SANS

Analyst Program

Survey

Breaking IT/OT Silos With ICS/OT Visibility

Written by Jason Christopher

June 2023

TREND MICRO

Executive Summary

As the threat landscape continues to grow across industrial sectors, it is more important than ever that these organizations understand their networks and gain visibility across critical systems. In light of recent developments, including the discovery of the PIPEDREAM modular industrial control system (ICS) attack framework last year,[1] companies and utilities in critical infrastructure must mature their security operations to gain insights from both information technology (IT) and operational technology (OT) networks in order to prevent disruption, degradation, and even destruction of industrial environments.

In this 2023 ICS/OT Visibility survey, the results provide a glimpse into the relationship between IT and OT security operations and provide key insights, including:

- While SOC capabilities are expanding to include more ICS/OT, there are still significant gaps in OT-specific visibility as well as staffing and education issues across enterprise IT.
- Even in the areas where IT and OT SOC capabilities are merging, the visibility is still incomplete.
- OT security programs are less mature than their IT counterparts, specifically in the areas of identifying, containing, and eradicating threats in their environments and overall incident response.
- Although staffing and lack of education and training were identified as the greatest challenges for security operations, there are also significant gaps due to legacy technology and limitations in implementing IT capabilities in OT environments.

Survey results also indicate that these are the areas that could benefit from more automation (because they require more resources) and where respondents feel IT and OT could complement each other more.

This survey explores how respondents are currently tackling ICS/OT visibility challenges, the gaps across the IT-OT boundary, the roadblocks for expanding visibility, and the maturity comparisons from both domains.

This year's survey had nearly 350 respondents across a wide variety of industrial sectors. Details are shown in Figure 1 on the next page.

[1] "Alert (AA22-103A), APT Cyber Tools Targeting ICS/SCADA Devices," www.cisa.gov/uscert/ncas/alerts/aa22-103a

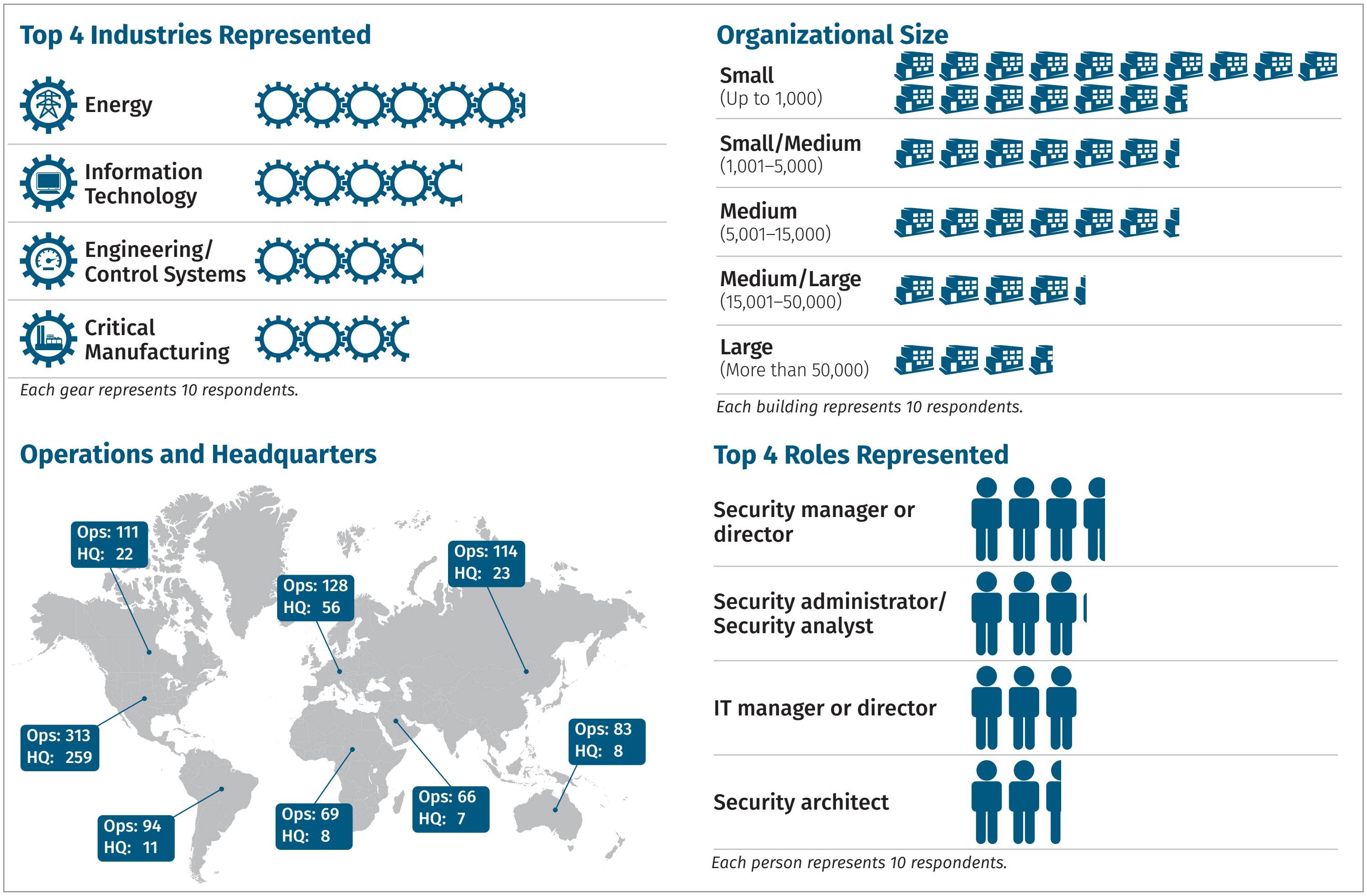


Figure 1. Demographics of Survey Respondents

Respondents represented organizations of various sizes, both in terms of workforce and the number of industrial facilities being operated. Roughly 20% of respondents, the largest pool of survey results, worked in organizations with 101–500 people while nearly 30% of respondents operated 1–10 industrial facilities (and another 18.5% operated 10–25 industrial facilities). That said, some surveyed firms were more than 50,000 people strong (14.5% of respondents) and had operations spanning more than 1,000 industrial sites (6.3% of respondents).

IT and OT Visibility Concepts

Traditional IT visibility usually relies on a combination of network data, asset and application data, and the ability to correlate each dataset for decision-making capabilities during incident detection and response. Over the years, this combination has led to specific developments across the people, processes, and technologies that support visibility objectives in enterprise IT networks.

