SANS | Research Program

Survey

SANS 2024 State of ICS/OT Cybersecurity

Written by **Jason D. Christopher**

Foreword by **Tim Conway**

October 2024

Cyolo

Foreword

By Tim Conway, Technical Director of ICS and SCADA Programs, SANS Institute

For asset owners and operators of critical infrastructure, staying ahead of emerging threats and adapting to technological advancements is not just a necessity—it's a responsibility. Many of us in the ICS/OT cybersecurity community understand the immense value of data-driven insights and the power they hold in shaping robust security programs. This report is more than just a collection of statistics and trends; it's a potential roadmap that can help every organization understand where their peers are, strengthen their defenses, and prepare for the challenges ahead.

The findings in this report offer practical, actionable guidance that can be directly applied to improve ICS/OT security programs. Whether it's aligning with industry standards, enhancing workforce capabilities, or adopting new technologies, the data presented here provides benchmarks for industrial organizations to measure their progress and plan for the future. I strongly encourage you to take these insights and use them to drive meaningful change within your organization, ensuring that your security strategies not only meet today's demands but also are poised to tackle tomorrow's challenges.

I'd like to extend my deepest gratitude to the many professionals who took the time to contribute to this survey. Your participation is invaluable, not just for the insights it provides but also for the way it enriches the entire ICS/OT community. It's through efforts like these that we continue to grow, learn, and ultimately, secure the critical systems that underpin our modern world.

Executive Summary

Since 2017, the annual State of ICS/OT Cybersecurity survey has offered key insights and benchmarks for industrial cybersecurity programs worldwide. This year's report continues that tradition. Based on inputs from over 530 professionals across multiple critical infrastructure sectors, it provides actionable guidance as to how organizations can manage industrial cyber risk effectively. The SANS 2024 State of ICS/OT Cybersecurity report is structured around the SANS Five ICS Cybersecurity Critical Controls, offering practical insights applicable to ICS/OT programs regardless of size, budget, or sector.[1] As industrial environments evolve, driven by increased threats, regulatory requirements, and IT–OT integration, the need for a resilient and adaptive security posture is more critical than ever.

Key Industry-Wide Insights

- **Slightly cloudy—26% of respondents are now utilizing cloud technologies for ICS/OT applications, marking a significant (+15%) increase from previous years.**
- **Workforce growing pains—51% of respondents do not hold any ICS/OT-specific certifications, indicating a critical need for access to enhanced training and certification programs.**
- **Incident response "haves and have-nots"—56% of organizations have a dedicated ICS/OT incident response plan, though 28% still lack such a plan.**
- **MFA for (almost) everyone—75% of respondents have implemented multifactor authentication (MFA) for remote access to industrial sites, showing steady improvement in securing access points.**
- **Limited AI adoption—Only 10% of respondents are currently using AI in their ICS/OT security strategies, though interest is growing.**
- **Standards and intel lead maturity—Throughout the report, one thing is clear: the more organizations use both industry-adopted standards *and* ICS-specific threat intelligence, the more mature their overall cyber capabilities are.**

[1] "The Five ICS Cybersecurity Critical Controls," November 7, 2022, www.sans.org/white-papers/five-ics-cybersecurity-critical-controls

Although advancements in cloud adoption and security technologies are promising, ongoing workforce development and aligning budget priorities with actual risks remain critical challenges. This report provides the data and analysis organizations need to refine their security strategies and better protect critical infrastructure in an increasingly complex cyber threat landscape. Figure 1 provides a snapshot of respondents' demographics.

