Booz | Allen | Hamilton®

ESTABLISHING AN ICS/OT THREAT DETECTION AND RESPONSE PROGRAM

CONSULTING | ANALYTICS | DIGITAL TRANSFORMATION | ENGINEERING | CYBER

INTRODUCTION

As industries move to leaner staffing models and more automated processes, the availability of rich data from plants has enticed many organizations to connect these previously air-gapped systems to the enterprise and beyond. While greater interconnectivity has brought benefits in terms of business and operations, it has also elevated concerns about cyber threats. Since Stuxnet, the first well-known attack using a cyber weapon against an industrial control system (ICS)/operational technology (OT), there have been several high-profile incidents (e.g., Petya/NotPetya) that caused unprecedented consequences. Organizations across critical infrastructure sectors have attempted to address these growing threats by investing in their cyber defense strategies. Since ICS/OT environments are designed to maintain the highest safety, uptime, and productivity, a tailored approach to deploying cyber defense strategies for ICS/OT is required to properly protect these environments without causing disruptions.

As part of these cyber defense strategies, many organizations are moving beyond prevention measures and investing in a variety of tools and managed response services to enable a proactive approach to cyber defense in their environment. Whether insourcing or outsourcing the response capability, the reality is that there is no "magic box" or single tool that can provide the level of visibility needed to detect threats. Therefore, a comprehensive threat detection program needs to be established. While building this program is not without its challenges, there is an increasing need to advance detection capabilities to reduce the time to detection.

Since ICS/OT environments are designed to maintain the highest safety, uptime, and productivity, a tailored approach to deploying cyber defense strategies for ICS/OT is required to properly protect these environments without causing disruptions.

ICS THREAT DETECTION CHALLENGES

With the rise of cyber attacks causing business disruptions, IT security has been asked to expand their oversight and help bridge the visibility gap between enterprise and ICS/OT environments. While the general objective is to secure the organization as a whole, the approach to secure each environment must vary due to each mission. ICS/OT environments consist of a blend of traditional IT and uniquely OT equipment. While IT has the tendency to change quickly with technology refresh rates roughly every 3-5 years, the same is not seen in the OT space. The aphorism "if it ain't broke, don't fix it" is more commonly applied as the expenses to refresh technology reach well beyond the hardware. Automation processes rely heavily on software programs that have been developed, tested, tuned, and sometimes even validated by an external governing body to run operations with extreme precision and reliability.

The software licenses and engineering labor needed to get the process to this perfected state greatly overshadows the expense of the hardware. Even modifying the existing equipment to incorporate new tools or software causes hesitation as vendors often do not recommend it. Since they are not certain how it may impact operations, often they will make the organization liable for any unintended consequences caused by the modifications. Therefore, the cost of changing out workstations or servers to run on the latest and greatest is only the tip of the iceberg and often not worth the expense.

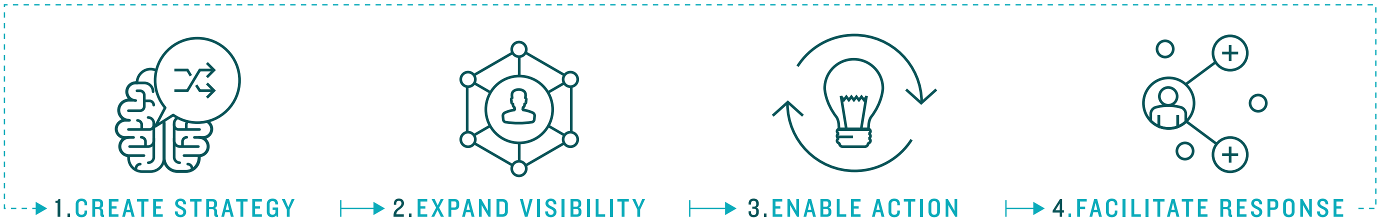
Due to this aversion to technology refreshes on existing production lines, equipment running plants often includes a substantial percentage of unsupported or no longer manufactured devices. Furthermore, the OT-specific equipment required to run the process without a millisecond delay was built to primarily provide real-time communication. Therefore, any delays that happen due to authentication or other methods of security have largely been non-existent until recent years. Taking into account the increasing interconnectivity and hesitation to change, threat detection is critical to sustaining operations and detecting potential disruptive risks.

