ARMIS®

WHITE PAPER

Fortifying the Future

A Comprehensive Guide to Securing Cyber Physical Systems

Foreword

Securing Cyber Physical Systems (CPS) has become a critical priority for organizations worldwide. The blending of IT and Operational Technology (OT) systems has significantly increased the complexity of managing these environments, presenting unique challenges that require innovative and effective solutions.

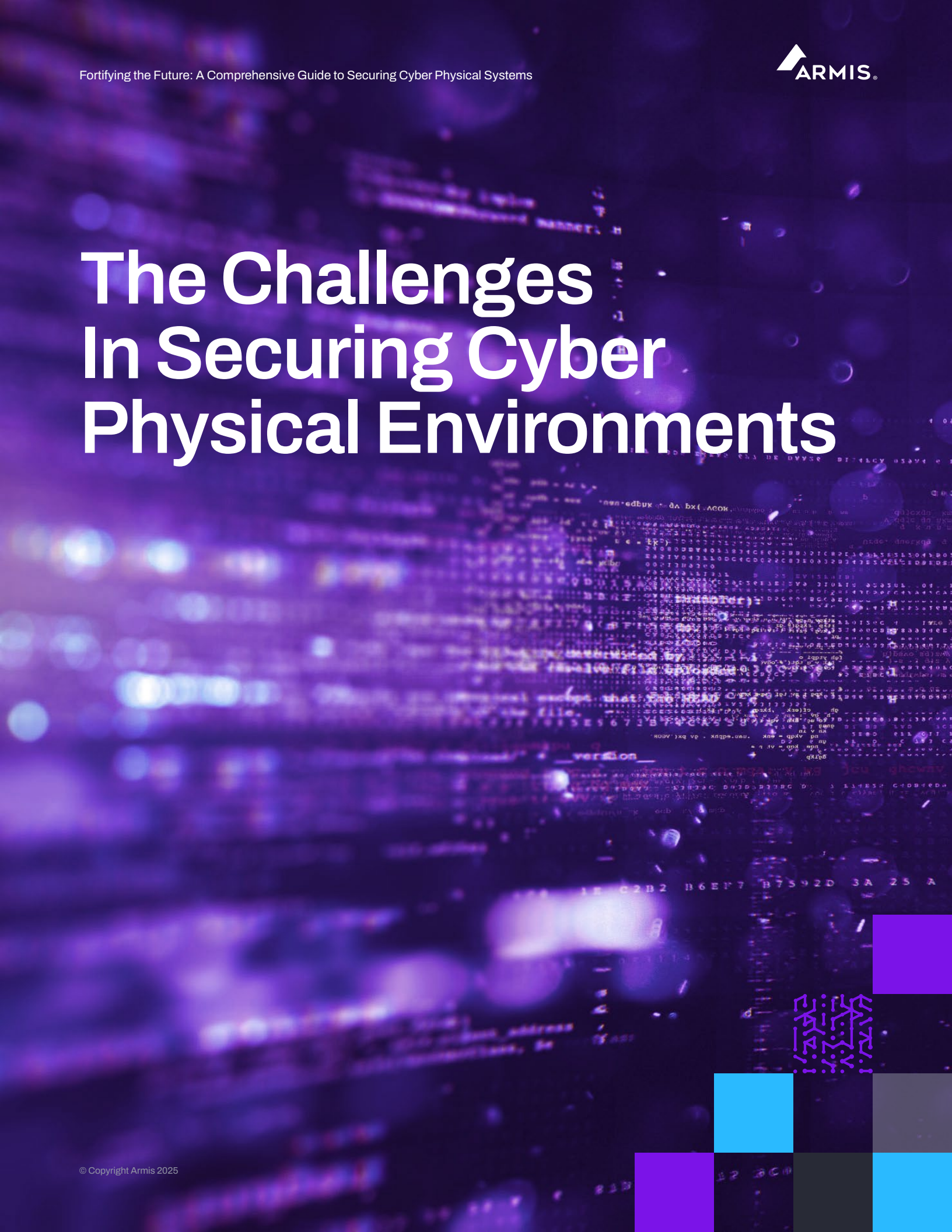
Examining the multifaceted challenges enterprises encounter in securing their cyber-physical ecosystems is a great way to begin formulating a security strategy. Key topics to address include navigating the ownership conundrum, balancing operational and cyber risks, and creating comprehensive threat response playbooks. All things that are addressed in this paper.

