching isn't feasible.
- Infosys C&A IoT&OT supports clients by:
  - Mapping software components to impacted products.
  - Assessing attack paths based on component exposure.
  - Advising actionable mitigations (e.g. block malicious update URLs, harden firewall configs, disable services).
- We strongly recommend:
  - Maintaining an up-to-date OT Software Bill of Materials (SBOM)
  - Requesting component disclosure transparency from vendors.
  - Establishing coordinated disclosure channels and engaging supply chain partners early—Infosys shares private PoC's with affected vendors to accelerate patches.

The Forecast

As embedded open-source tools and third-party firmware continue to be reused across ICS ecosystems, **supply chain CVEs will likely account for a growing proportion of ICS advisories**. Proactive third-party risk management—including software inventory tracking and exploit triage—will be critical for OT security resilience.

Leadership Recommendations for Proactive ICS Vulnerability Management

To stay ahead of these challenges, ICS leadership should adopt a strategic, OT-focused approach:

1. Establish an ICS-Specific VM Program

   Build a vulnerability management process tailored to

   OT. This means prioritizing "Now" ICS vulnerabilities first, and integrating OT risk metrics (safety impact, availability requirements) into triage. Use dedicated ICS scanning tools and inventory to avoid IT-centric blind spots.

2. Enforce Robust Segmentation (Purdue Model)

   Maintain strict network zones between IT and OT, and between each Purdue layer. Limit cross-zone communication to essential data flows and use firewalls/gateways to control access. Require that all remote/engineering connections go through secure jump servers or VPNs. This way, even if an external server or workstation is breached, it cannot easily reach control devices.

3. Maintain Comprehensive Asset & Bill-of-Materials Inventories

   Keep an up-to-date registry of every PLC, HMI, firmware component, and third-party library in the OT environment. When a new ICS CVE is published, immediately check this inventory to see which systems might be affected (the "scramble" process). This allows targeted and efficient patching or mitigation.

4. Partner with Vendors and Industry

   Demand that ICS product vendors follow OT-safe vulnerability practices: accurate CVSS scoring, timely patches, and clear mitigation steps. Participate in industry working groups and CERT programs to share intel. Infosys C&A IoT&OT team (and partners like Dragos, Claroty, Armis, Nozomi) contributes vulnerability analyses and whitepapers; leverage these community resources. For known ICS malware (e.g. PIPEDREAM), ensure your SOC or IDS solutions are updated with relevant IOCs and detection rules.

5. Adopt "Compensating Controls" for Slow Patches

   Recognize that some ICS patches will be delayed by operational needs. Plan for this by deploying compensating controls ahead of time. Examples: enabling restrictive firewall rules, using application whitelisting on engineering stations, or employing host-based RASP solutions on Windows-based HMIs. Infosys's analysis often finds that applying simple network segmentation or protocol filtering can neutralize a vulnerability until a patch is applied.

6. Continuous Monitoring and Incident Response

   Implement OT-aware intrusion detection and anomaly monitoring to catch exploitation attempts (especially for "Now" threats). Conduct regular incident response drills focused on ICS scenarios (e.g. simulated exploit of a critical PLC). Follow ICS Cybersecurity Frameworks: Adopt standards such as ISA/IEC 62443 or the SANS ICS Critical Controls as the foundation of your security program. These frameworks emphasize visibility, control access, and rapid patching in an OT context.

By leading with an OT-centric security culture – one that understands the unique risks and constraints of ICS – executives can significantly reduce the likelihood and impact of cyber disruptions. In particular, focusing on the small subset of truly critical vulnerabilities (as identified by our Now/Next/Never model and threat intelligence) prevents wasted effort on low-risk issues, and ensures that safety and availability remain protected.

Conclusion

ICS vulnerabilities are rising, patch gaps persist, and OT-IT convergence amplifies risk. Organizations must prioritize critical threats by enforcing segmentation and adopting compensating controls for delayed patches. Supply chain risks demand SBOM tracking and vendor transparency. With proactive triage, robust zoning, and continuous monitoring, enterprises can safeguard operations and stay ahead of adversaries.

About the Author

Michel Bruggeman
Principal Consultant | EMEA IoT & OT Lead

Michel Bruggeman is a cybersecurity leader with 25+ years of experience, specializing in operational technology (OT) security, cyber resilience, and industrial cybersecurity architecture. He has held strategic roles across the manufacturing, insurance, energy, and semiconductor sectors, focusing on ICS/OT risk assessments, secure cloud adoption, and incident response readiness. He is a SANS/ISA Mentor and Microsoft Certified Trainer, with deep expertise in NIST, IEC 62443, ISO 27001, DORA, and NIS2.

For more information, contact askus@infosys.com

Infosys®
Navigate your next