Over the past several years, many new security tools have been brought to market that aim to be the solution to threat detection within ICS/OT. Detection technology is a foundational requirement—but without the proper processes and people in place, the benefits of added visibility will not be realized. A well-balanced ICS/OT threat detection and response program requires a suite of data sources to be collected at various levels in the ICS/OT environment, appropriate enrichment data to centralize and correlate events and identify the highest priority alerts, and skilled staff with ICS/OT knowledge to respond appropriately.

CHALLENGES IN ICS THREAT DETECTION

- Legacy equipment and vendor restriction limit endpoint tool coverage
- Sensitivity in ICS environments requires many tools to be passive
- No one tool/sensor can provide visibility into all threats
- Limited cybersecurity skills in operations and manufacturing knowledge in the SOC
- Threats are continuously changing and adversaries are advancing techniques

OUR APPROACH



1.CREATE STRATEGY → 2.EXPAND VISIBILITY → 3.ENABLE ACTION → 4.FACILITATE RESPONSE

Building a sustainable ICS/OT threat detection and response program is no small endeavor; however, maturing from a reactive to a proactive response has many long-term benefits. Our approach reflects the best practices we've gained through our experience helping global enterprises stand up and manage ICS/OT threat detection and response programs. The goal of these programs is primarily to reduce cyber risk to the organization by detecting a potential cyber attack early and mitigating it before it impacts operations.

It takes commitment from the organization to establish an ICS/OT threat detection and response program with all its necessary parts, such as adequate staffing for security operations, review of existing data for integration, investment in security tools, refinement of existing processes, creation of appropriate use cases, and development of response playbooks. While each organization may choose a different path for their ICS/OT threat detection and response program journey, several objectives should be met to reduce cyber risk.

1.CREATE STRATEGY

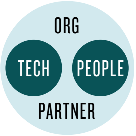
The first step in any new venture is planning. A high-level strategy should be established before any people, process, or technology changes take place. While it might be more enticing to get started as soon as possible in order to see results sooner, acting without a strategy can result in extra time doing re-work and poor decision making due to lack of information. A well-thought-out strategy contains an initial list of targeted use cases, a rollout strategy containing a proof-of-concept phase, skill sets needed to perform the work, staff required to facilitate the work at the site, and a basic timeline. Examples of use cases include receiving an alert when a USB drive is plugged into specific critical servers or when a certain controller begins sending a greater-than-usual volume of traffic. As part of this planning, the organization should start identifying if they will require additional support and visibility through a managed detection and response (MDR) capability. There are several ways an organization can leverage an MDR; however, the optimal solution balances the organization's need for scale and control while enhancing the cybersecurity investments implented as part of the overall OT threat detection program. The graphic below shows three MDR models that organizations can leverage to respond to events within their environment:

IN-SOURCE MODEL

MODEL STRUCTURE:
- Procure own tooling and resources
- Leverage partners for advisory services only

ORGANIZATION'S ROLE:
- Oversee and manage all operations
- Monitor/govern own performance

BENEFITS TO ORGANIZATION:
- Full control and visibility over operations
- Full visibility into all operations

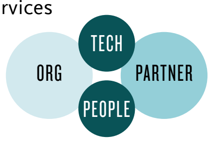


HYBRID MODEL

MODEL STRUCTURE:
- Complete or partial managed services
- Leverage partner's or organization's technology and people
- Leverage partner to manage or direct vendor

ORGANIZATION'S ROLE:
- Shape and implement strategy
- Monitor/govern all parties' performance