Our aim is to empower those in charge of handling these environments with the proactive data necessary to protect their assets effectively.

In addressing the challenges associated with centralized asset inventories, siloed teams and complex sprawling networks, leaders can establish a foundation for more secure and efficient operations. The path forward must consider the true cost of implementation, integration capabilities, and vendor support. In considering all of the above, we can move towards effectively securing the future of cyber physical environments.

ARMIS

The Challenges In Securing Cyber Physical Environments



Organizational Challenges in Operational Industries

The Ownership Question

Operational/ cyber physical environments are complex by nature, a fundamental challenge faced by organizations is the ambiguity surrounding the ownership of cybersecurity risks. The delineation of cybersecurity responsibilities is often blurred between information technology (IT) and operational teams. This ambiguity not only complicates the establishment of a clear cybersecurity strategy but also significantly hampers effective risk management.

Ownership of cybersecurity in cyber physical settings is pivotal because it dictates how resources are allocated, how decisions are made, and ultimately, how protective measures are implemented. Without clear ownership, there can be a detrimental lack of accountability, leading to gaps in the cybersecurity defenses that are critical for maintaining the integrity and availability of OT systems.

Operational Risk versus Cyber Risk

The relationship between operational priorities and cybersecurity needs is often complex and fraught with conflict. On one hand, operational teams are primarily focused on uptime, productivity and safety. They prioritize maintaining continuous operations and often perceive cybersecurity measures as a potential hindrance to operational efficiency. On the other hand, cybersecurity teams are tasked with safeguarding systems against threats, which sometimes requires implementing measures that can temporarily disrupt operations, such as system updates, patches, and downtime for security audits.

This dichotomy creates a scenario where the objectives of operational and cybersecurity teams can appear oppositional, even though they are fundamentally related. Both teams aim to ensure the system's integrity and availability, but their approaches and immediate priorities can differ significantly. Bridging this gap requires a concerted effort to align both teams' objectives, emphasizing that cybersecurity is a crucial component of operational integrity.

Building OT Expertise into Security

Deciding whether to integrate OT expertise into an existing central security function or to establish a dedicated OT security team is a strategic decision that organizations must make based on their specific operational landscapes and security needs. Integrating OT expertise into central security can foster a more unified approach to organizational cybersecurity, ensuring that both IT and OT are aligned under the same strategic umbrella. This integration can enhance the sharing of best practices and threat intelligence, providing a comprehensive view of organizational security.

Conversely, creating specific OT vulnerability and Security Operations Center (SOC) teams can allow for a more focused approach to specific challenges associated with Cyber Physical systems. Dedicated teams are often better equipped to address the unique technical and procedural nuances of OT environments, such as the need for specialized knowledge of industrial control systems and the specific threats they face. These teams can develop tailored security measures that adequately balance operational and security needs without compromising the functional integrity of OT systems.

Buy in from Key Stakeholders on Preventative Processes

Securing buy-in from the business for key preventative cybersecurity processes is crucial for the successful implementation of security measures. This buy-in is often challenging to achieve, particularly in environments where the impact of cybersecurity on operational efficiency is not well understood. To effectively gain this support, it is essential to communicate the value of cybersecurity investments in terms that resonate with business and operational leaders.

This involves:

- Demonstrating the potential impact of cybersecurity incidents on the business: Including potential costs of downtime in contrast to the cost of proactive measures, reputational damage, and regulatory penalties- including personal fines in some cases.
- Highlighting the alignment of cybersecurity measures with business objectives: Such as maintaining long-term operational integrity and reliability.
- Providing clear examples of successful interventions: Showcasing scenarios where preventative measures have effectively mitigated risks can help underline their value.
- Engaging stakeholders early in the security planning process: This ensures that their concerns are addressed, and their insights are incorporated, making the security measures more robust and applicable.

By addressing organizational ambiguity directly, aligning the objectives of operational and cybersecurity teams, making strategic decisions on the integration of OT expertise, and effectively securing buy-in for preventative measures, organizations can enhance their cybersecurity posture while maintaining operational efficiency.

This holistic approach not only protects critical infrastructure but also supports the organization's broader business objectives, ensuring sustainability and resilience in an increasingly complex cybersecurity landscape.