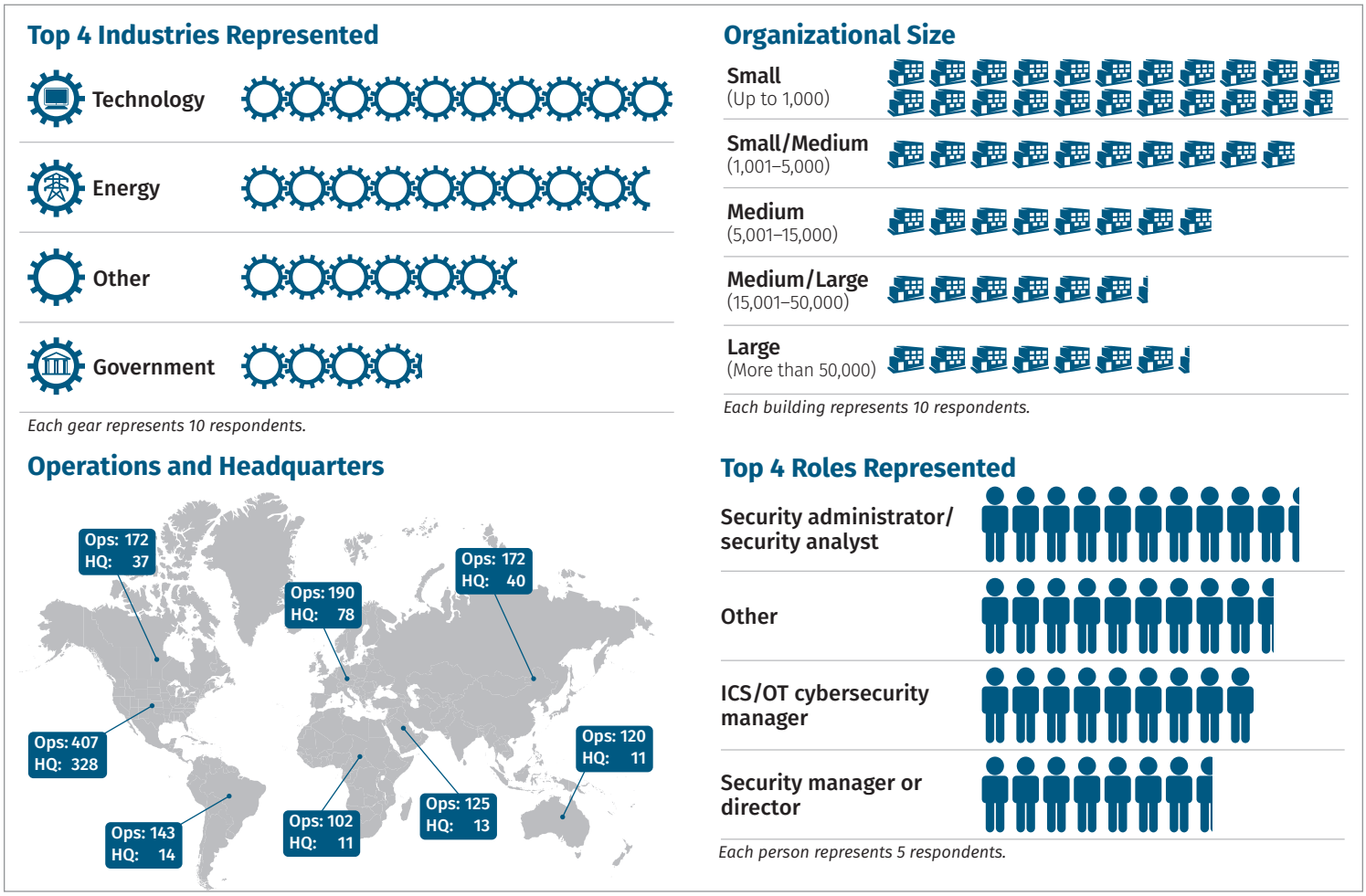


Figure 1. Survey Demographics

2024 Workforce, Governance, and Technology Changes

The 2024 survey examined key shifts in governance, workforce, and technology within the ICS/OT security landscape. As IT and OT roles further rely on one another, organizations must adapt their security governance and workforce strategies to address new challenges. This section focuses on current trends in budget allocation, leadership priorities, and workforce skills, as well as the adoption of emerging technologies like cloud computing and artificial intelligence. By analyzing these developments, organizations can better align their security efforts with industry standards and prepare for the evolving demands of industrial cybersecurity.

ICS-Specific Workforce Development: The Path to Maturity

The workforce is the beating heart of any ICS/OT security program. A trained and experienced team can help inform strategies, what technologies to invest in, and the best approaches for managing industrial cyber risk.

As industrial environments become more interconnected, the convergence of IT and OT roles is increasingly common.[2] The data shows that 36% of respondents are responsible for both IT and OT security, reflecting this growing integration. However, this trend is not universal; 34% of respondents still focus exclusively on OT/ICS operations, and 24% are dedicated primarily to IT/business enterprise activities—splitting the "IT vs. OT" camps into similar populations.

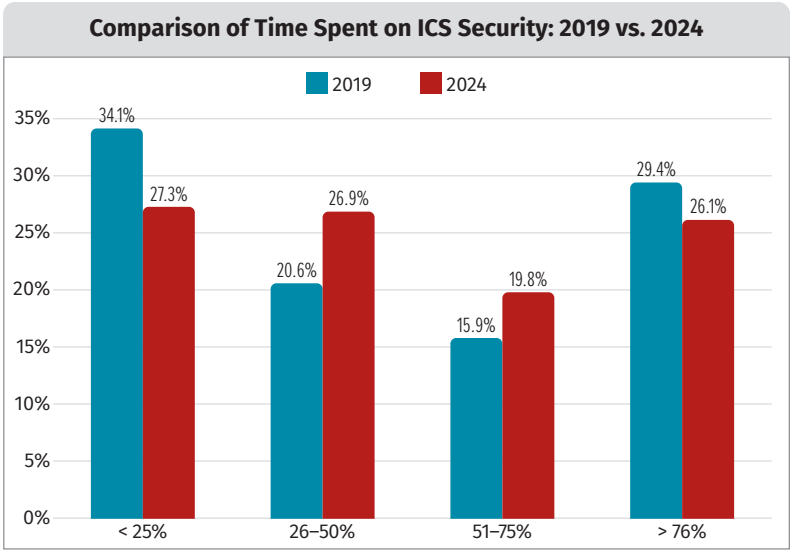


Figure 2. Time Spent on ICS Security

Regardless of their IT/OT placement, respondents reported that, on average, over half of their time was spent on ICS cybersecurity. Figure 2 shows how this has shifted over the past five years. Although ICS/OT cybersecurity is still a "part-time job" for many respondents, over 12% of respondents in 2024 described ICS/OT cybersecurity as taking 100% of their assigned duties.

Over 50% of the ICS workforce has less than five years of experience, highlighting the urgency for knowledge transfer and mentorship to build deep expertise within the industry.

[2] For the purposes of this survey, "convergence" refers to the interdependency and interwoven nature of applying IT and OT controls across industrial cybersecurity programs—not the more popular marketing use for specific tools in ICS environments.

The workforce demographics indicate that most respondents have five or fewer years of experience, as seen in Figure 3. Years working within an industry does not directly correlate to knowledge and skills—instead, this statistic highlights the industry's "youth" compared to its IT counterpart. This presents opportunities for fresh perspectives but underscores the need for mentorship to transfer knowledge from seasoned professionals.

