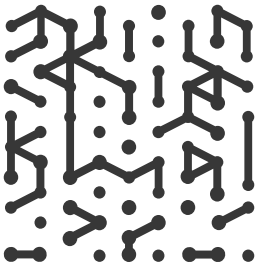
WHITE PAPER

Reclaiming the Advantage in OT: Proactive Cybersecurity in the Age of AI

Table of Contents



Executive Summary

Operational Technology (OT) environments including factories, hospitals, power grids, transportation hubs are more connected than ever. That connectivity brings efficiency, but also unprecedented risk. Sophisticated attackers are targeting OT systems using AI-enhanced techniques, and most defenses are still built for traditional IT.

This whitepaper explores how critical infrastructure operators should be taking steps to move from reactive security to a proactive, risk-based model, one built on real-time visibility, attacker behavior analytics, and AI-powered early warning systems. In OT, where downtime can mean lives lost or millions lost in productivity, the shift from detection to prevention is not optional, it's mission-critical.

2. The OT Threat Landscape: A Shifting Battlefield

Operational Technology (OT) environments were once thought to be secure by virtue of their obscurity and isolation. Air-gapped networks, proprietary protocols, and bespoke hardware offered a false sense of security. That paradigm no longer holds. As organizations embrace digital transformation, OT networks are being pulled into the broader enterprise ecosystem, often without adequate preparation for the new threat landscape.

OT networks today are:

- **Over 50% Of an OT environment is not OT**
- **40% Of OT devices are dormant**
- **80% of assets are unseen or unmanaged**
- **Armis Labs 2025**

Increasingly integrated with IT networks

The convergence of IT and OT is driven by the need for efficiency, analytics, and centralized control. This integration has dissolved traditional perimeters. As a result, vulnerabilities once confined to IT environments now extend into OT systems, exposing them to malware, lateral movement, and insider threats.

Exposed via remote access systems, legacy devices, cloud services, and smart sensors

Modern industrial environments depend on connectivity. Engineers access systems remotely, cloud-based analytics platforms monitor performance, and IIoT (Industrial Internet of Things) devices feed real-time data. These entry points dramatically expand the attack surface, often without corresponding improvements in security posture.

Dependent on legacy equipment that was never designed for security

Much of today's OT infrastructure was deployed decades ago, in an era when cybersecurity wasn't a design consideration. These systems often lack basic safeguards such as encryption, authentication, or the ability to be patched. This makes them prime targets for exploitation.

Attackers are fully aware of these weaknesses. What has changed is not just the exposure of OT systems, but also the intent and sophistication of the adversaries. Ransomware groups now routinely target industrial control systems (ICS), not only for monetary gain but also to cause widespread disruption. Nation-state actors see critical infrastructure as strategic targets in geopolitical conflicts. Even routine supply chain compromises can have cascading effects in tightly coupled OT environments.

Consider the following examples:

> **Colonial Pipeline:** Yes, it's an attack that occurred 4 years ago, but it sticks on our minds for a reason. A ransomware attack led to a week-long shutdown of the largest fuel pipeline in the United States. This caused widespread fuel shortages and panic buying across the East Coast. Although the attack initially hit IT systems, the operational impact forced a complete halt to pipeline operations. This is a stark example of how IT vulnerabilities can affect physical infrastructure.

> **Ukraine Power Grid Attacks:** In two separate incidents, cyber attackers successfully brought down parts of Ukraine's power grid. These were among the first publicly known cases of hackers causing actual physical blackouts through cyber means. The attacks demonstrated coordinated use of malware, manual operations, and deep knowledge of industrial systems. They marked the beginning of a new era in cyber warfare.

These incidents underscore a critical truth: OT security is no longer optional or secondary. The stakes have escalated, shifting from data loss to national security. Defenders must adapt to this new reality with equal urgency and sophistication.

3. Why Traditional IT Security Fails in OT

Most cybersecurity strategies were built for IT. But OT is different:

Characteristic	IT Environment	OT Environment
Priorities	Data confidentiality	Availability, uptime, safety
Downtime Tolerance	Hours or days	Zero tolerance
Update Cycles	Frequent patching	Rare patch windows, strict change control
Device Types	Workstations, servers	PLCs, RTUs, HMIs, field devices
Protocols	Standardized (HTTP, DNS)	Proprietary (CIP, S7Comm, Modbus TCP, DNP3, BACnet, etc.)

