# State of Industrial Cybersecurity 2025: Attack Vectors, Geopolitical Risk, and Defensive Imperatives in the Manufacturing Sector

## Executive Summary: The New Cyber-Kinetic Reality for Manufacturing

The global manufacturing sector in 2025 confronts a threat landscape where the boundary between digital risk and physical consequence has effectively dissolved. Cyberattacks are no longer abstract threats to data; they are direct, tangible assaults on operational continuity, safety, and the integrity of global supply chains. This report provides an exhaustive analysis of the emerging attack vectors, adversary tactics, and geopolitical pressures defining this new cyber-kinetic reality, with a specific focus on the intelligence and events of June, July, and August 2025.

The analysis reveals four critical, overarching trends that demand immediate strategic attention from industrial leaders. First, the manufacturing sector has become the undisputed epicenter of industrial cyber conflict. It is the most targeted industry by a significant margin, accounting for over two-thirds of all ransomware incidents targeting industrial organizations. Adversaries, particularly financially motivated ransomware groups, exploit the sector's extreme sensitivity to downtime, transforming operational pressure into financial leverage.

Second, the nature of the initial intrusion has fundamentally shifted. The dominant attack vector is no longer a sophisticated exploit targeting the operational technology (OT) network directly. Instead, adversaries are "logging in" to the corporate information technology (IT) environment using stolen credentials—harvested at an industrial scale by infostealer malware—and moving laterally into OT systems. This pivot towards identity-based attacks renders traditional perimeter defenses insufficient and makes early-stage threat detection significantly more challenging.

Third, geopolitical instability has become a direct and measurable cyber risk. Heightened conflicts, particularly between Iran and Israel, are fueling a surge in state-sponsored and hacktivist campaigns against U.S. critical infrastructure. Concurrently, international trade disputes and physical shipping disruptions are creating systemic fragility in supply chains, a vulnerability that threat actors are systematically exploiting to amplify the impact of their attacks. The modern supply chain is a cyber-physical system, and its integrity is now a key front in global strategic competition.

Fourth, defensive strategies must undergo a paradigm shift. The obsolescence of the "air gap" and the ineffectiveness of perimeter-only security models necessitate a move towards a resilience-focused, threat-informed posture. This requires grounding security architecture in Zero Trust principles, implementing rigorous identity and access management at the IT/OT boundary, and developing robust, OT-aware incident response capabilities designed to manage cyber-kinetic events. Frameworks such as NIST SP 800-82 Revision 3 and IEC 62443 provide the strategic roadmaps, but their successful implementation demands a deep, contextual understanding of the specific adversary playbooks and vulnerabilities detailed in this report. The stakes are no longer just financial; they are operational, reputational, and in some cases, existential.

## I. The 2025 Industrial Threat Landscape: A Convergence of Risk

The security landscape for industrial control systems (ICS) in 2025 is defined by a convergence of technological, financial, and operational risks. The traditional security models that once protected manufacturing environments have been rendered obsolete by digital transformation, creating a deeply interconnected and profoundly vulnerable ecosystem. This section analyzes the foundational trends shaping this new era of industrial cyber risk.

### 1.1 The Dissolution of the Air Gap: IT/OT Convergence as the Primary Threat Vector

The foundational premise of modern industrial cybersecurity is that the "air gap"—the physical or logical separation between IT and OT networks—is no longer a viable defense. The relentless pace of digital transformation, driven by Industry 4.0 initiatives, has created a hyper-converged environment where enterprise resource planning (ERP) systems, cloud platforms, and AI models now interact directly with SCADA, MES, HMIs, and PLCs.1 This convergence, while unlocking significant operational efficiencies, has simultaneously dismantled the perimeters that once protected critical processes.1

The data from 2025 provides unequivocal evidence of this trend's security implications. A SANS survey reveals that IT compromises are the leading initial attack vector for OT incidents, identified by 58% of responding organizations. This is followed by internet-accessible devices (33%) and transient devices like USBs (27%), all of which highlight the porosity of the modern industrial network.4 The belief in a mythical air gap is dangerously misguided; research from Claroty confirms that 40% of industrial organizations have OT assets, such as PLCs and HMIs, that are insecurely connected to the public internet.5 Even historically isolated environments are now being connected to support remote diagnostics, feed AI models, or optimize energy consumption, creating new and often unmonitored pathways for adversaries.1

This convergence introduces IT-centric threats directly into the OT domain, an environment fundamentally ill-equipped to handle them. OT systems were designed to prioritize uptime, speed, and deterministic control, not security.1 Consequently, legacy industrial protocols like Modbus and OPC-UA, which form the backbone of many manufacturing operations, lack basic encryption or authentication mechanisms.1 Once an attacker successfully traverses the IT/OT boundary, they often find a soft, undefended landscape where they can move with relative impunity.

### 1.2 The Escalating Scale and Impact: From Data Breach to Physical Disruption

While some metrics suggest a stabilization in the raw volume of malicious objects detected on ICS computers 6, the tangible impact of successful attacks is escalating dramatically. The nature of the threat has evolved from data theft to direct, physical disruption of industrial processes. The 2025 OT Cyber Threat Report from Waterfall Security provides a stark illustration of this trend, documenting a staggering 146% increase in the number of industrial sites suffering physical consequences from cyberattacks, a figure that rose from 412 sites in 2023 to 1,015 in 2024.7

The financial stakes associated with these cyber-kinetic events are immense. A landmark 2025 report from Dragos and Marsh McLennan projects that the global financial risk exposure from OT cyber incidents could exceed $300 billion. Critically, this model demonstrates that the true cost of an OT incident extends far beyond the initial ransom or direct recovery expenses. Indirect losses—such as those from precautionary shutdowns, disrupted supply chains, contractual penalties, and reputational damage—account for up to 70% of the total financial impact of a breach.2 This reframes OT cyber risk as a systemic economic threat, not merely an isolated corporate problem. An attack on a single manufacturer, for instance, can trigger a cascading failure across an entire supply chain, forcing shutdowns at downstream partners and customers.8

Case studies from 2025 vividly illustrate this reality. In May, a cyber incident at Nucor Corporation, the largest steel producer in the United States, forced the company to suspend production across several facilities.9 Similarly, a ransomware attack in March against National Presto Industries, a manufacturer of consumer goods and defense products, led to a system-wide outage that disrupted manufacturing, shipping, and back-office functions.11 These incidents confirm that IT-level breaches are now routinely causing the cessation of physical industrial operations.