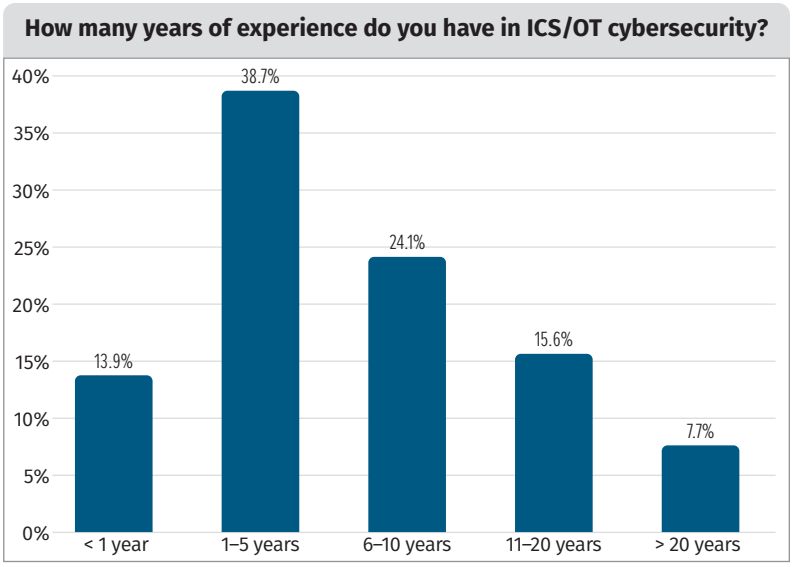


Figure 3 ICS Workforce Experience Levels

Certifications can help enable a maturing workforce by providing standardization, a common lexicon for security concepts, and demonstrative proof of a foundational understanding required for various jobs and tasks. Unfortunately, roughly half (49%) of respondents reported lacking cybersecurity-related certifications, as seen in Figure 4.

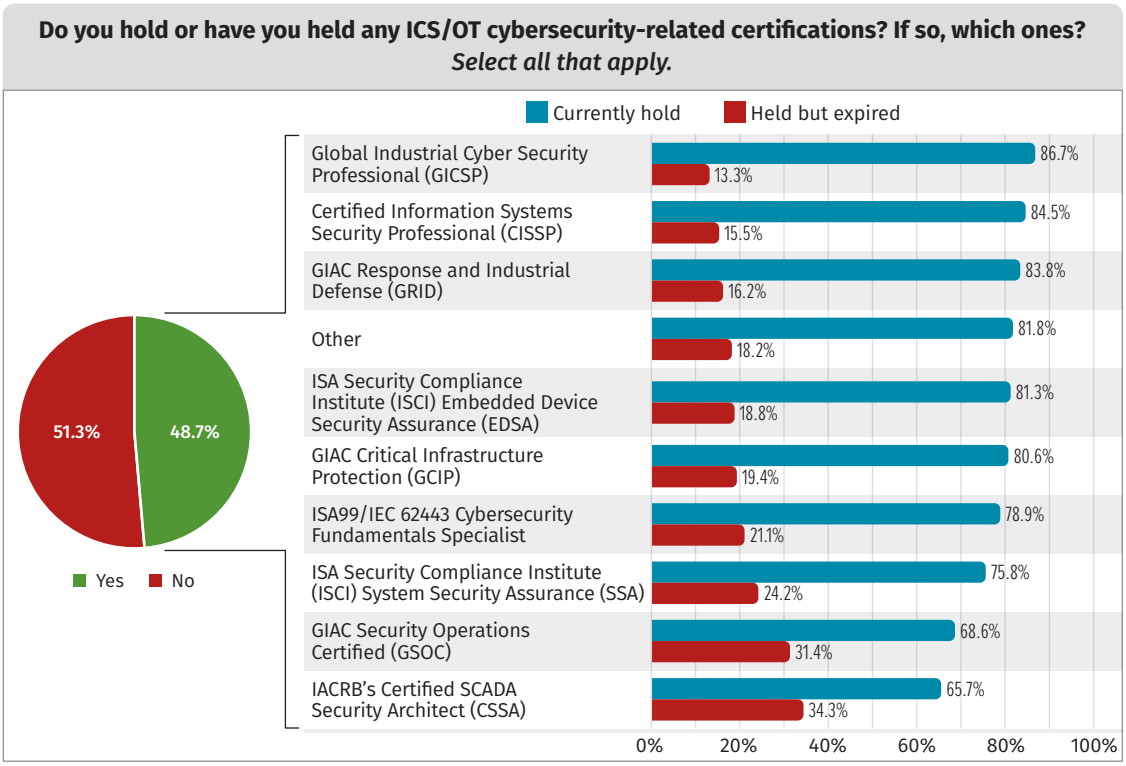


Figure 4. Certifications Across the ICS Security Workforce

Interestingly, the size of an organization had no bearing on this rate of certification, indicating that size and budget may not be a direct link to obtaining a professional certification. Notably, those with GIAC Critical Infrastructure Protection (GCIP), GIAC Response and Industrial Defense (GRID), and System Security Assurance (SSA) certifications tend to have more hands-on ICS experience, spending over 70% of their time on ICS security. That said, this overall lack of certification suggests that many professionals may be operating without formalized, industry-specific training. This gap in certification coverage could undermine the effectiveness of security measures and contribute to a less resilient ICS security environment.

The challenges faced by the ICS/OT security workforce are further deepened by the technical and operational complexities of integrating legacy systems with modern IT environments. The survey identifies technical integration of aging ICS/OT technology and IT systems as a major hurdle, with 65% of respondents citing this as a significant issue. Additionally, the survey highlights a lack of understanding of ICS/OT operational requirements among IT staff, noted by 50% of respondents, and a shortage of labor resources, reported by 46%. These challenges point to a critical need for more specialized training and a deeper appreciation of the unique demands of ICS environments within the broader cybersecurity workforce.

