SAFEGUARDING CRITICAL INFRASTRUCTURE BY EVOLVING MONITORING AND RESPONSE CAPABILITIES

Whitepaper

October 2024

GLOBAL CYBERSECURITY FORUM

aramco

Foreword

Basim Al Ruwaii
Saudi Aramco;
Chairman of the Knowledge Community:
Securing Industrial Systems for Global
Energy Supply

Today, it is more imperative than ever that we come together to address the root causes of the complex, persistent cybersecurity challenges in the industrial sector. Isolation alone is no longer an effective approach to secure our environments. The convergence of Information and Operational Technologies, the massive amounts of data utilized for Artificial Intelligence applications, and the emergence of advanced threats present both new challenges and opportunities.

Forming communities that bring together different industry players is a foundational effort to drive change toward a more resilient future.

Together, we navigate the complexities of industrial cybersecurity, share knowledge, and work collaboratively to ensure the resilience and security of critical infrastructure globally.

Together, with the Global Cybersecurity Forum (GCF), we are proud to bring the collective thought of pioneering industrial systems leaders across our domain, and we invite leaders to take proactive steps to navigate beyond the status quo and uplift cybersecurity capabilities.

Lead Authors

- **Noora A. Alfayez -** Saudi Aramco
- **Norah Alkhathlan -** Saudi Aramco
- **Tamer Charife -** Deloitte & Touche (M.E.)
- **Mohamad Hamad -** Deloitte & Touche (M.E.)
- **Mujali AlKhaldi -** Cyberani
- **Razan Alghamdi -** Cyberani

Contributors

- **Salem Elwi -** Saudi Aramco
- **Hisham Alsuwayied -** Saudi Aramco
- **Taede Rakhorst -** Deloitte & Touche (M.E.)
- **Abdallah El Chal -** Deloitte & Touche (M.E.)
- **Michael Mosaad -** Deloitte & Touche (M.E.)
- **Muhammed Alwashmi -** Cyberani
- **Tareq AlBassam -** Cyberani
- **Mohammed AlMintakh -** Cyberani

Knowledge Community: Securing Industrial Systems for Global Energy Supply

Founded by Aramco, the GCF Knowledge Community 'Securing Industrial Systems for Energy Supply' wors to fortify the world's energy lifelines and ensure a resilient and secure energy future for all.

We are dedicated to strengthening the cyber resilience of the global energy ecosystem, leveraging the diversity of expertise of our membership, which includes 14 international stakeholders.

Contents

1. Executive Summary

The global energy sector is undergoing a profound digital transformation, integrating advanced digital systems to improve production and operational efficiency.

As this transformation progresses, the convergence of Information Technology (IT) and Operational Technology (OT) environments has increased, creating a more interconnected landscape where Industrial Control Systems (ICS) play a vital role in managing infrastructure. However, this integration also exposes critical infrastructure to cyber threats, as OT systems become increasingly vulnerable to both internal and external attacks.

Cybersecurity for OT environments is no longer a secondary concern but a strategic priority. The rise in sophisticated cyber-attacks, such as ones targeting power grids or pipelines, underscores the need for robust OT cybersecurity measures. It demonstrates how attackers can exploit vulnerabilities in IT systems to infiltrate OT networks, disrupting essential services, compromising safety, and causing significant operational and financial damage.