BENEFITS TO ORGANIZATION:
- Maximize ROI on previous investments
- Ad hoc usage of critical services

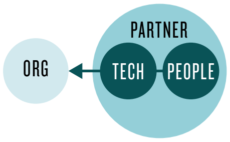


OUTSOURCE MODEL

MODEL STRUCTURE:
- Complete managed services
- Leverage partner's technology and people
- Consumption options based on deliverables and service mix

ORGANIZATION'S ROLE:
- Provide strategic guidance
- Monitor/govern partner performance

BENEFITS TO ORGANIZATION:
- Cost-effective access to expertise/tooling
- Flexibility to scale based on need



Communicating the strategy to staff and executive leadership to gain internal support sets the stage for a successful program. However, be cautious about over-planning and not acting until everything is fully defined. Unknowns are expected with any new project, and as time progresses, new information could be uncovered that helps to better shape the strategy.

A well balanced ICS/OT threat detection program requires a suite of data sources to be collected at various levels in the ICS/OT environment, appropriate enrichment data to correlate events and identify highest priority alerts, and skilled staff with ICS/OT knowledge to respond appropriately.

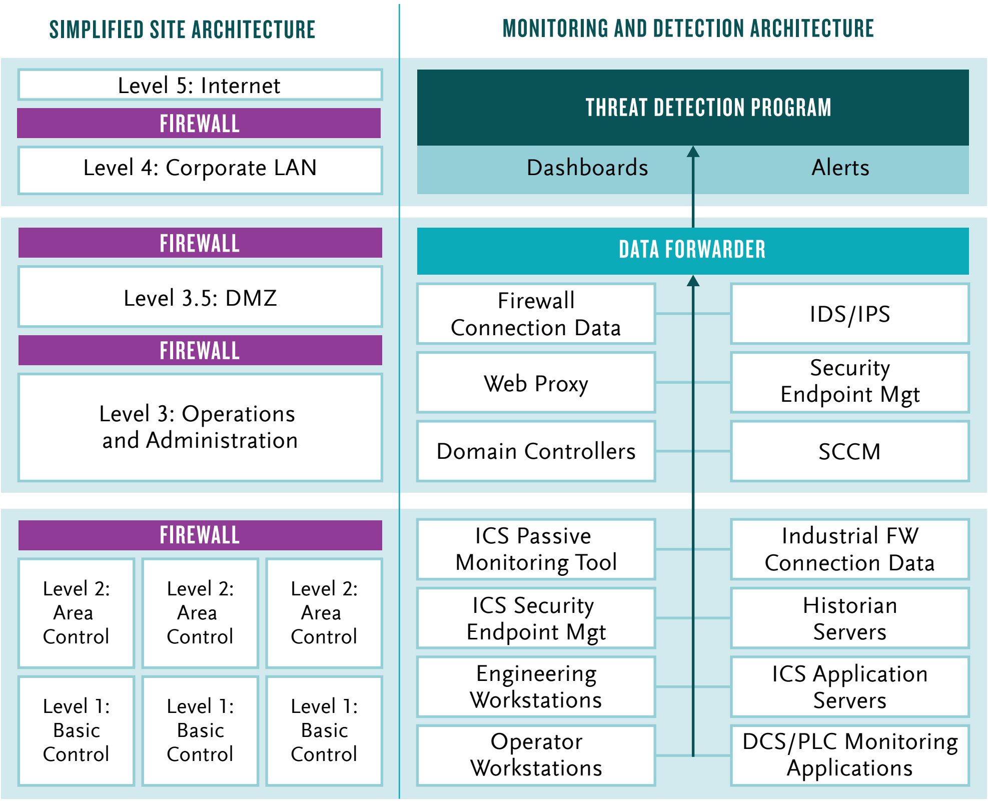
2.EXPAND VISIBILITY

ICS/OT environments have stringent uptime requirements. Security operation activities, such as implementing and configuring security tools and logging, have been a challenge for many organizations as they are perceived as a potential disruption to operations. However, visibility is at the foundation of an ICS/OT threat detection and response program—that's because organizations can't protect assets without knowing what exists in their environment.