The need to develop a robust ICS cybersecurity workforce has been recognized globally, including in regulations like the EU's NIS 2 Directive[3] and policies like the US's Call To Action: Building the Cyber Workforce the Nation Needs.[4] Although progress is evident, the industry must address the experience and certification gaps to foster a resilient, skilled, and unified ICS security community.

ICS-Specific Security Governance: Aligning Priorities with Practice

The governance of ICS/OT cybersecurity is drawing more attention at the executive level, but there are still significant gaps between perceived risks and actual investments. The 2024 survey indicates that the responsibility for setting ICS security policies is increasingly being centralized within the executive leadership, with a clear emphasis on integrating ICS security into the broader corporate security strategy.

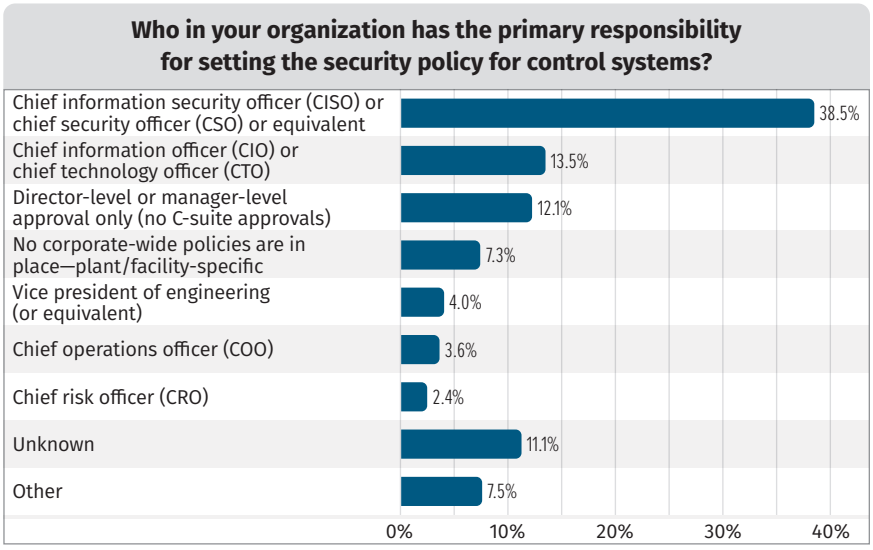


Figure 5. Roles Responsible for ICS/OT Cybersecurity

As Figure 5 shows, CISOs are the main drivers of ICS security governance (39%), integrating it with corporate security strategy. Respondents also highlighted that CIOs or CTOs contribute to ICS security policies (14%), further converging ICS security with IT governance and indicating most organizations centralize ICS security within the enterprise. We've seen this centralization occur over the past five years, with the industrial CISO consistently the primary owner of ICS/OT cybersecurity policy, as Figure 6 illustrates on the next page.

[3] "The NIS 2 Directive," www.nis-2-directive.com

[4] "Answering the Call to Build the Nation's Cyber Workforce," www.whitehouse.gov/oncd/briefing-room/2023/11/03/answering-the-call-to-build-the-nations-cyber-workforce

Most organizations (72%) map their control systems to recognized frameworks, with the NIST Cybersecurity Framework being the most popular (45%). Other standards, such as International Society of Automation/International Electrotechnical Organization (ISA/IEC) 62443 and North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP), are also widely used, showing a strong commitment to standardizing and strengthening ICS security practices. However, standard mapping depends on who governs ICS security. If a CISO owns the governance, 82% of ICS programs follow industry standards, compared to only 42% if there are no corporate-wide policies for ICS.

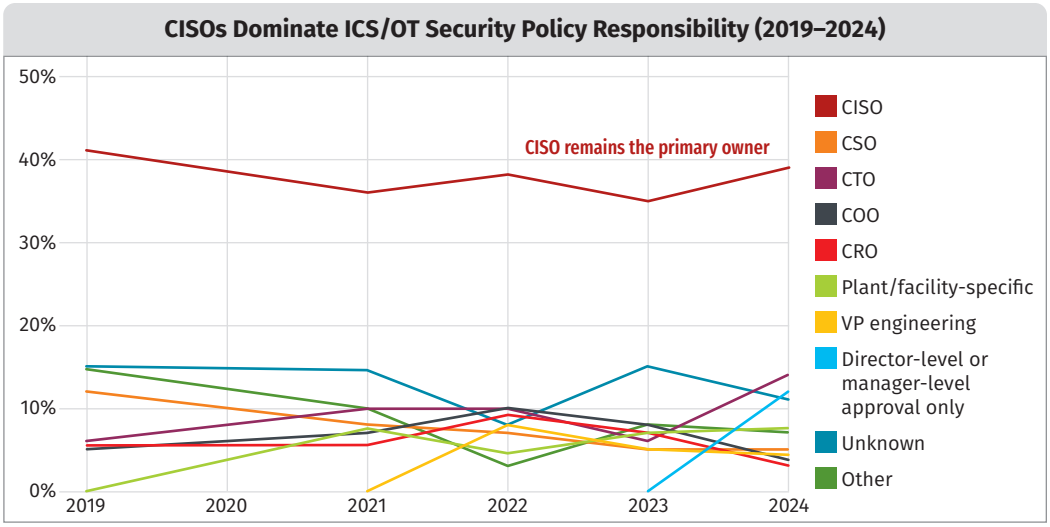


Figure 6. Trend for Ownership of ICS/OT Cybersecurity

Governance matters. In cases where the CISO owns ICS security, 82% of programs are mapped to standards, compared to 42% if no corporate-wide policies exist—a nearly 2x difference!