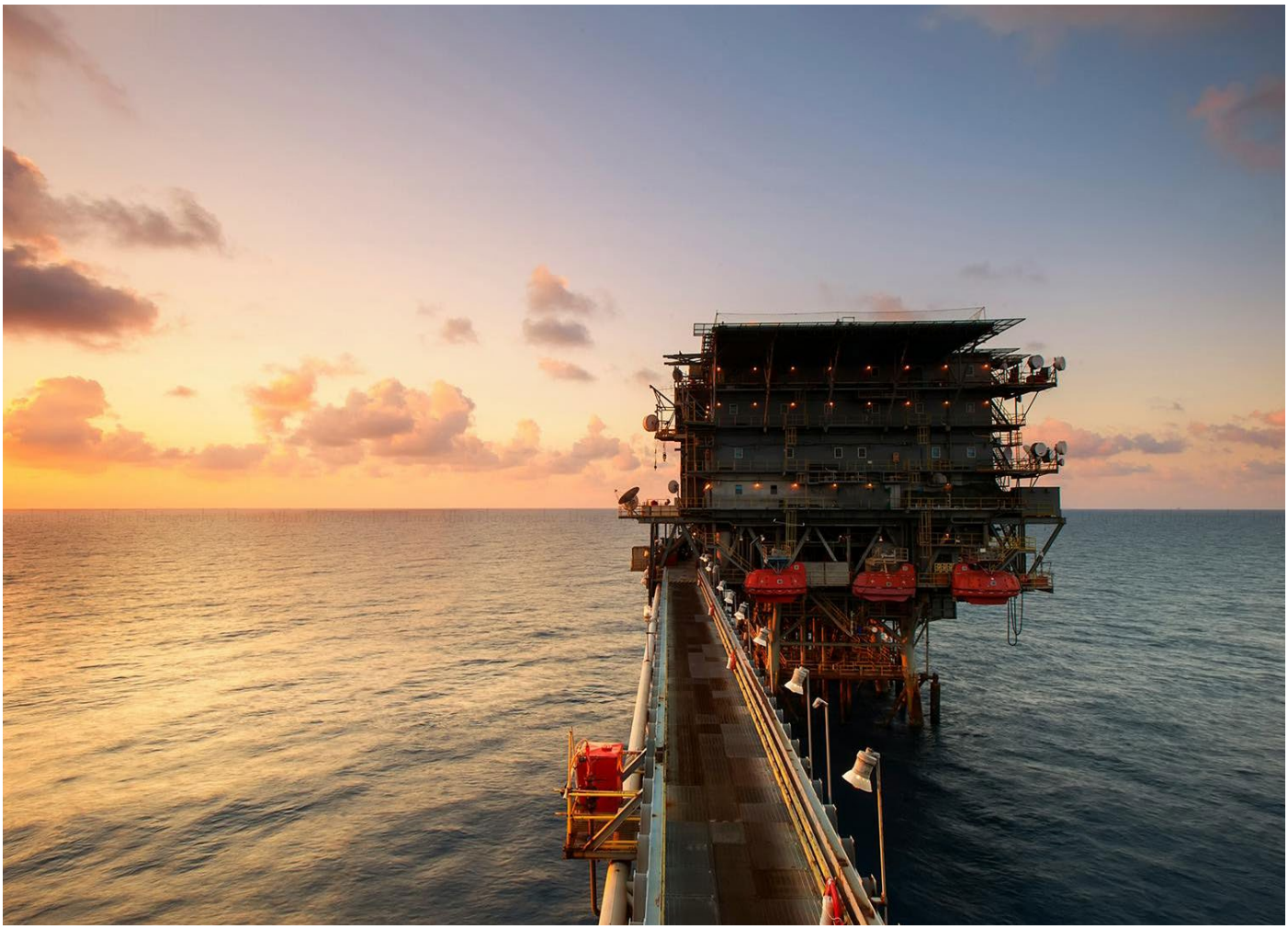
This whitepaper examines the importance of developing OT cybersecurity monitoring and incident response capabilities to safeguard ICS assets from growing cyber threats. It highlights key challenges related to governance, technology, and resources that energy sector organizations face when securing their OT environments. A major challenge is the alignment of IT and OT teams under a unified governance framework, as these traditionally siloed areas often follow different protocols and priorities. Legacy systems within OT environments, which are difficult to update or replace, further complicate efforts to maintain a secure infrastructure.

Supply chain risks also pose significant threats to OT systems. Many energy companies rely on third-party vendors who introduce IT tools that may not suit the OT environment. This lack of visibility into third-party practices can create blind spots, leaving critical infrastructure vulnerable to cyberattacks. Moreover, the scarcity of skilled professionals with expertise in both OT and cybersecurity is a barrier to implementing effective monitoring and response strategies, leading to delayed reactions during incidents.

To tackle these challenges, a multi-pronged approach is essential. This includes the development of a comprehensive governance framework that aligns IT and OT cybersecurity efforts under a unified strategy, ensuring that all protocols are adapted to OT's unique requirements. Continuous monitoring across both IT and OT environments must be implemented, allowing for early detection of threats and proactive mitigation of vulnerabilities. Network segmentation, Identity and Access Management (IAM), and clear incident response playbooks are also critical to preventing the spread of attacks across IT and OT systems.

Additionally, organizations need to strengthen their relationships with third-party vendors by enforcing stricter cybersecurity clauses in contracts and regularly monitoring vendor compliance. Investing in human capital by expanding the talent pool and offering specialized training programs for OT cybersecurity professionals is crucial to overcoming the skills gap.

By addressing these challenges and adopting robust cybersecurity measures, the energy sector can better protect critical infrastructure, ensuring resilience and safeguarding against the evolving cyber-threat landscape.



2. Introduction

Industrial systems in the energy sector are globally recognized as critical infrastructure, essential to the economy and the functioning of society.

Any disruption to these systems can cause a profound impact on public safety, economic stability, or result in major reputation damage to affected organizations. As technology advances, these systems have become increasingly interconnected, complex, and reliant on digital processes. Consequently, security of these systems remain as key priority.

It is no surprise that energy sector companies have launched multiple initiatives to safeguard their OT environments from potential threats. They face challenges and have undertaken various measures to enhance the overall security of their critical infrastructure.