### 1.3 The Resource and Budgeting Mismatch

Despite the clear and escalating risk, the allocation of resources for OT security remains a significant challenge, revealing a dangerous divergence between the magnitude of the threat and the organizational response. While 55% of organizations report budget growth for ICS/OT security, a 2025 SANS survey found that only 9% of cybersecurity professionals dedicate 100% of their time to it.4 This indicates a critical gap in specialized, dedicated expertise. The convergence of IT and OT has led many organizations to treat OT security as a mere extension of IT security, a structural flaw reflected in budgeting practices. Approximately 37% of organizations operate with a shared IT/OT budget, while in 31% of cases, the IT department controls the budget entirely.4

This structure often leads to OT-specific security needs—such as managing legacy systems, securing proprietary protocols, and addressing physical safety requirements—being overlooked in favor of traditional IT priorities. The unique constraints of OT, where a security tool misfire could cause physical harm or halt production, are not always understood or properly accounted for by IT-centric teams.3 This misapplication of resources and failure to address OT-specific vulnerabilities directly contributes to the rise in successful attacks with physical consequences. The problem is not simply a lack of budget but a structural and skills-based misalignment. Compounding this issue is a lack of mature, strategic financial planning; a significant 34% of organizations admit to being unsure about their overall security budget allocations, highlighting a reactive rather than proactive approach to managing this critical risk area.4

## II. Emerging Attack Vectors and Adversary Playbooks (Mapped to MITRE ATT&CK for ICS)

The effectiveness of modern adversaries lies not in overwhelming technical sophistication but in their ability to exploit the seams of converged IT/OT environments with stealth and precision. They are increasingly weaponizing the tools, credentials, and protocols native to the target environment, a doctrine of "legitimacy-as-a-weapon" that makes their actions difficult to distinguish from normal administrative activity. This section analyzes the evolving Tactics, Techniques, and Procedures (TTPs) of industrial threat actors, mapped to the MITRE ATT&CK for ICS framework.

### 2.1 Initial Access (TA0108): The Shift from "Hacking In" to "Logging In"

The primary evolution in adversary TTPs in 2025 is a decisive pivot toward identity-based attacks. Mandiant's M-Trends 2025 report reveals a landmark shift: for the first time, the use of **stolen credentials (T1078)** has surpassed **email phishing (T1566)** as the second most common initial infection vector, accounting for 16% of intrusions compared to phishing's 14%.12 This trend is fueled by an underground economy built on the industrial-scale harvesting of credentials via infostealer malware. The first half of 2025 alone saw an 800% year-over-year increase in credentials stolen by infostealers, creating a vast, readily available marketplace of valid accounts for adversaries to purchase and abuse.10 This method is profoundly effective because a "legitimate" login is far stealthier and more likely to bypass perimeter defenses than a noisy exploit attempt.

While identity is the new frontier, traditional vectors remain potent. **Exploitation of public-facing applications (T1190)** continues to be the most common initial access method overall, responsible for 33% of intrusions.13 In the OT context, this is particularly dangerous. Claroty's research found that 40% of organizations have OT assets insecurely connected to the internet, providing a direct path for attackers.5 This includes unpatched vulnerabilities in VPNs, RDP gateways, and other remote access services that are frequently exploited by ransomware groups.16

Furthermore, the human element is being targeted with unprecedented sophistication, creating a "trust crisis" at the last line of defense. The use of generative AI has led to a reported 1,265% increase in AI-driven phishing campaigns.10 These attacks are no longer characterized by the grammatical errors and generic lures of the past; they are hyper-personalized, context-aware, and linguistically flawless. Threat groups like BlackCat have taken this a step further, specializing in advanced social engineering and voice phishing (vishing), where they impersonate help desk staff in phone calls to trick employees into revealing credentials or approving MFA prompts.18 This evolution fundamentally undermines traditional security awareness training and shifts the defensive imperative from employee vigilance to technical enforcement.

### 2.2 Lateral Movement (TA0109) and Privilege Escalation (TA0111): Bridging the IT/OT Divide

Once an adversary gains a foothold in the IT network, their primary objective is to pivot to the high-value OT environment. This is accomplished through a patient and methodical process of discovery, credential theft, and lateral movement, often using legitimate administrative tools to "live off the land" and evade detection.

Upon entry, attackers use discovery techniques such as **Remote System Discovery (T1018)** and **Network Share Discovery (T1135)** to map the internal network architecture.20 Their goal is to identify critical assets that bridge the IT and OT worlds, such as Engineering Workstations (EWS), data historians, and HMI servers.

To move between systems, adversaries rely heavily on a common toolkit of legitimate and dual-use software. Tools like **PsExec**, the **Cobalt Strike** framework, credential dumpers like **Mimikatz**, and data transfer utilities like **Rclone** are consistently observed in industrial ransomware incidents.16 Because these tools are often used by system administrators, their malicious use can be difficult to detect without sophisticated behavioral analytics.

Privilege escalation within the Windows-dominated IT side of the house is a critical step. The Conti ransomware group's leaked playbooks show a heavy reliance on Active Directory reconnaissance tools like **ADfind** and **BloodHound** to identify misconfigurations. They then use techniques like **Kerberoasting (T1558.003)** to steal service account credentials and elevate their privileges, giving them the access needed to compromise key systems and push malware across the network.20

### 2.3 Impact (TA0105) and Impair Process Control (TA0106): The Cyber-Kinetic Endgame

The ultimate objective in a dedicated OT attack is to manipulate, disrupt, or destroy the physical process. Adversaries have a range of techniques at their disposal to achieve this cyber-kinetic endgame. Nozomi Networks reports that nearly half (48.4%) of all observed threat alerts in critical infrastructure occur in the "Impact" phase of the cyber kill chain, demonstrating a clear and persistent adversary intent to cause tangible disruption.22

A direct method is **Manipulation of Control (T0831)**, where an attacker who has compromised a PLC or DCS sends unauthorized command messages to alter a physical process—for example, changing a chemical mixture, over-pressurizing a vessel, or disabling a cooling system.23

A more sophisticated and dangerous approach involves targeting the systems designed to prevent such outcomes. Through the tactic of **Inhibit Response Function (TA0107)**, adversaries can disable safety, protection, and operator intervention functions. This can include techniques like **Alarm Suppression (T0878)**, where alarm thresholds are modified or disabled, effectively blinding operators to a developing hazardous state.23

Finally, ransomware remains a primary tool for causing impact. While **Data Encrypted for Impact (T1486)** is an IT-centric technique, its application in an OT environment has profound physical consequences. Encrypting the files on an HMI or a data historian server leads to a **Loss of View (T0829)** for operators. Unable to see or control the process, their only safe course of action is to initiate an emergency shutdown, resulting in a **Loss of Control (T0827)** and immediate production stoppage.23 This is precisely why ransomware is so effective against manufacturers: the threat of operational paralysis is often more compelling than the threat of data loss.