Meanwhile, there is a significant disconnect between perceived risks and budget allocation. Although 66% of respondents identified "people"—including employees and contractors—as the greatest risk to their ICS environments, most budget allocations continue to prioritize technology. Specifically, 52% of respondents allocate much of their cybersecurity budget to technology investments, whereas only 25% dedicate a comparable budget to workforce training, recruitment, and retention. This suggests that although organizations recognize the importance of addressing human factors in cybersecurity, their financial investments are geared toward solving this problem with technology. This shares a common theme with the trends uncovered in the previous section on ICS security workforce management.

Meanwhile, shared budgets are increasingly common. Some 38% of respondents reported having a shared IT–OT budget. This increases to 48% of respondents if a CISO manages the ICS/OT security program. In 2019, only 29% of respondents indicated that there was a shared IT–OT budget, further cementing the centralization of cybersecurity governance across industrial organizations. This trend could signal a growing recognition of the need for a unified approach to securing both IT and OT environments.

Who Has the Money?

Over the past five years, budgets have routinely shifted "toward the center" and are shared by both IT and OT security teams. In 2019, only 29% of respondents had a joint IT–OT security budget, compared to 38% in 2024.

The 2024 survey data shows that architecture and visibility are the top budget priorities among the SANS Five ICS Cybersecurity Critical Controls. Defensible architecture, which focuses on establishing robust perimeter defenses and securing the infrastructure, is ranked as the top priority by 33% of respondents, as seen in Figure 7.

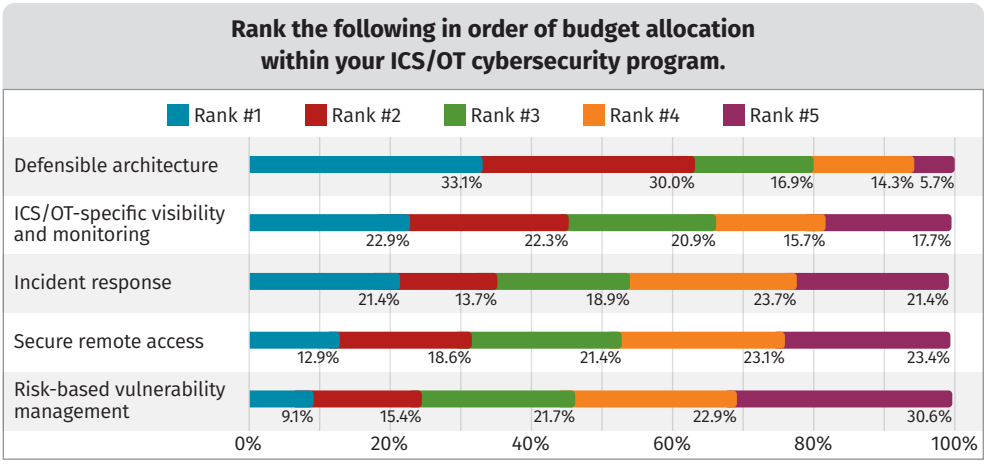


Figure 7. Priority Level of the SANS Five ICS Cybersecurity Critical Controls, Based on Budget Spend

Respondents value ICS/OT-specific visibility and monitoring, which help them see what is happening on their network, identify vulnerabilities, and spot malicious activities. Interestingly, incident response received a lower budget priority for organizations, implying either the tools and methodologies are less expensive—or there is a potential misalignment in organizational priorities. After all, without response, what good is detection?

Figure 8 highlights business impact priorities for industrial organizations—respondents place the highest importance on "safety of the industrial process/facility" and "reliability and availability of the industrial process." In contrast, areas such as "protecting company reputation and brand" and "meeting regulatory compliance" are ranked lower. Respondents in the IT sector, however, ranked "confidentiality of intellectual property" significantly higher—in fact, higher than safety and reliability—unfortunately highlighting a disconnect compared to industrial sectors, like energy and manufacturing.

