SANS | Research Program

2025 SURVEY

State of ICS/OT Security 2025

Written by **Jason D. Christopher**

November 2025

Acronis

Foreword

For nearly a decade, these surveys have tracked the industry's progress toward cybersecurity maturity and identified the key drivers behind actions, both taken and not taken, within each sector. In collaboration with industry experts, the SANS team designs the survey to deliver actionable insights for readers. In recent years, Jason Christopher has elevated this report to a new level of excellence.

Over the years, the world has evolved: organizations have deepened their capabilities, adversaries have adapted, and expectations for corporate cybersecurity performance continue to rise. Given this reality, both the survey questions and the analysis of responses must mature to capture the nuances that matter most to leaders shaping and advancing their programs.

In this year's survey, Jason Christopher delivers a true masterclass for the industry, capturing historical trends, identifying the current state of the field, and forecasting where it's heading. His work provides the ICS/OT community with valuable context on where peers stand today, why, and where they go next.

This report is essential reading for anyone in a leadership role across critical infrastructure environments.

I am excited to see how leaders across the industry put these insights into action, and I look forward to watching this survey continue to evolve as a vital tool in the defense of critical infrastructure worldwide!

Tim Conway
SANS Fellow

SANS 2025 STATE OF ICS/OT SECURITY SURVEY

Key Findings

Incidents remain high and disruptive.

More than one in five organizations (22%) reported a cybersecurity incident in the past year, with 40% causing operational disruption and nearly 20% taking over a month to remediate.

Detection is improving, but recovery lags.

Nearly half of incidents were detected within 24 hours and 60% contained within 48 hours, yet remediation often stretches into days or weeks (and can even take over a year).

Regulation drives maturity.

Sites under mandatory compliance had similar incident rates as peers but experienced ~50% fewer financial losses and safety impacts.

Threat intelligence pays dividends.

Organizations leveraging ICS-specific threat intelligence were more likely to adjust defensive priorities—improving monitoring, segmentation, and detection.

Remote access remains a top risk.

Unauthorized external access accounted for half of all incidents, yet only 13% of organizations have fully implemented advanced controls such as session recording or ICS/OT-aware access.

Preparedness is uneven.

Just 14% of respondents felt fully prepared for emerging threats, but those that included frontline technicians in exercises were nearly 1.7 times more likely to report strong readiness.

Investment momentum is clear.

Asset visibility, threat detection, and secure remote access dominate both 2025 deployments and 2026–2027 planned investments, showing where organizations see the greatest value.

Survey Author

Jason Christopher
SANS Certified Instructor

VIEW PROFILE

CURRENTLY TEACHING

ICS418: ICS Security Essentials for Leaders

ICS456: Essentials for NERC Critical Infrastructure Protection

Over the past 20 years, Jason D. Christopher has worked across multiple industries in unique roles ranging from engineering to incident response and national security. Most notably, Jason was the federal technical lead for the NERC CIPv5 while at the Federal Energy Regulatory Commission, where he was involved in several rulemakings and policy statements. Jason was also the program lead for the US Department of Energy Cybersecurity Capability Maturity Model (C2M2). He has served as a C-level executive, security researcher, and incident responder across his career. He previously held the role of director of Cyber Risk for Dragos, Inc. Today, Jason is the senior vice president of Cybersecurity and Digital Transformation for Research and Innovation at Energy Impact Partners (EIP), a $4 billion global investment firm custom-built to invest in the energy transition. Jason has been invited to speak before the US Congress on several occasions.

Expert Corner

The 2025 SANS State of ICS/OT Security Survey rightfully highlights the increasing frequency of disruptive incidents to OT organizations despite these incidents going underreported in media and traditional sources. Practitioners in this space have long understood that when we look more we start to find more; threats have gone undetected for far too long and we've had more "near misses" in the community than we can afford in the future. Leveraging the SANS ICS Five Critical Controls is a great baseline for organizations to follow to enhance their security posture without overspending against the risk. Government leaders and policymakers, board of director members, and OT cybersecurity practitioners are chiefly aware that we have broadly underinvested in the portion of our businesses that generates revenue and where our local and national security interests reside. It is imperative to influence the mindsets outside of these circles and in the traditional enterprise IT security leaders to highlight the rapid and appropriate investments necessary to protect our communities.

Robert M. Lee
SANS Faculty Fellow

VIEW PROFILE

COURSES TAUGHT

ICS310: ICS Cybersecurity Foundations

ICS515: ICS Visibility, Detection, and Response

FOR578: Cyber Threat Intelligence

Introduction

Since 2017, the *SANS State of ICS/OT Security Survey* has tracked the practices, challenges, and progress of organizations securing critical infrastructure worldwide. Over nearly a decade, these annual benchmarks have documented how the industry has matured—from ad-hoc protection measures to more structured programs shaped by regulation, threat intelligence, and incident response lessons learned.

This year's survey, based on responses from 330 professionals across diverse industrial sectors, arrives at a pivotal moment. Threat activity against operational environments continues to rise, with ransomware, supply chain compromise, and nation-state alignment shaping the landscape. At the same time, regulatory mandates are expanding in scope and enforcement, requiring organizations to demonstrate not just compliance but resilience.

The report explores the state of ICS/OT security through three lenses: past trends, current practices, and future plans—offering practitioners, executives, and policymakers a clear view of progress, gaps, and the actions needed to build sustainable, resilient operations. See Figure 1 for the full demographics.

Figure 1. Demographics

2025 Trends: Increased Threats and Evolving Regulations

Historically, ICS/OT cybersecurity programs have responded to two major external factors: threats and regulations. As explored in previous years, the most mature organizations for industrial security leverage ICS-specific threat intelligence and standards. This year's data supports those findings, as organizations that leverage both continue to demonstrate quicker detection, containment, and remediation during a cybersecurity incident.

Industrial Cyber Incidents

Similar to previous years, 22% of respondents suffered a cybersecurity incident. Of those, a majority (50%) came from unauthorized external access and/or ransomware (38%). A full breakdown of threat actors can be found in Figure 2.

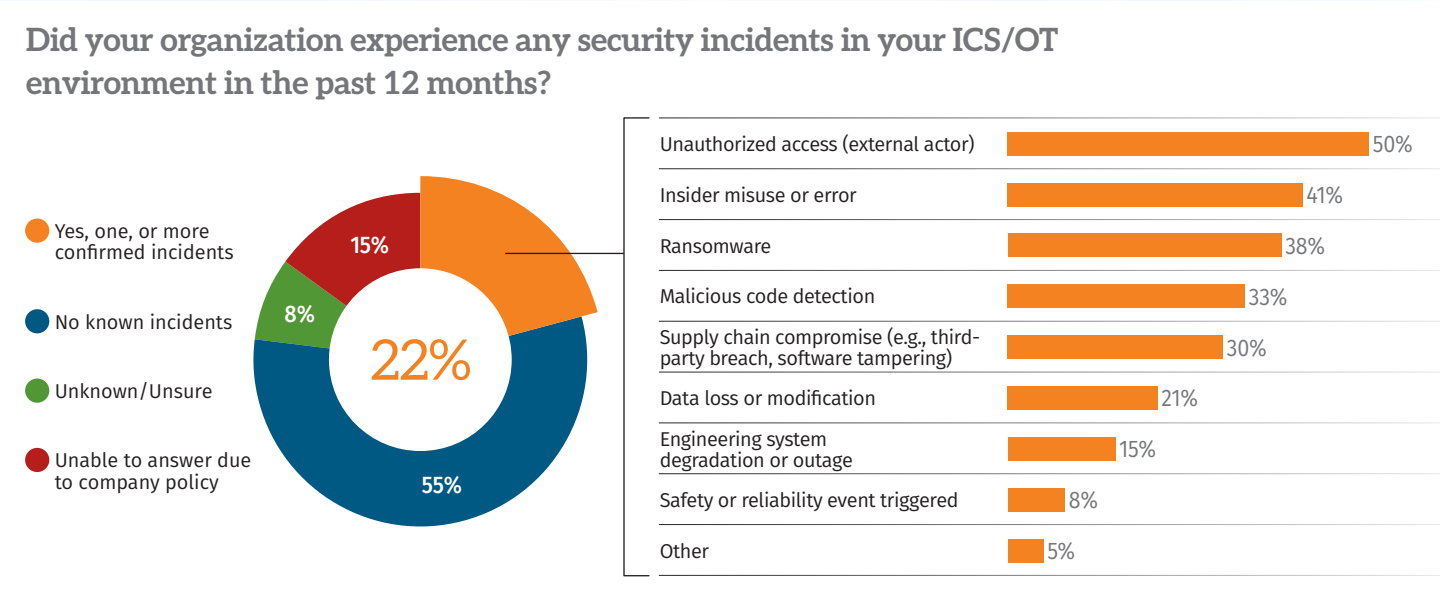

Figure 2. ICS/OT Security Incidents by Type

These incidents have real-world impacts, with 40% of incidents causing a disruption in ICS/OT operations, 13% resulting in financial losses or data compromise, 8% posing a risk to physical safety or reliability, and 6% involving the theft of intellectual property. Interestingly, regulated sites had roughly the same amount of ICS/OT incidents but both financial losses and risks to physical safety impacts were ~50% less than their unregulated peers.

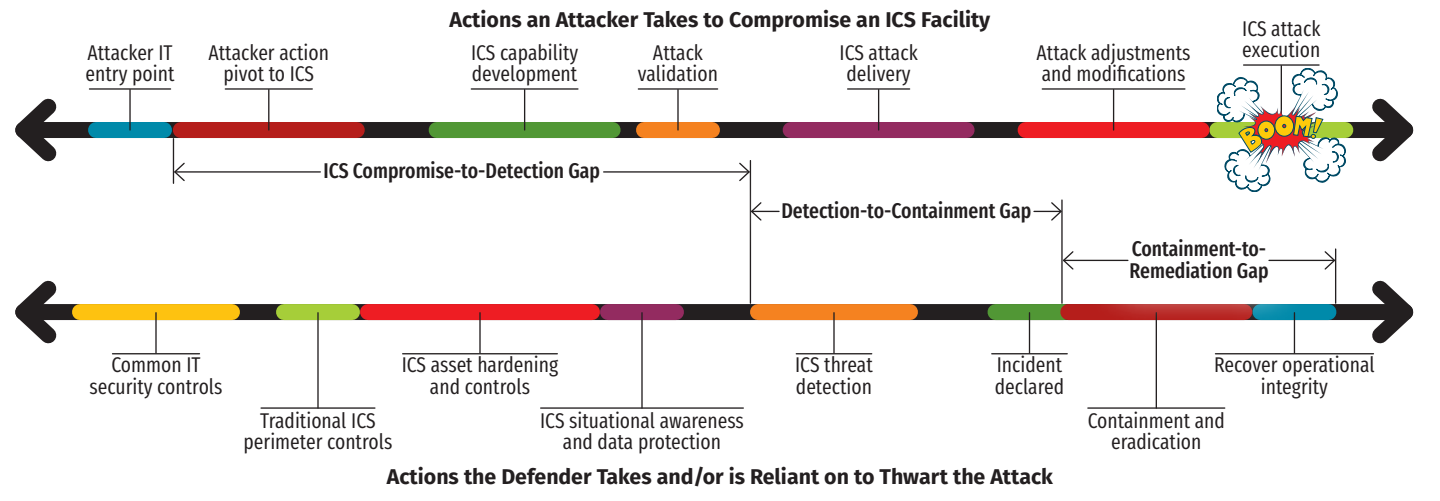

Figure 3. ICS Cyber Incident Timeline

As we teach across the SANS ICS curriculum, incident timelines can be broken into three distinct stages, as shown in Figure 3:

1. Compromise-to-detection
2. Detection-to-containment
3. Containment-to-remediation

The distributions for these timelines across the 2025 participants that suffered an ICS/OT cyber incident can be found in Figure 4.