## III. Analysis of Recent Vulnerability Disclosures in Manufacturing Technologies (June-August 2025)

The theoretical attack surface described in the previous section is grounded in a continuous stream of real-world vulnerabilities discovered in the hardware and software that underpin modern manufacturing. The summer of 2025 saw a significant number of disclosures affecting a wide range of ICS components, from high-level SCADA systems to low-level embedded controllers. This analysis highlights the most critical of these flaws, demonstrating the tangible and exploitable weaknesses present in the industrial ecosystem. A systemic weakness is emerging in how remote management interfaces are implemented in OT devices, leading to a crisis of critical, unauthenticated vulnerabilities that can grant attackers complete control.

### 3.1 SCADA and Radio System Vulnerabilities

High-level supervisory systems remain a prime target for attackers seeking broad control over an industrial process.

* **Mitsubishi Electric / Iconics SCADA (CVE-2024-1182, CVE-2024-7587, etc.):** In March 2025, details emerged regarding a cluster of high-severity vulnerabilities in the widely used Genesis64 and MC Works64 SCADA products. The flaws include DLL hijacking, incorrect default permissions, and uncontrolled search path elements. While these vulnerabilities require an attacker to be authenticated, they are perfect tools for the second stage of an attack. An adversary who has already gained a foothold and stolen credentials can leverage these flaws to escalate privileges, manipulate critical files, and execute arbitrary code on the SCADA server, effectively seizing control of the entire supervised process.25
* **TETRA Radio Systems (CVE-2025-52941, CVE-2025-52945, etc.):** A series of critical vulnerabilities were disclosed in Sepura radio firmware. These systems are used globally for voice and data communications in critical infrastructure, including as a transport layer for SCADA WANs. The flaws allow for the exfiltration of cryptographic keys and arbitrary code execution with only brief physical access to a device. More alarmingly, one vulnerability (**CVE-2025-52944**) allows for the injection of arbitrary messages onto the network. For a utility that uses TETRA to control remote assets, this could allow an attacker to send spoofed commands, creating a severe risk of physical disruption.26

### 3.2 Human-Machine Interface (HMI) Vulnerabilities

HMIs are the critical link between human operators and the industrial process. Vulnerabilities in these systems can blind operators or trick them into performing unsafe actions.

* **JTEKT HMI (CVE-2025-24317):** An unauthenticated resource allocation vulnerability was found in the ViewJet C-more series and GC-A2 series HMIs. A remote, unauthenticated attacker can exploit this flaw to cause a Denial-of-Service (DoS) condition. In a control room setting, this attack would crash the HMI screen, instigating a **Loss of View (T0829)** and forcing operators to perform an emergency shutdown of the process they can no longer see or control.27
* **CONPROSYS HMI (CVE-2025-34080):** A reflected Cross-Site Scripting (XSS) vulnerability was discovered in the CONPROSYS HMI System (CHS). This flaw could allow an attacker to execute malicious scripts in an operator's web browser by tricking them into clicking a specially crafted link. This could be used to steal the operator's session cookies, hijack their session, or present a fake login prompt to harvest their credentials.29

### 3.3 Programmable Logic Controller (PLC) and Embedded System Vulnerabilities

Vulnerabilities at the controller level represent the most direct threat to the physical process.

* **Erlang/OTP SSH Implementation (CVE-2025-32433):** This is one of the most severe vulnerabilities to emerge in 2025, with a maximum CVSS score of 10.0. It is a pre-authentication Remote Code Execution (RCE) flaw in the built-in SSH server of the widely used Erlang/Open Telecom Platform (OTP). The vulnerability is a simple logic bug where the server fails to reject post-authentication messages sent during the initial, unauthenticated handshake. An attacker with network access to a vulnerable device can send a single, specially crafted SSH packet to gain full root-level command execution without providing any credentials. Erlang/OTP is used in a wide range of embedded systems, including PLCs, IoT gateways, and other industrial controllers. This flaw allows for the complete, silent, and trivial takeover of any such device exposed on a network, making it a critical threat.30
* **Schneider Electric Modicon Controllers (CVE-2025-3905):** An XSS vulnerability was found that impacts PLC system variables. This flaw allows an *authenticated* malicious user to inject data that is then rendered in a victim's browser, potentially allowing for data modification or theft. While requiring prior authentication, this vulnerability is a prime example of an "authenticated but unsafe" flaw. An attacker who has already compromised IT credentials can use them to log into the PLC's web interface and then exploit this vulnerability as part of a longer attack chain to manipulate the controller or deceive an operator.31

### 3.4 Vendor-Specific Advisories (June-August 2025)

The consistent issuance of security advisories from major ICS vendors throughout the summer of 2025 underscores the pervasive nature of vulnerabilities in the industrial supply chain. CISA released dozens of advisories during this period, highlighting significant issues across multiple product lines.

* **Schneider Electric:** Was the subject of multiple advisories for its Modicon Controllers, EcoStruxure platform, and other products.32 Most notably, a critical vulnerability (  
  **CVE-2025-50121**) was disclosed in the EcoStruxure Data Center Expert (DCE) platform. This unauthenticated OS command injection flaw, with a CVSS score of 10.0, allows a remote attacker to achieve complete system takeover, posing a severe risk to data center environments that often support manufacturing operations.35
* **Rockwell Automation:** An advisory was released for a remote code execution vulnerability (**CVE-2025-6376**) in its Arena Simulation software. Exploitation requires a user to open a malicious file, a common phishing scenario, and could allow an attacker to execute arbitrary code on the engineer's system.36
* **Siemens:** Multiple security advisories were published, indicating an ongoing and active process of vulnerability discovery and remediation within their extensive product portfolio.37
* **Other Major Vendors:** Advisories also covered significant vulnerabilities in products from Johnson Controls, AVEVA, Honeywell, Delta Electronics, and Mitsubishi Electric, demonstrating that this is an industry-wide challenge, not an issue confined to a single supplier.32