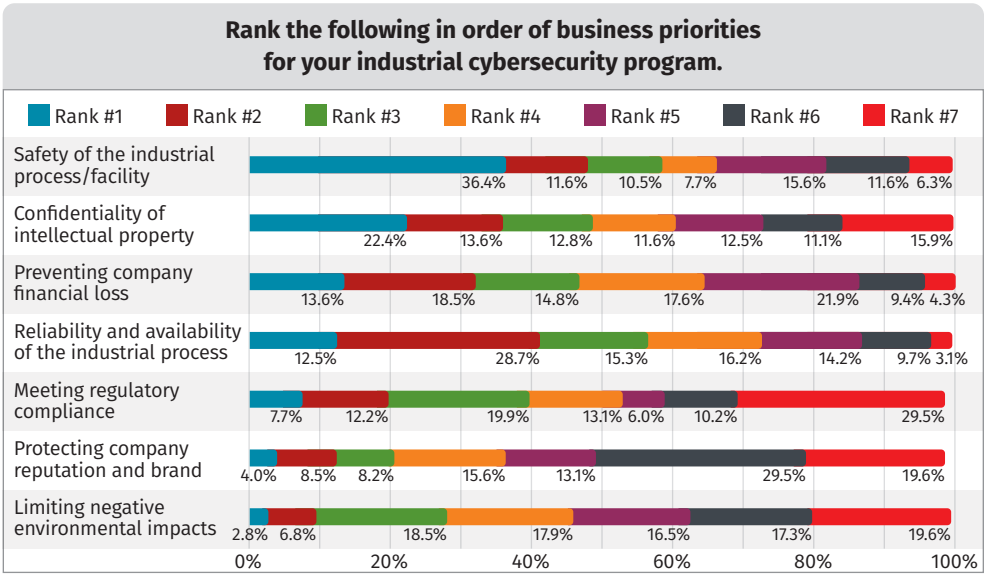


Figure 8. Business Impact Priorities

Technology Adoption in ICS/OT Environments: Cloud and AI

Cloud adoption in ICS/OT environments surged in 2024, with 39% of respondents using cloud-based services. This marks a major shift from traditional on-premises solutions, but 45% of respondents still avoid cloud services due to security and reliability concerns. Interestingly, the industrial sector matters most when considering cloud adoption. Energy sector respondents overwhelmingly *do not* use the cloud (at half the adoption rate [18%] of other sectors). This is likely due to regulatory uncertainty with standards like NERC CIP, which currently do not easily allow cloud usage within the North American Bulk Electric System.

Table 1. ICS Cloud Adoption 2023–2024 Comparison

ICS Cloud Category	2023 Usage	2024 Usage	Change
Remote monitoring only of configuration and analysis of operations telemetry	40.1%	55.8%	+15.7% ▲
Remote storage of data historian data	39.4%	34.7%	–4.7% ▼
Connection for third-party managed ICS/OT services (managed security service provider [MSSP])	32.9%	27.4%	–5.5% ▼
Remote processing of data historian data	29.5%	29.5%	—
Remote control of engineering field devices	25.8%	28.4%	+2.6% ▲
Process optimization	22.7%	25.3%	+2.6% ▲
Business continuity/disaster recovery planning	22.4%	33.7%	+11.3% ▲
Remote control of engineering operations (human–machine interface [HMI] in the cloud)	22.0%	31.6%	+9.6% ▲
Virtualized controllers	18.0%	15.8%	–2.2% ▼
Other	9.6%	4.2%	–5.4% ▼

Table 1 outlines striking trends in how cloud services are being used compared to last year's survey. For example, the increase in cloud usage for remote monitoring of configuration and analysis of engineering operations telemetry jumped from 40% to 56%, a significant 16% increase. Similarly, there has been an 11% rise in the use of cloud services for business continuity and disaster recovery planning, reaching 34% in 2024. The moderate jump (+10%) in HMI in the cloud may raise some eyebrows across the ICS/OT security community. That said, despite this increased usage, organizations are taking a cautious approach. Seventy-nine percent of respondents conduct risk assessments before cloud deployments, demonstrating a strong focus on risk management regarding the cloud.

We asked respondents about their use of artificial intelligence (AI) in ICS/OT environments, a new topic in this year's survey. The results show that AI adoption is still nascent, with only 10% of respondents using AI in both enterprise IT and ICS/OT networks. Another 19% are testing AI in lab environments, while 27% are limiting AI to enterprise IT environments, exploring its potential rather than fully integrating it into their industrial operations. A sizable 33% report no use or testing of AI at all, highlighting the early stages of AI in the industrial control sector.

That said, there is considerable interest in AI, with organizations planning to deploy AI technologies in the next 18 months across multiple categories, as seen in Figure 9. The areas of greatest interest include autonomy (64% planned), computer vision (58% planned), and decision science (66% planned). Natural language processing (NLP), the common category of generative AI used for consumer-grade tools like ChatGPT and Copilot, is currently in use across 50% of respondents using AI, with a nearly identical set of respondents planning future use. This, as well as machine learning (ML) usage, is arguably the most mature AI technology category.

What AI technologies or solutions do you currently have in use in your industrial organization? What new AI technologies or solutions is your organization looking to deploy in the next 18 months? ***Select only those that apply.***

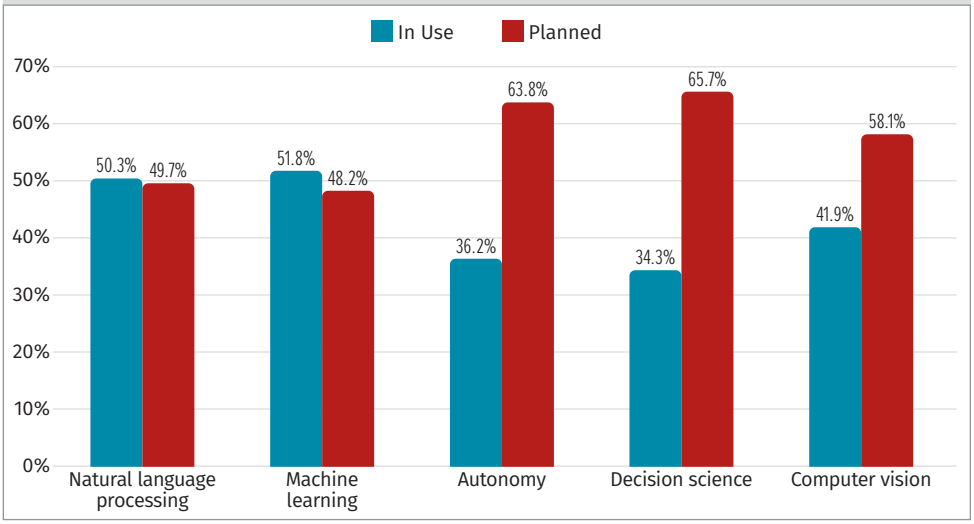


Figure 9. Current and Planned Usage of AI Categories

Despite the limited current use, organizations are proactively establishing AI cybersecurity policies, with 31% having policies that cover IT use cases and 12% including both IT and OT. This indicates a growing awareness of the need to address the cybersecurity implications of AI for industrial organizations.