Figure 4. ICS Cyber Incident Timeline Distributions for 2025

Two trends have maintained from previous years. First, industry continues to improve in detection times for ICS/OT incidents, with nearly 50% of incidents being detected within the first 24 hours. Second, we are similarly improving on containment, with over 65% of detection-to-containment gaps being addressed in the proceeding 24 hours. That means, on average, ICS/OT incidents are detected and contained within 48 hours.

That, however, is where the good news ends. Remediation, which includes the act of eradicating the threat and recovering operational integrity, still takes days to achieve, on average, with 22% taking two to seven days to recover. The risks here are real, with 19% of incidents in 2025 taking over a month to remediate (and a striking 3% taking over a year).

Preparation is still key to responding and recovering quickly during an industrial cyber incident. 57% of respondents have a dedicated ICS/OT incident response plan, a minor increase from previous years that represents further maturity across the industry. If an organization has both threat intelligence capabilities and is regulated, the coverage for ICS/OT-specific incident response plans jumps to 70%.

Without an ICS/OT-specific incident response plan, most organizations take up to a week just to detect an incident. Annual testing can cut that timeline down to hours.

Most organizations (39%) test their incident response plan annually. While this *decreased* from previous years, that is because we saw a sharp increase in the number of organizations that are now testing their incident response plan quarterly (25%). Interestingly, those that perform more regular incident response testing also have more variety in the ways they test, and they are far more likely to have operational drills, red and purple team exercises, and executive-level tabletops—ensuring a wide range of training and practical experience for responders. A full breakdown of testing methods can be found in Figure 5.

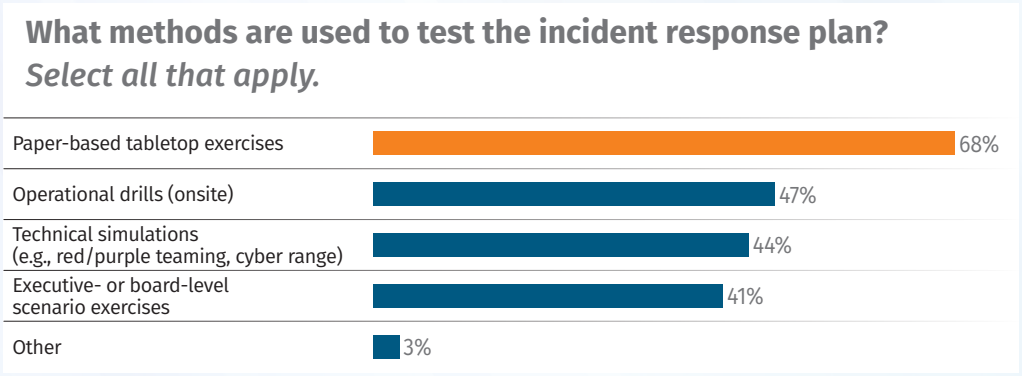

Figure 5. ICS/OT Incident Response Testing

Nearly 80% of respondents with incident response plans updated them in 2025. Beyond changes in the organization or technology used for incident response there were two major drivers for these updates: threat intelligence (41%) and regulatory changes or audit feedback (40%). This once again highlights how industrial cybersecurity is impacted by both external forces.

ICS/OT-Specific Threats, Intelligence, and Information Sharing

Starting with threat intelligence, 67% of respondents leverage threat intelligence in some capacity, with an additional 16% planning to use it over the next year. The majority (79%) of threat intelligence programs for ICS/OT environments are built on vendor-provided intelligence feeds, with government and public reporting sources coming in at a close second (77%) along with peers or industry information sharing and analysis centers (ISACs) (72%).

On ISACs in particular, there is room for improvement across industrial sectors with only a minority (22%) of participants actively contributing information and a third (34%) primarily consuming information without additional collaboration. For programs that rely heavily on ISACs or peer information sharing, there may be a false sense of security regarding the sample size of peers providing threat and vulnerability data.

That said, respondents that participate in information sharing activities noted clear benefits and measurable value for these activities, as seen in Figure 6.

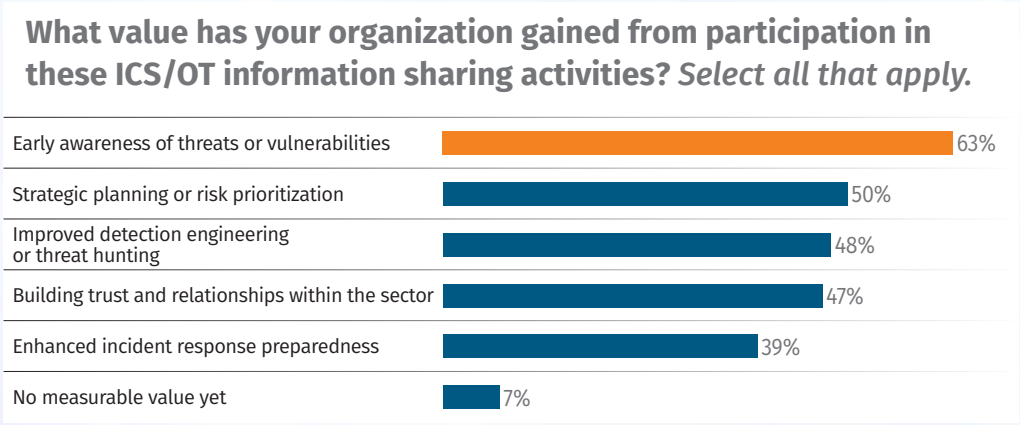

Figure 6. Observed Value of ICS/OT Information Sharing

Although threat intelligence and information sharing are separate activities, they both add to how industrial organizations categorize and monitor threats and, as mentioned, adapt their incident response capabilities. Based on these activities, respondents have seen an increase in ransomware targeting OT environments (64%), nation-state-aligned threats (57%) and supply chain compromises (52%) over the past year.

Similar to incident response, these threat trends further inform defensive priorities, as seen in Figure 7, where some clear benefits to increasing asset monitoring (53%) or accelerating segmentation or architecture improvements (49%) were a direct result of threat intelligence.

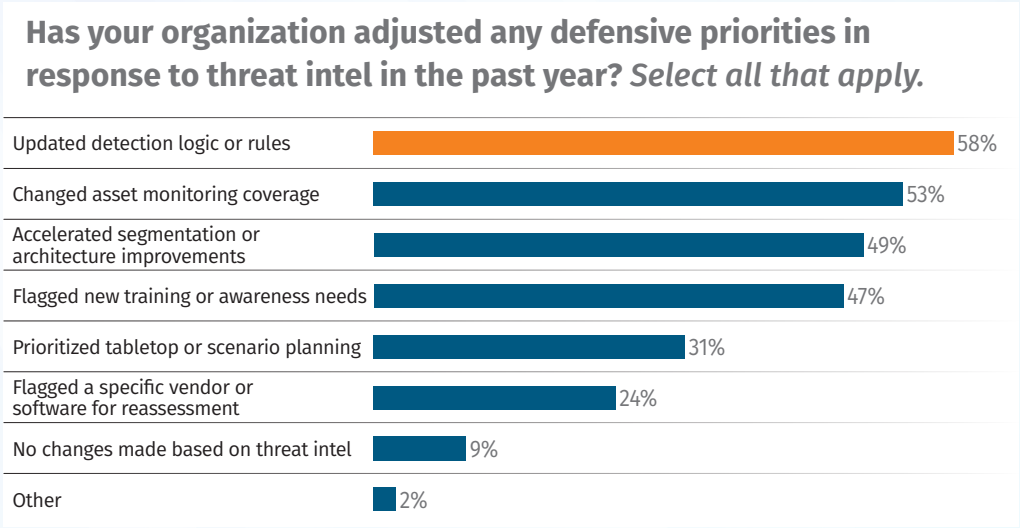

Figure 7. Threat-Informed Defensive Priorities

ICS-Specific Security Regulations

Across the SANS ICS curriculum, we have noted the increase in ICS/OT cybersecurity-specific regulations over the past few years.[1] It therefore came as no surprise that 58% of respondents reported having at least one facility subject to mandatory cybersecurity compliance requirements. Of that group, 26% reported having a possible violation from an audit or self-report. Smaller compliance programs (fewer than 10 facilities in scope) were mostly impacted, accounting for nearly 40% of those possible violations, indicating a possible need for additional resources in those environments.

Similar to threat intelligence, these compliance programs have direct impact on investment priorities for industrial organizations, as seen in Figure 8.

Regulations have had some clear benefits to programmatic improvement, including executive-level visibility and capabilities being prioritized. Although there are some pain points around evidence collection, many of these priorities are widely considered to be beneficial to overall ICS/OT cybersecurity.

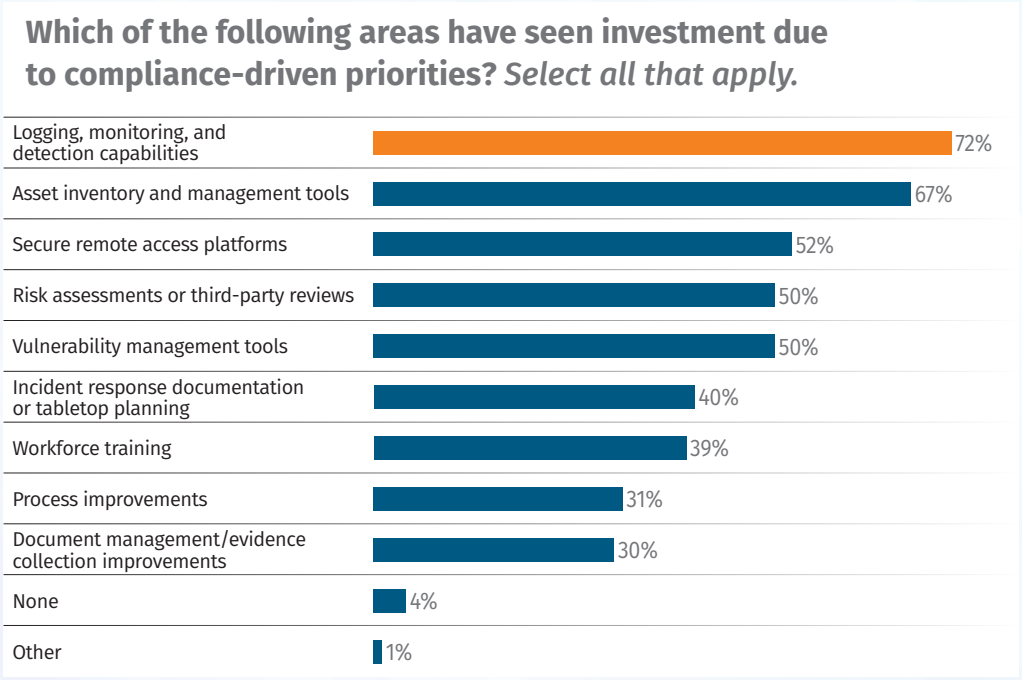

Figure 8. Compliance-Driven Investment Priorities

Detecting Today's Threats and Managing Vulnerabilities

Detection capabilities were a common theme across the 2025 data. They are the No. 1 prioritized response for threat intelligence (58% of respondents update threat detections based on intel) and compliance programs (72% have increased investment in logging, monitoring, and detection due to regulations). Increased detection also leads to improved incident response metrics.

