ARMIS®

WHITE PAPER

Prioritizing and Enhancing Full Situational Awareness in Operational Technology (OT) Assets

Executive Summary

OT systems serve as the backbone of critical infrastructure across a multitude of industries. The integration of OT systems into modern industrial environments brings with it a unique set of challenges that demand innovative security approaches. The distinctive characteristics of OT systems, including legacy equipment, extended life cycles, and their convergence with IT networks, present complexities that traditional security methods struggle to address effectively.

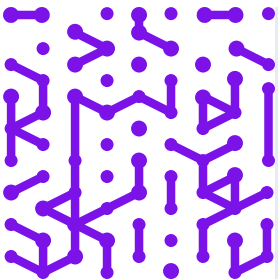
These inherent weaknesses in OT environments make them attractive targets for threat actors seeking to exploit high impact vulnerabilities. Consequently, safeguarding OT systems against cyber threats is paramount to ensuring reliability, safety, and resilience within industrial operations.

Full situational awareness in OT assets is no longer a luxury but a necessity. This paper explores the unique vulnerabilities of OT environments, the current threat landscape, and provides an authoritative perspective on implementing robust security measures to safeguard against potential cyberattacks.

> *"71% of breaches in OT environments came from known vulnerabilities, things that have known weaknesses inherently in them."*
>
> **Christopher Fielder**
> Arctic Wolf

Introduction

The security of OT systems is key to ensuring the continuous operation of critical infrastructures such as power plants, manufacturing facilities, and transportation networks. These systems, designed for longevity and reliability, now face an evolving array of cyber threats due to their legacy nature and increased connectivity with IT networks. The importance of prioritizing OT security cannot be overstated, given the high financial stakes, safety and reliability risks, and stringent compliance requirements.



Current OT Threat Landscape

01 Legacy Systems and Third-Party Risk

Many OT systems were installed decades ago, long before cybersecurity was a prevalent concern. These legacy systems are inherently vulnerable due to their lack of designed-in security features and the complexities involved in applying patches. The reliance on third-party vendors for the management of complex OT systems introduces further security vulnerabilities into the ecosystem.

02 Convergence with IT Networks

The integration of OT and IT systems represents a significant advancement in industrial operations, promising streamlined processes and enhanced data analysis capabilities. However, this convergence also introduces a new frontier of cybersecurity challenges.

By connecting OT systems to IT networks, organizations gain the ability to access and analyze operational data more efficiently- this increased access poses a potential problem. Traditionally, OT environments operated in isolation in air gapped environments, with limited connectivity to external networks, thus providing a degree of protection against cyber threats. What became apparent is that it was very hard to ensure that accidental convergence did not happen due to an errant action or unmanaged device such as a thumbdrive, cell phone or even a printer.

This convergence creates new avenues for cyber threats, exposing OT systems to malicious activities such as malware infections, ransomware attacks, and unauthorized access. Threat actors can therefore exploit vulnerabilities in IT systems to gain entry into OT networks.

03 Evolving Threats and AI Development

The landscape of cyber threats is continuously evolving, marked by the emergence of increasingly sophisticated tactics and adversaries. Among these advancements, AI-powered attacks and the involvement of nation-state actors pose particularly grave risks to OT networks.

AI-powered attacks leverage machine learning algorithms to automate and enhance the efficiency of cyber assaults, enabling threat actors to execute targeted and highly adaptive attack strategies. Furthermore, the involvement of nation-state actors adds a layer of complexity and geopolitical significance to cyber threats targeting OT infrastructure. These actors possess substantial resources, advanced technical capabilities, and strategic motivations to conduct cyber operations aimed at disrupting critical infrastructure, stealing intellectual property, or advancing political agendas.

Addressing these sophisticated threats requires equally advanced countermeasures and proactive security strategies. Organizations must invest in AI-driven threat detection and response/ remediation capabilities, to effectively identify and mitigate evolving cyber threats in real-time (or ideally before they ever have a chance to come to fruition).

Seven Days to Weaponize

It takes organization 105 days to patch 15x longer than threat actors to weaponize.

- Armis Labs

Why Prioritize OT Security?

The consequences of a successful cyberattack targeting Operational Technology (OT) systems extend far beyond financial losses. They encompass a wide range of potential risks, including safety hazards, operational disruptions, environmental harm, and regulatory non-compliance.