These measures include developing an effective governance model for OT Security Operations Centre (SOC) monitoring, increasing visibility across the OT network for accurate asset inventory, developing appropriate use cases and response playbooks for monitoring OT systems, and leveraging processes and resources for IT and OT cyber monitoring and response convergence.

3. Adapting to New Realities Due to the Shifting Threat Landscape

Energy is the fourth most attacked industry, representing 11.1% of all attacks.[1]

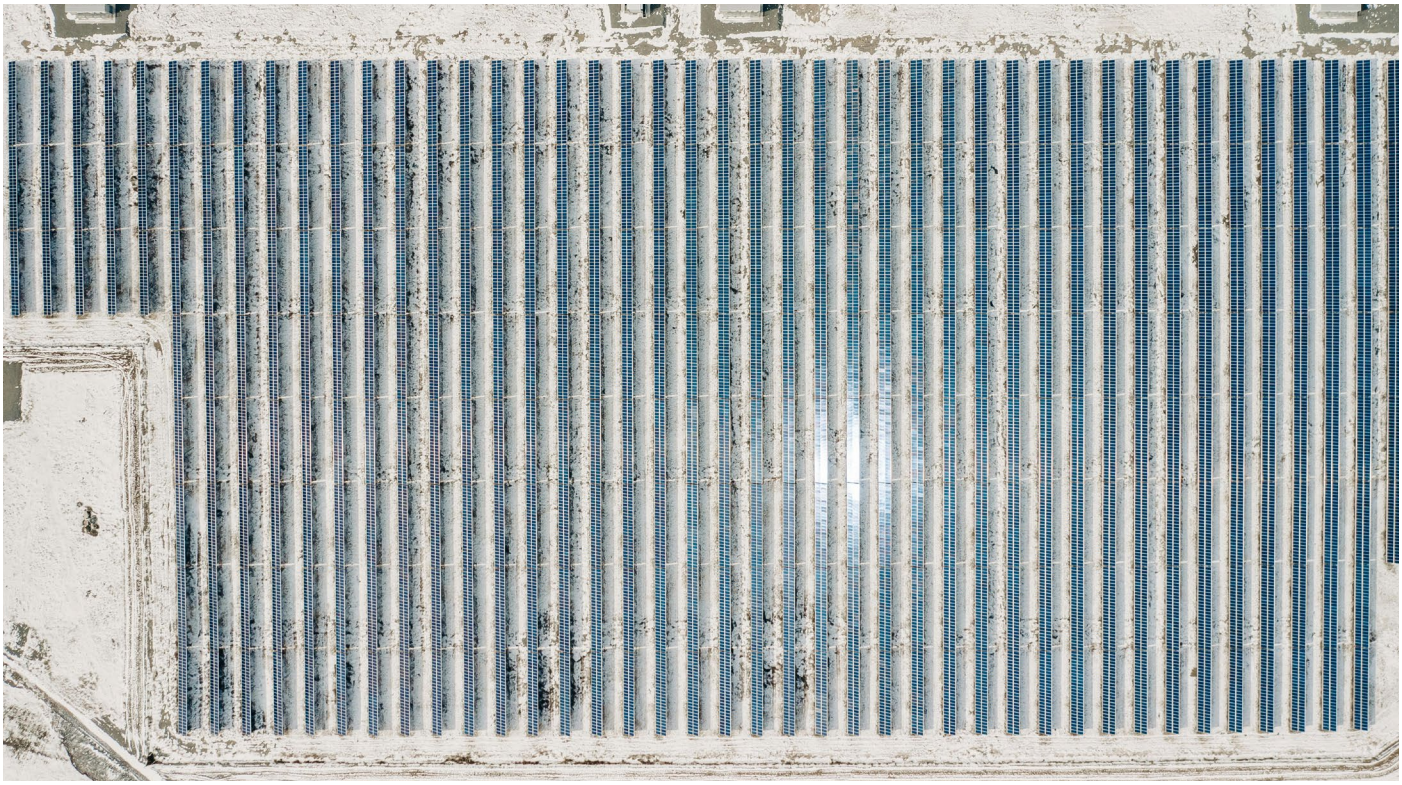
Furthermore, cyber-attacks against OT systems have become increasingly prevalent and sophisticated in recent years. According to Fortinet, 73% of organizations experienced intrusion that impacted either OT systems only or both IT and OT systems in 2024, up from 49% in 2023.[2]

The cyber threat landscape has drastically shifted and expanded within the OT environment as more threat vectors and techniques emerge due to increased digital transformations and interconnected systems. Notable incidents, such as the Stuxnet, TRISIS malware and BlackEnergy cyberattacks, have demonstrated that threats against the energy sector can impact operations, employee safety, public safety and the environment.

In recent years, cyberattacks on the energy sector have highlighted the vulnerabilities in critical infrastructure. For instance, attacks on power grids have compromised operational technology (OT) systems, leading to widespread power outages and affecting thousands of households.