**Table 1: Summary of Critical ICS Vulnerabilities (Q3 2025)**

| CVE ID | Affected Vendor/Product | Vulnerability Type | CVSS Score (v3.1) | Potential Impact on Manufacturing Operations |
| --- | --- | --- | --- | --- |
| **CVE-2025-32433** | Erlang/OTP (in PLCs, IoT) | Pre-Authentication RCE | 10.0 | Complete, unauthenticated takeover of PLC/controller; manipulation of physical processes; implantation of persistent backdoors. |
| **CVE-2025-50121** | Schneider Electric EcoStruxure DCE | Unauthenticated OS Command Injection | 10.0 | Full compromise of data center monitoring systems, potentially leading to cascading failures impacting plant operations. |
| **CVE-2024-1182** | Mitsubishi Electric / Iconics SCADA | DLL Hijacking | 7.8 (High) | Privilege escalation on SCADA server; potential for process manipulation and full system takeover by an authenticated attacker. |
| **CVE-2025-6376** | Rockwell Automation Arena | Remote Code Execution | 7.8 (High) | Compromise of engineering workstation via malicious file; potential pivot point into the OT network. |
| **CVE-2025-52944** | TETRA Radio Systems (Sepura) | Arbitrary Message Injection | High | Injection of spoofed commands into SCADA WANs, causing disruption to remote utility or manufacturing process controls. |
| **CVE-2025-24317** | JTEKT HMI ViewJet / GC-A2 | Unauthenticated Resource Allocation (DoS) | 5.3 (Medium) | Blinding of HMI, forcing operational shutdown due to Loss of View; disruption of operator oversight. |

## IV. The Ransomware Epidemic in Manufacturing: Threat Actor Deep Dive

Ransomware has evolved from a threat against data to a primary driver of operational shutdowns in the industrial world. For manufacturing, an industry built on just-in-time production and minimal tolerance for disruption, this evolution has been catastrophic. The sector is now ground zero for industrial ransomware, targeted by a sophisticated and industrialized ecosystem of cybercriminals who have honed their tactics to maximize operational pain and, by extension, their financial returns.

### 4.1 Manufacturing: Ground Zero for Industrial Ransomware

An overwhelming consensus from multiple threat intelligence sources confirms that manufacturing is the most heavily targeted industrial sector. Dragos's quarterly analyses show that manufacturing consistently accounts for the vast majority of industrial ransomware incidents, representing 68% of the total in Q1 2025 (480 incidents) and 65% in Q2 (428 incidents).11 This finding is corroborated by Bitsight's 2025 "State of the Underground" report, which identifies manufacturing as the most targeted industry for the third consecutive year and notes that nearly half of all breaches in the sector are ransomware-related.8

The motivation behind this intense focus is purely economic. Adversaries understand that the business model of modern manufacturing is predicated on continuous operation. According to Siemens, unplanned downtime accounts for approximately 11% of annual revenue for Fortune 500 companies.8 When a production line stops, the financial losses are immediate and substantial, making manufacturers highly susceptible to extortion and more likely to pay a ransom to restore operations quickly.8

### 4.2 Threat Actor Profiles: The Dominant and the Dangerous

The ransomware threat is not monolithic. It is a dynamic ecosystem composed of specialized groups, each with distinct TTPs, business models, and targeting preferences. Understanding these key players is critical for developing a threat-informed defense.

* **Qilin:** Emerged as the most active group in Q2 2025, responsible for 101 industrial incidents. Qilin has evolved beyond a typical criminal enterprise into a sophisticated, state-aligned threat actor, aggressively recruiting affiliates from defunct groups and professionalizing its Ransomware-as-a-Service (RaaS) platform. Its TTPs include the rapid exploitation of critical vulnerabilities in edge devices, particularly Fortinet products, for initial access.42
* **Cl0p:** This group was responsible for a massive surge of attacks in Q1 2025, with 154 industrial incidents. Cl0p's primary TTP is the exploitation of zero-day vulnerabilities in Managed File Transfer (MFT) software, such as products from Cleo and CrushFTP. Their strategy often forgoes encryption entirely, focusing instead on mass data theft followed by extortion. This "encryption-less" model is highly effective against manufacturing supply chains, where the threat of leaking sensitive intellectual property or customer data is a powerful motivator for payment.11
* **LockBit 3.0:** Despite significant law enforcement disruption, LockBit and its affiliates remain a persistent threat. A May 2025 leak of the group's internal database provided unprecedented insight into its operations. The data revealed a strategic bias toward the Asia-Pacific region and a "volume over value" approach, targeting smaller, less cyber-mature organizations for faster, smaller payouts. A key TTP is a strategic delay—sometimes days—between initial compromise and the final encryption, a period used for extensive data exfiltration and lateral movement.44
* **BlackCat (ALPHV):** A prolific RaaS operator known for its triple-extortion tactics: demanding payment to decrypt files, to prevent the leaking of stolen data, and to avoid a Distributed Denial-of-Service (DDoS) attack.46 BlackCat affiliates are adept at advanced social engineering, using tools like Evilginx2 to bypass MFA and deploying legitimate remote access software like AnyDesk for persistence. They disproportionately target manufacturing alongside healthcare and business services.18
* **Conti (and Successors):** Although the Conti brand is defunct, its leaked internal playbooks, training materials, and toolsets continue to be used by numerous successor and splinter groups. The Conti TTPs represent a masterclass in modern ransomware operations, detailing the extensive use of open-source and legitimate tools for discovery (ADfind, BloodHound), credential access (Invoke-Kerberoast), lateral movement (PsExec), and data exfiltration (Rclone).16
* **Emerging Groups of 2025:** The landscape is constantly fragmenting and evolving. New and resurgent groups identified in mid-2025 include **FunkSec**, which operates a hybrid RaaS/hacktivist model; **DragonForce**, which evolved from a hacktivist collective into a financially motivated ransomware operation; and other notable players like **SafePay**, **Akira**, and **Play**.11 This dynamism indicates a resilient and adaptive criminal ecosystem.

### 4.3 Evolving Ransomware TTPs

Beyond the specifics of individual groups, several overarching trends in ransomware TTPs were prominent in 2025.

