SYGNIA

BUILDING YOUR ICS/OT THREAT DETECTION STRATEGY

TAMIR MARGALIT
DIRECTOR OF ICS/OT SECURITY AT SYGNIA

Table of Contents

Building Your ICS/OT Threat Detection Strategy

Author: Tamir Margalit, Director of OT Security at Sygnia

Establishing visibility and threat detection in Industrial Control System (ICS) and Operational Technology (OT) environments is often challenging and, as a result, frequently deprioritized. At Sygnia, as an incident response and security consulting firm we have witnessed firsthand how many organizations overlook this critical aspect of cybersecurity in their CISO-led programs, despite its importance as a foundational pillar for detecting attacker presence and protecting OT assets. In other cases, we see clients relying on mainstream security solutions that are neither the most efficient nor optimally configured for their specific environment or threat landscape, resulting in inadequate visibility and detection for safeguarding their ICS/OT environments.

Several factors contribute to this oversight. A key challenge is that ICS/OT environments are typically managed separately from IT, often by teams who may lack familiarity with cybersecurity. Meanwhile, SecOps teams may not fully understand the complexities of ICS/OT environments and the control processes. Bridging these two worlds, coupled with strained relationships between security teams and the ICS technical teams, vendor constraints, and the challenges of implementing effective detection mechanisms due to safety and operational concerns, complicates the situation further. Additionally, the need to comply with the Purdue model's segregation and maintain isolation from the internet adds more complexity.

Scope of this guide

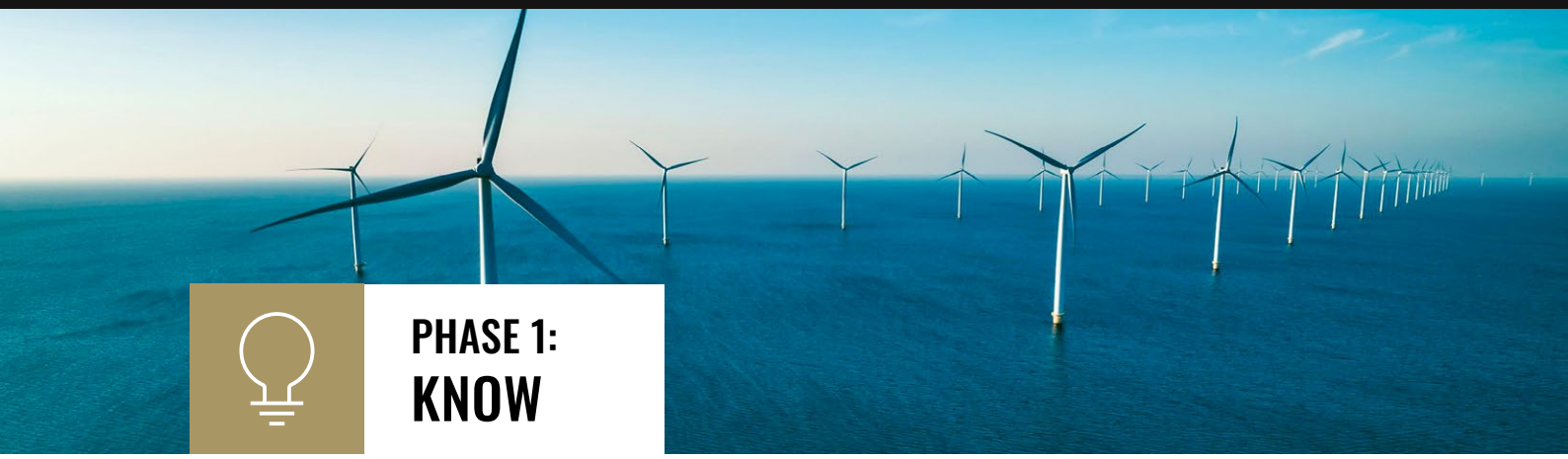
This guide provides key considerations and guidelines for building an effective ICS/OT threat detection strategy. It focuses exclusively on detection, leaving out prevention and response, which merit separate, in-depth discussions. It's important to recognize that the principles discussed here, as well as specific detection strategies, will vary across industrial sectors such as energy, oil and gas, manufacturing, critical infrastructure and others. Even within the same sector, companies may adopt different approaches due to variations in business contexts, technology, operational models, threat landscapes, and organizational maturity. Just as we don't use the same burglar alarms for every protected asset, ICS/OT threat detection solutions must be tailored to the unique needs and risks of each environment.