Similarly, ransomware attacks targeting IT systems have forced the precautionary shutdown of OT systems, resulting in significant disruptions, such as fuel shortages and energy supply issues. These incidents illustrate the interconnectedness of IT and OT environments and how weaknesses in one area can lead to large-scale disruptions across the energy sector.

The rise of such threats has pushed entities to build their cyber capabilities to monitor their OT environments and establish dedicated cyber response teams to address cyber threats across different systems and networks. This has been confirmed by expected increases in cybersecurity investments by energy companies, from $6bn in 2019 to $10bn in 2025.[3]



4. Strengthening Monitoring and Incident Response in OT Environments

Developing monitoring and response capabilities is crucial for enhancing an organization's cyber resilience.

The goal is to detect anomalies and issues by analyzing network traffic and logs from various devices and users. Effective monitoring provides insights into connected assets and the types of traffic they generate within the OT network. By monitoring the environment effectively, organizations can detect malicious behaviors and enable response teams to intervene accordingly.

4.1 OT Cyber Monitoring Models

A sufficient cyber monitoring and incident response program requires full visibility across OT systems, providing a holistic view of all assets, network traffic, and potential threats. One of the significant challenges in the OT environments is the lack of visibility which hinders the detection and response to cyber threats in a timely manner. The lack of visibility makes it difficult for organizations to fully understand their systems' interconnectivity and data flow, which in turn become difficult to detect anomalies and respond to incidents effectively.

Given the complexity of OT monitoring, which involves multiple types of network traffic, various technologies, and a vast array of software and devices, comprehensive monitoring of every device or network individually is challenging. Engineers have implemented different monitoring models to address specific challenges.

Passive Monitoring
Consists of analyzing network traffic without directly interacting with devices to avoid disrupting critical processes. Techniques include network traffic analysis using port mirroring, packet capture, and log analysis.

Active Monitoring
Involves direct engagement with devices on the network through vulnerability scanning, pulling system logs and events and network scans. This method enables comprehensive insights into device configurations and potential vulnerabilities.

Hybrid Monitoring
Integrates various techniques and technologies to provide comprehensive monitoring visibility across the industrial systems. This approach aims to achieve a more inclusive and balanced security posture, surpassing the limitations of relying solely on either method.

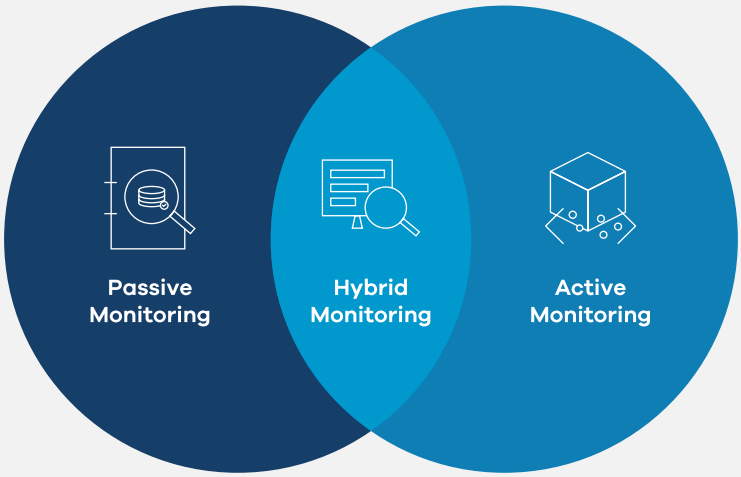


Figure 1 - OT Cyber Monitoring Models

4.2 Swift Actions Required for Incident Response

A secure OT environment can never be guaranteed; networks remain prone to cyber threats.

Therefore, organizations should proactively develop robust incident response plans to manage security incidents effectively. These plans should outline response actions based on established procedures, including the roles of the entire Incident Response (IR) team, especially the IR leader and the escalation mechanism to the authorized team for making critical decisions on isolations, shutdowns, etc.

Early incident identification using appropriate monitoring tools and a well-defined response plan is crucial to minimize impact and contain security breaches. The IR team's role is critical in overseeing the incident response process, from initial detection to final resolution. This includes identifying, investigating, coordinating, and responding to security incidents within an organization's network or system.

"Notable incidents have demonstrated that threats against the energy sector can impact operations, employee safety, public safety and the environment."

5. Key Challenges

A holistic view of the challenges and obstacles hindering the enhancement of cyber monitoring and response capabilities within the energy sector involves assessing entities involved in energy operations, including technology providers, control system OEM vendors, and consulting firms. Based on this assessment, the following key challenges can be outlined.

Figure 2 - Key Challenges

5.1 Rapid Technological Advancement

Traditionally, IT and OT systems operated in isolation, often referred to as "air-gapping," which minimized OT's exposure to cyber risks common in IT environments.

However, digital transformation is closing the divide between IT and OT, driven by the need for real-time data and operational efficiency.