Lack of Foundational Data for Robust Processes

When it comes to CPS, one of the critical obstacles that impede the development of robust, strategic cybersecurity processes is the pervasive lack of foundational or situational data. The challenges associated with the collection, management, and utilization of OT asset data are multifaceted, stemming from issues in how data is stored, the complexity of asset discovery, and the fragmented nature of the asset inventories maintained by organizations. For starters, a lot of these inventories are still maintained in spreadsheets and stored locally.

Challenges with Central Asset Inventories

A primary issue in many organizations is that OT assets are not systematically populated in the central asset inventory systems that IT teams typically use, such as Configuration Management Databases (CMDB). This oversight can lead to significant gaps in the visibility of these assets, which are often critical to the operational integrity of cyber physical systems. The lack of integration into centralized systems stems not only from organizational silos between IT and OT but also from the technical challenges associated with cataloging highly specialized OT equipment.

Cost Implications of Storing a Proliferation of Cyber Physical Assets

Integrating Cyber Physical assets into sophisticated central management systems like CMDBs introduces another layer of complexity—cost. CMDB platforms are often designed with IT assets in mind and adapting them to accommodate OT assets can require extensive customization, which comes with high costs. These expenses can be prohibitive for many organizations, leading them to rely on less integrated and often less effective solutions for asset management.

Difficulties in Cyber Physical Asset Discovery

The discovery of OT assets presents unique challenges. Unlike IT assets, which are typically connected to network systems that support automatic detection, many OT assets are part of isolated networks or operate independently with minimal connectivity. This lack of connectivity, essential for ensuring operational safety and stability, complicates traditional network scanning and asset discovery methods, making it difficult to achieve comprehensive visibility.

Fragmentation in OT Device Inventories

The fragmented nature of OT device inventories further exacerbates the challenge. Without a centralized view of all assets, it becomes nearly impossible to assess holistic risks accurately or to strategize effectively about cybersecurity measures. Fragmentation leads to a piecemeal approach where security measures are often reactive and tailored to individual situations rather than being part of a unified strategy.

The Need for Comprehensive Risk Data

For OT, foundational data must encompass more than just a list of assets. It needs to include detailed information about:

> **Network Activities/Connections:** Understanding how devices communicate within the network is crucial for identifying potential vulnerabilities and pathways that could be exploited in a cyber attack.

> **Model/Firmware Vulnerabilities:** Information about the specific models and firmware versions of OT devices is critical for identifying known vulnerabilities and determining the necessity of updates or patches.

Consequences of Bifurcated Data

Bifurcated data not only results in a bifurcated process but also reflects a misalignment with the realities of today's OT environments. In an era where the integration of IT and OT is increasingly necessary for operational efficiency and security, maintaining separate datasets for each leads to inefficiencies and missed opportunities for comprehensive risk management. A holistic view of risk, essential for developing robust processes, cannot be established on top of bifurcated data. This separation hinders the ability to perform comprehensive risk assessments and to deploy strategic, proactive cybersecurity measures effectively.

Moving Forward

Addressing these challenges requires a concerted effort to improve the breadth of Cyber Physical asset discovery processes, integrate these assets into centralized management systems cost-effectively, and develop unified inventories that provide comprehensive visibility and detailed risk data. By overcoming these hurdles, organizations can lay the groundwork for robust cybersecurity processes that enhance both the security and the operational efficiency of their operational and IT environments. This strategic improvement not only supports the organization's immediate security needs but also its long-term resilience and adaptability in an increasingly interconnected and technologically complex landscape.

Procedural Challenges in Operational Technology Security

The ability to respond effectively to threats in OT environments is critical for maintaining the integrity and continuity of operations within cyber physical environments. However, many organizations face significant challenges due to the lack of established processes for threat response and prevention. This absence of clear protocols can lead to delayed actions, inconsistent responses, and ultimately, increased vulnerability to cyber threats.

Responding to Threats Against OT Assets

When a threat is identified on an OT asset, the immediate question that arises is, “How do we act?” The complexity of CPS systems, where operational continuity is paramount, means that the response to any threat must be swift and precise to minimize impact. However, without predefined response processes, staff may hesitate or take incorrect actions, exacerbating the threat. Establishing clear, actionable steps that are tailored to the specific characteristics of CPS systems is essential. This includes determining who is responsible for what actions, how communication should flow, and what tools are available to assist in mitigating the threat.