* **AI-Enhanced Social Engineering:** Threat actors are leveraging generative AI to automate and scale the creation of highly convincing phishing emails and social engineering lures. Groups like Black Basta have been observed using AI-assisted tactics, including impersonating IT support personnel in sophisticated vishing campaigns, to trick employees into granting remote access.17
* **Systematic Targeting of the Supply Chain:** Adversaries increasingly recognize that targeting a third-party vendor or software supplier is often an easier path into a hardened manufacturing target. This makes supply chain security a critical defensive battleground.8 The attack by the SafePay group on a major global technology and supply chain services provider exemplifies this trend, where the compromise of one entity had cascading implications for its many customers.43
* **Exploitation of Edge Devices and Remote Management Tools:** The network perimeter remains a key point of entry. Vulnerabilities in VPNs, firewalls (e.g., Fortinet), and Remote Monitoring and Management (RMM) software (e.g., SimpleHelp) are actively sought out and exploited by ransomware affiliates to gain initial access and move laterally into victim networks.17

**Table 2: Profile of Top Ransomware Groups Targeting Manufacturing**

| Group Name | Primary TTPs (Initial Access, Exfiltration, Impact) | Notable 2025 Targets/Campaigns | Key MITRE ATT&CK Techniques |
| --- | --- | --- | --- |
| **Qilin** | Exploits Fortinet VPNs (CVE-2024-21762); professionalized RaaS platform; aggressive affiliate recruitment. | Dominant group in Q2 2025; state-aligned; targets manufacturing, transportation. | T1190: Exploit Public-Facing Application, T1486: Data Encrypted for Impact |
| **Cl0p** | Mass data theft via MFT zero-day exploits (e.g., Cleo); primarily uses "encryption-less" extortion model. | Massive surge in Q1 2025 targeting manufacturing supply chains; over 154 industrial victims. | T1190: Exploit Public-Facing Application, T1567: Exfiltration over Web Service |
| **LockBit 3.0** | Uses stolen credentials; strategic delay between compromise and encryption; focuses on data exfiltration. | Leaked database revealed focus on APAC and smaller firms; still active despite law enforcement takedown. | T1078: Valid Accounts, T1048: Exfiltration Over Alternative Protocol |
| **BlackCat (ALPHV)** | Advanced social engineering (vishing) to bypass MFA; RaaS model; triple extortion (encrypt, leak, DDoS). | Consistently targets manufacturing and healthcare; uses legitimate remote access tools for persistence. | T1566: Phishing, T1219: Remote Access Software, T1486: Data Encrypted for Impact |

## V. Geopolitical Flashpoints and Supply Chain Cyber Risk (June-August 2025)

In the interconnected global economy of 2025, geopolitical conflict and trade disputes are no longer separate from cybersecurity; they are threat vectors in their own right. The summer of 2025 was marked by a volatile international climate that directly fueled cyber operations against industrial targets and placed unprecedented stress on manufacturing supply chains. Adversaries are leveraging this instability, transforming logistical challenges into cybersecurity crises.

### 5.1 State-Sponsored Threats in a Tense Global Climate

The period of June through August 2025 saw a significant escalation in cyber activity linked to geopolitical tensions, particularly the ongoing conflict between Israel and Iran. This conflict has spilled over into cyberspace, with both state-sponsored Advanced Persistent Threat (APT) groups and ideologically motivated hacktivist collectives launching waves of attacks.19

In response, U.S. cybersecurity and intelligence agencies issued joint advisories urging organizations in critical infrastructure sectors to adopt a "Shields Up" posture. These alerts specifically warned of increased cyberattacks from Iranian state-sponsored actors and their affiliates targeting U.S. entities, with a particular focus on the Defense Industrial Base (DIB) and sectors with ties to Israel.49 The threat is not abstract; Waterfall Security's 2025 report notes that nation-state threats have tripled, with actors employing tactics like widespread GPS jamming and spoofing that have direct, disruptive consequences for transportation and logistics, which are integral to manufacturing supply chains.7 The World Economic Forum's Global Cybersecurity Outlook confirms this trend, with nearly 60% of organizations reporting that geopolitical tensions have directly affected their cybersecurity strategy, and a third of CEOs expressing concern about state-sponsored cyber espionage.50

### 5.2 The Weaponization of the Supply Chain

The modern supply chain is a complex, globally distributed cyber-physical system, and its inherent fragility is being systematically weaponized. Geopolitical and trade disputes create physical and logistical disruptions that, in turn, create opportunities for cyber adversaries.

* **Physical Disruptions as a Catalyst for Cyberattacks:** Ongoing Houthi attacks in the Red Sea have forced a 75% reduction in container traffic through the Suez Canal, compelling ships to take longer, costlier routes and causing severe delays.51 Simultaneously, new international trade disputes have led to a sharp increase in tariffs on crucial manufacturing materials like steel and aluminum, which rose to 50% in June 2025.51 This environment of constant disruption, re-routing, and supplier changes creates widespread confusion. Adversaries exploit this chaos to launch highly effective social engineering campaigns. An email from a "supplier" about a "shipping delay" is now a common and believable pretext for delivering a malicious payload.
* **Targeting the Weakest Link:** Threat actors understand that the security of a manufacturing enterprise is defined by the security of its weakest partner. The summer of 2025 saw a marked increase in attacks targeting third-party suppliers and logistics providers. A July 2025 analysis of global breaches revealed that third-party exposure was the dominant cause of the month's largest incidents. Major breaches at retailers Co-op and airline Qantas, for example, stemmed not from their own networks but from compromises at a loyalty program provider and a contact-center platform, respectively.52 In the industrial space, the cyberattack on United Natural Foods, a major food distributor, underscored the vulnerability of logistics networks that are critical to the manufacturing and consumer goods sectors.19
* **Software and Developer Ecosystem Compromises:** The risk extends beyond physical goods to the software supply chain. Incidents involving malicious packages being uploaded to developer repositories like NPM demonstrate how adversaries can compromise a single software component and have that malicious code propagate downstream to countless manufacturing organizations that rely on it.52 This exploitation of implicit trust within the supply chain represents a sophisticated and scalable attack vector.

## VI. Strategic Recommendations for Building a Defensible OT Architecture

The complexity and severity of the 2025 threat landscape demand a fundamental evolution in how manufacturing organizations approach cybersecurity. A reactive, compliance-driven posture is no longer sufficient. The strategic imperative is to build a threat-informed, resilience-focused security program designed to withstand and recover from attacks with minimal operational disruption. This section provides actionable recommendations, structured around globally recognized frameworks, to build a defensible and resilient OT architecture.

### 6.1 Foundational Strategy: Adopting a Threat-Informed, Resilience-Focused Posture

The starting point for any effective OT security program is the acknowledgment that a breach is not a matter of if, but when. Data shows that 27% of organizations experienced one or more security incidents involving ICS/OT systems in the past year.4 Therefore, the primary goal must shift from perfect prevention to operational resilience.

