WHITE PAPER

Foundations of OT Visibility: Why It Matters and How to Get Started

By Pascal Ackerman, Brett Seals and Jason Vigh

Many organizations struggle with fragmented views into their operational technology assets and systems. A structured visibility strategy can help protect their operational technology systems, maintain operational reliability and defend against modern cyberthreats.

Cyber-physical systems (CPS) are the foundation of critical infrastructure, enabling safe and reliable delivery of essential services such as energy and water and industries such as manufacturing. As these OT systems grow increasingly interconnected with IT networks and external systems, they face escalating cyber risks. For organizations managing OT environments, visibility and contextual awareness are not just technical capabilities — they are foundational requirements for operational security, resilience and efficiency.

Many organizations struggle with limited or fragmented visibility into their cyber-physical systems. Without a clear understanding of what assets exist, how they operate and what is happening in real time, leaders cannot effectively protect their systems or optimize performance. This paper outlines why OT visibility is critical and provides a road map for organizations to build an effective strategy.

Importance of OT Visibility

OT visibility is the ability to observe and understand the assets, processes and communications occurring within an OT environment. This goes beyond simply knowing what devices are connected. The goal is to gain contextual awareness of the behaviors and interactions between devices, because this is necessary to identify risks, respond to emerging threats and ultimately optimize operations.

Many organizations lack a comprehensive inventory of their OT assets, particularly in environments where legacy systems and shadow devices are not capable of integrating with modern inventory management systems. These blind spots create vulnerabilities that attackers could exploit. For example, safety and operational continuity might be at risk if devices are not patched or are susceptible to unauthorized remote access.

Case Study: Secure Remote Access and Firewall Attack Campaign

In April 2024, attackers exploited a vulnerability in Cisco firewalls, compromising the secure remote access systems of critical infrastructure providers worldwide. This large-scale, coordinated cyber campaign underscored the growing risks to operational continuity from sophisticated automated attacks. In response, 1898 & Co. worked closely with utility asset managers subscribed to our 24/7 Threat Detection and Response service to implement strategic defenses. Our actions included improving network visibility, strengthening authentication controls and deploying proactive threat monitoring. By leveraging real-time analytics and industry best practices, we minimized security blind spots, secured operational continuity and reinforced resilience against evolving cyberthreats.

This proactive approach not only mitigated immediate risks but also reinforced long-term cyber resilience. By prioritizing continuous monitoring, rapid incident response and strategic risk mitigation, utilities enhanced regulatory compliance and operational reliability. This case highlights the importance of a robust security posture for critical infrastructure organizations, demonstrating how executive-led investment in cybersecurity can safeguard both digital and physical assets against emerging threats.

As IT and CPS systems become increasingly interconnected, the traditional separation between these environments has eroded. This convergence often leaves OT systems exposed to risks that were previously confined to IT. Well-defined and -implemented visibility provides a unified view of both environments, enabling organizations to manage these interdependencies effectively.

CPS environments face a growing range of threats, from ransomware targeting critical infrastructure to nation-states attacking industrial control systems. Real-time visibility allows organizations to detect anomalies, such as unauthorized access and unusual traffic patterns, before they can escalate into major incidents.

Beyond cybersecurity, visibility contributes to operational excellence. By monitoring system performance in real time, organizations can identify inefficiencies, prevent equipment failures and reduce downtime.

Case Study: Enhancing OT Security Following a Watering Hole Attack

A North American electric utility encountered a cybersecurity incident in 2024 when a watering hole attack was executed via malicious software downloaded from the Microsoft Store. An administrative support staff member unknowingly installed a compromised PDF-to-Word conversion tool that engaged in DLL hooking, a technique used to manipulate system processes. Analysts from 1898 & Co. detected the malicious activity early, classifying it as a positive security event. Through rapid response, containment actions were executed to prevent lateral movement, confining the malware to the user's workstation before it could escalate into a full-scale breach. DNS record analysis revealed that the tool's developer domain had changed ownership in the past year, serving as the likely vector for the compromise. Subsequent malware reverse engineering confirmed its malicious capabilities.

Following containment, 1898 & Co. implemented enhanced monitoring across the affected user, endpoint and network segments, reinforcing detection mechanisms. The utility received a remediation plan emphasizing stricter controls over software installations, an updated inventory of trusted vendors, and user training to prevent similar incidents. Additionally, visibility enhancements were introduced for monitoring routers, switches, firewalls, identity provider (IDP) audit logs and secure remote access gateways — extending coverage from the internet perimeter firewall to default gateways of human-machine interfaces and point-of-sale terminals. This proactive security approach reduced blind spots and improved the detection of anomalous activities tied to third-party tools. A comprehensive lessons-learned review refined incident response playbooks, strengthened staff awareness and significantly reduced the risk of recurrence. By leveraging 1898 & Co. services, the utility not only mitigated an immediate cyberthreat but also strengthened its long-term resilience.