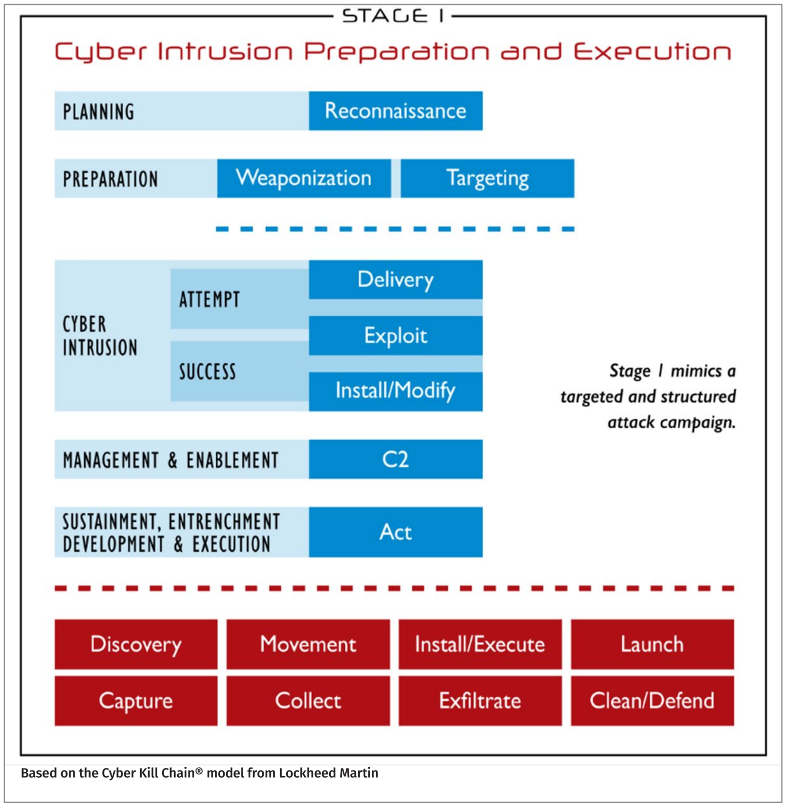
ICS and OT environments, however, face a different set of challenges when it comes to determining how to achieve visibility. Historically, it has been difficult to expand network visibility into the control system network, let alone capture other meaningful artifacts from host-based logs, process/data historians, process controller logs, or specific ICS software events and alarms. Network visibility expansion requires planning across engineering and operations personnel, IT and OT security professionals, and ICS/OT equipment vendors. The overall process to achieve ICS/OT visibility could take months or years, depending on the environment.

As threats continue to target ICS/OT environments, it is critical for industrial organizations to gain visibility across both IT and OT systems. Doing so facilitates quicker incident response, tailored defenses based on unique OT architecture, and a more complete picture of an organization's attack surface.

Using the ICS Cyber Kill Chain

Because ICS/OT cyberattacks involve unique systems and impacts, it is important to briefly visit the concept of the ICS Cyber Kill Chain[2] to understand why visibility across the IT-OT boundary matters.

The ICS Cyber Kill Chain is a framework used to describe the various stages of a cyberattack on ICS/OT systems. Stage 1 of the ICS Cyber Kill Chain is identical to the IT-specific version, as outlined in Figure 2.



Based on the Cyber Kill Chain® model from Lockheed Martin

Figure 2. Stage 1 of the ICS Cyber Kill Chain

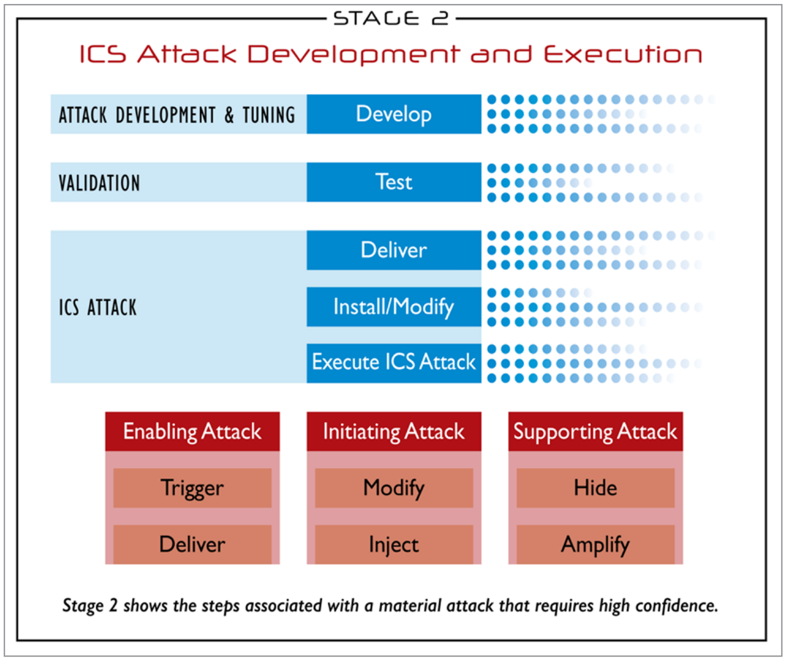
Stage 1 requires:

- **Planning—**During this stage, the attacker identifies their target and researches potential vulnerabilities in the target's security defenses. The attacker also may gather information about the target's employees, partners, and customers to better understand the target's security posture.
- **Preparation—**In this stage, the attacker prepares their tools and techniques for the attack. They may create malware or phishing emails, set up command and control infrastructure, or conduct reconnaissance to identify potential targets.
- **Cyberintrusion—**This is the stage where the attacker gains access to the target's network or system. They may use a variety of tactics, such as exploiting vulnerabilities, using stolen credentials, or social engineering techniques to gain access.

[2] For more information on the ICS Cyber Kill Chain, visit www.sans.org/white-papers/36297

- **Management and enablement—**During this stage, the attacker establishes a foothold in the target's network and begins to move laterally to expand their access. They also may install additional tools or malware to maintain persistence and evade detection.
- **Sustainment, entrenchment, development, and execution—**In this final stage, the attacker focuses on achieving their goals, such as stealing data, disrupting operations, or installing ransomware. The attackers also may work to maintain their access and evade detection, and they may continue to develop new tactics and techniques for future attacks.

This may be the entire universe of considerations for an IT-only cyberattack. However, this does not address potential ICS/OT impacts, which involve the *physics* of a process. Figure 3 shows where Stage 2 of the ICS Cyber Kill Chain comes into play.



Stage 2 shows the steps associated with a material attack that requires high confidence.

Figure 3. Stage 2 of the ICS Cyber Kill Chain

Once the attacker focuses on the ICS/OT system, they must leverage specific techniques to affect the process being controlled, either through loss, denial, or manipulation of the view, control, or safety of the system.

Without visibility across both IT and OT, the ability to identify an attacker or their actions across the IT-OT boundary (and Stage 1–Stage 2 of the kill chain, respectively) is limited. To successfully execute an industrial cyberattack, threat actors need to have successful actions across both Stage 1 and Stage 2, similar to the 2015 cyberattack on the Ukrainian power grid, as seen in Figure 4.