Because of this, many OT environments face critical security gaps:

Limited endpoint protection or EDR

Most OT systems have limited implementation and weak policies for basic security tooling like antivirus or endpoint detection, often due to concerns about stability and compatibility. This leaves them blind to intrusions and lateral movement.systems, the operational impact forced a complete halt to pipeline operations. This is a stark example of how IT vulnerabilities can affect physical infrastructure.

Obsolete devices with known CVEs

Legacy equipment is common in OT, often running outdated software with unpatched vulnerabilities. Replacing or updating these systems is risky and costly, so they remain exposed.

No unified visibility into networked assets

Many organizations cannot see all the devices connected to their OT networks in real time. This lack of asset visibility makes it nearly impossible to detect threats or enforce security policies effectively.

4. The Rise of AI-Driven Threats in Critical Infrastructure

AI Isn't Just Helping Defenders, It's Supercharging Attackers. While AI strengthens OT defenses, it also equips attackers with powerful, adaptive capabilities. Three key trends are reshaping the threat landscape:

> **Autonomous, Adaptive Malware is on the rise.** Attackers now deploy malware powered by AI that learns and evolves in real time. These autonomous agents analyze their environment, adjust behavior to evade detection, and move laterally across OT networks, all while blending into normal traffic, making early detection extremely difficult.

> **Deepfake-Driven Phishing is trending upwards.** AI enables highly targeted phishing attacks using realistic deepfake audio and video. By mimicking executives, vendors, or even system alerts, attackers can trick operators into taking dangerous actions, bypassing traditional training and awareness safeguards.

> **Script Kiddie Tools are now supercharged.** Low-skill attackers now have access to AI-powered tools that weaponize known OT vulnerabilities. These user-friendly platforms scan, select, and exploit industrial targets with minimal effort, lowering the barrier for sophisticated attacks.

These threats move faster than human response teams and often mimic routine OT activity. More dangerously, they can hit both human operators and machines at once, disrupting safety protocols while creating confusion on the plant floor. The result is a threat landscape where speed and deception are the new norm.

5. The Visibility Gap: Foundation of Risk in OT Networks

Ask any plant manager, CISO, or reliability engineer:

"Do you know every device on your network right now?"

Unmanaged Assets in OT and CPS Environments

Operational Technology environments are complex, with layers of legacy systems, proprietary protocols, and tightly integrated processes. Many assets in these environments were never designed with cybersecurity in mind. Devices such as legacy PLCs, RTUs, field devices, and older HMIs often lack basic features like authentication, encryption, or logging. They frequently go unmonitored, creating significant visibility gaps.

Compounding the challenge, many of these assets do not communicate directly with the core network. Instead, they rely on serial connections or intermediary systems, making them harder to detect using traditional network monitoring tools. These blind spots give attackers opportunities to persist undetected, move laterally, or manipulate processes without triggering alerts.

As OT and IT systems become more interconnected, the risk grows. An attacker can exploit a weak point in a non-critical device and impact higher-level operations through trusted communication paths. This makes unmanaged assets a key part of the overall attack surface.

Reducing this risk starts with comprehensive asset discovery and visibility. Passive detection, ICS-aware monitoring, and up-to-date inventories are essential for understanding what exists in the environment and how it behaves. Without this foundation, effective access control and anomaly detection are nearly impossible.

Unmanaged assets may not be the most visible part of the infrastructure, but they are often the most vulnerable. Addressing them is critical to any serious OT security strategy.

Flat Networks in OT and CPS Environments

A common vulnerability in OT and CPS networks is the use of flat architectures with little or no segmentation. In many cases, once an attacker gains access to the network, they can move laterally across systems without encountering meaningful barriers. This increases the risk that a single breach could compromise critical operations.

Flat networks often lack internal firewalls, VLAN separation, and role-based access controls. As a result, malicious activity can spread quickly from non-critical assets, such as operator workstations, to core systems like PLCs or safety controllers. Many of these environments were not originally designed with security in mind, and retrofitting segmentation can be complex due to operational constraints and legacy technology.

Effective segmentation, such as zoning based on the Purdue model or IEC 62443 framework, is essential for limiting the blast radius of a compromise. It provides necessary boundaries between enterprise IT, OT systems, and safety-critical functions, reducing the risk of operational disruption and improving incident response.

Inconsistent Asset Inventory

Asset tracking is frequently manual, relying on siloed tools, spreadsheets, or whiteboards. This leads to outdated or incomplete inventories, making it hard to detect unauthorized changes or respond quickly.

Without knowing what's connected, what's vulnerable, and what's critical, organizations can't protect themselves.