This requires a threat-informed defense strategy. Organizations must move beyond generic security controls and actively map their defenses against the specific TTPs used by adversaries targeting their sector. Leveraging the **MITRE ATT&CK for ICS framework** is essential for this process. It provides a common language and a structured knowledge base of real-world adversary behaviors, enabling security teams to conduct gap analyses, prioritize defensive investments, and run threat hunting exercises based on the most likely attack paths.53

### 6.2 Implementing a Modern OT Security Architecture (NIST SP 800-82 Rev. 3)

The National Institute of Standards and Technology's (NIST) Special Publication 800-82 Revision 3, "Guide to Operational Technology (OT) Security," provides a comprehensive roadmap for securing modern industrial environments. It expands the scope from legacy ICS to the broader category of OT and places a significant emphasis on cybersecurity in today's interconnected world.57 Key recommendations for manufacturers include:

* **Develop a Cross-Functional OT Cybersecurity Program:** Security cannot be the sole responsibility of the IT department. NIST guidance emphasizes the need to establish a dedicated, cross-functional team that includes IT security personnel, control engineers, plant operators, and physical safety experts. This ensures that security decisions are made with a full understanding of their potential impact on operations and safety.57
* **Conduct OT-Specific Risk Assessments:** Risk assessments must go beyond traditional IT-centric models to fully account for the potential for physical damage, environmental impact, and threats to human safety. A best practice is to integrate cyber-attack scenarios into existing engineering risk analysis processes like Process Hazard Analysis (PHA) and Failure Mode and Effects Analysis (FMEA).59
* **Implement a Zero Trust Architecture for OT:** Given that compromised credentials are a primary initial access vector, a Zero Trust architecture is no longer optional. This security model operates on the principle of "never trust, always verify." It requires strict identity verification and least-privilege access for every user, device, and application attempting to access a resource on the OT network, regardless of whether they are inside or outside the traditional perimeter. This is critical for controlling access across the IT/OT boundary.59

### 6.3 Achieving Target Security Levels (IEC 62443)

The ISA/IEC 62443 series of standards offers a structured, risk-based methodology for implementing security controls in Industrial Automation and Control Systems (IACS). It is designed to be applied across all industrial sectors and provides a framework for shared responsibility among asset owners, system integrators, and product suppliers.62 For manufacturers, key implementation steps include:

* **Define Zones and Conduits:** The first and most critical step is to perform a detailed audit of all network assets and segment the network into logical zones based on function and criticality (e.g., enterprise zone, manufacturing/process zone, safety zone). All data flows between these zones must be strictly controlled through secure conduits, which are protected by firewalls, unidirectional gateways, or other security technologies.62
* **Determine and Implement Target Security Levels (SLs):** IEC 62443 defines four Security Levels (SL 1-4) that represent increasing levels of protection against more sophisticated threats. A risk assessment should be used to determine the appropriate target SL for each zone. A critical safety system, for example, may require SL3 or SL4 controls, while a less critical monitoring system might be adequately protected at SL2. This allows for a cost-effective, risk-based application of security controls.62
* **Use a Defense-in-Depth Strategy:** This foundational security principle involves layering multiple, independent security controls throughout the architecture. This includes perimeter protection, network segmentation, device hardening (e.g., disabling unused ports and services), application control (whitelisting), and continuous monitoring. The goal is to ensure that the failure of a single control does not result in a complete system compromise.64

### 6.4 Prioritized Tactical Mitigations for 2025

Based on the specific threats and TTPs identified in this report, the following tactical actions should be prioritized to achieve the greatest immediate risk reduction:

1. **Harden the IT/OT Boundary with Strong Identity and Access Management (IAM):** The abuse of valid credentials is the most effective adversary tactic in 2025. Counter this by enforcing phishing-resistant Multi-Factor Authentication (MFA) for all remote access into the industrial network and for any user or system accessing critical OT assets. Implement robust Privileged Access Management (PAM) solutions to vault, rotate, and monitor the use of all administrator and service accounts that have access to OT systems.
2. **Establish Comprehensive OT Visibility and Monitoring:** An organization cannot protect what it cannot see. Deploy network monitoring solutions specifically designed for OT environments. These tools should be capable of deep packet inspection for industrial protocols (e.g., Modbus, Profinet, EtherNet/IP) to establish a baseline of normal operations and detect anomalous behavior indicative of adversary activity, such as unauthorized device communication, unusual command messages, or attempts at lateral movement.65
3. **Develop a Risk-Based Vulnerability Management Program:** The "patch everything" approach of IT is often impossible and unsafe in OT. Instead, develop a risk-based program that prioritizes vulnerabilities not just by CVSS score, but by their real-world exploitability, their potential impact on the specific industrial process, and the presence of any compensating controls. Critical, unauthenticated RCE vulnerabilities like CVE-2025-32433 on internet-facing or otherwise accessible devices demand immediate action, which may involve isolating the device from the network until a patch can be safely applied.24
4. **Strengthen Supply Chain Cyber Hygiene:** A manufacturer's security is only as strong as its weakest supplier. Make cybersecurity a core component of procurement and vendor management. Mandate adherence to standards like IEC 62443 in vendor contracts. Conduct rigorous security assessments of critical suppliers, and strictly enforce the principle of least privilege for all third-party network access.
5. **Create and Rehearse a Cyber-Kinetic Incident Response Plan:** Traditional IT data breach response plans are inadequate for OT incidents. Develop and regularly test specific playbooks that integrate OT engineers, plant operators, and safety personnel. Conduct tabletop exercises that simulate the most likely and most damaging scenarios identified in this report, such as a ransomware-induced plant shutdown, the blinding of an HMI during a critical process, or the compromise of a safety instrumented system.