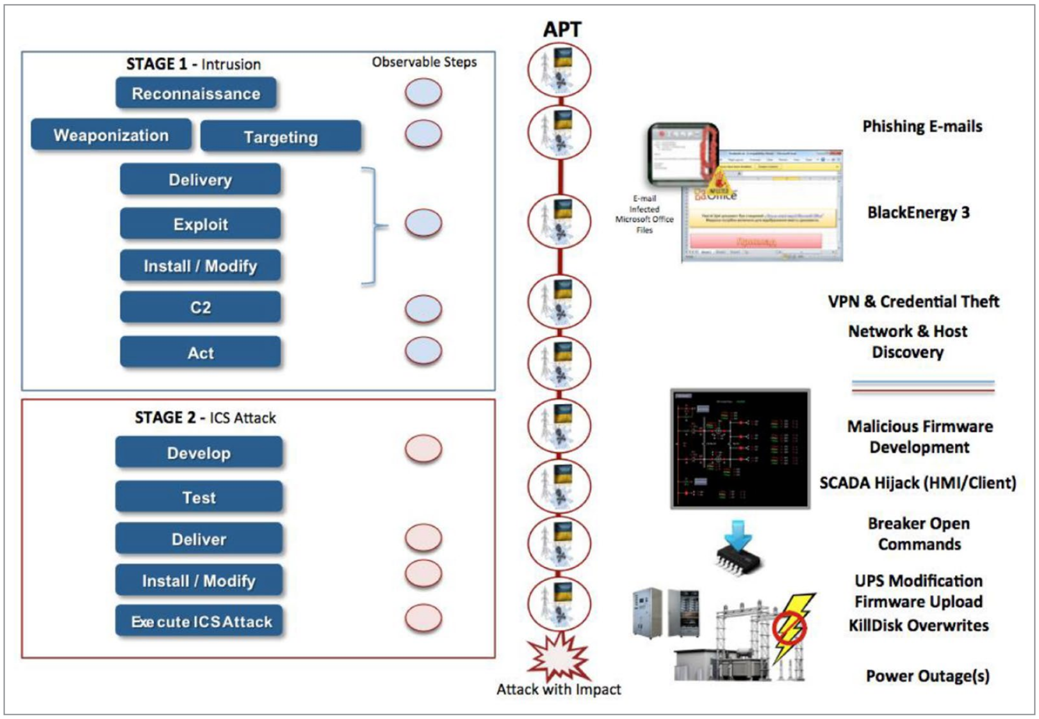


Figure 4. ICS Cyber Kill Chain Example from the 2015 Cyberattack on the Ukrainian Power Grid[3]

[3] For more information, visit https://ics.sans.org/duc5

IT and OT Convergence

Discussions around IT-OT “convergence” further muddy the conceptions around visibility and who should be responsible for the overall protection, detection, and response functions for ICS/OT cybersecurity. For the purposes of this survey, convergence is understood as the integration of information technology with operational environments. In that sense, convergence already has taken place in many industrial organizations where computers, modern human-machine interfaces (HMIs), and historian servers reside.

Just because an IT computer exists in an OT environment, however, does not mean that the computer is “IT.” The placement of the technology and what it interacts with and controls matter. In simplest terms, for the purposes of this survey, anything that interacts with, views, or controls the physical process and means of production is “OT,” while anything that is enterprise-based would be considered traditionally IT. This paper covers this idea further during the discussion of the Purdue Model in Section 4, Gaps in OT-Specific Visibility.

Integrated IT-OT SOC Capabilities

Lastly, before reviewing the survey results, let’s define the technical and procedural differences between IT and OT security operation center (SOC) capabilities. A SOC is a combination of people, processes, and technology that proactively searches for abnormalities in the respective environment to identify and respond to security incidents. Due to the evolution, and relative successes, of IT-based SOCs, organizations have recently explored applying similar concepts to OT.

As SOCs expand in OT environments, they not only must determine what data can be integrated to increase visibility but also what services will be performed by an OT-capable SOC. This determination could include anything from passive defense to threat hunting to intelligence functions—each of which may have its own prerequisites, metrics, and feasibility in any given environment.

Furthermore, within security operations, there are three levels of analysts that will need to have some level of OT training to be successful. They are:

- **Tier 1—**This is the first level of analysts in a SOC. Their primary responsibility is to monitor security alerts and events, triage incidents, and perform initial investigation and analysis. Tier 1 analysts typically have entry-level security skills and use predefined playbooks and workflows to investigate alerts.
- **Tier 2—**If an incident requires further investigation, it is escalated to Tier 2 analysts. These analysts have more experience and knowledge than Tier 1 analysts and are responsible for conducting more in-depth analysis and investigation of security incidents. They also may be responsible for identifying and documenting new threats, creating custom playbooks, and working with Tier 1 analysts to improve overall SOC efficiency.

- **Tier 3—**Tier 3 analysts are the most experienced and knowledgeable analysts in a SOC. They are responsible for investigating and resolving the most complex and sophisticated security incidents. They also provide guidance and training to Tier 1 and Tier 2 analysts, as well as working with other departments in the organization to improve overall security posture. Tier 3 analysts also may be involved in developing new security policies and procedures.

It's important to note that some routine tasks performed by Tier 1 analysts in an IT-specific SOC may cause large problems in an integrated OT SOC. For example, if a Tier 1 analyst were to leverage endpoint protections to quarantine or delete files in an infected ICS/OT asset, or reimage it entirely, such an action could have impacts on the industrial process being controlled, depending on the system or the timing of such actions. As such, an OT-specific (or integrated) SOC likely would need to escalate more often to the Tier 3 ICS/OT analyst with knowledge of those systems and the people operating them.

Expanding Visibility

With that foundation, we can now explore the survey results specific to ICS/OT visibility and larger discussions around IT and/or OT security operation centers. Out of the nearly 350 respondents operating industrial facilities, 80% have monitoring capabilities within their ICS/IT environment. As observed throughout the survey responses, however, the lower level of the Purdue Model significantly lacks visibility across industrial facilities. Of the respondents, approximately 50% claim that their enterprise SOC includes some level of ICS/OT visibility.[4] With or without an enterprise SOC, 37% of respondents indicated that they had an ICS/OT-specific SOC.

Interestingly, survey results from the energy sector largely indicated a preference for an enterprise-wide SOC with OT visibility, while engineering and critical manufacturing sectors preferred an OT-specific SOC, which tends to have smaller workforces, according to survey respondents. These preferences could suggest that the OT SOC functions are performed locally at plant locations compared to the energy sector, which traditionally has pockets of centralized operations.

Of the survey respondents that had no ICS/OT visibility in their SOC (or a standalone OT-specific SOC), 67% indicated there were plans to expand their SOC to include these capabilities.

As mentioned previously, the SOC may perform several different services for the organization's business units. When asked about one of the more foundational services, incident response for OT, nearly 40% of respondents indicated that only IT staff would respond to the incident. An additional 6% stated that there was no OT-specific incident response plan. Unfortunately, OT cybersecurity incidents require a combination of IT and OT expertise, specific to the safety and reliability of the ICS/OT environment. In a related statistic, 54% of respondents also identified training for IT staff in OT cybersecurity as the No. 1 challenge for expanding security operations.

[4] Visibility gaps are covered in the next section, *Gaps in OT-Specific Visibility*, and this result does not imply full ICS/OT visibility.

Gaps in OT-Specific Visibility

Whereas SOCs are more formal constructs around the centralized people, processes, and technologies that are monitoring, detecting, responding to, and analyzing cybersecurity incidents, there are several capabilities that may or may not involve a SOC but still account for OT-specific visibility. OT-specific visibility is reliant upon what data sources can be collected and analyzed, which may require dedicated resources and maturity across the industrial organization, as highlighted by the SANS Institute's Five ICS Cybersecurity Critical Controls (see Figure 5).[5]