Existing Sources

Before any new technology is put in place, organizations need to evaluate what data is currently available and how it aligns with their use cases. An ICS/OT environment, like a traditional IT environment, contains numerous data sources that can be tapped to provide visibility if configured properly. While the technology seen in an ICS/OT environment includes fewer common devices like controllers and actuators, it quite often still runs largely on an ethernet backbone utilizing switches, firewalls, servers, and workstations. These sources can be configured to capture logs to be sent to a central repository for analysis.

Additionally, ICS/OT environments contain millions of data points to run their operations. Software that already has access to that data, such as Open Platform Communications (OPC) servers and historians, can be configured to maximize the data it sees, log it, and pass it up to the same central repository. Correlating both sets of data in a single location allows an organization to chain together suspicious events.

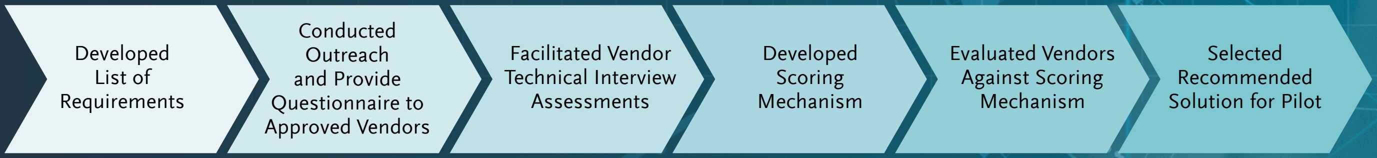


New Sources

When there is a lack of visibility into the network, an organization won't be able to effectively detect potential cyber threats and mitigate cyber risks in their ICS/OT environment. Therefore, new tools should be considered to provide the gaps in visibility not provided by existing sources. When considering new security tools for an ICS/OT environment, passive is preferred because no extra traffic is added to the network and OT devices will not have their resources taxed by additional data requests. While the tools under consideration may have active responses available, these features should be turned off and set to only record events. Over time, certain active features may be able to be turned on, but only after a long period of analysis of the passive data to ensure the organization comprehends the potential impact.

The biggest takeaway here is there is no single tool that provides visibility for ICS/OT environments. Organizations don't rely on an individual software product (e.g., antivirus) as their entire strategy for protection, but rather a suite of tools and tactics. Every piece of software on the market has strengths and weaknesses, and each is only as good as it is set up to be. Most will agree that firewalls are a great tool to deploy, but if they are not installed in appropriate network locations or not properly configured to block traffic, then they are just expensive routers providing little to no protection.

As there are many passive OT asset management software options available in the market, selecting and adding the right tool to the arsenal can be a challenging task. Therefore, a well-planned vendor assessment and selection process must be followed. The technology selection process should start by developing a list of requirements, which are then broken down into two categories: features that you would like to have (wants) and features that are considered a necessity (must-haves). Those requirements should then be ranked based on priorities in terms of mission-criticality, desirability, and "nice to have." At a high level, the selection process can be broken down into six steps as shown:



Developed List of Requirements

Conducted Outreach and Provide Questionnaire to Approved Vendors

Facilitated Vendor Technical Interview Assessments

Developed Scoring Mechanism

Evaluated Vendors Against Scoring Mechanism

Selected Recommended Solution for Pilot

Vendors should be selected based on the client's needs, their industry experience, reputation, and past interactions with the tools in various capability areas. A technical demonstration of their product can help validate the vendor claims and the list of requirements. It is recommended to pilot a few products and assess each vendor on the features offered, derive an overarching score based on vendor responses to the requirements questionnaire, and then determine the scalability of their product. A well-designed weighting system can help with ranking the products under assessment.