The 2025 State of ICS/OT Security Survey highlights the old phrase "protection is ideal, detection is a must."

Only one in eight organizations report full ICS Kill Chain visibility—but those that achieve it almost always run a SOC with IT and OT sharing detection tools.

[1] A more in-depth breakdown can be found in our 2023 SANS ICS Summit presentations: www.youtube.com/watch?v=3mhkEJ9QrL4

Unfortunately, there is a lot of improvement required to improve on ICS/OT detection and its relationship to threats and real-world incidents. When asked, only 13% of respondents reported having full visibility across the ICS Cyber Kill Chain with a clear majority (42%) reporting partial visibility with major gaps.[2] The remaining 31% reported minimal or no alignment across IT and ICS/OT environments to provide visibility across the entire kill chain (from initial access to ICS/OT impacts).

Compounding this issue, only 49% of respondents have ICS/OT-specific detection with significant gaps in capabilities as seen in Figure 9. Of those with detection, only 26% describe their capabilities as "highly effective" in identifying ICS-relevant threats with a majority (53%) describing their detection program as "moderately effective," highlighting areas for improvement both in terms of coverage and actionability with their current investments.

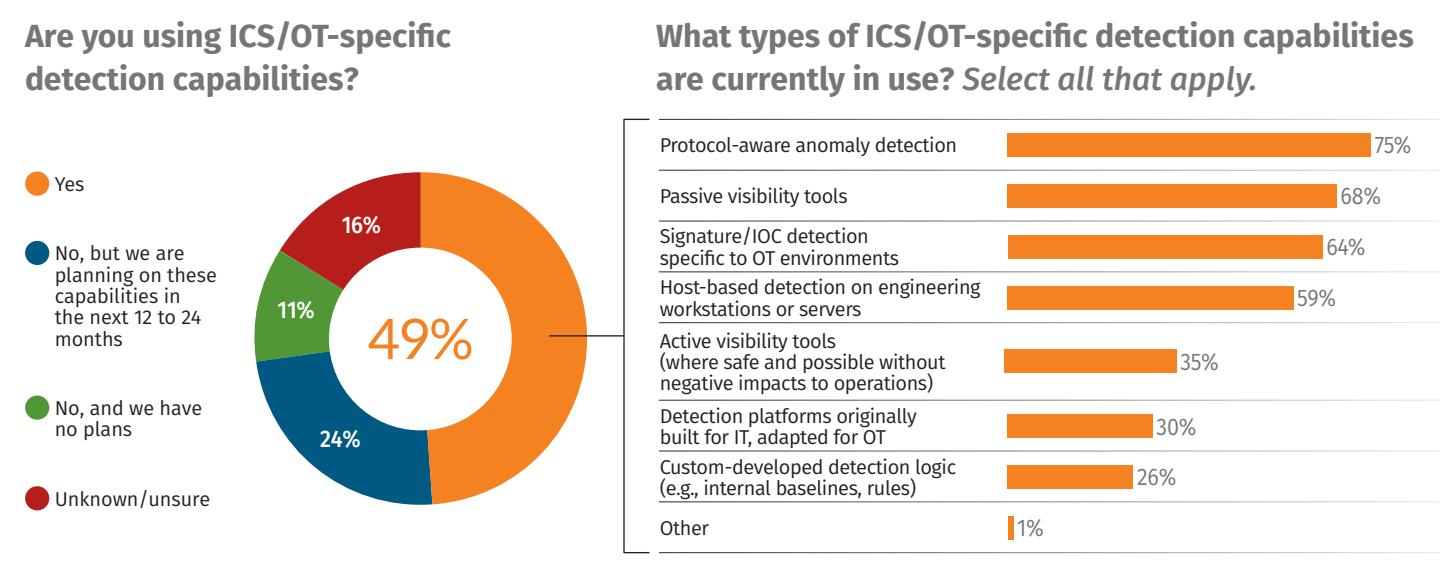

Figure 9. ICS/OT Detection Capabilities

Organizations that have achieved some level of visibility across the ICS Cyber Kill Chain largely do so through coordinated, but separate, IT and OT teams with shared log aggregation and correlation tools, as seen in Figure 10.

Although a security operations center (SOC) is not necessary for visibility, most organizations find the constructs useful for aligning capabilities. A majority (57%) of respondents either have a single IT-OT SOC or a parallel OT-specific SOC, with another 23% performing centralized monitoring without a SOC.

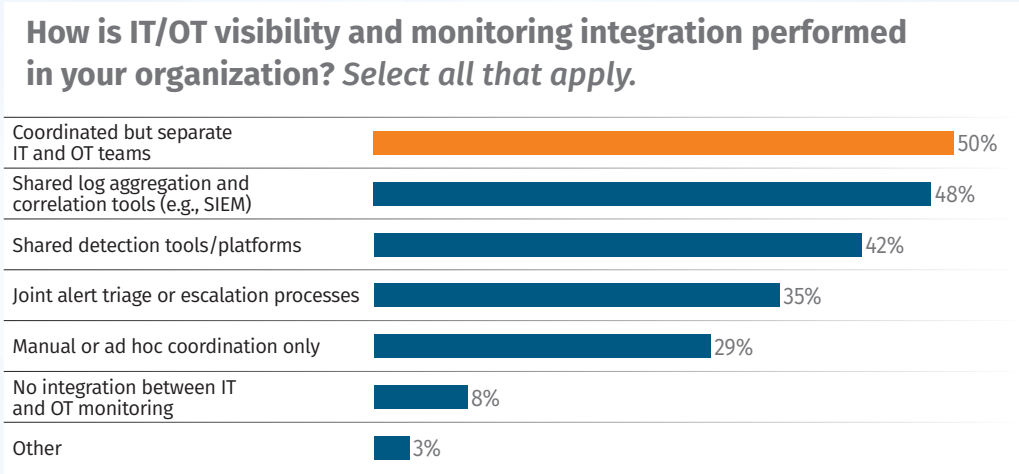

Figure 10. Integration of IT and OT Visibility

[2] More information about the Industrial Control System Cyber Kill Chain can be found at www.sans.org/white-papers/36297

Cloud and Secure Remote Access

As previously explored, 50% of incidents reported in the 2025 survey originated from unauthorized external access. External access can come in many forms, and cloud access, in particular, has certainly become an increasing part of everyday life for industrial operations. Only 17% of respondents reported no cloud usage in their ICS/OT environments or IT networks, meaning 83% of respondents need to actively integrate cloud visibility to monitor for threats. As seen in Figure 11, there are some coverage concerns as only 13% reported fully integrated visibility and cloud monitoring for ICS/OT or IT networks. The majority (58%) report gaps or minimal coverage for cloud, which may have direct and persistent access to the ICS/OT network.

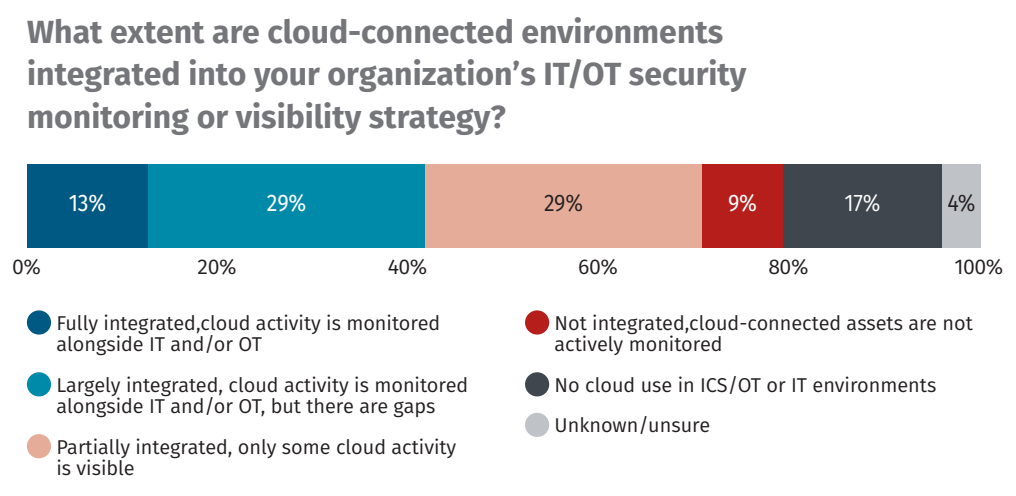

Figure 11. Cloud Monitoring Across IT/OT Networks

When monitoring of the cloud environment is performed, there is no clear "winner" regarding capabilities, as outlined in Figure 12, with cloud-native logging or telemetry as the most popular solution (46%) and dedicated third-party monitoring tools

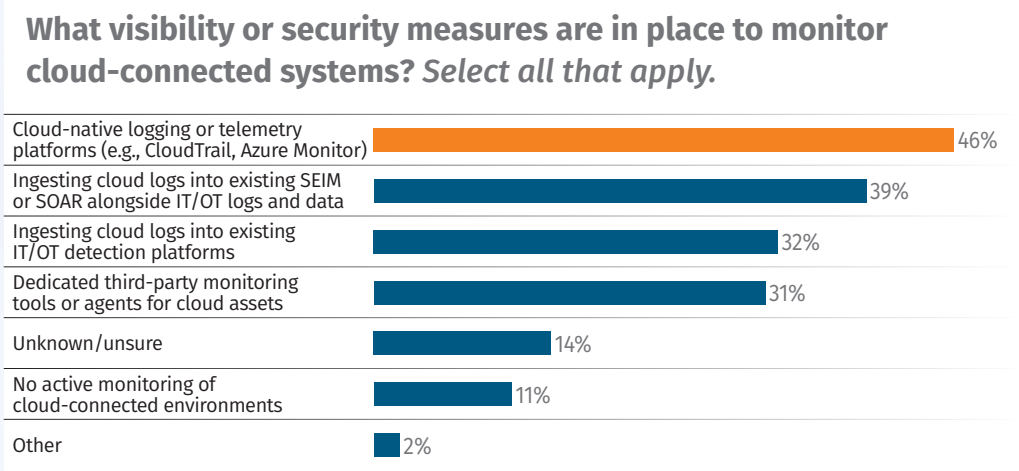

Figure 12. Cloud Monitoring Capabilities

and agents the least (31%).