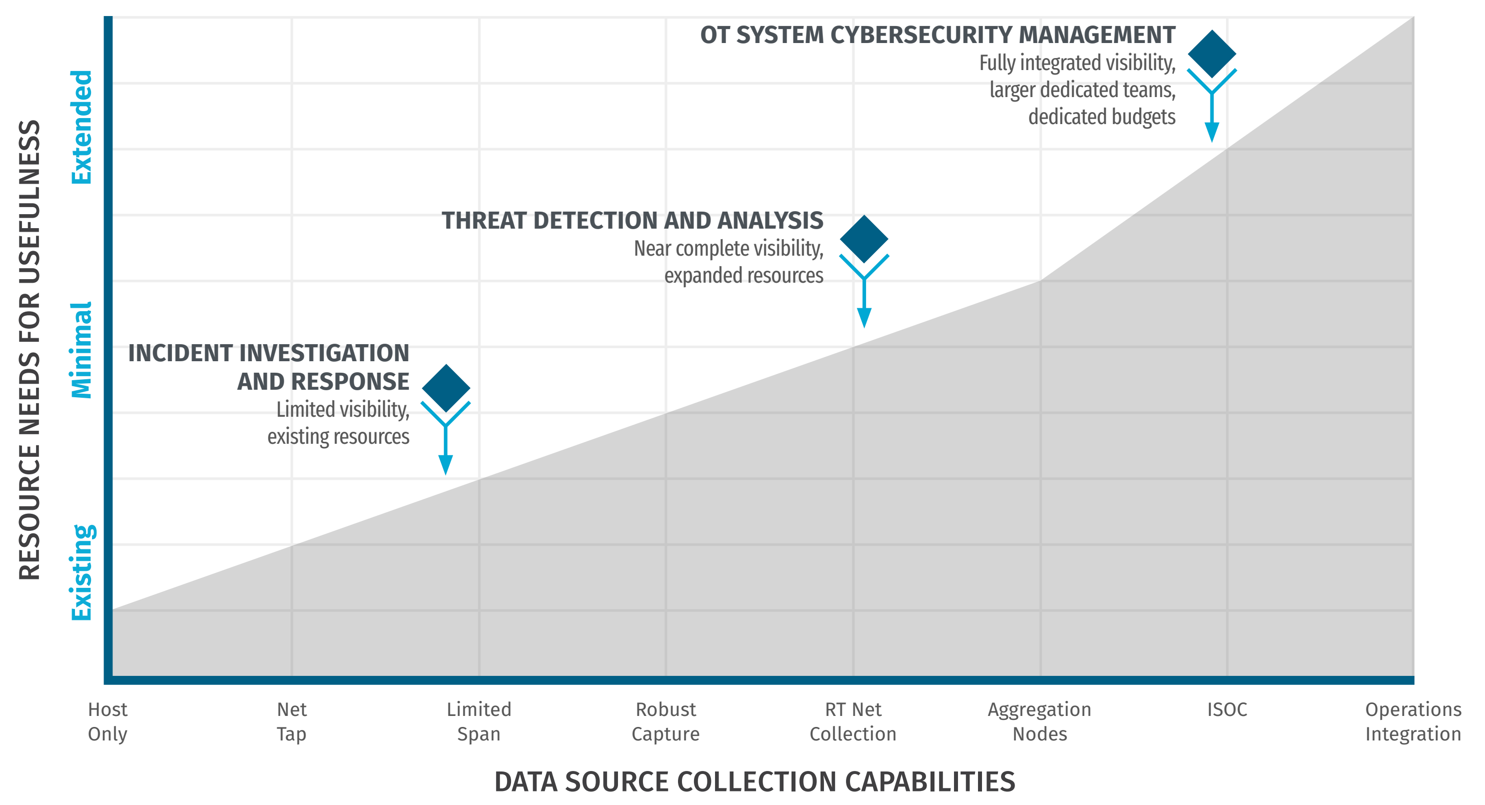


Figure 5. ICS Visibility, Maturity, and Capability Considerations from the SANS Five ICS Cybersecurity Critical Controls

Even in the case where respondents had a more expansive SOC, only 53% of their ICS/OT environments provided data for detection purposes.

To understand where more of these gaps may lie, we asked explicitly about endpoint detection and response tools on assets and what capabilities exist for internal network security monitoring specific to ICS/OT environments.

[5] The whitepaper on the Five ICS Cybersecurity Critical Controls can be found here: www.sans.org/white-papers/five-ics-cybersecurity-critical-controls

Endpoint Detection and Response

As shown in Figure 5, host-based controls are the initial starting point for many ICS/OT visibility programs. As such, we asked respondents where endpoint detection and response (EDR) technologies were deployed, based on the asset classifications in Figures 6, 7, and 8.

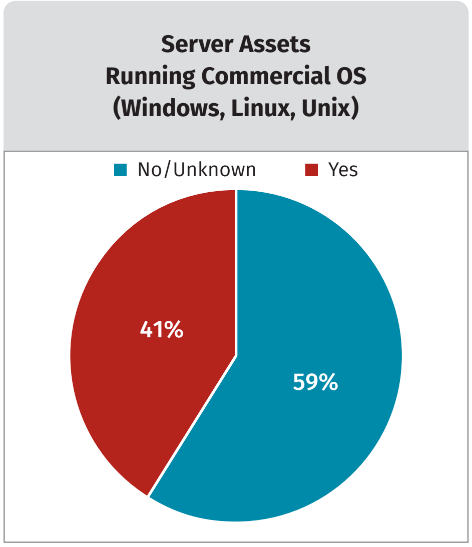


Figure 6. Server Assets Running Commercial OS

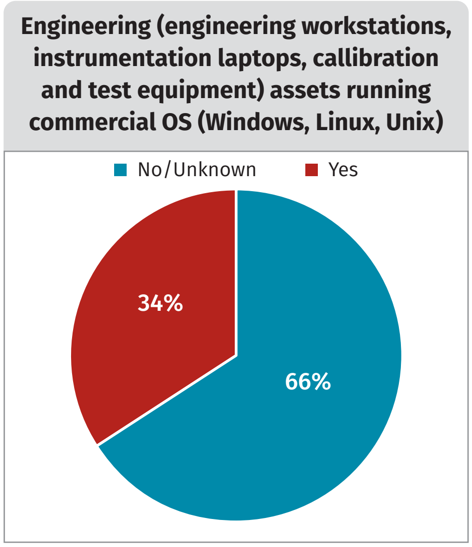


Figure 7. Engineering Assets Running Commercial OS

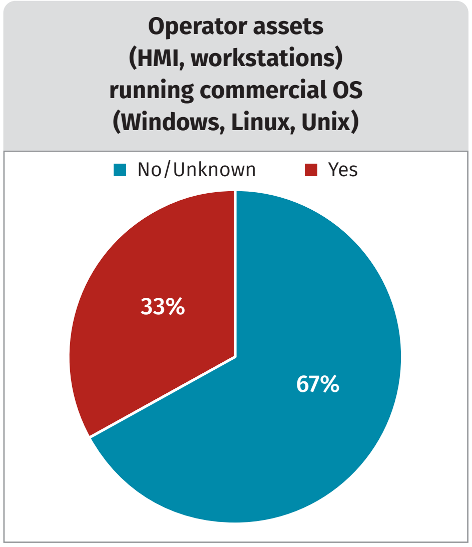


Figure 8. Operator Assets Running Commercial OS

Unsurprisingly, most EDR solutions were deployed on servers running commercial operating systems such as Windows, Linux, and Unix. However, the coverage varied wildly based on industrial sector and the number of industrial facilities being monitored. For example, the energy sector and engineering sectors were nearly identical in coverage across servers (51–52% had EDR deployed where possible), engineering assets (such as workstations, instrumentation laptops, and calibration and test equipment), and operator assets (HMIs and workstations) were both similar with over 40% having EDR where possible. However, in critical manufacturing, 68% of servers had EDR deployed where possible and only 30% of engineering assets had it. Critical manufacturing had a similar amount of coverage for operator assets as the energy and engineering sectors, but respondents in the chemical sector reported that only 10% of operator assets had EDR installed, one of the lowest percentages across the survey.