This year's survey asked specifically about AI technologies following the categories from the "AI Index," which identifies the categories as follows:[5]

- **Natural language processing (NLP)—**NLP focuses on enabling machines to understand, interpret, and generate human language. It powers applications like chatbots, language models, and automated translation systems.
- **Machine learning (ML)—**ML involves training systems to learn patterns from data to make decisions or predictions. It's a key driver in AI advancements, particularly in tasks like recommendation engines and predictive analytics.
- **Autonomy—**Autonomy refers to AI systems' ability to perform tasks without human intervention. It is often seen in robotics, self-driving cars, and autonomous drones.
- **Decision science—**This area uses AI to support decision making by analyzing data to provide actionable insights. It's widely applied in fields like economics, healthcare, and logistics for optimization and strategy.
- **Computer vision—**Computer vision enables AI to interpret and understand visual information from the world. It is used in image recognition, facial detection, and even self-driving technology.

[5] "The AI Index," https://aiindex.stanford.edu

The SANS Five ICS Cybersecurity Critical Controls

The SANS Five ICS Cybersecurity Critical Controls, published in November 2022, serve as foundational guidance for securing ICS and OT environments.[6] These controls help organizations mitigate risks and ensure the safety and reliability of critical infrastructure. In this report, we use these controls as broad categories to analyze current trends and guide the enhancement of industrial cybersecurity programs.

The SANS Five ICS Cybersecurity Critical Controls are:

- **ICS incident response—**Focuses on developing and maintaining a tailored incident response plan to ensure resilience and swift recovery in ICS environments
- **Defensible architecture—**Emphasizes the design and implementation of robust ICS architectures that support visibility, segmentation, and process communication enforcement
- **ICS network visibility and monitoring—**Advocates for continuous network security monitoring with protocol-aware tools to enhance visibility into ICS interactions and identify vulnerabilities
- **Secure remote access—**Stresses the importance of securing remote access to ICS networks, particularly against threats from hybrid work structures and supply chain vulnerabilities
- **Risk-based vulnerability management—**Prioritizes the management of ICS vulnerabilities based on risk, focusing on those that could enable adversary access or disrupt operations

Each section of this report will expand on these controls and link them to specific findings and trends to aid organizations in growing and maintaining their ICS/OT security programs.

SANS ICS Cybersecurity Critical Control #1: 2024 Incident Response Trends

ICS/OT incident response plans must be customized to the specific facilities, processes, and impacts of each industrial environment. The US Department of Homeland Security warned in 2009 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." Yet, 15 years later, nearly a third (28%) of respondents still lack an ICS-specific incident response plan (IRP). This statistic is virtually unchanged from last year's survey.

For those that *do* have a plan (56% of respondents), testing of the IRP is commonly on an annual basis. And those that test annually have largely based their plans on standards like NERC, ISA/IEC, and the like. Interestingly, respondents that test more often (quarterly or monthly) represent a small fraction (16% and 8% of respondents, respectively), and typically have a broader set of IRP influences, including standards, threats, and consequence-driven engineering scenarios.

Those that test more often have a broader set of IRP influences, like standards, threat intelligence, and consequence-driven engineering scenarios, indicating increased maturity.

Regular ICS-specific IRP testing, not surprisingly, correlates to more informed capabilities for ICS incident response. For example, an impressive number of annual testers have exercised an ICS network outage resulting in production outages (65%) and are confident they can operate in manual mode (66%). However, this is dwarfed by those who test quarterly (75% have exercised an ICS network outage and 72% can operate their ICS in manual mode). Respondents who tested their IRP *monthly* were true masters of their craft, with nearly 90% having exercised such outages. Those that train regularly clearly have the upper hand in mature ICS incident response capabilities.

When asked about what types of exercises are performed, respondents leveraged a large range of capabilities, with paper-based tabletop exercises being the most widely used, as seen in Figure 10.

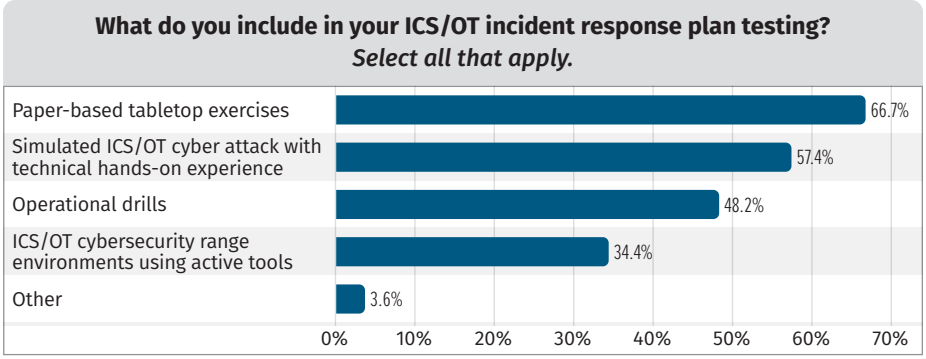


Figure 10. IRP Exercise Types

Industrial Impacts from Ransomware in 2024

This year's survey saw a decrease in respondents reporting ransomware impacts, with only 12% of respondents reporting ransomware incidents in the previous 12 months. Half of those ransomware attacks impacted ICS/OT networks, and 38% compromised the safety or reliability of the physical process, as seen in Figure 11. Although the overall trend seems to have decreased, the impacts are still potentially catastrophic and should be considered for all ICS/OT-specific incident response programs.