Industrial Facility

1. Industrial Control Systems (ICS)
2. Industrial Network Infrastructure
3. Manufacturing Equipment
4. Facility and Safety Systems
5. IIoT and Edge Devices
6. Enterprise IT Systems Interfacing with OT
7. Communications and Collaboration

CPS spans multiple industries but they all have one thing in common. OT/ IoT/ IoT/ IoMT assets are everywhere.

6. From Reaction to Prevention: Proactive Security for OT

The reactive model (detect, alert, investigate) is broken in OT. Downtime is not an acceptable outcome.

A Proactive Model for OT Security using Prioritization and Prediction:

As threats evolve, OT security must move from reactive to proactive. The Prevent, Prioritize, and Predict model offers a forward-looking approach that aligns cybersecurity with operational resilience.

Core Principles

Continuous Monitoring

Gain full visibility without disrupting fragile OT devices. Monitoring is done passively, ensuring no impact on uptime or legacy systems.

Integrations for Visibility and Maturity

Integrations are essential to extend the value of discovery tools across OT and CPS environments. While many organizations have system and network tools in place, these often provide limited, siloed views. By integrating asset discovery with platforms like SIEMs, CMDBs, and vulnerability scanners, organizations can correlate data, identify monitoring gaps, and uncover blind spots.

This integrated view also supports maturity assessments. Mapping asset and threat data to frameworks like NIST CSF or IEC 62443 helps measure progress, highlight gaps, and prioritize next steps. In effect, integrations turn discovery into a strategic function, one that enhances both operational visibility and governance alignment.

Active Querying

Actively query assets at times that work best for you and your production line. Actively query in a safe way with native protocols and not persistent that never disturb or disrupt your uptime.

Real-Time Asset Intelligence

Continuously identify every device, protocol, and behavior. This dynamic baseline enables faster detection of anomalies and unauthorized activity.

Early Warning of Exploits

Leverage global telemetry and known attacker behaviors (TTPs) to detect threats early, before damage is done.

Operational Context

Focus on what matters most to safety and productivity. Risks are prioritized based on their potential impact to core operations, not just technical severity.

This model makes security a partner in uptime and safety, not an obstacle. By proactively defending what matters most, organizations can strengthen both their cybersecurity and their operational performance.

7. Early Warning Systems in Operational Environments

A proactive approach using evidence-based exploit intelligence that can inform you of vulnerabilities being actively exploited in the wild is one of the best ways you can prioritize your remediation efforts.

Early warning systems can give you:

- Weeks to months of lead time on emerging vulnerabilities (e.g., Log4Shell, PwnKit)
- Real-world exploit insight: Which threats are being used today, not just listed in CVE databases
- OT-specific threat mapping and attack pathway mapping: Identifying how attackers pivot from IT to OT systems

This capability is vital for patch-deficient environments. When patching isn't possible, prioritization and containment must be.

8. Generative AI in Proactive ICS & SCADA Defense

As operational technology (OT) environments become increasingly complex and interconnected, a reactive security posture is no longer sufficient. Instead, leading organizations are adopting proactive, intelligence-driven strategies, and Generative AI (Gen AI) is becoming central to that shift.

Proactive Security with Generative AI

Rather than waiting for threats to materialize, Gen AI empowers defenders to anticipate and adapt. Key pillars of a proactive strategy include:

Dynamic Risk Modeling: Gen AI continuously analyzes data from ICS and SCADA networks to simulate potential attack paths, predict the most likely intrusion methods, and prioritize vulnerabilities based on contextual risk.

Synthetic Threat Simulation: Instead of relying solely on known threat signatures, Gen AI can generate novel, realistic attack scenarios. These are used to test defenses, uncover blind spots, and improve incident response readiness, before a real threat occurs.

Intelligent Anomaly Detection: Traditional rule-based systems struggle with the variability of OT environments. Gen AI can learn complex operational baselines and detect subtle deviations that may indicate early-stage compromise, reducing false positives and surfacing real threats faster.

Automated Threat Hunting: Gen AI can augment SOC analysts by continuously generating hypotheses about suspicious behavior, automating the collection of supporting evidence, and recommending next steps, turning human defenders into force multipliers.

Smart Honeypots: Adaptive Deception at Scale

As part of this proactive toolkit, AI-enhanced smart honeypots offer a powerful way to engage adversaries directly and extract intelligence before they reach critical systems.

These aren't just static decoys, they're adaptive simulations powered by Gen AI that can:

Emulate Cyber-Physical Systems like gas turbines, MRIs, or industrial control systems with high fidelity.