The Objectives of an ICS/OT Threat Detection Strategy

As in traditional IT environments, the primary objectives of a threat detection strategy for ICS/OT are to provide visibility, alert on abnormal or malicious activity, incorporate relevant threat intelligence, and maintain data sets for triage and forensic investigation by CIRT teams. However, based on Sygnia's extensive experience managing incidents, ICS/OT environments introduce additional challenges due to limited visibility and restrictions on data collection and investigative tool deployment. Furthermore, obtaining real-time intelligence and insight into the status and nature of an attack is critically important but can be challenging. This information can significantly impact organizational effectiveness and decision-making during an incident, particularly when determining whether to halt or continue production.

A key factor is the ability to detect and having an efficient indication whether an attacker has pivoted from a Stage 1 attack (solely within the IT environment), to what's known as a Stage 2 attack (compromising the ICS/OT environment), which is pivotal in incident response. Real-time insight into the attack's progress and understanding the attack objectives is crucial when deciding whether to stop production, which could potentially cost millions or even tens of millions of dollars per day or continue operations if the ICS/OT environment remains uncompromised. The ability to reassure senior management that production can continue safely, even after an IT network breach, is invaluable, especially for a CEO facing the difficult decision of whether to shut down operations, wholly or partially. A CISO capable of providing this level of assurance will be highly valued and appreciated, saving the company significant costs and preventing extensive damage.

Achieving this level of confidence requires a well-architected security strategy, including strong network separation between IT and OT environments. A notable example highlighting the need for real-time, actionable intelligence is the Colonial Pipeline incident. In that case, a Stage 1 attack on the IT network led to an ICS/OT shutdown, despite any confirmed breach of the control environment. This incident underscores the critical importance of creating a detection strategy that addresses this issue and provides timely, accurate intelligence to guide decision-making during a cybersecurity event, helping to avoid significant financial losses and production downtime.



PHASE 1: KNOW

Start by gaining a thorough understanding of your environment by identifying critical assets and assessing potential threats.

Know Your ICS/OT Environment and Crown Jewels

Developing an effective detection strategy begins with a comprehensive understanding of your ICS/OT environment and its critical assets. Start by mapping key components such as network boundaries, external interfaces, architecture, and infrastructure. Next, gain insight into your SCADA/DCS architecture and its implementation, including the communication protocols used for management and operation, and understand the connectivity of your controllers, safety systems, and field devices. Recognizing the entities within your system and their routine communication patterns, which are typically predictable in ICS/OT environments, is crucial.

Additionally, familiarize yourself with the operational model and governance practices that manage this environment, including how your engineering team handles projects, as well as how they manage and operate their environment. This knowledge, combined with a thorough understanding of your network and system architecture, will help you identify potential vulnerabilities and prevent service disruptions.

Learn Your Threat Landscape and Vulnerabilities

Understanding your threat landscape and adversaries relevant to your business is key to enhancing threat detection capabilities in your ICS/OT environment. Start by identifying the most relevant types of threats: Are you exposed to potential risk from nation-state threat actors focused on espionage or disruption, a cybercriminal deploying ransomware, or an insider with intimate knowledge of your systems? Each adversary exhibits distinct behaviors that require tailored detection strategies. For example, detecting a nation-state threat actor in action may involve monitoring for sophisticated stealth activities, and potential zero-day exploits, while ransomware detection focuses on rapid identification of file encryption and privilege escalation. Monitoring insider threats often necessitates closer tracking of access logs and unusual commands.

Next, map out specific vulnerabilities in your ICS/OT systems, such as legacy equipment, insecure protocols, third-party or non-secure remote access, and interfaces between IT and OT networks. Prioritizing detection around these vulnerabilities ensures you can identify and mitigate threats before they disrupt operations.