Once a tool has been identified through the selection process for meeting the client's need, communicating this information to the operational team is key. Whether the operations staff will be direct users of the tool or not, they need to understand the benefits that will be provided by it and how it may/may not impact operations. This education will help to get their buy-in and assistance with the installation, but more importantly, it will increase the likelihood of ownership and usage of the tool to help secure their environment. These communications should be ongoing to build relationships with staff that can assist with troubleshooting and responding to suspicious events.

3.ENABLE ACTION

The most important function of any security program is the ability to continuously detect and respond to potential threats in their early stages. For threat detection to be effective and efficient, alerts from security tools and system logs need to be forwarded and stored in a centralized repository. Aggregating data from the various data sources will help correlate and contextualize it into actionable tasks. Many tools can be “noisy” by alerting every little change, and not all system logs are relevant, so selecting the appropriate pieces of data needed to accurately support the development of use cases or alerts is critical. This is where the mindset shift from reactive to proactive security needs to take place.

Use case or alert development should be a coordinated activity between staff from site automation, IT, and the Security Operations Center (SOC). Site staff should weigh in on use cases regarding what needs to be monitored and common indicators of abnormality. IT staff can then determine the feasibility of existing data sources for the use case, while SOC staff develop relevant detection logic and queries correlating available data sources. Without this collaboration, irrelevant alerts may occur and cause frustration, leading their audience to ignore them and not take appropriate action to mitigate potential threats.

While some security professionals may be dedicated to incident response, the volume of alerts and competing activities minimize the time available to respond. Furthermore, the staff needed to assist in the incident investigation and containment have their own set of daily tasks that aren’t focused on security. Therefore, alerts need to be properly prioritized by the importance of the asset in relation to operations in order to ensure alerts on more critical devices are elevated. To enable this prioritization, a unified effort must be made to identify and characterize the devices supporting operations. This information can then be sent to the centralized repository as another data source.

4. FACILITATE RESPONSE

Cyber attacks in ICS/OT environments have become more sophisticated as attackers realize the potential impact they can have on operations and the business' bottom line. A solid orchestrated response process stemming from an alert or other discovery will enable an organization to mitigate an incident effectively, determine the attack vector, and refine detection methods. For a collaborative response to be effective, there needs to be ongoing integration between the staff involved and pre-determined response workflows or playbooks to minimize the time needed to determine what action to take or who to call. Delays in response because of poor collaboration can result in greater business impacts and increased remediation costs.

Prior to any alert becoming active, target audiences should be determined based on job roles and a response process should be established. An alert on a Programmable Logic Controller (PLC) behavior deviation should be distributed to appropriate ICS/OT automation staff with a follow-up workflow action to let the SOC know whether the alert warrants additional investigation. If alert delivery was in the reverse order, it may not receive proper or timely attention from the lack of context. Automation staff are intimately familiar with their systems and processes, so empowering them with the first line of response for alerts requiring site-specific knowledge, with follow-up to the SOC, distributes response activities so that action can take place quicker. Establishing such workflows will help an organization focus on the response instead of on the bureaucracy.

For some, bureaucracy, budget, and staff contraints may limit the organization's ability to effectively respond to events within the ICS/OT environment. An effective alternative is to employ an MDR service that understands the unique requirements to responding to events within the ICS/OT environment. This brings several immediate advantages such as cybersecurity expertise, 24/7 coverage, threat intelligence, added visibility at the IT/OT layer, and usable information in the form of reports, assessments, and mitigation steps.