Morph their behavior in real time based on attacker tactics, mimicking real-world system responses to keep adversaries engaged.

Capture novel malware, attacker techniques, and lateral movement attempts for analysis and future prevention.

By integrating smart honeypots with broader AI-driven detection and response systems, organizations gain early warning capabilities and deep insight into attacker behavior, long before real damage is done.

9. Risk Prioritization That Matches the Operational Mission

Most security tools rank CVEs based on theoretical criticality.

But OT leaders ask:

“Will this vulnerability actually affect my plant operations?”

Capabilities that go beyond CVSS: Context-Driven Risk Prioritization CVSS scores alone don’t reflect the real-world impact of vulnerabilities in OT environments. Enhance risk assessment by factoring in:

- **Exploit Activity** Tracks which vulnerabilities are being actively exploited in real OT networks, not just those with theoretical risk.
- **Device Function** Assesses whether the device is critical to uptime, safety, or production, prioritizing based on operational impact.
- **Network Role** Considers the device’s exposure. An internet-facing system carries more risk than one deep inside a segmented network.
- **Remediation Feasibility** Evaluates whether vulnerabilities can be safely patched or mitigated without disrupting operations.

This results in true risk-based prioritization that aligns with maintenance windows, safety requirements, and production schedules.

10. Building a 'Proactive Blueprint' for Critical Infrastructure Operators

As cyber threats targeting critical infrastructure become more sophisticated and persistent, reactive security strategies are no longer sufficient. Operators must adopt a proactive approach that focuses on visibility, context, early warning, and tailored response. Below is a practical blueprint to help organizations shift from passive defense to active resilience in OT and CPS environments.

Step 1: Deploy Holistic Asset Visibility Methods

Begin by gaining full visibility into all assets (IT, OT, and IoT) across the environment. This requires a non-intrusive, passive monitoring approach that respects operational constraints while delivering real-time intelligence.

- **Use holistic discovery** to build and maintain a live asset inventory without disrupting operations.
- **Enable safe active querying** for environments where deeper inspection is needed, using vendor-approved methods.
- **Auto-classify devices** by type, vendor, function, and communication behavior to support risk scoring and segmentation planning.

Step 2: Map Threats to Asset Context

Not all assets carry the same risk. Understanding the context of threats is essential for prioritization and response.

- **Identify vulnerable, exposed, or anomalous devices** using behavioral baselining and vulnerability mapping.
- **Correlate local findings with global threat intelligence** from honeypots, malware analysis, and dark web activity to understand what attackers are actually targeting.
- **Use attack path mapping** to visualize how a threat could move through the environment, **enabling informed mitigation decisions.**

Step 3: Integrate Early Warning into OT Risk Management

Traditional OT environments often lack mechanisms to anticipate threats before they materialize. Integrating early warning intelligence into operational risk management enables faster, more strategic responses. This intelligence-driven approach helps bridge the gap between threat awareness and operational decision-making.

- **Receive timely alerts** about vulnerabilities, malware strains, and TTPs observed in similar industrial environments.
- **Use this intelligence** to prioritize patching, isolation, or segmentation efforts based on what is most likely to be exploited.

Step 4: Build OT-Specific Incident Response Playbooks

Incident response in OT is fundamentally different from IT. The focus must be on containment and continuity, not just eradication.

- **Develop response playbooks** that prioritize safe isolation of affected zones or devices while maintaining core operations.
- **Align actions with operational goals,** ensuring that response measures do not introduce additional safety or reliability risks.
- **Test and rehearse playbooks** with cross-functional teams, including engineering and operations, to ensure readiness under real-world constraints.

By building playbooks tailored to OT realities, organizations can respond with speed and precision when incidents occur.

This proactive blueprint offers a scalable, practical path for critical infrastructure operators seeking to move beyond compliance and build real cyber resilience. It ties together asset intelligence, threat context, and operational response into a unified strategy for defending the systems that matter most.

11. Conclusion

OT environments face a perfect storm: increasing connectivity, evolving threats, and outdated protection models. AI has tilted the field toward attackers, but it can also help us take it back.

With the right security vendor, you can:

- Know every asset in your environment
- Predict the threats most likely to impact you
- Prevent disruptions before they occur

This is cybersecurity aligned with mission-critical operations. It's not just about alerts, it's about avoiding downtime, protecting lives, and maintaining control.

Want to discuss implementing a strategy like this?

TALK TO ARMIS HERE

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