Secure remote access continues to be a challenge for ICS/OT environments. Although industry has improved with multifactor authentication (MFA), there are still plenty of coverage gaps and capabilities missing in standard

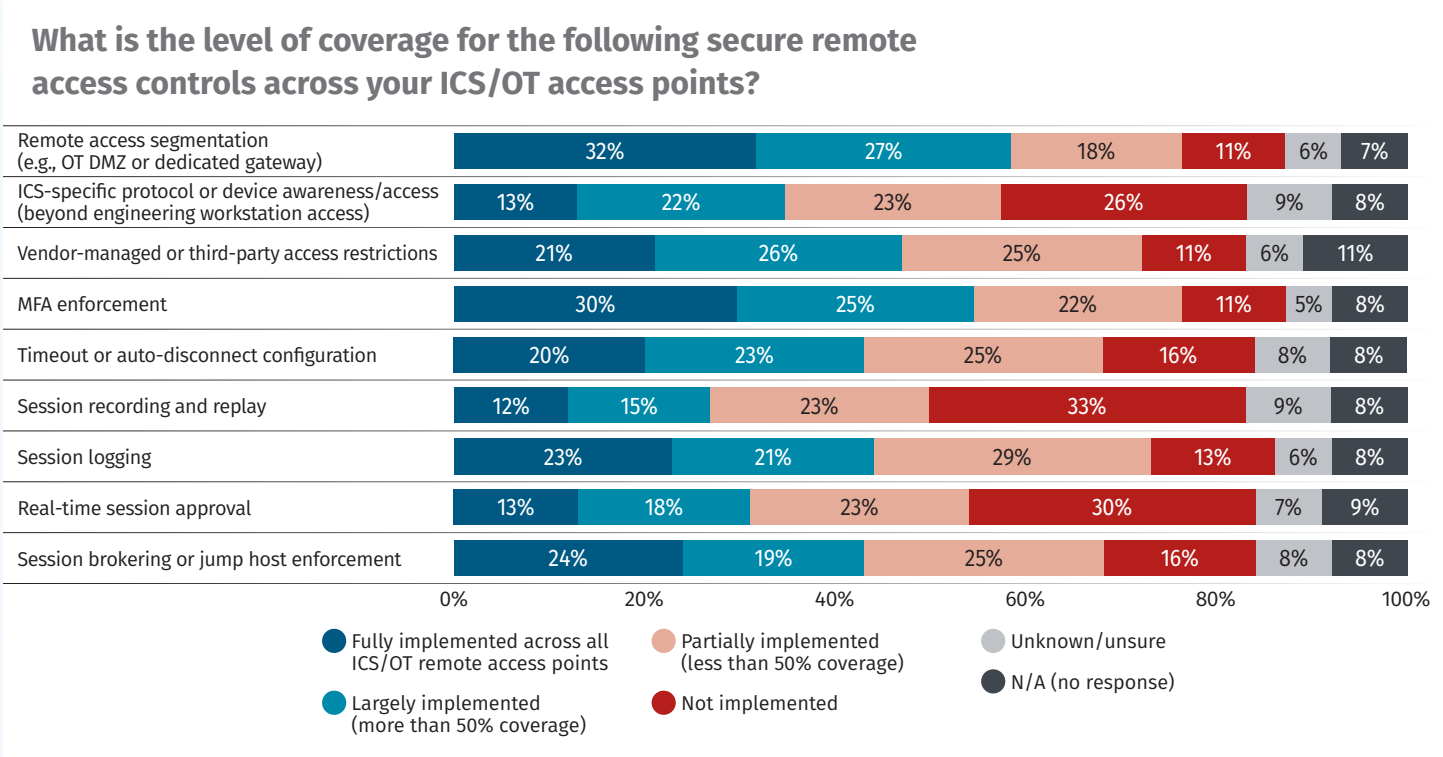

Figure 13. ICS/OT Secure Remote Access Capabilities

Standard practices, like remote access segmentation, MFA, and vendor-managed/third-party access restrictions, are all fairly high in level of implementation. These capabilities are all drastically increased when looking at regulated sites, where there are common secure remote access mandatory compliance obligations. There are still plenty of industrial environments, however, that may benefit from exploring ICS-specific protocol or device awareness/access, session recording and replay, and real-time session approvals, which were all reported as "fully implemented" by 13% or less across the 2025 survey respondents. Considering the high degree of real-world incidents stemming from

Half of 2025 incidents began with external access. Yet fewer than 15% of organizations have advanced remote access controls in place. This remains the weakest link.

remote access, these capabilities may benefit many industrial organizations as they plan for increased cyber defenses.

When asked what is preventing organizations from achieving full implementation of secure remote access controls across ICS/OT environments, the top blocker was lack of internal resources (60%), followed by legacy system compatibility limitations (46%), as reported in Figure 14.

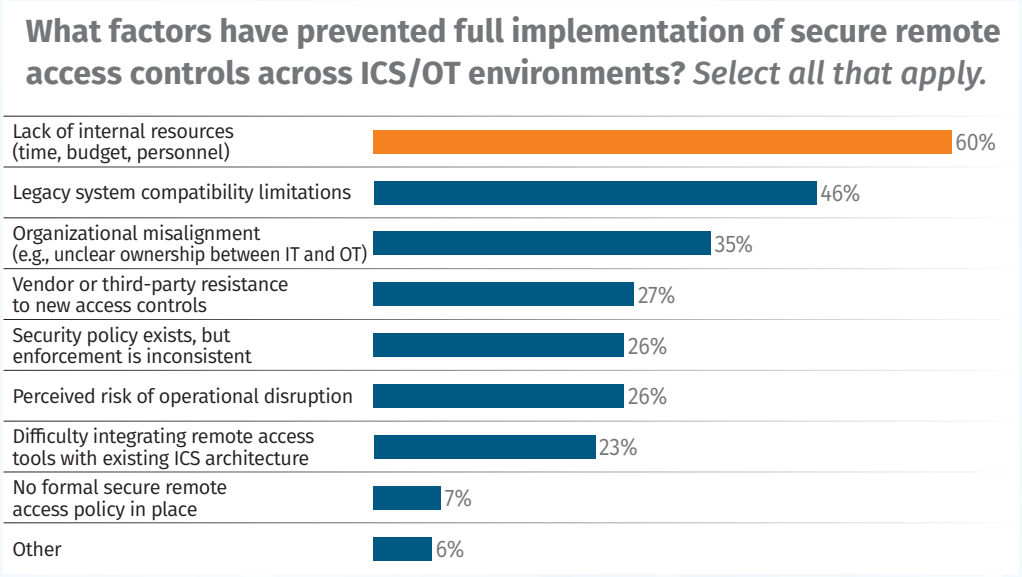

Figure 14. ICS/OT Secure Remote Access Blockers

Combined with the fact that roughly one-third (31%) of respondents have no formal centralized inventory—or no inventory at all—of active ICS/OT remote access points, there is an obvious divide between the "haves" and the "have-nots" in the world of secure remote access for industrial environments. As threats evolve and real-world incidents continue to target these assets, many organizations should prioritize these capabilities and provide adequate resources for teams requiring remote access.

Planning for Tomorrow's Cyber Risks

Further examining industrial organizations and threat intelligence, it is apparent that ICS/OT cybersecurity professionals believe, by wide margins (as shown in Figure 15), that industrial systems are more likely to be targeted than in previous years.

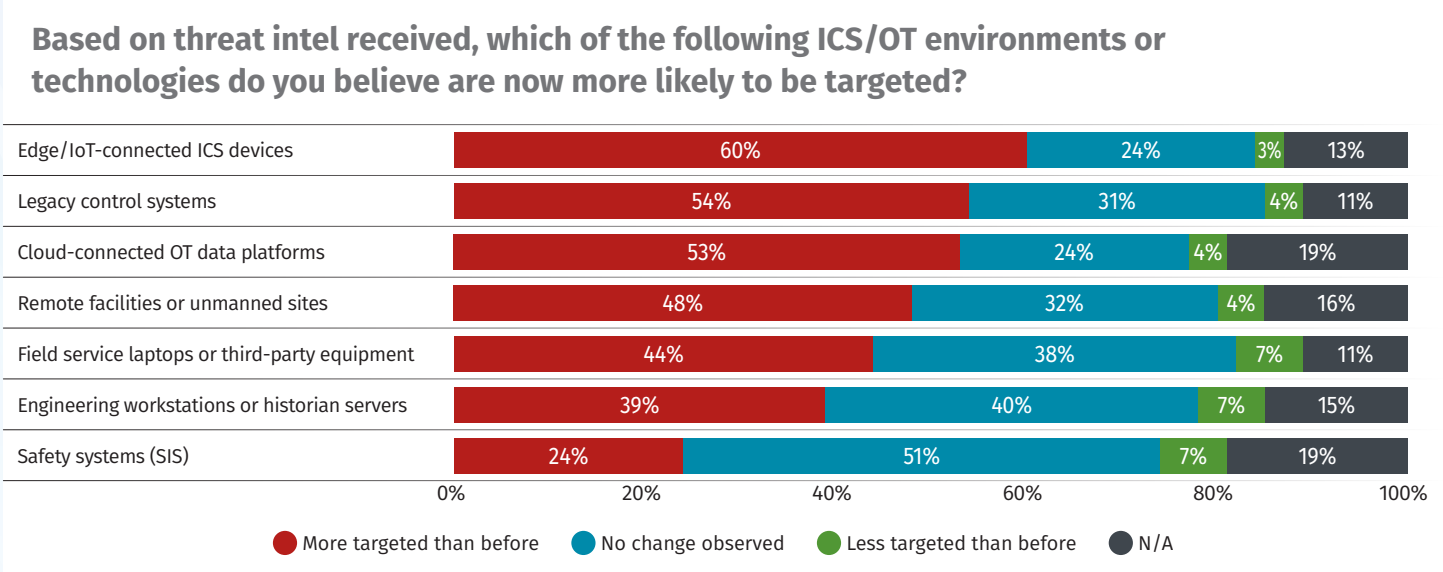

Figure 15. Threat-Focused ICS/OT Targets

Exploring future threat scenarios can be challenging, but a majority (60%) of respondents base their preparedness on industry threat intelligence and reports, followed by real-world incidents (54% of respondents). Unsurprisingly, as seen in Figure 16, the most popular scenario is ransomware targeting OT environments with 72% of respondents having considered the impacts as part of their planning or preparedness exercises.