Organizational size absolutely scaled with EDR deployments. Smaller organizations (1–25 industrial facilities) had EDR on 50% of their servers, while mid-sized organizations (100–500 industrial facilities) reported 75–80% EDR coverage on their server assets. The coverage dipped again for organizations between 500–1,000 industrial facilities, but then for organizations with more than 1,000 industrial sites, more than 80% of server assets with EDR was deployed where possible. Size had no discernable impact on engineering or operator assets—and, in fact, having an enterprise-wide SOC correlated with higher server EDR deployments, implying that the server assets are centrally managed compared to the on-site engineering and operator assets.

Regardless of the current coverage, if EDR is already deployed, 76% of respondents said they had plans to expand their EDR deployments in ICS/OT environments over the next 24 months, with a full 23% saying that coverage would expand by 50% or more in those environments.

Network Security Monitoring

Internal network security monitoring (NSM) within ICS/OT environments comes in all shapes. Where is the monitoring occurring? Can the technology detect abnormalities specific to ICS/OT traffic? What's the coverage in each environment based on ICS protocols? Each of these questions requires additional investigation by industrial organizations when examining NSM capabilities.

Using the Purdue Model as a reference architecture, we asked our respondents about where NSM technology was deployed. The averages across all respondents are shown in Figure 9.

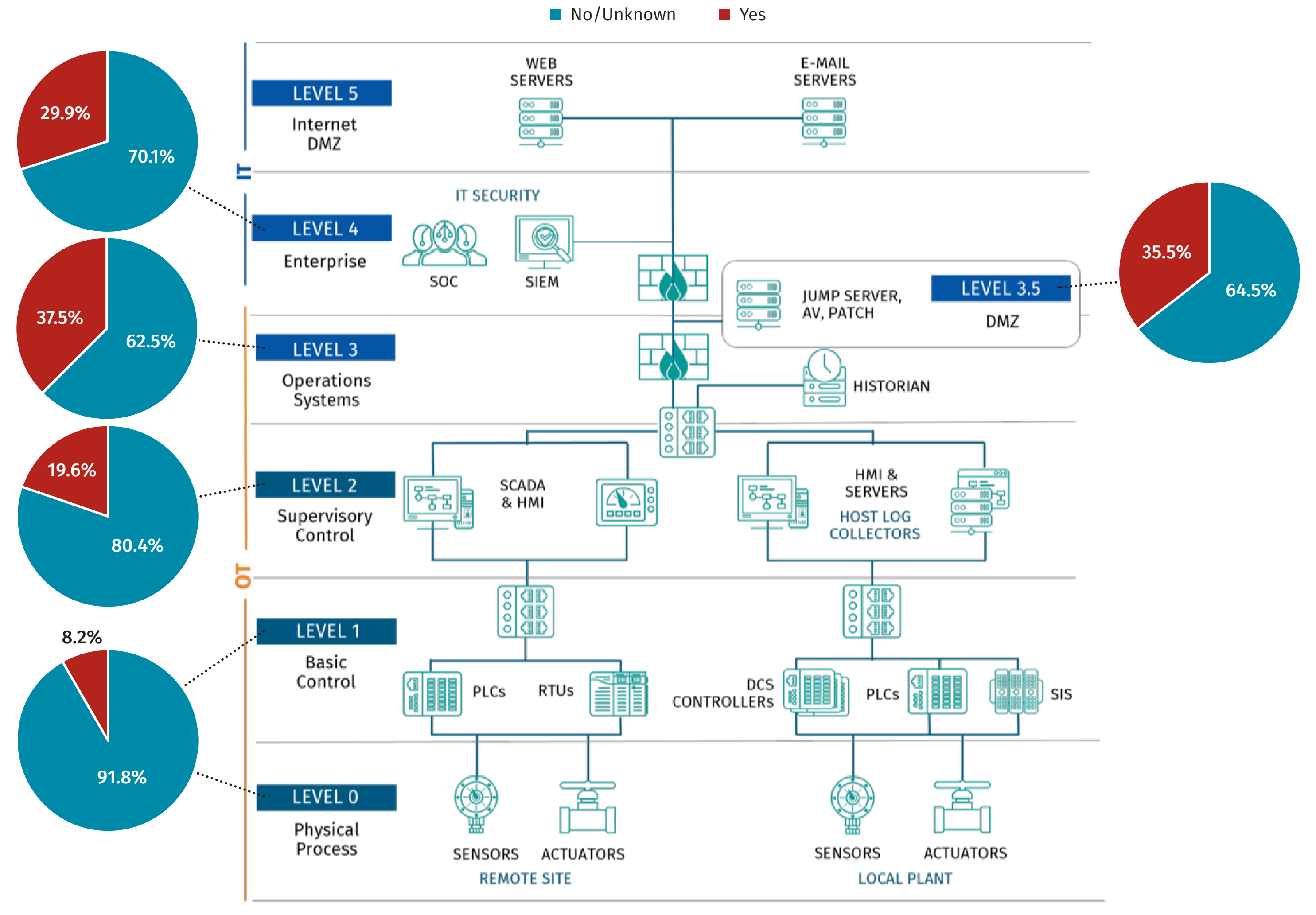


Figure 9. NSM deployments Across IT and OT

On average, only 30% of respondents had network monitoring on their IT enterprise networks, while 38% had NSM deployed at Purdue Level 3 (Operations Systems) and 35% within the DMZ between those two levels. As things get deeper into ICS/OT networks, there is less and less visibility; fewer than 20% of respondents monitored devices at Level 2 and fewer than 10% and Level 0/1. Those that are monitoring at Level 1 and Level 2, however, are not necessarily more mature—those respondents equally lack coverage in Level 3, Level 3.5, and Level 4.

Our survey indicated that the energy sector has deployed more networking monitoring technologies; on average, 10% more than all other sectors combined. Interestingly, unlike EDR, having a SOC (enterprise-wide or with OT capabilities) had no bearing on NSM deployments. Similar to EDR, 70% of respondents indicated that there are plans to expand NSM over the next two years if they already have it deployed in ICS/OT environments, with 23% saying that expansion would be more than 50% of their current visibility.

Deploying technologies, however, is not enough. Having logs and data across IT and OT environments is useful for identifying the root cause during an incident, but what about detecting something *before* an incident? That is where reviewing logs becomes an important ask. As seen in Figure 10, roughly 30% of respondents monitor their ICS/OT environments at least hourly.

Having an enterprise SOC slightly improved the numbers in favor of more frequent monitoring. A drastic spike is seen, however, in "continuous monitoring" of the ICS/OT environment when the enterprise-wide SOC has visibility into ICS/OT environments (up to 38%) or a dedicated ICS/OT SOC (up to 30%). Regardless of having a SOC, if EDR and NSM are deployed *at all*, monitoring activity frequency jumps, increasing an additional 6-10% among respondents with continuous monitoring when those technologies are present. It appears that if people invest in technology in their ICS/OT environments, they also want to see how well they are doing and will increase monitoring capabilities as well.