Assessing the Impact of Threats

Deciding what threat justifies operational impact is another critical consideration. Not all threats pose the same level of risk, and not all require actions that might disrupt operations. The decision-making process for assessing the impact of a threat involves understanding the potential consequences of both the threat itself and the response actions. This requires a deep understanding of the operational processes involved and the vulnerabilities of the OT assets. Criteria should be developed that help categorize threats based on their potential impact, guiding decision-makers on when operational disruptions are justified to mitigate risks.

Developing a Playbook for Response

A well-crafted playbook for response is crucial for ensuring consistency and effectiveness in handling security incidents. This playbook should outline specific procedures for different types of threats, providing a step-by-step guide that staff can follow during an incident. Each playbook should be tailored to the unique aspects of the OT environment, reflecting the specific technologies, processes, and personnel involved. Key elements of a response playbook include:

- Identification of roles and responsibilities for all involved parties.
- Step-by-step response actions based on the severity and nature of the threat.
- Communication protocols, including who needs to be notified and how.
- Documentation and follow-up procedures to analyze the response and apply lessons learned.

Preventative Measures and Process Development

Beyond responding to immediate threats, establishing preventative measures is crucial for reducing the likelihood of incidents occurring in the first place. These measures include regular security assessments, vulnerability discovery tailored to OT environments (utilizing safe querying methods), and employee training programs focused on security awareness and response protocols. The processes for these preventative measures should be integrated into the regular operational routines, ensuring they are consistently applied without disrupting the normal function of OT systems.

Additionally, preventative processes should include:

- Awareness of external threat trends and cyberattacks affecting industries similar to yours. Access to threat intelligence feeds/ early warnings can allow you to focus on the risk findings that matter most to you.
- Continual monitoring of CPS systems for unusual activities that could indicate potential threats through mechanisms like behaviour baseline rules.
- Regular updates and patches to OT software and firmware, applied in a manner that minimizes operational disruption.
- Development of redundancy and fail-safe operations to maintain system integrity in the event of a cyber incident.

The absence of defined processes for managing threats in CPS environments can critically weaken an organization's defense against cyber incidents. By establishing precise response playbooks, accurately evaluating threat impacts, and enacting strong preventative strategies, organizations can bolster their resilience. These measures mitigate security incident effects and enhance operational efficiency and safety in industrial settings, crucial for ensuring long-term security and operational sustainability in a complex, threat-laden environment.

ARMIS®

Building The Future

The First Steps

As OT organizations look to bolster their operational security, the first step in building a robust defense lies in gaining a comprehensive understanding of the existing asset landscape. This process begins with the thorough discovery of OT assets and their situational data, maintaining a centralized inventory, categorizing these assets effectively, and developing detailed response playbooks tailored to various threat levels and asset criticalities.

Situational Awareness of Every Asset

The discovery phase is crucial and often reveals the hidden complexities of an organization's operational infrastructure. Identification of this gap was made possible through the deployment of discovery tools combined with physical audits, highlighting the necessity of integrating both digital and manual asset tracking methods.

The asset discovery process doesn't stop at hardware, but involves understanding their network configurations, operating systems, and firmware versions. Tools like continuous network monitoring and smart active querying can be deployed, depending on the sensitivity and accessibility of the equipment. In critical systems where active scanning could disrupt operational functionality, passive monitoring techniques are preferred to collect data without impacting system performance.

One Source of Truth in a Central Inventory

Once assets are discovered, the next step is to maintain this information in a central inventory that can be accessed and updated in real time. The centralization of asset data solves numerous challenges, particularly in environments where information is traditionally siloed. A leading petroleum company implemented a centralized asset management system that not only standardized data across various installations but also enabled real-time updates which significantly enhanced their ability to respond to vulnerabilities and threats as they were identified.

This inventory should include detailed information on each asset, such as location, operational criticality, network behavior, and any known vulnerabilities. The costs of an asset inventory platform can be justified by the significant value it adds in terms of centralized control and compliance readiness.

Categorizing Assets by Impact and Risk

Effective categorization of assets is fundamental in prioritizing security efforts. Assets should be categorized not just by their physical characteristics or location but more critically by their operational impact and the risk associated with their downtime. For instance, an energy provider may categorize control systems operating in critical substations with a higher risk profile compared to less critical monitoring devices.