For instance, AI and ML are increasingly being integrated into power plants or substations to analyze data in real-time, optimize operations, and predict equipment failures. Additionally, real-time access to critical infrastructure allows for predictive maintenance and remote monitoring, reducing downtime. The shift to remote work has further accelerated the need for seamless integration between IT and OT, allowing people to manage operations without being physically present at each facility.

The rapid technological changes in the OT environment expands the attack surface, allowing vulnerabilities in IT networks to be exploited as entry points into OT systems. Once compromised, attackers can move laterally between IT and OT environments, posing significant risks to critical infrastructure and increasing the complexities of incident response.

5.2 Legacy Systems

We must recognize that many existing systems, some of which are over 50 years old, still play a crucial role in energy production and distribution.

These legacy systems often lack the resilience needed to withstand modern threats, and retrofitting them presents significant challenges, ranging from obsolete hardware to vendor lock-in and high costs associated with upgrades.

Legacy systems are notoriously difficult to maintain and monitor due to outdated designs and often a lack of essential monitoring and logging capabilities. These systems can rely on proprietary protocols and outdated communication methods that are incompatible with modern security tools, hindering real-time monitoring and detection of potential security incidents. Over time, legacy systems become increasingly vulnerable because they no longer receive vendor support or patches, leaving them exposed to known threats.

Unlike IT environments, where legacy systems are gradually being phased out, OT environments often depend heavily on these technologies. For example, a Manufacturing Execution System (MES) might still require a Windows 2003 server for operation, or OT controls may only function on unsupported platforms like Windows XP.

These outdated systems cannot easily be replaced due to compatibility issues with newer technologies, and attempting to upgrade can lead to significant operational disruptions. This reliance on legacy systems creates substantial security gaps, making it difficult to apply modern security solutions and leaving critical infrastructure vulnerable to cyber threats.

5.3 Supply Chain Risk Management

Securing the supply chain in OT environments is complex due to the deep, heterogeneous, and opaque nature of vendor relationships.

Third-party access poses significant security risks, with many OT security decision-makers seeing supply chain vulnerabilities as one of the top concerns. These risks arise simply because third-party vendors bring in IT tools that would not normally be present in an OT environment, potentially exposing critical infrastructure to cyber threats.

Additionally, vendors may have weaker security protocols and/or often pay less attention to security practices – it can be as simple as vendors plugging their personal devices onto a client's OT system – further increasing the risk of attackers exploiting these vulnerabilities and infiltrating OT systems.

A key challenge is reduced visibility into third-party technology landscape / cybersecurity protection. OT systems rely on proprietary technologies, making it difficult to effectively monitor vendor activities across the entire landscape effectively. This lack of visibility can lead to blind spots, where unauthorized access or anomalies go undetected, increasing the likelihood of breaches. Inconsistent security standards across vendors further complicate the enforcement of a uniform security strategy, leaving exploitable gaps.

Supply chain security is also complicated by the reliance on multiple critical vendors, each using distinct technologies. Without seamless integration of security measures across vendor systems, fragmentation can weaken the overall security posture. This fragmentation not only creates vulnerabilities but also slows down incident detection and response, as misaligned protocols and varied capabilities among vendors hinder effective collaboration during breaches.

Incorporating cybersecurity clauses into vendor contracts is one solution, but negotiations can be lengthy and delay implementation. Even with agreements in place, continuous monitoring of vendor cybersecurity practices is crucial, as periodic assessments may miss emerging threats. Monitoring helps detect security gaps early and allows for the implementation of remediation plans. If vendors fail to address these issues, additional compensating controls, such as restricting access or enhancing internal monitoring may be necessary.

5.4 Operating Model

One of the most significant challenges in OT environments is the lack of a well-defined governance structure that aligns cybersecurity, IT, and OT teams.

The cybersecurity function should act as a second line of defense, overseeing both IT and OT to ensure alignment between these traditionally siloed teams. However, this coordination is often underdeveloped, leading to fragmented security efforts.

A key issue is that cybersecurity policies are typically tailored to IT systems and fail to account for OT's unique needs. OT teams may create their own guidelines, further complicating alignment. Extending cybersecurity policies to OT is crucial, but these policies must be adapted to OT's specific requirements, such as differing approaches to patch management, where simply deploying a patch without extensive testing can significantly disrupt operations.

The lack of clearly defined operating models results in fragmented efforts and inefficient incident response. Without a unified framework, IT and OT teams often follow different protocols and priorities, further complicating cybersecurity strategies.

The diverse technologies and operational needs in OT environments make it difficult to harmonize threat detection and response, increasing security vulnerabilities.

Additionally, the absence of comprehensive guidelines and documentation makes it difficult to effectively monitor OT devices or include them in incident response plans. OT systems are diverse, using proprietary technologies that require systematic approaches to function effectively.