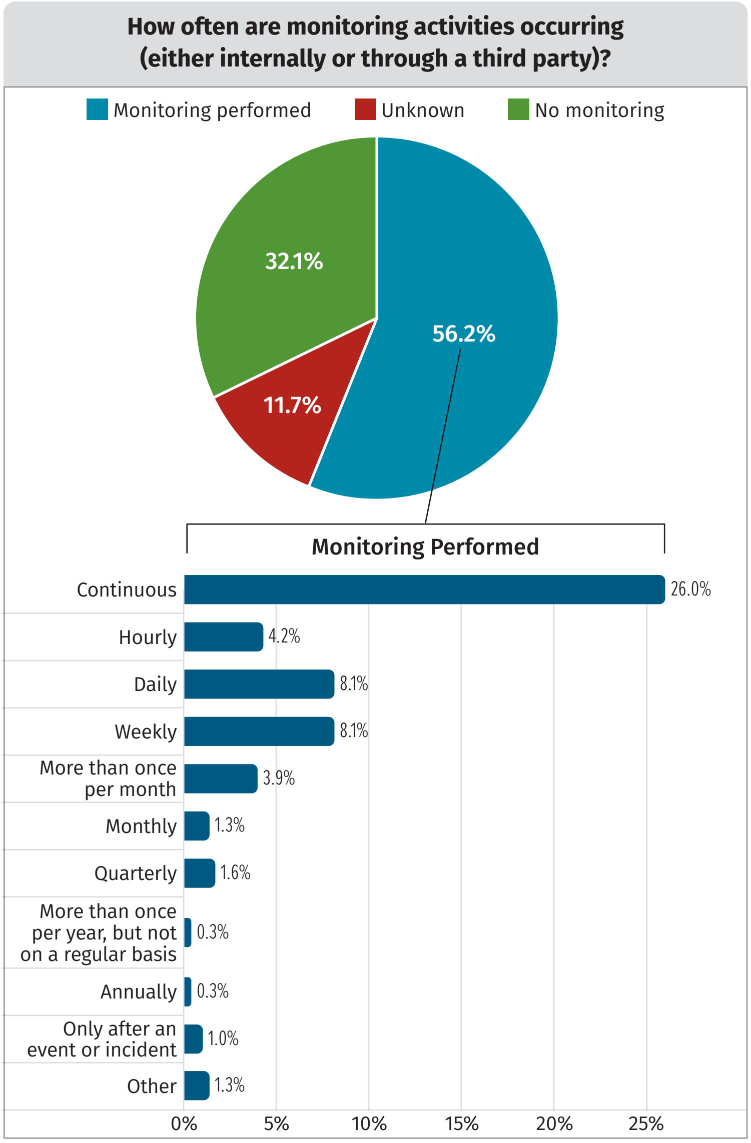


Figure 10. Monitoring Event Frequency for ICS/OT

Relative Maturity and Level-of-Effort for OT Security

Monitoring the ICS/OT environment is only one aspect of overall OT security. We delved further into the responses to understand how ICS/OT security operations compared to their IT equivalents. We leveraged the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) to organize various activities and asked survey participants if, when performing the same activities in IT and OT, was OT less mature, more mature, or at the same relative level of maturity. See Figure 11 on the next page.

CSF Category	Activity	More Mature	Same Level	Less Mature
Identify	Asset inventory	24.7%	35.4%	35.4%
	Cyber risk management and impact evaluation	17.5%	39.0%	35.9%
	Threat management and intelligence	14.3%	41.3%	39.9%
Protect	Configuration management	23.3%	36.3%	37.2%
	Identity and access management	18.4%	32.7%	42.6%
	Cybersecurity workforce management	17.5%	39.5%	35.4%
	Cybersecurity policies and procedures	19.3%	40.8%	33.6%
	Vulnerability management	17.5%	32.7%	43.5%
Detect	Cyber event detection	15.7%	33.6%	45.7%
	Cyber event analysis	17.0%	34.5%	40.8%
	Cyber incident determination	15.7%	38.1%	39.5%
Respond	Cyber incident containment	17.0%	35.4%	41.3%
	Cyber incident eradication	15.2%	35.9%	40.8%
Recover	Cyber incident recovery	17.5%	36.8%	40.4%
	Cyber incident lessons learned	19.3%	34.1%	40.4%

Figure 11. Comparison of ICS/OT Security Capabilities to IT Security Capabilities as Grouped by the NIST Cybersecurity Framework Functions

Across the board, respondents believe—overwhelmingly so—that OT is the same or less mature than IT in every NIST CSF function.[6] Diving a bit further into specific capabilities provides additional insights. For example, asset inventories and configuration management scored nearly identically in the same level of maturity as the IT counterparts (35 and 36%) and had the highest scores for "more mature" than IT at 23 and 24%. This makes sense because asset management in ICS/OT deals with far fewer assets overall, though the specific activities involved in inventorying and configuring those assets may be more labor-intensive. This is why we also asked about how labor-intensive these activities are in ICS/OT security (see Figure 12).

CSF Category	Activity	Low Labor Intensity	Moderate Labor Intensity	High Labor Intensity
Identify	Asset inventory	13.6%	43.0%	42.1%
	Cyber risk management and impact evaluation	11.3%	47.5%	38.0%
	Threat management and intelligence	12.7%	42.1%	35.3%
Protect	Configuration management	12.2%	38.0%	47.5%
	Identity and access management	12.7%	46.2%	38.0%
	Cybersecurity workforce management	11.3%	49.3%	33.9%
	Cybersecurity policies and procedures	13.6%	49.3%	34.8%
	Vulnerability management	10.4%	42.1%	45.2%
Detect	Cyber event detection	14.5%	43.0%	39.4%
	Cyber event analysis	10.9%	43.9%	41.2%
	Cyber incident determination	9.0%	44.3%	41.6%
Respond	Cyber incident containment	7.7%	38.9%	46.2%
	Cyber incident eradication	5.9%	33.9%	54.3%
Recover	Cyber incident recovery	8.1%	37.1%	47.5%
	Cyber incident lessons learned	12.2%	45.7%	35.7%

Figure 12. Labor Intensity of ICS/OT Security Capabilities as Grouped by the NIST CSF Functions

[6] More information about the NIST CSF can be found at www.nist.gov/cyberframework.

As mentioned, respondents viewed configuration management as requiring a high level of effort to manage in ICS/OT security programs with 47.5% of respondents reporting it as a highly labor intensive. Similarly, vulnerability management also was listed as requiring a higher level of effort, with 45.2% of respondents agreeing.

One theme became readily apparent when looking at both the level of effort and the relative maturity compared to traditional IT practices: *ICS/OT incident response and recovery is difficult*. Survey respondents overwhelmingly listed cyber incident containment, eradication, and recovery as requiring the highest levels of effort (46.2%, 54.3%, and 47.5% of respondents, respectively). Meanwhile, every single task in the following list for incident response was listed as less mature compared to IT.

- Cyber event detection (45.7% of respondents listed it as less mature than IT)
- Cyber event analysis (40.8% of respondents listed it as less mature than IT)
- Cyber incident determination (39.5% of respondents listed it as less mature than IT)
- Cyber incident containment (41.3% of respondents listed it as less mature than IT)
- Cyber incident eradication (40.8% of respondents listed it as less mature than IT)
- Cyber incident recovery (40.4% of respondents listed it as less mature than IT)
- Cyber incident lessons learned (40.4% of respondents listed it as less mature than IT)

These results indicate that there are likely areas where further education and automation not only can help improve the relative maturity of incident response capabilities but also help decrease the overall manual labor required.

Challenges in Collaborating Across the IT-OT Divide

As industrial sectors continue to look at digital transformation and advancements in Industry 4.0, the lines between IT and OT will continue to blur. As mentioned in the discussion about convergence, there are many "IT assets" that now operate within ICS/OT environments. Shifts to edge cloud connectivity have, in several sectors, already been implemented. The proposed benefits are shown in Figure 13.