#### Works cited

1. How Cyber Risk Is Reshaping Manufacturing in 2025, accessed August 15, 2025, <https://manufacturing-today.com/news/how-cyber-risk-is-reshaping-manufacturing-in-2025/>
2. OT cyber risk could exceed $300 billion, pushed by indirect losses ..., accessed August 15, 2025, <https://industrialcyber.co/risk-management/ot-cyber-risk-could-exceed-300-billion-pushed-by-indirect-losses-and-cascading-system-failures/>
3. Guide to Industrial Control Systems (ICS) Cybersecurity | Claroty, accessed August 15, 2025, <https://claroty.com/blog/cybersecurity-dictionary-industrial-control-systems-ics-security>
4. 2025 ICS/OT Cybersecurity Budget: Spending Trends ... - OPSWAT, accessed August 15, 2025, <https://info.opswat.com/hubfs/OT%20-%20Assets/Survey_2025-ICS-OT-Budget.pdf>
5. Claroty exposes OT security crisis, reveals insecure Internet ..., accessed August 15, 2025, <https://industrialcyber.co/industrial-cyber-attacks/claroty-exposes-ot-security-crisis-reveals-insecure-internet-connections-amid-rising-ransomware-threats/>
6. Threat landscape for industrial automation systems. Q1 2025 ..., accessed August 15, 2025, <https://ics-cert.kaspersky.com/publications/reports/2025/05/15/threat-landscape-for-industrial-automation-systems-q1-2025/>
7. The 2025 OT Cyber Threat Report | Waterfall Security Solutions, accessed August 15, 2025, <https://waterfall-security.com/ot-insights-center/ot-cybersecurity-insights-center/2025-threat-report-ot-cyberattacks-with-physical-consequences/>
8. Supply Chains Under Siege: Inside the Cyber Threats on Manufacturing, accessed August 15, 2025, <https://www.bitsight.com/blog/inside-cyber-threats-in-manufacturing-2025>
9. Major Cyber Attacks Targeting Manufacturing Industry in 2025 ..., accessed August 15, 2025, <https://socradar.io/major-cyber-attacks-manufacturing-industry-in-2025/>
10. Top Industries Hackers Hit in 2025: 26% on Manufacturing, accessed August 15, 2025, <https://deepstrike.io/blog/top-industries-targeted-by-hackers-2025>
11. Dragos Industrial Ransomware Analysis: Q1 2025, accessed August 15, 2025, <https://www.dragos.com/blog/dragos-industrial-ransomware-analysis-q1-2025/>
12. M-Trends 2025: State-Sponsored IT Workers Emerge as Global Threat - SecurityWeek, accessed August 15, 2025, <https://www.securityweek.com/m-trends-2025-state-sponsored-it-workers-emerge-as-new-global-threat/>
13. M-Trends 2025: Data, Insights, and Recommendations From the Frontlines - Google Cloud, accessed August 15, 2025, <https://cloud.google.com/blog/topics/threat-intelligence/m-trends-2025>
14. Mandiant report finds rise in financially motivated cyber attacks - SecurityBrief Asia, accessed August 15, 2025, <https://securitybrief.asia/story/mandiant-report-finds-rise-in-financially-motivated-cyber-attacks>
15. M-Trends 2025 Report - Google Services, accessed August 15, 2025, <https://services.google.com/fh/files/misc/m-trends-2025-en.pdf>
16. Conti Ransomware | CISA, accessed August 15, 2025, <https://www.cisa.gov/news-events/alerts/2021/09/22/conti-ransomware>
17. Dragos reports surge in ransomware attacks as AI-powered tactics drive sharp rise in industrial targeting, accessed August 15, 2025, <https://industrialcyber.co/industrial-cyber-attacks/dragos-reports-surge-in-ransomware-attacks-as-ai-powered-tactics-drive-sharp-rise-in-industrial-targeting/>
18. #StopRansomware: ALPHV Blackcat | CISA, accessed August 15, 2025, <https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-353a>
19. CISO Alert for June 2025: Top 10 Cyber Threats Amid Geopolitical ..., accessed August 15, 2025, <https://legioncyber.com/ciso-alert-for-june-2025-top-10-cyber-threats-amid-geopolitical-turbulence/>
20. Leaked Tools TTPs and IOCs Used by Conti Ransomware Group, accessed August 15, 2025, <https://www.picussecurity.com/resource/leaked-tools-ttps-and-iocs-used-by-conti-ransomware-group>
21. Conti Ransomware and the Health Sector | HHS.gov, accessed August 15, 2025, <https://www.hhs.gov/sites/default/files/conti-ransomware-health-sector.pdf>
22. Nozomi Networks Labs Report Finds Wireless Networks ..., accessed August 15, 2025, <https://www.nozominetworks.com/press-release/nozomi-networks-labs-report-finds-wireless-networks-unprotected-as-threats-to-critical-infrastructure-escalate>
23. MITRE ATT&CK for ICS Detections in the Dragos Platform | Dragos, accessed August 15, 2025, <https://www.dragos.com/mitre-attack-for-ics/>
24. Dragos finds ransomware attacks on industrial sector surge 87%, manufacturing hit hardest as OT targeting rises, accessed August 15, 2025, <https://industrialcyber.co/reports/dragos-finds-ransomware-attacks-on-industrial-sector-surge-87-manufacturing-hit-hardest-as-ot-targeting-rises/>
25. Details of Vulnerabilities Targeting SCADA Systems Revealed ..., accessed August 15, 2025, <https://cbernet.com/en/details-of-vulnerabilities-targeting-scada-systems-revealed/>
26. Multiple flaws found in TETRA radio systems, exposing law enforcement, military, critical infrastructure communications - Industrial Cyber, accessed August 15, 2025, <https://industrialcyber.co/threats-attacks/multiple-flaws-found-in-tetra-radio-systems-exposing-law-enforcement-military-critical-infrastructure-communications/>
27. CVE-2025-24317 : Allocation of resources without limits or throttling ..., accessed August 15, 2025, <https://www.cvedetails.com/cve/CVE-2025-24317/>
28. CVE-2025-24317 - Red Hat Customer Portal, accessed August 15, 2025, <https://access.redhat.com/security/cve/cve-2025-24317>
29. CVE-2025-34080 Detail - NVD, accessed August 15, 2025, <https://nvd.nist.gov/vuln/detail/CVE-2025-34080>
30. CVE-2025-32433: Unauthenticated RCE Vulnerability in Erlang ..., accessed August 15, 2025, <https://www.cybereason.com/blog/rce-vulnerability-erlang-otp>
31. CVE-2025-3905 Detail - NVD, accessed August 15, 2025, <https://nvd.nist.gov/vuln/detail/CVE-2025-3905>
32. CISA Releases Seven Industrial Control Systems Advisories, accessed August 15, 2025, <https://www.cisa.gov/news-events/alerts/2025/08/12/cisa-releases-seven-industrial-control-systems-advisories>