In the **past 12 months** alone, we have witnessed strategically executed cyberattacks that underline the vulnerability and global scope of critical infrastructure. Three examples include:

November 2023

- Denmark faced an unprecedented challenge when twenty-two of its power companies fell victim to what has been recorded as the nation's largest cyberattack. Orchestrated by Russian hackers, this meticulously planned operation initiated in May 2023 was not merely an attack but a calculated campaign to infiltrate Denmark's power grid. By exploiting a critical command injection flaw, the hackers demonstrated how unpatched systems could be leveraged to sustain access over months.

September 2023

- Brought to light a cyberattack against Israel's railroad network, attributed to Iranian hackers. Employing a cunning phishing campaign, the attackers aimed at the heart of the country's electrical infrastructure, showcasing the increasing sophistication of cyber threats. This attack was not isolated - similar tactics were reportedly used against Brazilian and UAE companies, highlighting a pattern of targeting essential services and infrastructure on a global scale.

September 2023

- Suspected Chinese hackers carried out a calculated assault on the national power grid of an unnamed Asian country, utilizing malware traced back to China. By corrupting a widely used Windows application, the attackers not only gained entry but also achieved lateral movement within the target's network, an alarming demonstration of how state-sponsored actors are elevating the complexity and stealth of cyber operations.

Solutions for Enhancing Asset Situational Awareness in OT Environments

Visibility and Continuous Monitoring

Achieving full situational awareness in OT environments requires a comprehensive understanding of all assets and their vulnerabilities. Armis provides organizations with unparalleled visibility into their OT networks, offering a detailed inventory of connected devices, including Internet of Things devices and industrial control systems. With Armis, organizations can continuously monitor network traffic and device behavior in real-time. By analyzing this data, Armis detects anomalies that may signify potential threats, enabling proactive threat mitigation and enhancing overall security posture.

> *"We rolled out Industry 4.0 in all our facilities and needed a holistic view of the manufacturing floor as we know you can't protect what you can't see. Armis is critical for us to identify and protect all our assets as part of our Industry 4.0 efforts."*
>
> **Friedrich Wetschnig**
> CISO & VP Enterprise Information Technology

Lifecycle Management

Efficient lifecycle management helps to mitigate security risks associated with outdated or unmaintained OT assets. As technology evolves, manufacturers discontinue support and security updates for older equipment, leaving them vulnerable to cyber threats. Hackers often target End of Life devices due to the lack of security patches, making them easy entry points for malicious activities. By proactively maintaining, retiring and replacing these assets, organizations can reduce their exposure to cybersecurity risks and strengthen their overall security posture.

EOL management begins with the identification and quantification of assets on the network, irrespective of their operating system (OS) type or firmware version. By streamlining reporting workflows and replacing manual, often error prone processes and extensive hours in spreadsheets, organizations can effectively navigate the complexities of the full spectrum of the asset management lifecycle.

Network Segmentation and Patch Management

Network segmentation is a critical component of OT security, helping to restrict the lateral movement of malware and isolate critical systems from compromised ones. Armis facilitates network segmentation by providing granular visibility and control over network traffic, allowing organizations to create and enforce segmentation policies effectively. Additionally, Armis streamlines patch management by identifying and prioritizing patches for known vulnerabilities. Through automated patch deployment and tracking, Armis helps organizations stay ahead of emerging threats and maintain a secure OT environment.

Powerful Global Contextual Intel

Arming your business with Armis doesn't just mean securing your assets; it means redefining how you perceive and interact with them. It's about taking what might seem like an individual puzzle and understanding it as part of a vast, interconnected global network. With Armis, your assets are no longer siloed entities operating in a vacuum—they are part of a global ecosystem, compared and contrasted against billions of others, offering insights that propel security, efficiency, and innovation.

The Armis Asset Intelligence Engine:

Comprehensive Visibility:

Gain an unprecedented overview of your digital assets, including OT, IoT, Internet of Medical Things and Industrial Control Systems, ensuring no component remains unchecked.

Risk Assessment and Management:

By understanding how your assets operate in comparison to a larger global database of assets, the Armis Centrix™ platform delivers precise risk assessments, identifying vulnerabilities, threats and potential attack vectors.

Benchmarking and Standardization:

Position your asset management and security strategies in the context of global standards and practices. The Armis Asset Intelligence Engine offers critical comparative insights, enabling your organization to benchmark against global counterparts, fostering continual improvement and compliance with international regulations.