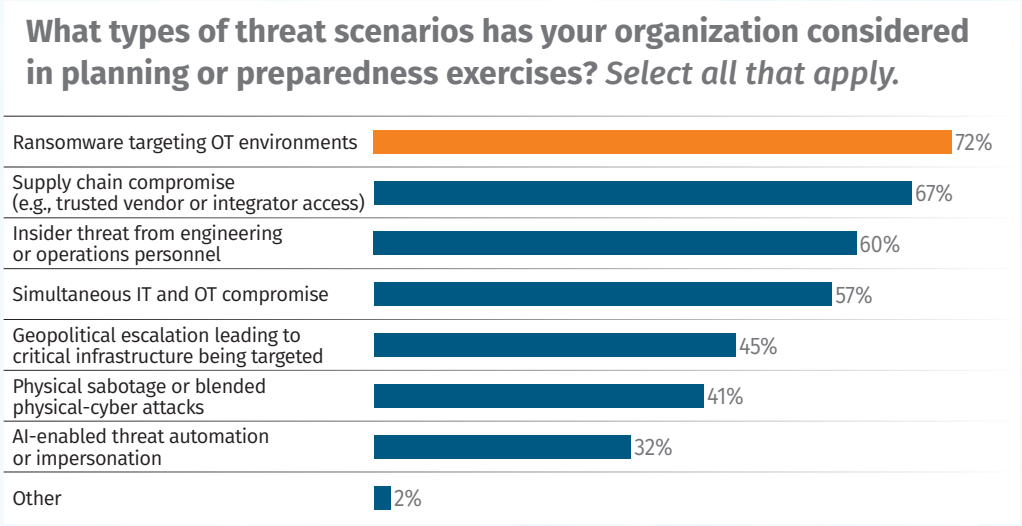

Figure 16. Cyber Threat Scenarios Used for Planning and Preparedness

Combined with the previously reported trend on increased threat information regarding ICS/OT targets, it is apparent that threat capabilities and targeting efforts have continued to grow across industrial environments. Unfortunately, when asked how prepared organizations are to respond to future threats, only 14% felt that they were fully prepared for a range of plausible and emerging threats. As seen in Figure 17, respondents are clearly divided between feeling fully or largely prepared (47%) and partially or not prepared (46%).

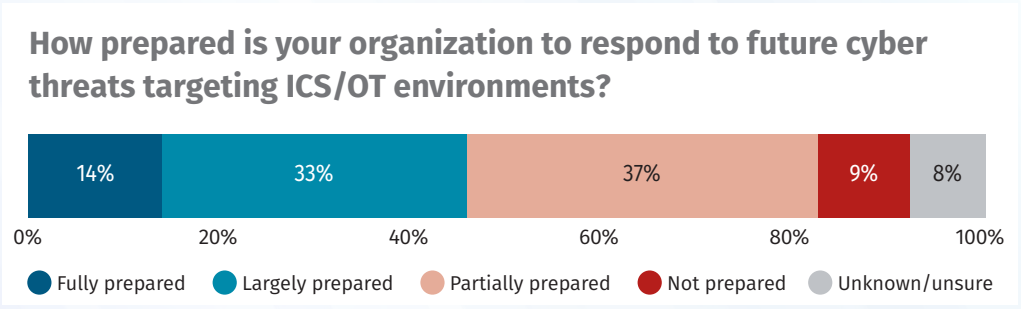

Figure 17. Perspective on Future Cyber Threats and Preparedness

Expert Corner

The data proves what ICS/OT cybersecurity defenders and engineering staff know about protecting our critical infrastructure: Engineering-informed cyber preparedness cannot be siloed. It must extend across the entire plant floor and engineering operations. Involving field technicians, engineers, and operators in ICS/OT tabletop exercises and industrial incident response planning nearly doubles the likelihood that an organization with ICS/OT is ready to face emerging threats that can directly impact safety. That's no coincidence. Those closest to the control loops, HMIs, and PLCs understand better than anyone how cyber incidents ripple into safety, reliability, and process integrity. By embedding engineering staff and having them lead the way into ICS/OT cybersecurity exercises, ICS/OT organizations and critical infrastructure operations transform preparedness from a compliance checkbox into a true resilience capability. One that protects the operational environment as well as continuity and human safety. After all, in an organization that has ICS/OT, the ICS/OT is the business.

VIEW PROFILE

Dean Parsons
SANS Principal Instructor

COURSES TAUGHT

ICS418: ICS Security Essentials for Leaders

ICS515: ICS Visibility, Detection, and Response

Cyber preparedness requires collaboration across multiple stakeholders ranging from executives to managers to external partners. When asked which groups were involved in tabletops, after action reporting, or other threat-aware activities to specific ICS/OT cyber risks, respondents largely deferred to ICS/OT security teams, enterprise IT, and engineers/operators, as seen in Figure 18.

Those organizations that felt "fully prepared" shared unique characteristics, including being 66% more likely to include field technicians in their preparedness exercises. They also were almost four times more likely to have full visibility across the ICS Cyber Kill Chain and maintained more secure remote access controls. Another notable difference is that a majority (57%) of these organizations actively contribute to information sharing.

Which group of stakeholders is involved in tabletops, after action reporting, or other threat-aware activities specific to ICS/OT cybersecurity? ***Select all that apply.***

Figure 18. Stakeholders Involved in ICS/OT Cyber Preparedness Activities

ICS/OT Threat Hunting and Red/Purple Exercises

As previously discussed, tabletops and specific ICS/OT cybersecurity scenarios are valuable preparedness tools when examining future threats. However, on the more technical end of the spectrum, organizations should also consider ICS/OT threat hunts and red (or purple) team exercises.

Do you want to boost preparedness? Involve field technicians. Fully prepared organizations were seven times more likely to engage them in exercises than their peers.

ICS/OT threat hunting is a proactive, hypothesis-driven search for stealthy adversary activity or unsafe changes in industrial environments. Analysts pivot through ICS-specific evidence, such as PLC/HMI logs, historian data, engineering-workstation activity, and protocol captures (e.g., Modbus, DNP3), all under strict safety and change control. Complementing this, ICS/OT red teams safely emulate real-world attacker paths from IT to OT to test segmentation, remote access, and response. This can be done under safe conditions at production sites, but is often conducted in a lab, digital twin, or tightly controlled window to avoid process impact. Purple teaming adds a collaborative loop: Red teams and defenders iterate in real time to tune detections, playbooks, and monitoring for ICS-specific behaviors.

Although generally considered a mature set of practices, many organizations can benefit from the technical information (and after-action items) that come from a completed threat hunt or red/purple team exercise. Unfortunately, as seen in Figure 19, only one in five respondents reported performing either preparedness activity.

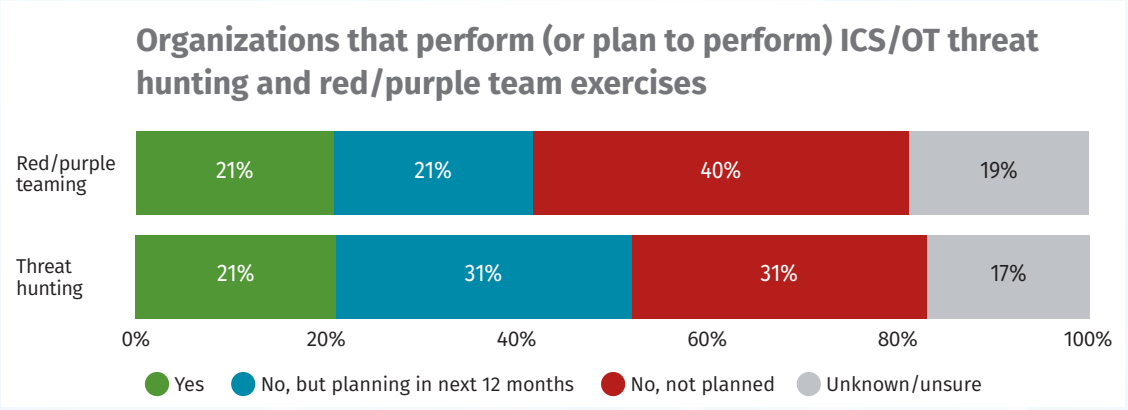

Figure 19. Preparedness Activities Performed or Planned

Again, the organizations that identified themselves as being fully prepared for future cyber threats are at the top end for either, with over 55% performing ICS/OT threat hunts today and nearly half (48%) performing red or purple team exercises.

By the Levels: Detection and Proactive Capabilities in the Purdue Model

In the 2025 survey, we wanted to further explore how mature certain capabilities were across the Purdue Model,[3] namely:

- ICS/OT-specific detection
- Risk-based vulnerability management
- ICS/OT threat hunting
- Safety-minded penetration testing (red/purple team exercises)

To do so, we asked about coverage across each. For example, if ICS/OT-specific detection was in place, what was the degree of visibility across each level of the Purdue Model?

A comprehensive breakdown can be found in Figure 20 (seen on the next page) and the data provides some insights into the gaps across ICS/OT security programs. For example, while 49% of respondents reported having ICS/OT-specific detection capabilities, most do not have full visibility across their environments. Only 20% report full visibility at Level 3, which drops in half to 10% for Level 2. Remote sites similarly lack in any significant level of visibility with 18% reporting visibility as largely or fully covered by their ICS/OT visibility program.

[3] A more complete discussion of the Purdue Model can be found in the Appendix.

And detection is, by far, the most mature capability discussed in this year's survey. Vulnerability management has moderate coverage across the higher levels of the Purdue Model, with threat hunting and penetration testing barely peaking above 20% of respondents in *any* level as partially covered or better.

When revisiting real-world incidents, increased threats, and evolving regulations across ICS/OT the message is clear: Our industry needs to bridge gaps across our programs and critical sites to meet tomorrow's challenges.