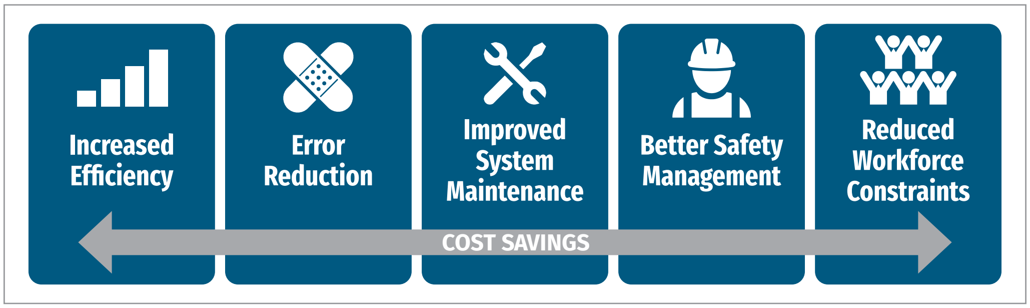


Figure 13. Proposed Benefits for Digital Transformation Across Industrial Organizations

As these boundaries become more porous, we asked respondents what, if any, capabilities should be integrated across IT and OT. The results are shown in Figure 14.

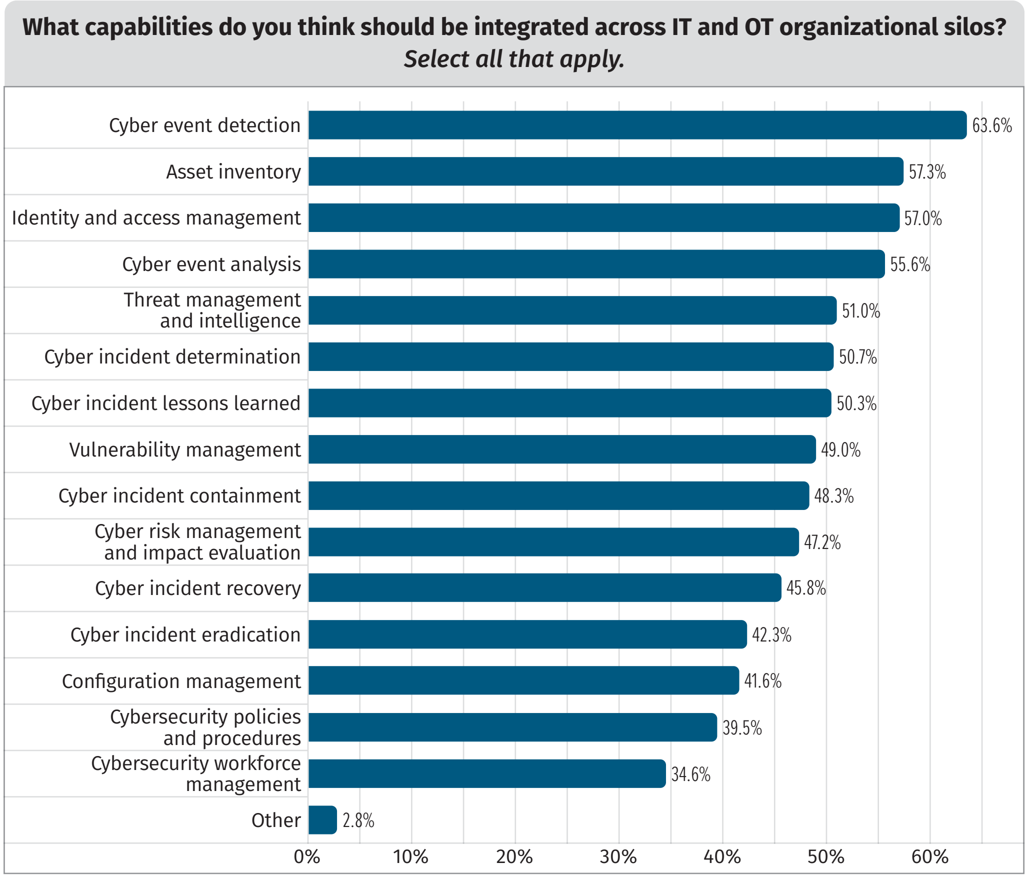


Figure 14. Potential Areas for IT-OT Convergence

The top categories absolutely align with increased visibility across Stage 1 and Stage 2 of the ICS Cyber Kill Chain—having convergence where logs and security operations can track potential malicious traffic across IT and OT is vital for root cause analysis after an event. As organizations expand their monitoring capabilities, this could even lead to preventing Stage 2 attacks and impacts. The bottom categories also make sense as to where this is less likely to have some overlap. From security workforce training and management to policies and procedures to configuration management, there are more likely to be unique considerations for ICS/OT that will have minimal overlap with IT. Similarly, incident eradication and recovery activities will need to have operations and engineering considerations baked in. IT incident response plans can have unintended consequences in ICS/OT environments, as noted by the US Department of Homeland Security, which states that "standard cyber incident remediation actions deployed in IT business systems may result in ineffective and even disastrous results when applied to ICS cyber incidents, if prior thought and planning specific to operational ICS is not done."[7]

While there are noted benefits of aligning some parts of the IT and OT security programs, there are also plenty of barriers to success. When asked about the greatest challenge in aligning security operations across the IT-OT boundary, 51.2% of respondents listed "people" as the biggest obstacle. See Figure 15.

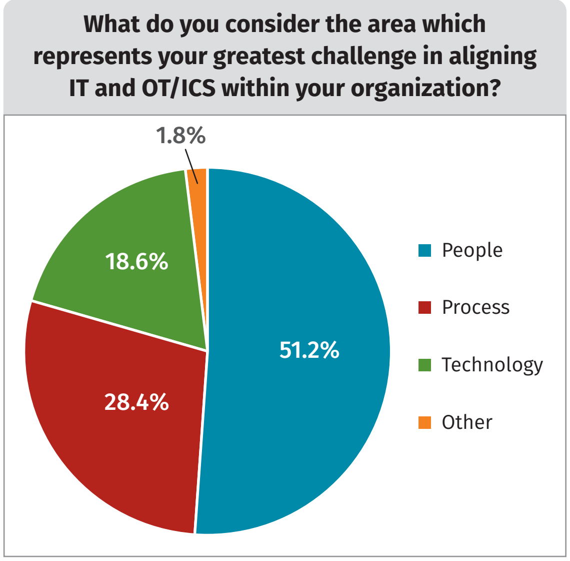


Figure 15. Challenges for IT-OT Alignment Based on People, Processes, and Technology

[7] "Developing an Industrial Control Systems Cybersecurity Incident Response Capability," The Department of Homeland Security, https://us-cert.cisa.gov/sites/default/files/recommended_practices/final-RP_ics_cybersecurity_incident_response_100609.pdf

We wanted to revisit this concept based on our original premise concerning IT-OT monitoring; respondents shared their top barriers to expanding ICS/OT visibility as seen in Figure 16.