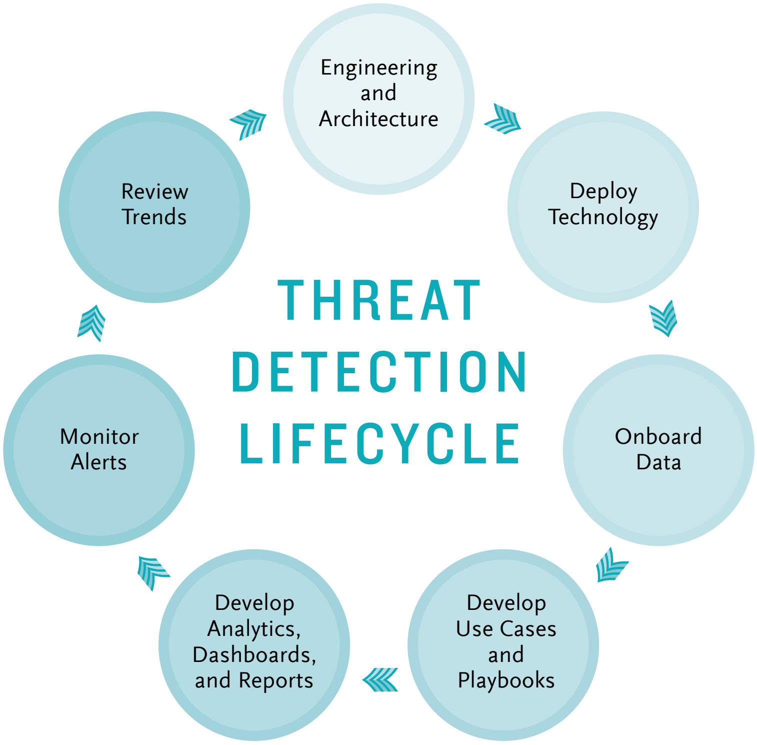
While traditional MDR services focus on reduction of mean-time-to-detect and respond, an MDR for an ICS/OT environment should balance response and remediation plans with ensuring that the manufacturing and critical infrastructure processes continue running with minimal downtime. In addition, any MDR solution should continue to coordinate with staff from site automation, IT, and the SOC to enable remediation within the environment. By establishing a hybrid analyst that has an understanding of both the cybersecurity response processes and the ICS/OT environment constraints, these individuals can help facilitate remediation plans and enable the response to events more efficiently.

REDUCING CYBER RISK

The journey to secure ICS/OT systems is neverending, and as threats evolve, so do the defensive techniques. As new technology is introduced, there is a constant need to iterate on the threat detection and response capability. This could include the tuning of analytics, the development of new use cases, or even the introduction of new technology solutions. Successful programs follow a lifecycle process to ensure the program continues to evolve along with the threats.

This threat detection lifecycle starts with the engineering and architecting of solutions being implemented to provide visibility into OT. Once a design has been completed, the technology can be deployed and the data from these tools can be onboarded into the centralized environment. The generated events can then be used to develop use cases for analytic development and playbooks to respond to events. Once developed, the alerts, dashboards, or reports will need to be monitored, analyzed, and cataloged to provide trending data. This process helps tune analytics, develop new use cases, or identify potential solutions that can further mitigate threats. These new solutions need to be architected and engineered, restarting the lifecycle.

In an industry where leaders live and die by the efficiency of their operational environment and supply chains, there is hyper-focus on productivity.
While shifting the prevailing mindset to understand the value/importance of an ICS/OT threat detection and response program will take time and come with a unique set of challenges, it's critical to ensuring continued efficiency within the environment.


Engineering and Architecture
Deploy Technology
Onboard Data
Develop Use Cases and Playbooks
Develop Analytics, Dashboards, and Reports
Monitor Alerts
Review Trends
THREAT DETECTION LIFECYCLE

About Booz Allen

For more than 100 years, business, government, and military leaders have turned to Booz Allen Hamilton to solve their most complex problems. They trust us to bring together the right minds: those who devote themselves to the challenge at hand, who speak with relentless candor, and who act with courage and character. They expect original solutions where there are no roadmaps. They rely on us because they know that—together—we will find the answers and change the world.
To learn more, visit BoozAllen.com.

For more information,
please contact:

Kyle Miller

miller_kyle@bah.com

Hien Nguyen

nguyen_hien@bah.com

Pia Capra

capra_pia@bah.com

ICS_Security@bah.com