Strategic Decision-Making:

With data on over 4 billion assets, the Armis Asset Intelligence Engine provides a solid foundation for making informed, strategic decisions about asset acquisition, deployment, and lifecycle management. This ensures not only security but also efficiency and cost-effectiveness throughout the asset's lifecycle.

From Predictive to Proactive:

Leverage the power of predictive analytics to anticipate future trends, attacks still in the formulation stage and challenges in asset management. By understanding global movements and evolutions observed across the extensive Armis AI capabilities that are designed to deliver "early warning insights", your organization can stay ahead, adapting proactively to forthcoming threats and technological shifts.

A Proactive Approach

Early warnings form the backbone of Armis' approach to delivering a proactive security strategy for organizations. By harnessing the power of cutting-edge algorithms and deep dark web insights, Armis leverages its proprietary AI capabilities to sifts through vast amounts of data in real-time, identifying potential threats before they can cause harm. General CVE/ exploitability discoveries uncovered by Armis Centrix™ for Early warnings strengthen the Armis OT solution, enabling businesses to stay one step ahead of cyber adversaries, transforming traditional reactive security measures into a dynamic, forward-thinking defense. With actionable insights at their fingertips, organizations are not only able to thwart imminent attacks but also to anticipate future vulnerabilities.

Stakeholder Responsibility

The collaboration and proactive involvement of key stakeholders play a pivotal role in fortifying defenses and mitigating risk in OT spaces.

OT Plant Managers, Chief Information Security Officers (CISOs), and Vulnerability Managers are at the forefront of this endeavor, each contributing unique expertise and responsibilities.

Responsibilities of CISOs

CISOs are tasked with establishing overarching security strategies and policies, aligning them with business objectives while safeguarding against potential threats. With Armis' comprehensive security platform, CISOs can develop and enforce robust security policies across OT environments, leveraging features like policy enforcement and vulnerability management to maintain compliance and protect against cyber threats.

Contributions of OT Plant Managers

OT Plant Managers oversee the operational infrastructure, making them integral in implementing security measures and ensuring the resilience of critical systems. With deep asset inventory capabilities, they gain real-time visibility into connected devices, enabling proactive asset management and security monitoring.

Role of Vulnerability Managers

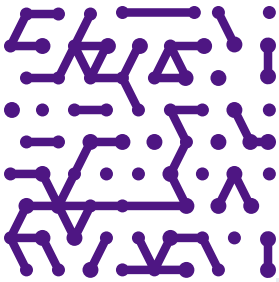
Vulnerability Managers play a crucial role in identifying and assessing vulnerabilities within OT systems, facilitating timely remediation efforts to prevent exploitation. Armis' vulnerability management capabilities empower Vulnerability Managers to conduct thorough assessments, prioritize vulnerabilities and other security findings based on risk, and automate patch deployment based on asset criticality to the business and maintenance windows to ensure the security of OT assets.

Manufacturers' Responsibilities

Manufacturers of OT devices bear a significant responsibility in enhancing security measures. They must integrate robust security features into new products and provide ongoing support for legacy systems. Armis works closely with manufacturers to promote secure design principles and facilitate the integration of security features into OT devices, contributing to a more resilient OT ecosystem.

Internal and External Engagement

Internally, educating organizational leadership on the severe consequences of OT security incidents is paramount to garnering support and resources for cybersecurity initiatives. Externally, engaging with manufacturers and advocating for secure procurement processes is essential for elevating the overall security posture of OT environments. Armis provides educational resources and support to help organizations build awareness, gain buy-in and establish secure procurement practices.



Conclusion

The path to securing OT systems in an increasingly complex cyber threat landscape involves a multifaceted approach. Full visibility, proactive security measures, continuous monitoring, network segmentation, and engaging stakeholders are all critical components of a robust OT security strategy. As the consequences of successful cyberattacks on OT systems can be catastrophic, investing in full situational awareness, comprehensive security and control is not an option but a necessity for safeguarding our critical infrastructure.

By prioritizing OT security and engaging with manufacturers and other stakeholders, we can work towards a more secure and resilient OT environment for the present and future. So, it is imperative that organizations take immediate steps to enhance their full situational awareness in OT assets and prioritize OT security as a key aspect of their overall cybersecurity strategy.