Lastly, while not all threats can be fully addressed, especially where safety and operational constraints exist, detection should be prioritized to ensure timely alerts and responses to emerging attacks.

Understand Adversary's Tactics

It is essential to develop a solid understanding of attacker tactics, techniques, and procedures (TTPs). Key TTPs include infiltration methods, privilege escalation, lateral movement, and execution, among others. Developing familiarity with attack tactics may help you anticipate attacker behavior, enabling more effective detection efforts. Incorporating TTPs into your security strategy can significantly strengthen both detection and defense and may be more efficient than relying solely on indicators of compromise (IOCs), which are typically tied to specific threat actors and attacks. To do so, use the MITRE ATT&CK® framework for ICS (figure 1), which provides both a comprehensive overview of common attack techniques in industrial control system environments and offers a structured methodology for categorizing threats. Use this framework to map TTPs to your specific environment and assess your current detection capabilities. Based on these assessments, prioritize threat scenarios and actively monitor known attack groups targeting your business sector. Understanding their tactics will help you better counter their strategies and stay one step ahead.

These insights will help you develop a more effective monitoring strategy that aligns with the architecture and operational model of your environment. For instance, if your Historian server is identified as a key bridge between your IT and OT environments, prioritizing monitoring and deploying sensors on that machine becomes essential. Anticipate tactics like privilege escalation, credential dumping (e.g., LSASS injection), and the use of tools like Mimikatz and PowerShell on that server. By focusing your monitoring efforts on critical systems and attacker-favored methods, you'll not only enhance your ability to detect and disrupt malicious activity early but also stay one step ahead of evolving threats.