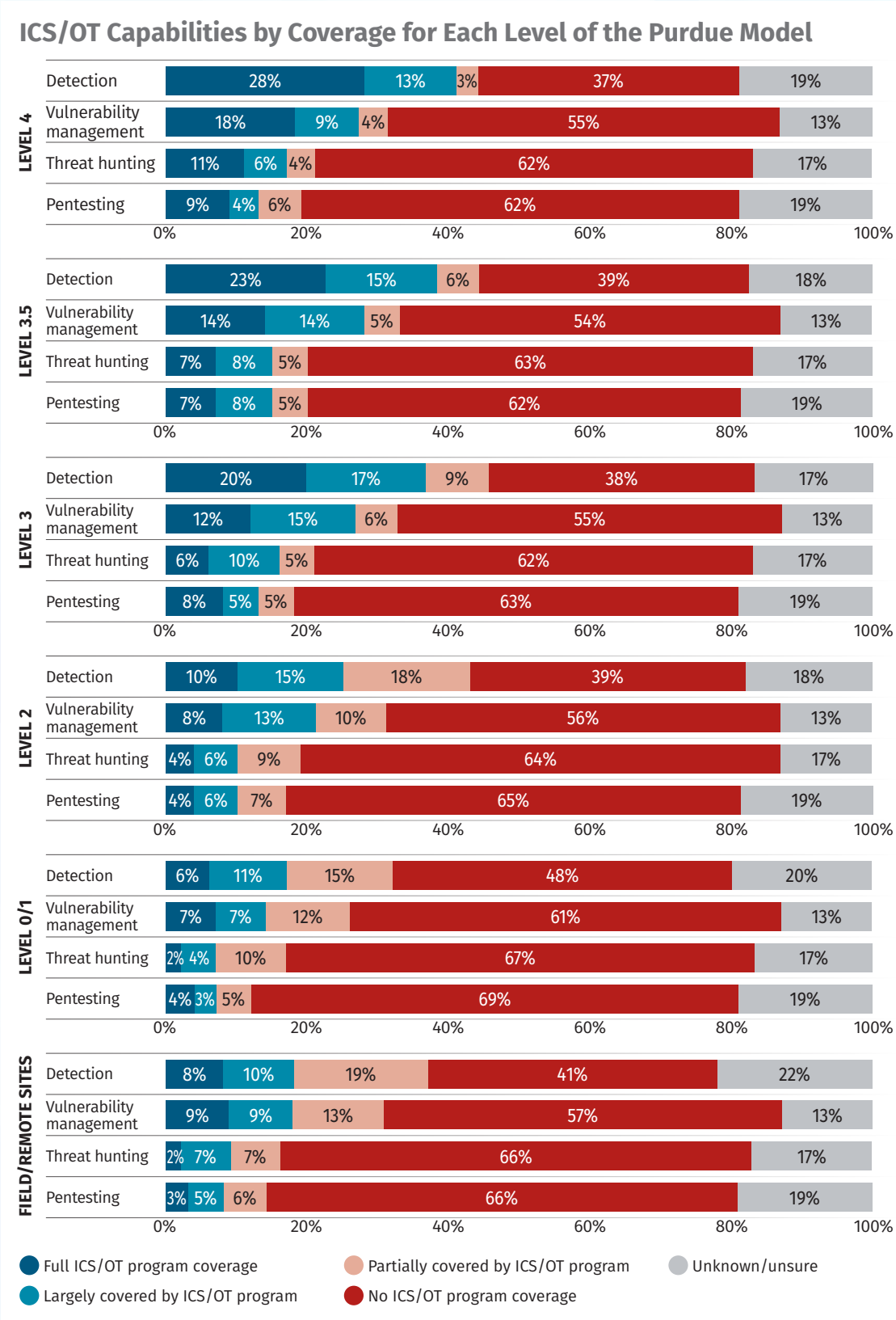

Figure 20. ICS/OT Capabilities by Coverage for Each Level of the Purdue Model

Cyber Resilience, Business Continuity, and Disaster Recovery Planning

Cyber resilience, like other aspects of risk management, must be incorporated into broader enterprise-level efforts to be successful. This should include areas that industrial organizations have clear strengths in—namely business continuity and disaster recovery (BC/DR) planning. While typically relegated to natural disasters, supply chain risks, or other reliability and operational concerns, cybersecurity should be a key element in both disaster recovery and business continuity planning. As seen in Figure 21, less than 10% describe cybersecurity as being fully integrated into enterprise-wide BC/DR planning—and nearly half (50%) describe it as partially or not integrated at all.

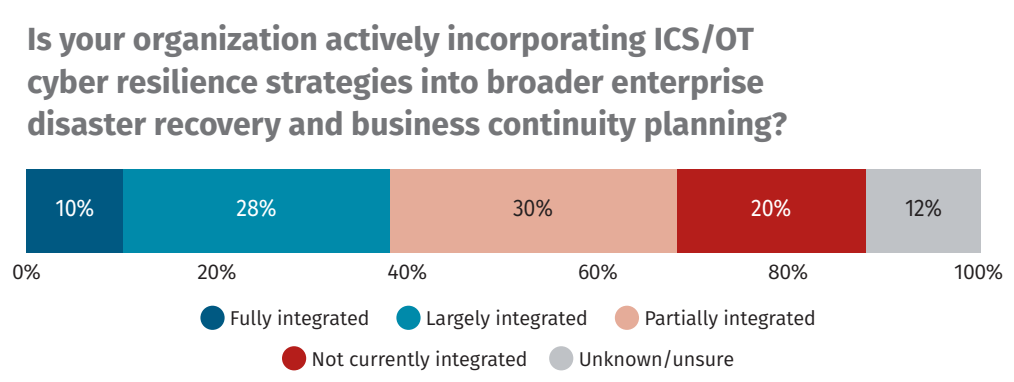

Figure 21. Cybersecurity Integration into BC/DR Planning

Business continuity and disaster recovery planning for ICS/OT usually defaults to backups, as seen in Figure 22. However, BC/DR is a full chain from knowing what matters to how fast you must recover to practicing recovery safely. Most organizations have the technical safety net in place: OT-specific backups/failover are common (66%), and about half have done the homework to integrate OT into enterprise business-impact analysis (53%) and to define recovery time and point objectives (RTO/RPO) (52%). Where resilience thins is in execution: Only one-third test or simulate OT-specific recovery, and 31% keep site-level playbooks for cyber events—both crucial to proving recoverability. More advanced, risk-focused practices such as cyber-informed engineering (CIE/CCE) (29%) and aligning OT cyber risks with safety assessments (e.g., HAZOP, PHA, or similar) (23%) are still emerging. Notably, 9% report no OT-specific resilience planning, underscoring a maturity gap between documented intent and exercised capability.

Figure 22. BC/DR Activities and ICS/OT Cybersecurity

Testing of these ICS/OT specific resilience plans (e.g., recovery, failover, engineering rebuilds, etc.) is also uncommon, with only 32% testing annually with either a tabletop or hands-on validation. Although there is a small population (9%) that only tests after an incident or "near-miss," a larger cohort (16%) admit to never formally testing their resilience plans.

Technology Deployments: Past, Present, and Future

Cyber preparedness for industrial environments requires a careful alignment across business processes, technology deployment, and workforce skill and culture. While many ICS/OT systems measure life cycles in *decades*, not years, the combination of cyber threats and new regulations and standards requires ICS/OT professionals to constantly adapt to changes.

Over the last year, industrial organizations invested in a variety of new technologies, as seen in Figure 23. The top areas, asset inventory and visibility (50%) and secure remote access with MFA (45%), align with the threats and real-world incidents that were reported, along with increased segmentation (32%). Other categories, like ICS-specific tabletop exercises (17%) and threat intelligence integration (21%) were low, which correlates with previous topics and highlights a need for increased investment in these areas as they each have a demonstrable impact on incident response detection, containment, and remediation timelines. ICS/OT-specific security orchestration, automation, and response (SOAR) was the lowest area of technology investment (12%). This trend remained true regardless of preparedness, regulations, or if the organization had a SOC (where SOAR may provide tangible benefits).

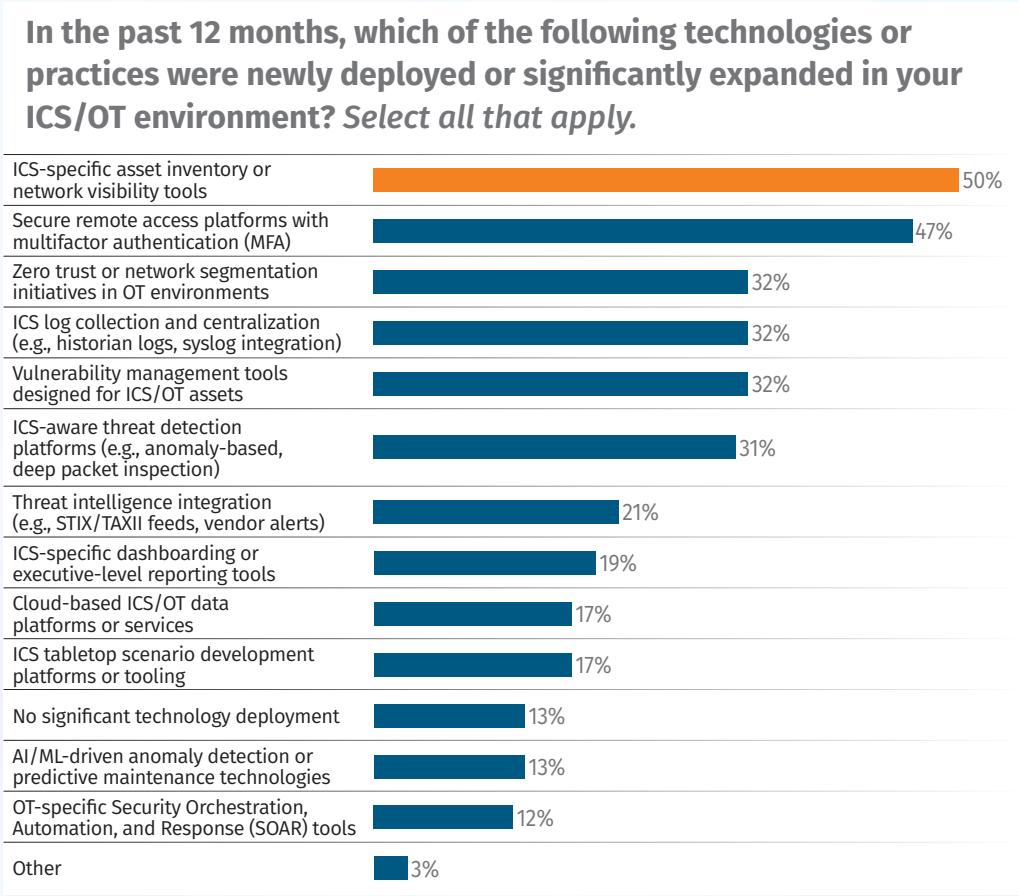

Figure 23. Technology Deployments Over the Previous 12 Months

Organizations that suffered an incident in 2025 invested heavily in response tools—after the fact. Don't wait for a breach to justify the budget.

To help organizations with ICS/OT cybersecurity roadmaps and associated metrics, the 2025 survey also included future-looking technology deployments to examine what investments industrial sectors will deploy over the next 12 to 24 months, as seen in Figure 24.

Heading into 2026–2027, organizations will continue to invest heavily in asset inventory and visibility (54%) and secure remote access (40%) as they did over the past 12 months. However, threat detection (43%) and vulnerability management (41%) also round out the top investments—at a higher rate than 2025 deployments.