This categorization allows organizations to apply a tiered approach to security, focusing resources and stricter controls on high-impact assets while maintaining balanced protection across the board. For example, during a ransomware threat that targeted the auto manufacturing sector globally, one company was able to quickly isolate and protect high-impact assets because they had clear categorizations based on the potential impact of downtime, preventing widespread disruption.

Building Playbooks Based on Severity of Threats

The final foundational step is the development of response playbooks. These playbooks should be specific, detailing actions based on the severity of the Common Vulnerabilities and Exposures (CVE) identified, the nature of the threat, and the categorized impact of the asset involved. For instance, a playbook might specify different response protocols for a known-exploited CVE impacting a critical control system, versus an unexploited CVE affecting a non-critical monitoring tool.

In Short

Building a resilient future in CPS security requires meticulous planning and execution beginning with these foundational steps. By systematically discovering assets, maintaining a central inventory, categorizing assets effectively, and preparing detailed playbooks, organizations can not only defend against current threats but also prepare for future challenges in an increasingly interconnected and complex threat landscape. This strategic approach not only enhances security but also supports operational continuity and business resilience.

Strategic Considerations for Cyber Physical Security Solutions

Prevention is Better than Reaction

In cyber physical environments, prevention is far more effective than reacting to incidents after they occur. By becoming proactive, organizations can anticipate and mitigate threats before they disrupt critical systems, ensuring the safety and reliability of their operations. Integrating early warnings and external risk analysis into this strategy enables organizations to prioritize vulnerabilities based on real-world data, allowing them to focus on the most significant risks. This proactive approach not only minimizes potential damage but also optimizes resource allocation, ensuring that the most critical vulnerabilities are addressed first, thereby enhancing overall security posture.

An array of diverse solutions exist for protecting and managing industrial environments, each promising to enhance operational integrity. However, as organizations chart their paths toward a more secure and resilient OT environment, it is crucial to proceed with a discerning eye. This section offers an examination of common pitfalls in selecting OT security solutions and underscores strategic considerations that can guide you in making decisions that align with long-term operational and security goals.

Understanding the True Cost of Implementation

One of the first considerations in choosing an OT security solution is understanding the full spectrum of costs involved. It's common to encounter solutions that appear financially viable on the surface but may lead to significant indirect costs. For example, systems that require extensive customizations or frequent manual updates can escalate operational costs and strain resources over time. The financial implications of implementing a security solution extend beyond the initial purchase; they encompass integration, maintenance, and the potential for future scalability without substantial additional investments.

Evaluating the Efficacy of Asset Discovery

Effective asset discovery is the cornerstone of robust OT security. Some solutions in the market struggle with providing a thorough and accurate inventory, particularly in complex environments where OT assets are diverse and not standardly networked. Solutions that offer comprehensive discovery capabilities are vital. These capabilities ensure that all assets, regardless of their connectivity or configuration, are accounted for and protected.

Assessing Flexibility and Integration Capabilities

Another pitfall is investing in solutions that offer limited flexibility in terms of integration with existing systems. In today's OT environments, where nothing operates in isolation, the ability to seamlessly integrate with other IT and OT systems is crucial. Solutions that support open standards and offer extensive API integrations can facilitate smoother interoperability and more cohesive security posture management across diverse technological landscapes.

Considering Long-term Vendor Support and Development

The rapidly evolving nature of cybersecurity threats necessitates solutions that are not only effective today but continue to evolve. Choosing a solution from a vendor that has a clear roadmap for development and offers ongoing support and updates is essential. Solutions that may offer immediate compatibility and functionality but lack a commitment to future development can quickly become obsolete, leaving organizations vulnerable to emerging threats.

Analyzing a Solution's Response to Real-world Threats

Lastly, the theoretical effectiveness of a security solution can differ vastly from its performance in real-world scenarios. It's crucial to consider how solutions have enabled OT teams to respond to actual security incidents in the past. Solutions that have consistently responded quickly and effectively to emerging threats, demonstrating adaptability to new vulnerabilities, provide not only robust security but also a sense of reliability and assurance.

Conclusion

In navigating the market of security solutions designed for CPS environments, it is essential to look beyond surface-level features and evaluate deeper operational and strategic impacts. By being mindful of these considerations, organizations can avoid common pitfalls and select a solution that not only addresses immediate security needs but also aligns with long-term operational resilience and strategic goals. This approach ensures that investments in OT security yield sustainable benefits, enhancing both the security and efficiency of critical everyday operations.

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