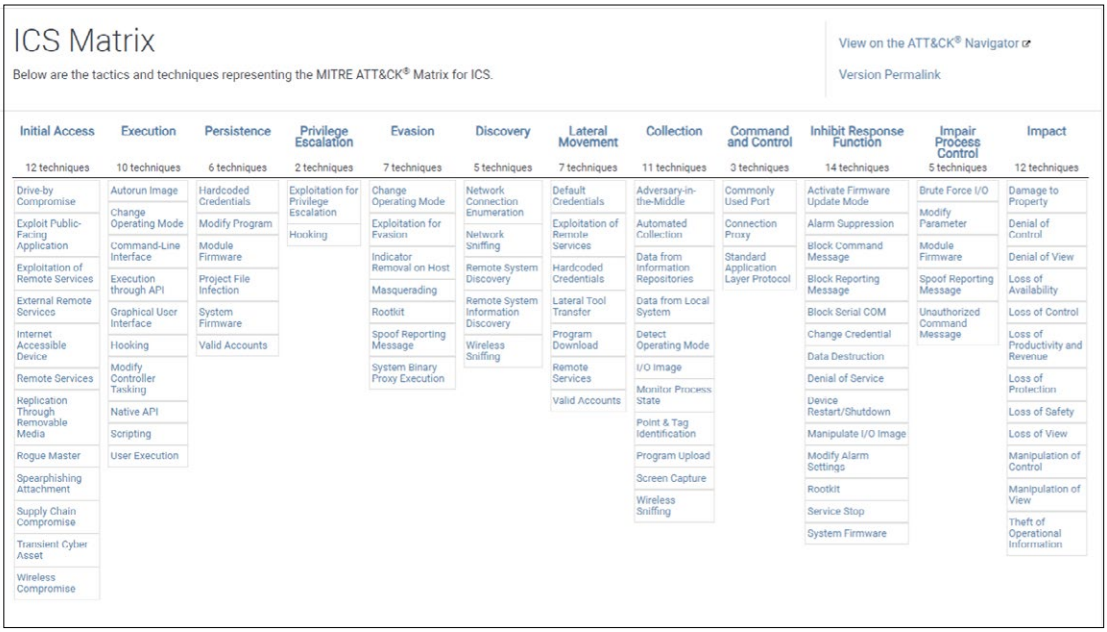


Figure 1: MITRE ATT&CK® Matrix TTPs for ICS/OT Environments

PHASE 2: ASSESS

Assess Your Current Detection Capabilities

Identify areas in your environment where visibility is lacking, and determine where enhanced monitoring is needed, such as external interfaces, inbound/outbound traffic, VPN access, and on lower layers of the Purdue model that support the control processes. Ensure comprehensive monitoring of critical systems like Active Directory, privileged identities, SCADA/DCS servers, privileged workstations, HMIs, Historians, and controllers. Evaluate your detection capabilities against both common cyberattacks and OT-specific advanced persistent threats (APTs) relevant to your industry. For example, in the energy sector, you might simulate scenarios involving threats like CrashOverride and BlackEnergy, while the oil and gas sector could focus on threats such as TRITON/TRISIS. Identify strengths, weaknesses, and blind spots, and assess how quickly you can detect and respond to an attack. Explore opportunities to improve detection and response times.

Assessing your detection capabilities also involves evaluating your team's ability to analyze data in real time and ability to distinguish between malicious activity and false alarms. This requires both well-defined and customized detection systems, as well as a deep familiarity within the CIRT team responsible for your ICS/OT environment. Effective event analysis and a proper triage process are not always straightforward and demand professionalism and prior experience from your team. This assessment is essential for refining your threat detection strategy.

PHASE 3: PLAN

Build Your Collection Management Framework

Once you have a clear understanding of your environment, threat landscape, and attacker TTPs, and have identified areas where visibility needs improvement, you can begin building your **Collection Management Framework (CMF)**. The CMF provides a structured approach for identifying data sources and determining what information can be obtained from each. Think of it as a table listing each data source, the types of data, logs, or alerts that can be collected, the importance of each dataset, and whether it is already being collected, along with its priority. The CMF will help you govern and optimize data collection, ensuring comprehensive visibility while preparing your organization for potential forensic investigations.

A typical ICS/OT CMF may include data from sources such as network traffic, network devices, servers, endpoints, security agents, user access logs, SCADA/DCS systems, applications, databases, Active Directory, virtualization, storage, and backups, as well as control devices and sensors, HMIs, Historians, and even control telemetry and process trends. External threat intelligence should also be included as a critical data source to enhance detection capabilities.

As your organization matures, you may expand data collection to cover business operations and control processes, enabling the detection of abnormal activities by monitoring telemetry and process trends. Figure 2 below illustrates a sample Collection Management Framework (CMF) for an ICS/OT environment.

Data Source	Type of Data	Detection objectives	Importance	Collected	Action Required
Network Traffic	Packet captures, flow data	Detect unauthorized communication, abnormal traffic, suspicious external IPs, OT commands.	Critical	Yes	Regular monitoring, optimize collection.
Endpoints	Event logs, security logs	Detect malware, unauthorized access, abnormal user/application behavior.	High	Partially	Implement full endpoint detection.
Security Agents	Alerts, logs, system state	Detect malicious software, unauthorized file changes, unusual process executions	Critical	Yes	Tune alerts to minimize false positives

Figure 2: An example of a CMF table showcasing a partial list of collection sources

PHASE 4: OPTIMIZE

Refine and enhance monitoring capabilities and improve collaboration across teams to ensure a cohesive approach to security.

Elevate Your Network Monitoring

Network monitoring is one of the primary methods for detecting malicious activity in ICS/OT environments, particularly in safety-driven operations where active or agent-based sensors are unacceptable. It involves collecting data and logs from devices such as firewalls, switches, IDS, proxies, NAC, and others, with the goal of identifying abnormal or suspicious network traffic, whether internal, inbound, or outbound. In addition to gathering logs from common network devices, using out-of-band passive sensors is another effective approach to monitor networks without disrupting operations. Network Security Monitoring (NSM) solutions like Claroty, Nozomi, Dragos, Microsoft Defender for IOT, and others are widely available. While each solution offers unique benefits, they share core capabilities such as baseline triggering, machine learning for anomaly detection, signature-based detection, and customizable rules tailored to your environment. However, these solutions can be expensive and may not always deliver a good return on investment if not properly configured. There is no one-size-fits-all approach to implementation; the effectiveness of network monitoring depends on your specific business context and network architecture, so what works for one organization may not work for another.