Which of the following are top investment priorities for your ICS/OT cybersecurity program in the next 12 to 24 months? *Select all that apply.*

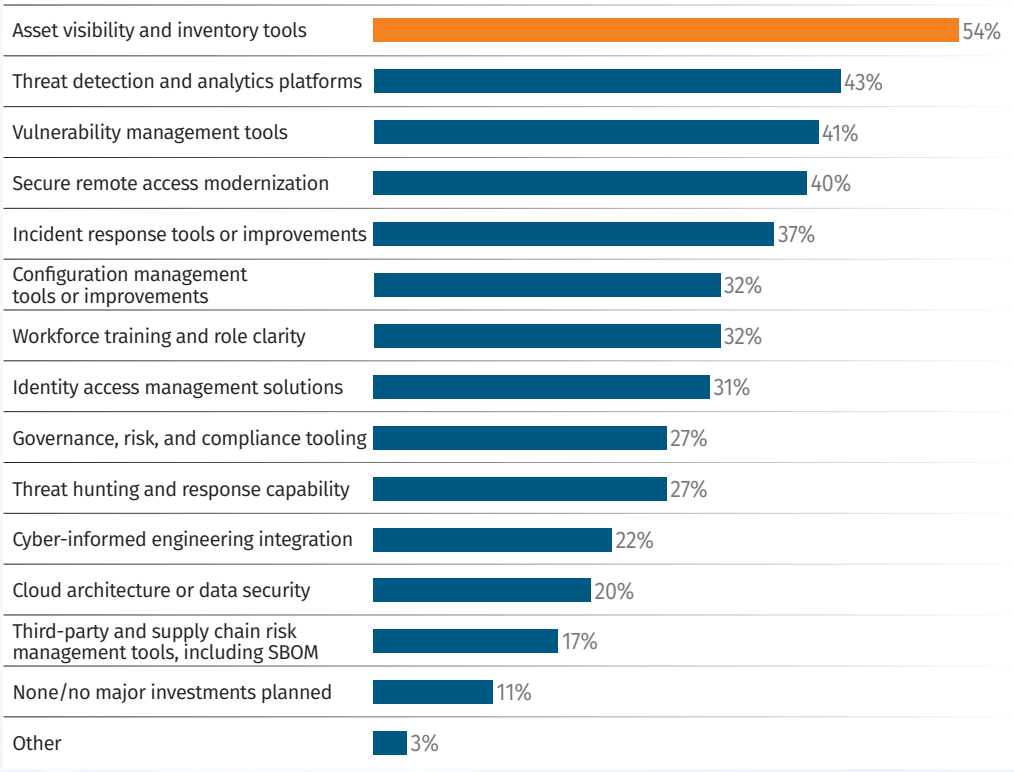

Figure 24. Technology Investments Over the Next 12–24 Months

There are several factors that influence what technologies industrial organizations invest in. For example (and unsurprisingly), regulated facilities track higher in every category for both past and future technology deployments. As a matter of fact, both regulatory requirements and threat landscape were listed as the top drivers for technology deployments (both at 61%, as seen in Figure 25). However, the most significant determining factor and unique profile for investment came from industrial organizations with SOCs that include ICS/OT in some fashion—those organizations are more likely to have invested (and continue to invest) in asset visibility (63% in 2025 *and* 2026–2027), threat detection (47% in 2025 compared to 32% for organizations without a SOC), and log collection/centralization (43% in 2025 compared to 32% for their non-SOC peers).

What factors have driven the technology deployments or expansions you selected above? *Select all that apply.*

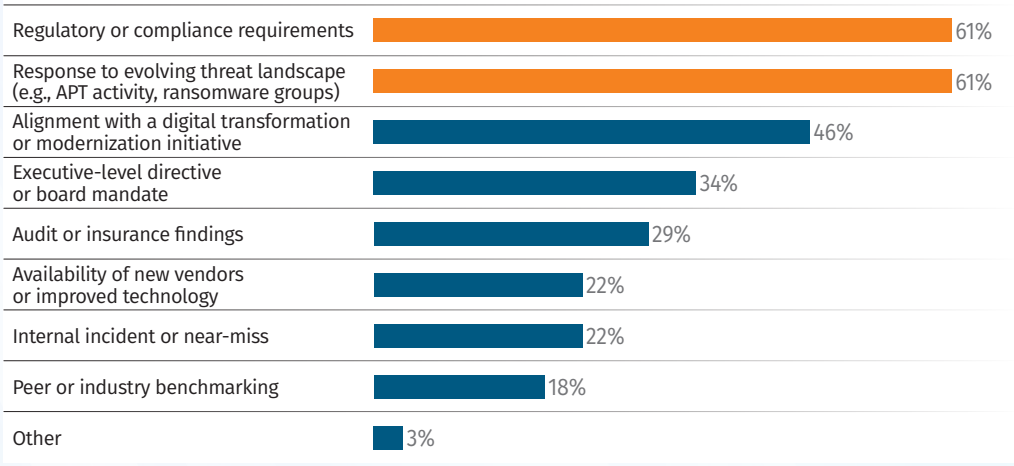

Figure 25. Technology Deployment Drivers

Organizations that previously identified themselves as fully prepared for future cyber threats also invested in technology differently from their peers, likely because they already had heavy capabilities in threat detection and secure remote access. In 2025, these organizations invested more in threat intel integration (43%), log centralization (40%), and vulnerability management (40%). For the next 12–24 months, these prepared organizations plan to continue to invest heavily in asset visibility (66%) and threat detection (55%), while adding configuration management (55%) to the top three categories.

The greatest shift in technology investment comes from organizations with ICS/OT SOC capabilities, who invest more in asset visibility, threat detection, and log centralization compared to their peers.

Despite this growth, our industry still lacks meaningful discussion on metrics and measuring success and effectiveness across ICS/OT technology deployments. Only 16% of respondents provide financial metrics and one in five (21%) respondents reported that they do not have any measures for success, though planning may be underway for some. Figure 26 highlights the most popular metrics as risk reduction, compliance/audit-readiness, and operational key performance indicators (KPIs).

Although cultural metrics (workforce change management, adoption rates, and similar) were relatively low (21%), ICS/OT practitioners believe that our industry is getting better at culture with a majority (62%) reporting that culture is either strong or improving, as seen in Figure 27.

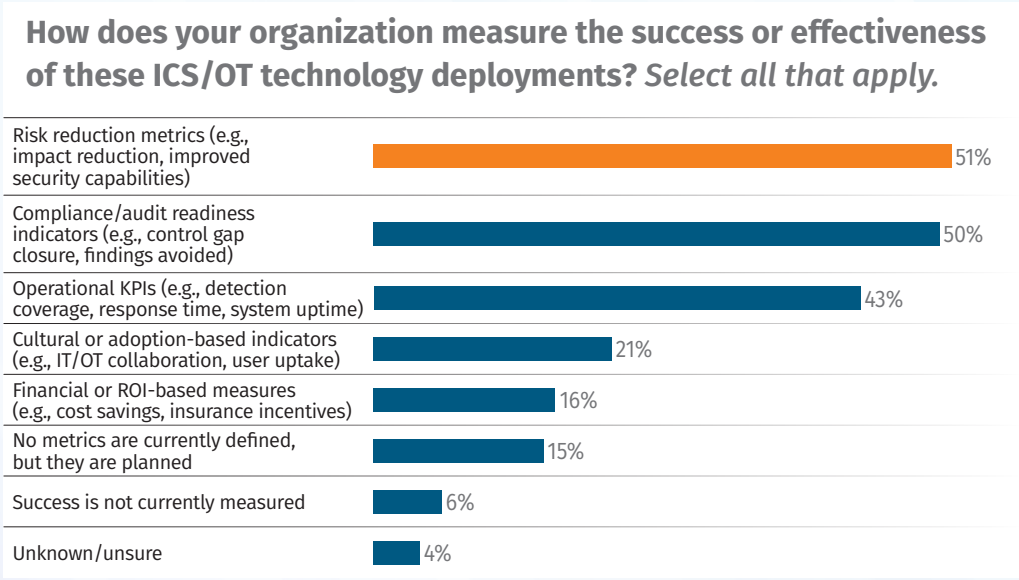

Figure 26. Technology Deployment Success and Effectiveness Metrics

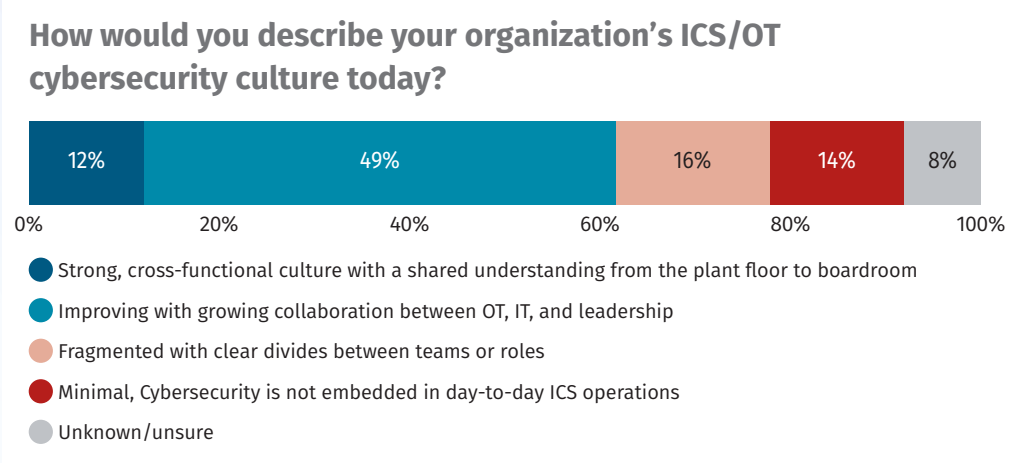

Figure 27. Culture Divide Between IT, OT, and Leadership

Interestingly, much of this sentiment is reflected in how ICS/OT cybersecurity is embedded into an organization's day-to-day activities, as highlighted in Figure 28. Similar to technology, there are multiple factors that correlate with improved culture. Regulated entities, for example, tend to have more embedded tasks and, as a high corollary, report stronger ICS/OT cybersecurity culture. However, what appears to be the No. 1 indicator for having a strong cybersecurity culture that stretches across IT, OT, and leadership may be a bit surprising: having an ICS-specific incident response plan. Respondents that had one were more likely to report a strong (17%) or improving (62%) culture with a majority reporting that IT understand OT constraints (57%), OT understands potential cyber impacts (55%), and security is embedded in OT decision-making (57%).

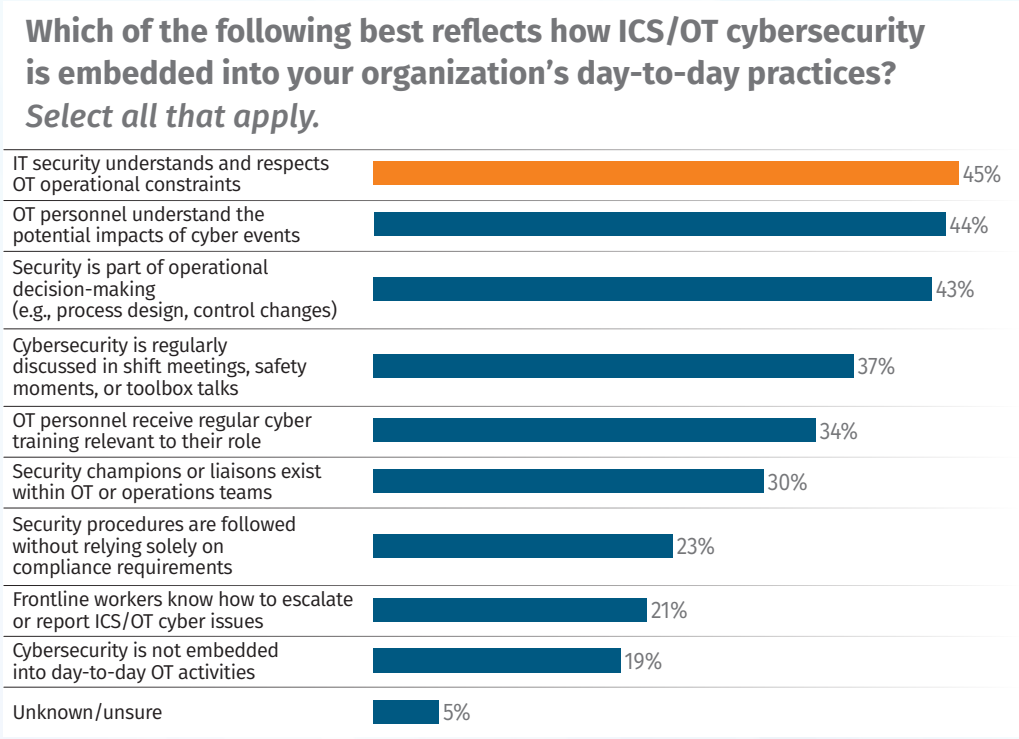

Figure 28. ICS/OT Cybersecurity as Part of Day-to-Day Activities

Culture follows capability: Organizations with an ICS/OT incident response plan report stronger IT-OT alignment, better leadership engagement, and more resilient day-to-day practices.