33. CISA Releases Eight Industrial Control Systems Advisories, accessed August 15, 2025, <https://www.cisa.gov/news-events/alerts/2025/06/24/cisa-releases-eight-industrial-control-systems-advisories>
34. [Control systems] Schneider Electric security advisory (AV25-277), accessed August 15, 2025, <https://www.cyber.gc.ca/en/alerts-advisories/control-systems-schneider-electric-security-advisory-av25-277>
35. Critical Schneider Electric Vulnerabilities Enable Remote OS Command Injection, accessed August 15, 2025, <https://cyberpress.org/critical-schneider-electric-vulnerabilities/>
36. CVE-2025-6376 Detail - NVD, accessed August 15, 2025, <https://nvd.nist.gov/vuln/detail/CVE-2025-6376>
37. CISA Releases Thirty-Two Industrial Control Systems Advisories, accessed August 15, 2025, <https://www.cisa.gov/news-events/alerts/2025/08/14/cisa-releases-thirty-two-industrial-control-systems-advisories>
38. [Control systems] Siemens security advisory (AV25-215), accessed August 15, 2025, <https://www.cyber.gc.ca/en/alerts-advisories/control-systems-siemens-security-advisory-av25-215>
39. CERT Services - Siemens, accessed August 15, 2025, <https://www.siemens.com/global/en/products/services/cert.html>
40. CISA Releases Six Industrial Control Systems Advisories, accessed August 15, 2025, <https://www.cisa.gov/news-events/alerts/2025/07/24/cisa-releases-six-industrial-control-systems-advisories>
41. CISA Releases Four Industrial Control Systems Advisories, accessed August 15, 2025, <https://www.cisa.gov/news-events/alerts/2025/07/03/cisa-releases-four-industrial-control-systems-advisories>
42. Dragos Industrial Ransomware Analysis: Q2 2025 | Dragos, accessed August 15, 2025, <https://www.dragos.com/blog/dragos-industrial-ransomware-analysis-q2-2025/>
43. Cyble reveals US primary target with 223 ransomware victims amid ..., accessed August 15, 2025, <https://industrialcyber.co/critical-infrastructure/cyble-reveals-us-primary-target-with-223-ransomware-victims-amid-rising-attacks-on-critical-infrastructure/>
44. What the LockBit 3.0 leak tells us about modern ransomware | Okoone, accessed August 15, 2025, <https://www.okoone.com/spark/technology-innovation/what-the-lockbit-3-0-leak-tells-us-about-modern-ransomware/>
45. Top Cyber Threats in Manufacturing | MxD, accessed August 15, 2025, <https://www.mxdusa.org/2025/02/13/top-cyber-threats-in-manufacturing/>
46. What Is BlackCat Ransomware? | How Does BlackCat Work? - Akamai, accessed August 15, 2025, <https://www.akamai.com/glossary/what-is-blackcat-ransomware>
47. Unmasking Embargo Ransomware: A Deep Dive Into the Group's TTPs and BlackCat Links, accessed August 15, 2025, <https://www.trmlabs.com/resources/blog/unmasking-embargo-ransomware-a-deep-dive-into-the-groups-ttps-and-blackcat-links>
48. Conti (Malware Family) - Malpedia, accessed August 15, 2025, <https://malpedia.caad.fkie.fraunhofer.de/details/win.conti>
49. U.S. Agencies Warn of Rising Iranian Cyber Attacks on Defense, OT ..., accessed August 15, 2025, <https://thehackernews.com/2025/06/us-agencies-warn-of-rising-iranian.html>
50. Geopolitical tensions, AI and more are complicating the ..., accessed August 15, 2025, <https://www.weforum.org/stories/2025/01/global-cybersecurity-outlook-complex-cyberspace-2025/>
51. International Trade and Supply Chain Disruptions 2025, accessed August 15, 2025, <https://www.gov.cy/media/sites/11/2025/06/supplychaindisruptions.pdf>
52. Global Data Breaches and Cyber Attacks in July 2025 - IT ..., accessed August 15, 2025, <https://www.itgovernance.co.uk/blog/global-data-breaches-and-cyber-attacks-in-july-2025>
53. Best Practices for Mapping to MITRE ATT&CK - CISA, accessed August 15, 2025, <https://www.cisa.gov/sites/default/files/2023-01/Best%20Practices%20for%20MITRE%20ATTCK%20Mapping.pdf>
54. MITRE ATT&CK ICS: Tactics, Techniques, and Best Practices - Exabeam, accessed August 15, 2025, <https://www.exabeam.com/explainers/mitre-attck/mitre-attck-ics-tactics-techniques-and-best-practices/>
55. Best Practices for MITRE ATT&CK® Mapping - CISA, accessed August 15, 2025, <https://www.cisa.gov/news-events/news/best-practices-mitre-attckr-mapping>
56. Cybersecurity Using ICS ATT&CK Strategies, accessed August 15, 2025, <https://gca.isa.org/blog/cybersecurity-using-ics-attck-strategies>
57. SP 800-82 Rev. 3, Guide to Operational Technology (OT) Security ..., accessed August 15, 2025, <https://csrc.nist.gov/pubs/sp/800/82/r3/final>
58. NIST Publishes SP 800-82, Revision 3 | CSRC, accessed August 15, 2025, <https://csrc.nist.gov/News/2023/nist-publishes-sp-800-82-revision-3>
59. NIST SP 800-82 Revision 3: Making the Case for OT Cybersecurity - Corsha, accessed August 15, 2025, <https://corsha.com/blog/nist-sp-800-82-revision-3-making-the-case-for-ot-cybersecurity>
60. SP 800-82 Rev. 3, Guide to Operational Technology (OT) Security | CSRC, accessed August 15, 2025, <https://csrc.nist.gov/pubs/sp/800/82/r3/ipd>
61. NIST SP 800-82 Revision 3 highlights and key differences - Secolve, accessed August 15, 2025, <https://secolve.com/nist-sp-800-82-revision-3-highlights-and-key-differences/>
62. IEC 62443 Standard: Enhancing Cybersecurity for Industrial ..., accessed August 15, 2025, <https://www.fortinet.com/resources/cyberglossary/iec-62443>
63. ISA/IEC 62443 Series of Standards, accessed August 15, 2025, <https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards>
64. Practical Overview of Implementing IEC 62443 Security ... - InstMC, accessed August 15, 2025, <https://www.instmc.org/_userfiles/pages/groupfiles/cyber_security/wp_implementing_iec_62443_security_levels_in_industrial_control_applications_1.pdf>
65. ICS Cybersecurity | Dragos​, accessed August 15, 2025, <https://www.dragos.com/cybersecurity-solutions/ics-cybersecurity-roadmap/>
66. Nozomi Expands ICS Embedded Security Offerings with Arc Embedded for Schneider Electric RTUs, accessed August 15, 2025, <https://www.nozominetworks.com/blog/nozomi-expands-ics-embedded-security-offerings-with-arc-embedded-for-schneider-electric-rtus>