One consideration when evaluating a network monitoring solution is how it should be deployed across the infrastructure. In segregated and complex environments, fully covering the entire network may require numerous sensors, significantly increasing both cost and complexity. Given these constraints, it's often impractical to monitor all network traffic, leading to a critical decision for the CISO: whether to prioritize East-West traffic monitoring, which refers to internal traffic within the lower layers of the Purdue model, or North-South traffic monitoring, which involves external-to-internal communication (across the OT network boundaries).

The right choice depends not only on the network architecture but also on the specific threat landscape. For instance, if the primary concern is cybercrime or ransomware, focusing on North-South traffic may be more effective. On the other hand, if your reference threat actor is expected to target field devices, controllers, or HMIs to disrupt communication protocols, prioritizing East-West traffic monitoring might be the better approach. Ultimately, the decision should be tailored to the specific use case and threat profile of your organization.

Enhance Endpoint Detection

While most of the clients we work with have managed antivirus systems installed across all endpoints and servers as standard practice, endpoint detection involves multiple layers. These layers start with monitoring Windows event logs and registry keys and progress through the deployment of security agents such as device control, application control, antivirus, and, at the higher end, Endpoint Detection and Response (EDR), which is less common in ICS environments. The deployment of these layers should be tailored to the environment and the endpoint's role and location within the control network. For example, antivirus may be more effective than EDR in certain situations. Consider an HMI (Human-Machine Interface) used by an operator, where one of the primary concerns is malware introduction via a USB stick. In this case, antivirus and device control may offer more effective protection than EDR. In contrast, EDR is better suited for detecting suspicious activities such as privilege escalation or lateral movement, which are more relevant for systems like Historians, which are often targeted by attackers as entry points to the ICS environment.

In more mature environments, we often see the use of data and logs collectors which collect data and event logs from endpoints, sending them to a log aggregator, and subsequently to the global SIEM. These collectors are often also leveraged to gather asset vulnerability data, which is crucial for visibility and compliance efforts, especially since active vulnerability scanning is typically prohibited in safety-driven operational networks.

Collecting Windows event logs, particularly security logs, is a best practice and is essential for forensic investigations. However, log collection should be customized based on the specific environment and threat landscape. For example, if an Engineering Workstation (EWS) is remotely operated using RDP, it is important to monitor remote user access, tracking who is accessing the machine, which user is involved, from where, and at what time. Similarly, if a vendor requires the use of a local admin account for managing the SCADA system or uses it as a service account, this account should be closely monitored for suspicious activity, such as remote access, interactive logons, or repeated login failures.

Other detection methods and capabilities, such as Data Loss Prevention (DLP) and application control, should be considered based on specific circumstances. For instance, in manufacturer R&D environments that store confidential data, DLP monitoring should be considered. On the other hand, legacy servers that cannot be fully hardened may need to rely solely on application control mechanisms to ensure adequate detection and protection.

Breaking Misconceptions Around EDR Adoption

Although the use of Endpoint Detection and Response (EDR) is often prohibited and considered taboo in ICS/OT environments, deploying EDR solutions can be an effective detection and prevention measure in certain cases, especially for protecting IT-OT convergence. In such instances, EDR can serve as a critical sensor for detecting when an attacker has progressed to a

Stage 2 attack after compromising the corporate network, providing vital indicators to inform the decision whether to halt or continue production. In general, deploying EDR in the upper layers of the Purdue model, particularly in layer 3.5 (PDMZ or IDMZ), can be a reasonable and efficient approach. This is especially true for endpoint servers that are not directly involved in control processes but remain highly vulnerable to attack. However, EDR deployment should be approached cautiously and assessed carefully on a case-by-case basis to avoid unintended operational or safety risks.

If you decide to deploy EDR in the upper layers of your network, it is essential to ensure it remains separate from the corporate EDR solution. It should not be managed using corporate credentials, corporate user accounts, or by the corporate SIEM. The SIEM should be limited to a view-only API key to access your EDRs.