Barriers to Achieving OT Visibility

Despite its importance, achieving comprehensive OT visibility remains a challenge. Common barriers include:

- **Legacy systems.** Many OT environments rely on legacy equipment that lacks built-in monitoring capabilities or is incompatible with modern tools.

- **Distributed assets.** In industries such as energy or transportation, OT environments often span large geographic areas, making centralized monitoring difficult.
- **Limited collaboration.** Misalignment between IT and OT teams can hinder efforts to implement visibility solutions that address both operational and security needs.

These barriers are not insurmountable. With a structured approach, organizations can begin to address their visibility gaps and build a strong foundation for OT security and efficiency.

How to Get Started

Organizations can take several practical steps to enhance OT visibility, laying the groundwork for a more secure and resilient environment.

Conduct an Asset Discovery Exercise

A comprehensive inventory of OT assets is the foundation of any visibility strategy. This process involves identifying all devices connected to the network, including their configurations, communication protocols and vulnerabilities. Tools such as passive network monitoring solutions can help identify devices without disrupting operations.

Establish a Baseline for Normal Operations

Understanding what “normal” looks like in an OT environment is critical for detecting anomalies. By analyzing typical network traffic, device communications and system behaviors, organizations can establish benchmarks that serve as a reference point for identifying potential issues.

Integrate IT and OT Monitoring

Visibility requires collaboration across IT and OT teams to create a unified view of the entire environment. This integration enables organizations to detect threats that cross IT-OT boundaries, such as malware moving from IT systems into OT networks.

Prioritize High-Risk Areas

Not all assets are created equal. Focus initial efforts on high-risk areas, such as devices that control critical processes or those with known vulnerabilities. This targeted approach allows organizations to address their most pressing risks while building momentum for broader visibility efforts.

Leverage Purpose-Built Tools

The tools used for IT monitoring are often insufficient for OT environments. Specialized OT visibility solutions — such as passive monitoring tools designed for industrial protocols — provide the granular insights needed to manage these environments effectively.

Case Study: Strengthening Resilience in Supply Chain for a Manufacturer

In the second quarter of 2024, a leading transportation manufacturing organization partnered with 1898 & Co. to address critical availability and resiliency challenges. Recognizing the high stakes of operational disruptions, the organization opted for a high-consequence event (HCE) tabletop exercise instead of a full offensive security assessment. This exercise, developed in collaboration with Idaho National Labs and Department of Homeland Security CCE trainers, provided a reduced-risk approach to uncovering vulnerabilities without impacting live environments. Through a passive security assessment and interactive tabletop workshops, the engagement exposed critical cyber-physical risks in the client’s infrastructure, revealing potential attack scenarios that could compromise safety, production integrity and regulatory compliance.

The exercise led to actionable, prioritized mitigations tailored to the organization’s unique risk profile. Key initiatives included architectural and configuration changes, enhanced security controls, and improved monitoring and detection strategies across cyber-physical domains. Additionally, adversary simulation drills were introduced to strengthen incident response readiness. By proactively addressing these vulnerabilities, the organization turned a high-risk scenario into an opportunity to fortify its operations, setting a new standard for resilience in the transportation manufacturing sector. This engagement highlighted the necessity of continuous evaluation and adaptation to evolving cyberthreats, maintaining long-term protection of critical systems and supply chain stability.

Conclusion

Real-time OT visibility is no longer optional for organizations managing critical infrastructure. It is the foundation for identifying risks, detecting threats and driving operational efficiency. While achieving visibility can be challenging, the benefits far outweigh the effort, enabling organizations to build a secure and resilient future.

By addressing the unique challenges of OT environments and leveraging purpose-built tools to implement tailored monitoring strategies, organizations gain the insights needed to secure operations, minimize risks and unlock new opportunities. Visibility is more than a technical goal — it is the key to operational confidence in an increasingly complex world.

About 1898 & Co.

1898 & Co. is a business, technology and cybersecurity consulting firm serving the industries that keep our world in motion. As part of Burns & McDonnell, our consultants leverage global experience in critical infrastructure assets to innovate practical solutions grounded in your operational realities. For more information, visit **1898andCo.com**.