Without clear guidelines or documentation, it is challenging to coordinate monitoring efforts or develop effective response strategies, especially for non-technical professionals.

Moreover, OT environments rely on coordination among multiple stakeholders—such as engineers, maintenance teams, and vendors—who often operate from different locations to fulfill a unified function. This complexity is further amplified by the need to collaborate with IT teams as the systems become more integrated. As a result, operational management and incident response become more challenging, with growing communication difficulties as more stakeholders are involved.

5.5 Human Capital

Due to the major differences between IT and OT in terms of objectives, priorities, strategies and implementations, many industries face significant challenges in building a dedicated OT cybersecurity team.

In addition, the specialized nature of OT environments, with their unique technologies and operational requirements, makes it challenging for traditional IT security teams to effectively monitor and secure OT systems.

Effective cybersecurity monitoring and incident response demand a unique skillset encompassing both cybersecurity and process engineering. However, a significant barrier in enhancing OT monitoring and incident response capabilities is the substantial skills shortage within the workforce, which hinders effective cybersecurity monitoring and response. This scarcity of skilled professionals results in delayed or absent responses from tactical teams, compromising the security and operational efficiency of OT environments.

OT environments require seamless collaboration between multiple stakeholders, including operational engineers, maintenance teams, and vendors, often dispersed across different locations. This geographic dispersion complicates both operational management and incident response, highlighting the need for clear communication and alignment of priorities. Adding to this complexity is the scarcity of cybersecurity talent, especially in the energy sector, where operations are frequently based in remote areas. This isolation further limits the availability of qualified OT professionals, making recruitment and retention a significant challenge for maintaining effective cybersecurity strategies.

6. Recommended Approach to Address Challenges

6.1 Elevating Technical Abilities

Figure 3 - Recommended Approach to Address Rapid Technological Advancement Challenges

6.1.1 Data validation and enrichment

To gain deeper insights into the OT environment, continually updating and enriching existing operational data with supporting information is crucial.

This approach enables the security team to comprehend normal daily activities, such as changes to control systems and applications, patching and backup cycles, and enhances their ability to respond effectively to incidents. This strategy involves monitoring network traffic, reviewing historical changes, and establishing baselines for normal activities to detect unexpected behaviors.

6.1.2 Monitoring tools

To ensure comprehensive event detection and mitigation, organizations need to establish coordinated monitoring across both IT and OT environments.

As these environments become increasingly interconnected, a breach in one domain can compromise the other, underscoring the need for unified monitoring. By integrating monitoring systems, organizations can enhance operational efficiency, gain real-time insights, and reduce downtime, while also strengthening the cybersecurity posture.

This holistic approach improves the visibility of vulnerabilities, ensuring threats are detected earlier and with enhanced accuracy. Additionally, coordinated monitoring enables quicker decision-making, predictive analytics, and unified incident response, reducing the risk of cascading failures. It also supports compliance with stringent cybersecurity regulations, safeguarding critical infrastructure and ensuring secure operations across all layers.

6.2 Legacy systems

Figure 4 - Recommended Approach to Address Legacy System Challenges

6.2.1 Securing legacy systems

Securing legacy systems is a vital consideration in enhancing monitoring and response capabilities. Because these systems often cannot receive security patches and upgrades, isolating them within the network is important, limiting their exposure to other devices. Additionally, applying a suitable monitoring model to network traffic around these systems helps ensure their security despite their limitations in receiving updates.

6.2.2 Network segmentation

Network segmentation is crucial in IT-OT environments for improving both cybersecurity and operational efficiency. By dividing networks into isolated segments, organizations can reduce their attack surface, limiting the spread of threats and preventing unauthorized access between IT and OT systems. This approach is particularly important in protecting critical infrastructure from cyberattacks.

Segmentation also enhances operational efficiency by optimizing network performance, ensuring smooth data flow, and simplifying compliance with regulatory standards. Additionally, it strengthens resilience by enabling faster incident response and protecting vulnerable legacy systems. Implementing network segmentation is essential for securing modern industrial environments.

Restricting access to specific users and prohibiting remote access are essential strategies for securing IT-OT environments. Limiting access to authorized personnel reduces the risk of unauthorized actions and enhances security by ensuring that only those who need to interact with OT systems can do so. Implementing Role-Based Access Control (RBAC) further strengthens this by assigning clear permissions, while monitoring access allows organizations to track user activities and ensure accountability. Disabling remote access reduces external threats by eliminating a common attack vector for cybercriminals. This measure also protects legacy systems, which may not support modern security protocols, and improves incident response by requiring on-site access for any system changes, ensuring better oversight and control. Together, these strategies enhance security, protect critical infrastructure, and improve operational resilience.