Optimize Identity Monitoring

Identity protection and monitoring are critical aspects of securing your environment, as attackers will likely exploit them to escalate privileges. Gaining domain admin access in your OT domain is often one of the first steps in an attack. Based on our experience, identity protection and monitoring are among the most effective measures for detecting attackers tampering with your systems.

Identity Threat Detection and Response (ITDR) solutions such as Microsoft Defender for Identity (MDI) or CrowdStrike Falcon Identity Protection can be highly effective, but they are often complex to deploy due to requirements such as internet access and remote management, which are not common for ICS/OT environments. If these solutions are not feasible in your specific environment, consider enhancing your Active Directory event collection to monitor key events related to common TTPs used by attackers to escalate privileges. These include activities such as DCsync, Kerberoasting, Pass-the-Hash, Pass-the-Ticket, Golden Ticket attacks, and adding new users to the Administrators or Domain Admins groups. Sending these events to the SIEM can efficiently help detect attack activity in its early stages.

Elevate Infrastructure Monitoring

Infrastructure monitoring encompasses any infrastructure hosted within your environment, starting with Tier-0 devices (critical, foundational components in your network) such as Active Directory, virtualization platforms, storage, and backup systems, as well as jump servers, application servers, databases, and more. As mentioned earlier, monitoring should be tailored to the specific environment and threat landscape.

Since Tier-0 devices, such as Active Directory, virtualization, storage, and backup systems, are prime targets, particularly in ransomware attacks, it's crucial to have efficient monitoring and event collection that aligns with your protection strategy. For example, if your security strategy restricts access to these assets solely through CyberArk PSM by specific users, any attempt to access them from another source or by an unauthorized user should trigger alerts. Similarly, multiple failed login attempts on backup systems or ESXi hosts should be monitored closely.

Jump servers, which play a critical role in managing and operating ICS/OT environments are often an easy target for attackers seeking to infiltrate the ICS/OT environment. This Achilles' heel is frequently exposed during our adversary simulation exercises, where red teams, after gaining full access to the corporate network, exploit password reuse, unfortunately a common practice among engineers, across environments. By using these reused corporate credentials, and in the absence of MFA, attackers can successfully log into the OT domain and the jump server.

Once attackers (or red teams) reach the jump server, they discover a treasure trove, where almost everything is within their grasp. This is especially true if the jump server isn't properly hardened. Credential dumping and reconnaissance of privileged user folders often reveal a slew of sensitive information, allowing the attacker to 'become king of the kingdom.' From that point, they can leverage built-in tools, effectively 'living off the land,' to further exploit the OT environment.

There are many lessons learned regarding this vulnerability, particularly from a protection perspective, such as implementing MFA, migrating to a PAM solution, and more. The key takeaway is that any jump server should be closely monitored, not only at the operating system level but also for suspicious behavior, anomaly detection, and any local or remote access and session management.

Other types of infrastructure that may exist within your network, especially those that pose higher risks, such as industrial Wi-Fi, LTE/5G modems, private/public APNs, and RF communication systems using backhauls to the backbone network, should be closely monitored to prevent unauthorized access or manipulation.

Lastly, for effective infrastructure monitoring, it's best to adopt common IT best practices and tailor them to your specific environment to ensure comprehensive protection.

Monitor Your ICS Process

Monitoring the Industrial Control System process requires deep expertise in ICS operations and close collaboration with ICS engineers and automation specialists. This process involves collecting and analyzing logs, events, and alarms from the ICS process itself, while also identifying anomalous behavior within the ICS system and its subsystems. Data is typically sourced from various components, including Human-Machine Interfaces (HMIs), SCADA/DCS servers, controllers, and Historian data such as trends, telemetry, and setpoints, with other data sources potentially relevant depending on the specific system and its use cases.

Such anomalous behavior, if detected, may be the result of an operational or technical problem, such as a pump or motor failure or malfunction. When properly implemented, monitoring the ICS process could significantly contribute to other operational and maintenance processes on the manufacturing floor, particularly to Predictive Maintenance.