Conclusions and Next Steps for Industry

The 2025 *State of ICS/OT Cybersecurity Survey* paints a mixed picture. On one hand, detection timelines are shrinking, incident response planning is more common, and regulatory pressure is driving long-term maturity. On the other, remediation remains slow, advanced practices such as threat hunting and red/purple team exercises are limited, and remote access continues to expose organizations to disproportionate risk.

By exploring the full Purdue Model and various security controls, like detection, vulnerability management, and threat hunting, we can gain a better understanding of a risk-based and threat-informed approach to ICS/OT security program management. The goal may not be to have "100% coverage" in all categories, but there needs to be an informed discussion on the trade-offs between detection, protection, and incident response. With only a small percentage of organizations reporting full visibility across the ICS Cyber Kill Chain—and even fewer feeling they are well-positioned for future cyber threats—it is apparent that coverage is sparse at best and concentrated far from where consequences are most severe, including remote field sites.

Taken together, this data reveals a divide between those building truly mature programs and those still struggling with foundational coverage. The characteristics of the most prepared organizations are clear: They integrate IT and OT monitoring, engage field technicians in preparedness, align resilience planning with safety engineering, and actively contribute to information sharing. They are also more likely to embed cybersecurity into daily OT decision-making—where culture becomes a force multiplier for technology investments.

Looking ahead, the path forward for industry is actionable:

1. **Improve coverage of ICS/OT security.** Leveraging a risk-based and threat-informed approach to ICS/OT security controls has proven to improve incident response times and decrease reliability, safety, and financial impacts.
2. **Shift from detection to resilience.** Shorter time-to-containment is not enough. Organizations must invest in faster, safer recovery through backups, failover, and cyber-informed engineering.
3. **Broaden participation.** Preparedness cannot be limited to security teams—field technicians, engineers, and executives alike need to play active roles in threat-aware exercises.
4. **Leverage regulation as a springboard.** Compliance requirements should be treated not as ceilings but as baselines for stronger detection, response, and cultural integration.

The industry has made tangible progress since this survey began in 2017. Yet as the appendix data shows, gaps persist at the very layers of the Purdue Model where consequences are most severe. The challenge for 2026 and beyond is clear: Close those gaps before adversaries exploit them and transform today's incremental improvements into tomorrow's resilience.

Appendix 1: Purdue Model Overview

The Purdue Model serves as the backbone for how ICS/OT environments are conceptualized and secured. By breaking down industrial networks into distinct layers, it provides a structured way to align defenses with operational realities, as seen in Figure 29.

Where:

- **Level 5 – Internet/DMZ—**External-facing services such as web and email servers. While not always included in ICS discussions, this zone defines the perimeter where enterprise IT connects to the outside world.
- **Level 4 – Enterprise IT—** Traditional corporate systems (e.g., business applications, SOC, SIEM). Security maturity here is generally the highest, but controls often stop at this boundary.
- **Level 3 – Operations Systems—** Plant-level management systems such as historians and operations servers. This level acts as a bridge between IT and OT and is a frequent target for attackers attempting lateral movement.

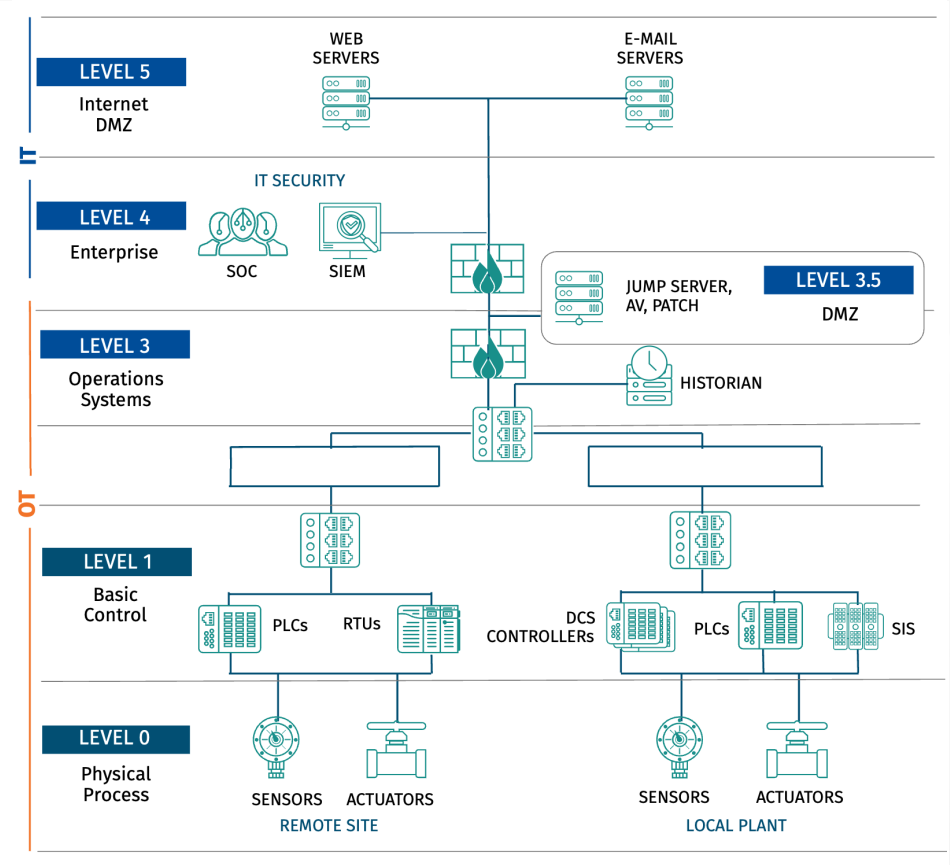

Figure 29. Purdue Model Concept

- **Level 3.5 – DMZ—**A buffer zone between IT and OT, often containing jump servers, patch servers, or antivirus update servers. It is a critical chokepoint for enforcing segmentation.
- **Level 2 – Supervisory Control—**Systems like SCADA and HMI that oversee and visualize industrial processes. Attacks at this level can disrupt visibility into operations or allow manipulation of setpoints.
- **Level 1 – Basic Control—**PLCs, RTUs, and controllers that execute commands. Compromise here directly affects process logic and reliability.
- **Level 0 – Physical Process—**The sensors and actuators tied to real-world operations—turbines spinning, valves opening, breakers tripping. Security here is minimal but consequences are most severe.
- **Remote Sites—**Extending across Levels 0–2, these environments (wind farms, substations, remote pumping stations) often face the same risks but with fewer local defenses and limited connectivity to central monitoring.

Appendix 2


SANS
INDUSTRIAL CONTROL SYSTEMS SECURITY
In a world that is seeing increasingly sophisticated and impactful industrial cyber threats, these courses prepare OT security professionals to lead, defend, and protect industrial control systems at the foundational, essential, management, tactical and advanced skill sets. With SANS ICS Security, train to defend what makes, moves, and powers the world.
ICS CAREER PROGRESSION
FOUNDATIONAL
ESSENTIAL
MANAGEMENT
TACTICAL
ADVANCED
ICS 310
ICS Cybersecurity Foundations™
Learn the cyber fundamentals to protecting ICS/OT environments
ICS 410
ICS/SCADA Security Essentials™
Gain the essential skills to keep industrial systems safe from cyber threats
GICSP
ICS 418
ICS Security Essentials for Leaders™
Manage the people, processes, and technologies for OT cyber-risk programs
ICS 456
Essentials for NERC Critical Infrastructure Protection™
Maintain a defensible compliance program up to NERC CIP standards
GCIP
ICS 515
ICS Visibility, Detection, and Response™
Monitor threats, perform incident response and enhance network security
GRID
ICS 612
ICS Cybersecurity In-Depth™
Identify threats in a real-world ICS environment to protect against adversary attacks
ICS 613
ICS/OT Penetration Testing & Assessments™
Perform safe, hands-on ICS/OT penetration testing and assessments to identify vulnerabilities and improve operational resilience
ICS Security Analyst
Acquires and manages resources, supports, and performs key industrial security protection while adhering to safety and engineering goals
ICS Security Architect
Ensures control system network security compliance and best practices for control networks
ICS Security Incident Responder
Executes specific industrial incident response for incidents that threaten or impact control system networks and assets, while maintaining the safety and reliability of operations
ICS Security Leader
Builds and maintains business relationships with engineering staff and C-suite stakeholders by communicating and managing cyber-to-physical risks while reducing security risk to engineering operations and simultaneously prioritizing safety
Process Control Engineering
Tests, programs, troubleshoots, and oversees changes of existing processes or implements new engineering processes through the deployment and operations of engineering systems and automation devices
ICS/OT Security Pen Tester
Discovers system vulnerabilities and works with asset owners and operators to mitigate discoveries and prevent exploitation from adversaries
Where multiple courses are shown for a given role, determination of the best course to take would be based on the number of years of experience and sector of work.
sans.org/ics
ics-community.sans.org/signup
@SANSICS
linkedin.com/showcase/sans-ics
youtube.com/c/SANSICSsecurity

Sponsor

SANS would like to thank this survey's sponsor:

Acronis

SANS | Research Program

About the SANS Research Program

The SANS Research Program is a key initiative by the SANS Institute and a premier global provider of cybersecurity research and information. SANS Research Program is designed to provide cybersecurity practitioners and leaders with data-driven insights, thought leadership, and solutions that help them better understand and respond to evolving security challenges. All content is authored by SANS instructor experts from around the world who apply their years of experience from hands-on practitioner work in the field, advisory roles, and the classroom to provide education, guidance, and actionable insights that help make the cyber world a safer place.

To learn about sponsorship opportunities for research, content, and in-person or virtual events, email us at **Sponsorships@sans.org** or go to **www.sans.org/sponsorship**.