6.3 Holistic Governance

Figure 5 - Recommended Approach to Address Governance Challenges

6.3.1 Governance framework

Defining a governance framework with focus on operating model and clear guidelines is pivotal in strengthening incident response capabilities and establishing a structured framework for entity interactions. It involves defining clear roles, responsibilities, and accountability to streamline decision-making, enforce policies, and coordinate efforts across diverse teams.

Therefore, developing a robust governance model is crucial for significantly elevating cybersecurity capabilities and ensuring cyber-resilient critical infrastructure.

6.3.2 Comprehensive asset management

It is critical to develop cyber monitoring and response capabilities by setting up an asset management process and a knowledge base. Precise knowledge of asset types, versions and ownership is essential for effective security monitoring and incident response.

Asset management provides clear visibility into the OT environment, identifies vulnerabilities and threats, and enhances communication and accountability during incidents. Conducting a business impact analysis at this stage is equally vital. This analysis helps assess the impacts of vulnerabilities and the criticality of assets, forming the foundation for classifying and prioritizing security alerts.

6.3.3 Security monitoring strategy

In developing a comprehensive cybersecurity monitoring strategy, it is imperative to maintain up-to-date records of all existing data sources, including the type of data, retention periods, and storage locations. Additionally, implementing an offline monitoring strategy for legacy systems is crucial and should be regularly re-validated.

This strategy should incorporate compensating controls to mitigate risks associated with inadequate security monitoring capabilities. Such measures ensure proactive risk management and enhance overall cybersecurity resilience.

6.3.4 Threat intelligence feeds integration

Integrating threat intelligence fees is essential to gaining real-time insights into the OT threat landscape. By incorporating threat intelligence, organizations can proactively identify vulnerabilities and understand the tactics, techniques and procedures threat actors employ to target OT environments.

This integration enables security teams to enhance their incident response capabilities and fortify defenses against emerging cyber threats. Leveraging frameworks such as the ICS MITRE ATT&CK provides a structured approach to mapping threats specific to OT, ensuring coverage of potential attack vectors.

Creating effective threat use cases and response playbooks requires overcoming organizational silos and technical expertise gaps between IT and OT teams. Aligning priorities and establishing clear communication channels are essential for ensuring that incident response strategies are cohesive and effective in addressing the unique challenges of OT cybersecurity.

“By incorporating threat intelligence, organizations can proactively identify vulnerabilities and understand the tactics, techniques and procedures threat actors employ to target OT environments.”

6.3.5 Risk assessment and business impact analysis

Risk profiling is a critical process that enables organizations to assess the importance of their systems to core operations. This process aims to pinpoint the most crucial systems within the organization's environment by evaluating the business impact, which considers potential consequences of successful attacks, and the technical characteristics, which assess vulnerability to exploits. Organizations can use this knowledge to identify and customize security controls tailored to specific components effectively.

Business Impact Analysis (BIA) and regular risk assessments should be conducted systematically on existing systems before deploying new technologies. These assessments offer valuable insights into identifying critical assets that require priority attention during incident response. Regular risk assessments also support proactively identifying vulnerabilities and implementing remedial actions before they can be exploited.

Before deploying any new technology, assessing and evaluating its potential impact on system availability is crucial. This evaluation is essential to mitigate the risk of disruptions or operational delays.

Understanding the added value of new technologies and their associated security implications allows organizations to explore additional non-technical factors that can enhance overall cybersecurity posture and incident response capabilities. This holistic approach ensures that technological advancements are implemented effectively while safeguarding operational continuity and security resilience.

6.3.6 Policies and procedures

Unified policies and procedures governing both IT and OT cybersecurity are critical. This documentation should include standardized policies, incident response procedures, access control protocols, and compliance requirements.

These policies must account for the unique security needs of OT systems, such as legacy equipment and real-time operations, while integrating with IT's focus on data protection and network security. Establishing clear guidelines and protocols will promote consistency in cybersecurity practices across both domains, reducing the risk of misalignment or conflicting security measures.

"Unified policies and procedures governing both IT and OT cybersecurity are critical."

6.3.7 Supply chain risk management

A holistic approach to supply chain risk management is essential for safeguarding organizational security. To do it properly, organizations need to first understand their risk appetite and determine the minimum cybersecurity exposure tolerated from suppliers.

During the contracting phase, implementing contractual clauses that enforce certain cybersecurity requirements can help ensure compliance from third parties. However, most importantly, centralized monitoring of vendors is crucial to protect the organization from potential breaches and to allow timely reaction. Collaborating closely with OT vendors to gain visibility into the network enhances effective monitoring and enables rapid incident response. These practices collectively strengthen the organization's ability to manage supply chain risks and maintain operational resilience.

6.3.8 Sufficient budget allocation

Adequate funding is crucial for maintaining a strong cybersecurity posture across IT and OT systems. A significant challenge is the discrepancy in budget allocations between these two areas, often leading to underfunded OT security measures. To address this, organizations should carry explicit discussions about the OT cybersecurity budget, considering the unique needs the OT environment.