Effective monitoring begins by utilizing the logging and alerting capabilities provided by ICS vendors' hardware and software. Next, the process establishes baselines and detects abnormalities by continuously tracking setpoints, thresholds, ICS commands, and operational trends. Detecting deviations from expected values or behaviors can serve as early indicators of potential issues or threats within the ICS/OT environment.

Key areas to monitor include changes in controller program logic, suspicious activities such as unauthorized logic modifications, unexpected logic uploads or downloads, unplanned controller resets or hard stops, and anomalies in historian data trends.

From a cost-effectiveness perspective, implementing monitoring for the ICS process is likely one of the "last miles" in your detection strategy. This is because ICS monitoring often serves as the last line of defense, so if alarms are triggered at this stage, it typically means the system has already been compromised, and the attacker has begun tampering with your control processes. So, is it worth focusing on this layer of detection? The answer depends on your industry and threat landscape. For example, for manufacturers of low-risk consumer products, such as consumer goods, a full-scale ICS process monitoring solution might be excessive. In such cases, it may be more cost-effective to focus on "quick wins" - monitoring measures that are easy to implement but offer significant protection, such as tracking controller state and logic integrity.

However, for critical infrastructure such as electrical power plants, which face risks from sophisticated adversaries like nation-state actors, this detection layer is essential. In these cases, Advanced Persistent Threats (APTs) may conduct reconnaissance on your ICS environment and launch attacks targeting the control processes. For such scenarios, implementing this detection layer is highly recommended.

Looking ahead, the future of ICS monitoring will likely see increased use of AI and Machine Learning (ML) capabilities. These technologies can enhance anomaly detection by identifying patterns and behaviors that might be missed by traditional monitoring systems. ML algorithms can learn the normal operational behaviors of ICS systems over time, making it easier to spot subtle deviations that could indicate early stages of an attack or malfunction. Additionally, AI-driven analytics can help streamline and prioritize alerts, reducing noise and ensuring faster response times. As these technologies continue to mature, they are expected to play a key role in enhancing the monitoring of ICS processes.

Leverage ICS Cyber Threat Intelligence

While cyber threat intelligence (CTI) is increasingly common in IT environments and considered essential for gaining visibility into potential threats, many organizations lack sufficient ICS-specific CTI. Even companies that subscribe to CTI services often fail to apply these insights to their ICS/OT environments. The lack of communication and familiarity with the ICS/OT ecosystem is a key reason for this gap.

Leveraging ICS-specific CTI, whether from national authorities like CISA or from free and paid sources, can provide valuable alerts on emerging threat actors targeting your sector or region, as well as new tactics, techniques, and procedures (TTPs) and advanced tools used by attackers. CTI is also critical for staying informed about vulnerabilities that could specifically affect your ICS/OT environment. Identifying publicly exposed vulnerabilities, potential threats, attacker intentions, artifacts or data leaks related to your assets, as well as cyber events or vulnerabilities affecting your supply chain, vendors, or the hardware and software stack you use, is vital for early warnings of an impending attack or attack planning.

Integrating ICS-specific CTI into your ICS/OT security strategy, alongside improving communication between the ICS/OT ecosystem and the broader CTI community, is essential for staying ahead of potential attacks and ensuring your organization is prepared to respond to emerging risks.

Enhance Collaboration Among Teams

Effective ICS/OT threat detection requires strong collaboration between IT, OT, and the security teams, which often operate in silos with different priorities. Breaking down these barriers is crucial to fostering an integrated approach to security. By developing a structured framework for collaboration, organizations can ensure that both engineering and security teams are aligned in their efforts to protect the ICS/OT infrastructure.

While there is no one-size-fits-all solution, establishing a joint governance model is a good starting point. In this model, representatives from IT, OT, security team and SOC collaborate to develop unified security policies and procedures. A cross-functional leadership team can ensure that initiatives are prioritized, resources are allocated effectively, and communication flows smoothly between teams. Equally important is creating a shared responsibility matrix that defines specific roles during security incidents, ensuring everyone knows their part in incident response and vulnerability management.