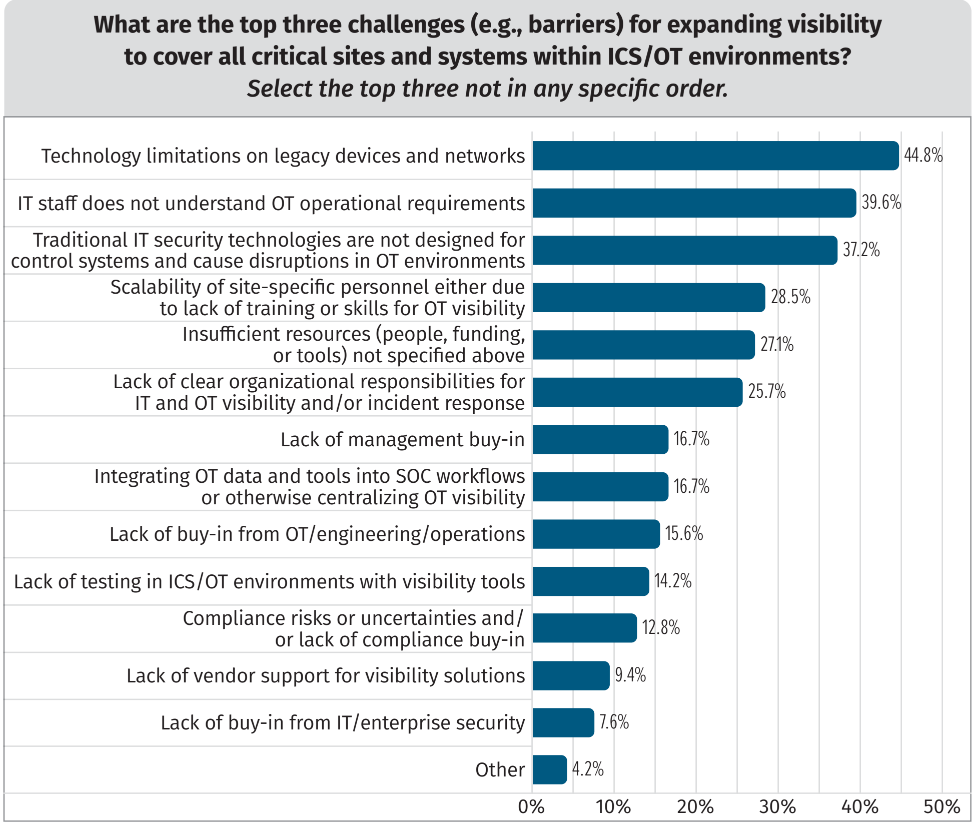


Figure 16. Top Barriers to Expanding ICS/OT Visibility

The top technology concern was limitations on legacy devices and networks, which may require extensive testing prior to deploying monitoring technologies—if it is even possible. Many ICS/OT environments have decades-old technology that will always be limited in their capabilities, in which case security practitioners must focus on optimizing within those constraints or leveraging other sources of data to check for abnormalities. The next top challenges are both related to IT not understanding OT, whether it be the communication between staff members themselves or the technology being deployed. As mentioned previously, ICS networks use different protocols than traditional IT networks and many IT-specific technologies will not work properly as a result. Or worse, they can cause a production outage. For example, active scanning on an ICS/OT network may overwhelm controllers and other operation assets, affecting their ability to function and even requiring a resetting of the device. The same can be true for a well-intentioned but untrained IT professional in an industrial environment that may be unaware of the safety or reliability impacts associated with IT-specific tools and methods.

It is not surprising, then, that when we asked about the top concern for aligning IT and OT security operations, the top concern was training for IT staff in OT environments. See Figure 17.

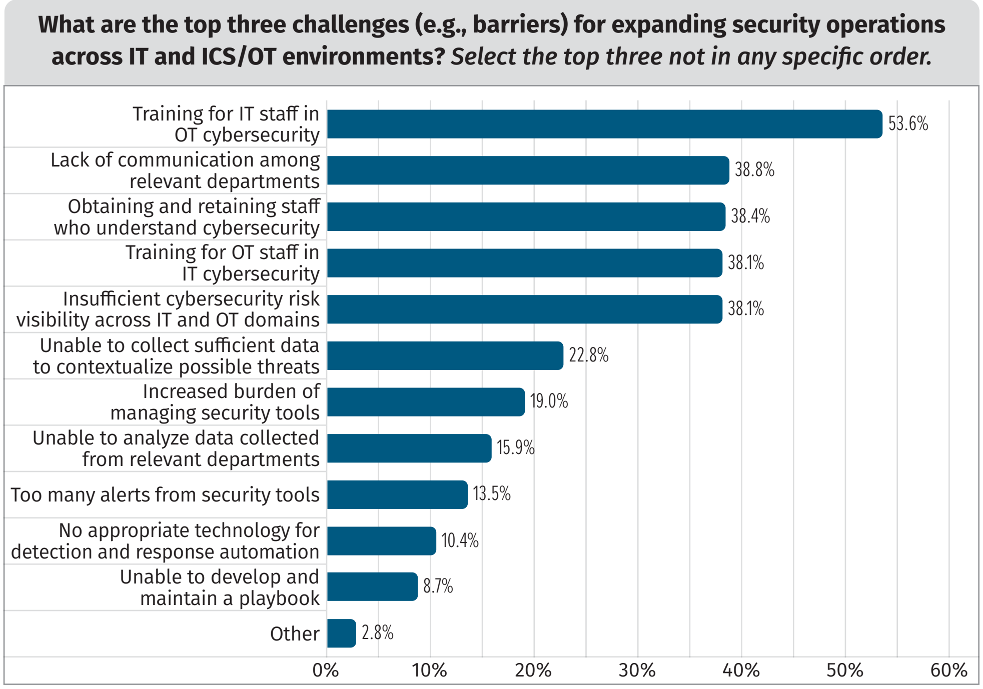


Figure 17. Top Barriers in Expanding Security Operations Across IT and OT

These results further highlight the need to help enable the workforce as the "people" part of the issues that arise from aligning IT and OT security operations. Training, as well as recruitment and retention of talent, was a common theme throughout the reported challenges from respondents.

Conclusions and Next Steps for Industry

Digital transformation and further IT-OT convergence is not only coming, it is already here for many industrial organizations. What were once isolated and rarely connected ICS/OT environments are now enabled with growing remote access connections and edge cloud connectivity to aid in both vendor management and business analytics. In order to better manage the associated industrial cyber risk, visibility across IT and OT environments needs to be a top priority for organizations.

This survey outlines the challenges—and opportunities—associated with aligning IT and OT security operations and increasing visibility. We explored the trends around SOCs and their impact on overall visibility, as well as the expansion of EDR and NSM deployments within industrial environments, noting that increasing technology usage in these areas greatly affects the overall coverage of visibility for those facilities and sites that have them.

On the relative maturity between IT and OT, the industry needs to understand not only where OT security can continue to improve but also where the fundamental differences between IT and OT need to be accounted for, such as incident response plans and capabilities. Understanding these challenges and opportunities is especially helpful for teams that are growing in ICS/OT security. This paper outlined which capabilities may require additional resources. These would be smart areas to further invest in as an ICS/OT security program matures.

As global regulations continue to focus on ICS/OT environments, it is vital to understand the impact and added value that visibility provides while acknowledging that IT security alone cannot solve these problems. It must be a collaborative effort among security professionals, engineers, and operators. Cross-training teams for security operations, understanding how cyber incidents traverse IT and OT boundaries, and working to alleviate the barriers listed across this survey will create a foundation of success for any ICS/OT security program.

Sponsor

SANS would like to thank this survey's sponsor:

TREND MICRO™