This budget should cover investments in cybersecurity tools, employee training, and technology upgrades specifically for OT systems, which may have traditionally been overlooked. A balanced approach to budgeting ensures that OT systems receive the same level of protection as IT, addressing vulnerabilities across the entire infrastructure. Additionally, justifying the allocation of budget to OT cybersecurity may require educating leadership on the critical importance of securing operational technology and its impact on business continuity.

6.4 Human capital

Figure 6 - Recommended Approach for Human Capital Challenges

6.4.1 OT Cybersecurity training and awareness programs

Vigilant staff are the first line of defense for any organization in maintaining the safe and reliable operation of OT systems.

Designing effective and tailored awareness and training programs to promote an OT cybersecurity culture and providing the required knowledge and skills to detect and respond to incidents proactively is vital.

Beyond the traditional methods of delivering awareness and training, it is advisable to include simulation-based training of relevant scenarios to ensure a comprehensive understanding of the risks associated with human behaviors and the appropriate defense mechanisms and best practices.

Providing trainings and hands-on experience, such as job rotations, can further enhance employee skills by exposing them to diverse environments and potential threats.

Additionally, creating cross-department teams fosters collaboration and knowledge-sharing, which strengthens the organization's overall ability to identify and mitigate OT cybersecurity risks.

6.4.2 Talent pool expansion

Expanding the talent pool is crucial to meeting the increasing demand for OT cybersecurity professionals.

Organizations should focus on attracting talent from diverse fields such as IT, engineering, and operations, recognizing that a broad skill set is beneficial for addressing the unique challenges of OT security.

By fostering partnerships with educational institutions, offering internships, and promoting career pathways into OT cybersecurity, organizations can cultivate a pipeline of qualified professionals. Additionally, investing in reskilling and upskilling current employees enables organizations to leverage internal talent, ensuring that they can adapt to emerging threats and technologies in the OT landscape. A well-rounded talent pool not only strengthens cybersecurity defenses but also enhances organizational agility and innovation.

6.4.3 Tailored threat cases and response playbooks

Developing tailored threat use cases and response playbooks is critical for aligning cybersecurity strategies with the operational realities of OT environments.

This process involves collaborating with a multidisciplinary team comprising IT and OT security professionals, operators, engineers, and Original Equipment Manufacturer (OEM) vendors. By customizing threat use cases and response playbooks, organizations can streamline incident response procedures, mitigate risks specific to OT systems, and improve overall cybersecurity resilience.

6.4.4 Global cross-industry collaboration

As part of supporting and collaborating within the OT community, it is essential to publish more resources and studies addressing critical topics across various OT sectors.

This effort necessitates ongoing collaboration among OT industry experts, technology providers, and OEM vendors to address current challenges. Establishing standardized, vendor-agnostic documentation can be used as a reference for developing robust security monitoring architectures and incident response capabilities. This collective approach ensures comprehensive support and advancement within the OT cybersecurity landscape.

7. Conclusion

Enhancing OT security monitoring and incident response capabilities requires a holistic approach that integrates strong governance, advanced technologies, and proactive risk management.

Establishing clear governance frameworks is essential for aligning IT and OT teams, enabling cohesive decision-making, and ensuring that cybersecurity policies are adapted to OT's unique requirements. By breaking down silos and fostering collaboration between these traditionally separate domains, a unified defense strategy that is both efficient and resilient can be created.

Leveraging real-time monitoring tools, predictive analytics, and advanced threat detection systems, can mitigate potential vulnerabilities before they are exploited. Continuous monitoring of network traffic and real-time insights into OT assets allow organizations to stay ahead of emerging threats, while network segmentation and access controls further strengthen defenses.

Continuous monitoring of third-party vendors, the isolation of legacy systems, and the development of specialized training programs also help ensure that security gaps are identified early and mitigated effectively. The energy sector must also invest in expanding its cybersecurity talent pool, equipping teams with the skills necessary to navigate the complexities of OT environments.

By integrating these strategies, organizations can future-proof their cybersecurity posture and ensure the uninterrupted, secure operation of critical infrastructure, especially as cyber threats grow in sophistication.

Endnotes

1. Dragos. (2017). TRISIS Malware: Analysis of Safety System Targeted Malware. https://www.dragos.com/wp-content/uploads/TRISIS-01.pdf

2. Fortinent. (2024) Press Release. https://www.fortinet.com/corporate/about-us/newsroom/press-releases/2024/fortinet-enhances-industry-most-comprehensive-ot-security-platform-protect-cyber-physical-systems#:~:text=According%20to%20the%20Fortinet%202024,from%2049%25%20in%202023).

3. Kaspersky. (n.d.). Stuxnet explained: What it is, who created it and how it works. https://www.kaspersky.com/resource-center/definitions/what-is-stuxnet


GLOBAL
CYBERSECURITY
FORUM
aramco