Regular joint workshops and cross-training sessions are essential for promoting knowledge sharing and building trust. IT teams can teach network security principles to OT personnel, while OT teams can share the operational realities of industrial systems. Incident response drills that simulate real-world ICS/OT attacks will help both teams practice working together, improving their coordination and response times during an actual threat.

In addition, implementing shared key performance indicators (KPIs) that measure both operational uptime and security performance can help align team objectives. Examples of KPIs could include the number of security incidents resolved or the speed of incident response. These metrics ensure that both IT and OT teams are equally invested in the organization's security outcomes.

Finally, fostering a culture of collaboration and trust is critical. Regular communication, whether through joint meetings, shared collaboration tools, or dedicated check-ins, keeps teams aligned on emerging threats and ongoing initiatives. Recognizing and celebrating cross-team successes also helps reinforce a cooperative mindset, ensuring that IT and OT teams see each other as partners in safeguarding the organization. By building this culture of collaboration, organizations can significantly enhance their threat detection capabilities and create a more resilient security posture across both IT and OT environments.

CONCLUSION

In today's rapidly evolving cyber landscape, establishing robust visibility and threat detection within ICS/OT environments is not just an option, it's a necessity. However, this can be challenging, and as we've seen with many industrial organizations, is often deprioritized. The complexities of ICS/OT environments, combined with the need to balance safety and reliability/operational requirements, make building an effective threat detection strategy a significant undertaking. But as the examples in this guide illustrate, the consequences of overlooking this critical aspect of security can be severe, potentially leading to significant financial losses, operational disruptions, and even risk to human life.

To build an effective ICS/OT threat detection strategy, start by gaining deep visibility into your organization's environments. This includes understanding key assets, identifying vulnerabilities, and monitoring network traffic and processes to detect potential threats. It's crucial to adopt a tailored approach, one that aligns with the unique architecture, operational model, and threat landscape of your organization. Whether it involves leveraging baseline behavior analysis, establishing comprehensive monitoring systems, or integrating advanced tools like EDR or identity protection solutions will vary from organization to organization, a one-size-fits-all approach simply won't work for ICS/OT security.

Fostering collaboration between IT and OT Security teams is essential to bridging the gap in communication and expertise. This partnership, along with ongoing use of threat intelligence, will help ensure that both sides of the organization are prepared to handle the distinct challenges of protecting critical ICS/OT infrastructure.

Finally, as seen in incidents like Colonial Pipeline, real-time intelligence during a cyberattack is crucial. The ability to detect when an attacker has moved from the IT network to the OT environment, and understanding the implications of such a move, can inform decisions that have far-reaching operational and financial consequences. Having a well-architected detection strategy in place will give your team the insight and confidence needed to make informed, timely decisions when it matters most.

In conclusion, developing a strong ICS/OT threat detection strategy is not just about selecting the right tools, it's about understanding your environment, tailoring your approach to its specific needs, and fostering collaboration across teams to ensure the organization is prepared to respond to any threat. By building these foundations, you'll be better positioned to detect, mitigate, and respond to attacks, ensuring the safety and continuity of your critical operations.

Whether you are seeking to create a new ICS/OT threat detection strategy or assess and optimize your existing strategy, Sygnia can help. With our industrial dome framework of IT/OT cyber security services, Sygnia provides services including cyber incident response, posture assessment, adversarial testing to evaluate the effectiveness of your security and managed detection and response.
To learn more, visit https://www.sygnia.co/solutions/ot-security/

SYGNIA

DISCLAIMER

For full disclosure, Sygnia is collaborating with NVIDIA in a joint research and development effort to develop a novel approach for detection and response at the edge of ICS/OT networks. The MDR technology under development should facilitate hardware-based host-level detection in the upper layers of the OT network (levels 2-3.5), using a combination of hardware, software and AI technologies from NVIDIA and Sygnia, to allow performing sophisticated detection and response operations while adhering to Purdue-based network separation principles. Such technology-based solutions, once available, will have implications on several concepts outlined in this paper, specifically those in the Optimize section, allowing further enhancements in elevating network monitoring, enhancing endpoint detection and elevating infrastructure monitoring.