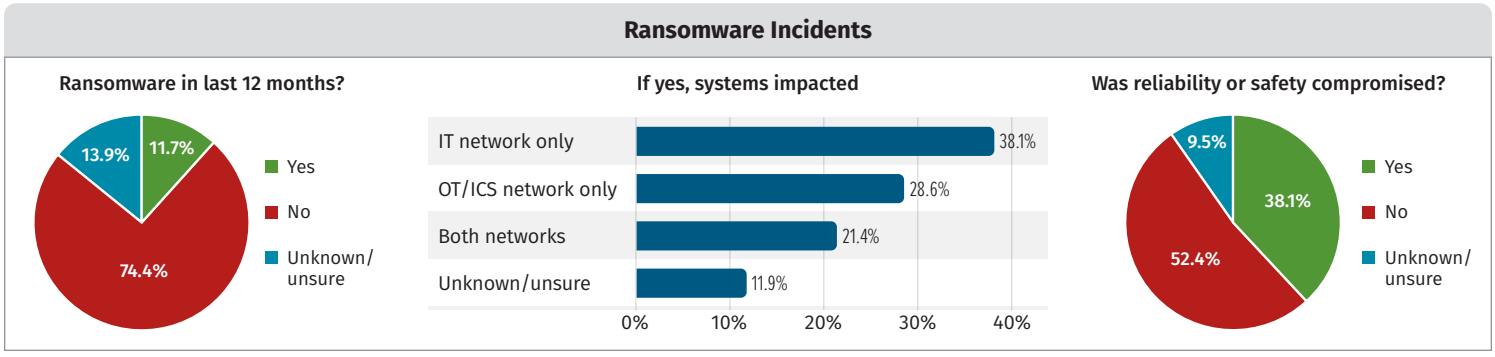


Figure 11. Ransomware Incidents over the Past 12 Months

[6] "The Five ICS Cybersecurity Critical Controls," November 7, 2022, www.sans.org/white-papers/five-ics-cybersecurity-critical-controls/

Non-Ransomware Incidents

Comparatively, there were more reported non-ransomware incidents, with 19% of respondents reporting one or more security incidents over the same period.

The reported attack vectors have changed over the years, as outlined in Figure 12, with an increased focus on IT-based attack vectors allowing threats into ICS/OT networks (which is historically the most commonly reported attack vector).

ICS/OT incident response is a team sport with multiple stakeholders involved. Over the years, the common question of "who would you contact during an incident?" has shifted within the industrial space—specifically for non-regulatory government agencies. Unlike other stakeholders, there has been a consistent decrease in voluntary reporting and/or participation with government entities, as seen in Table 2.

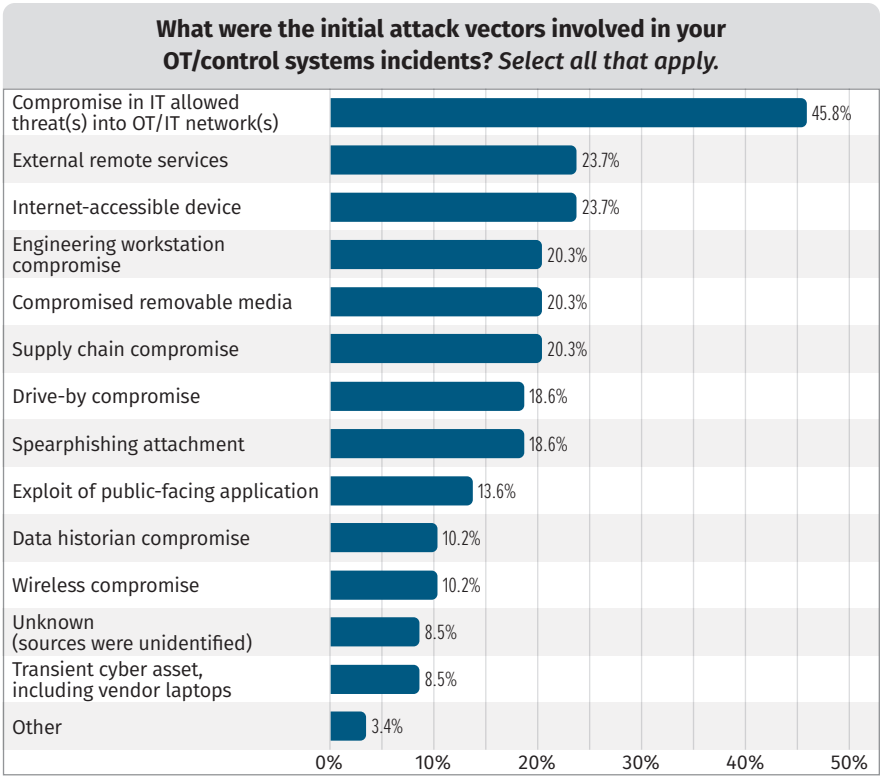


Figure 12. Initial Attack Vectors

Table 2. ICS Incident Response: Who Is Contacted After Detection

	2019	2021	2022	2023	2024
Cybersecurity solution provider	35.6%	48.1%	56.5%	43.2%	45.8%
Control system vendor	45.6%	32.7%	34.8%	36.4%	45.8%
Engineering consultant	13.4%	19.2%	34.8%	27.3%	18.6%
Internal resources	59.0%	44.2%	32.6%	37.5%	27.1%
Non-regulatory government organizations	40.6%	32.7%	23.9%	25.0%	11.9%
System integrator	15.1%	11.5%	19.6%	5.7%	25.4%
Security consultant	37.2%	32.7%	17.4%	17.0%	42.4%
IT consultant	18.4%	40.4%	13.0%	20.5%	18.6%
Main automation contractor	8.4%	11.5%	8.7%	13.6%	16.9%
Other	2.1%	3.8%	0.0%	1.1%	5.1%
IT security team				33.0%	50.8%

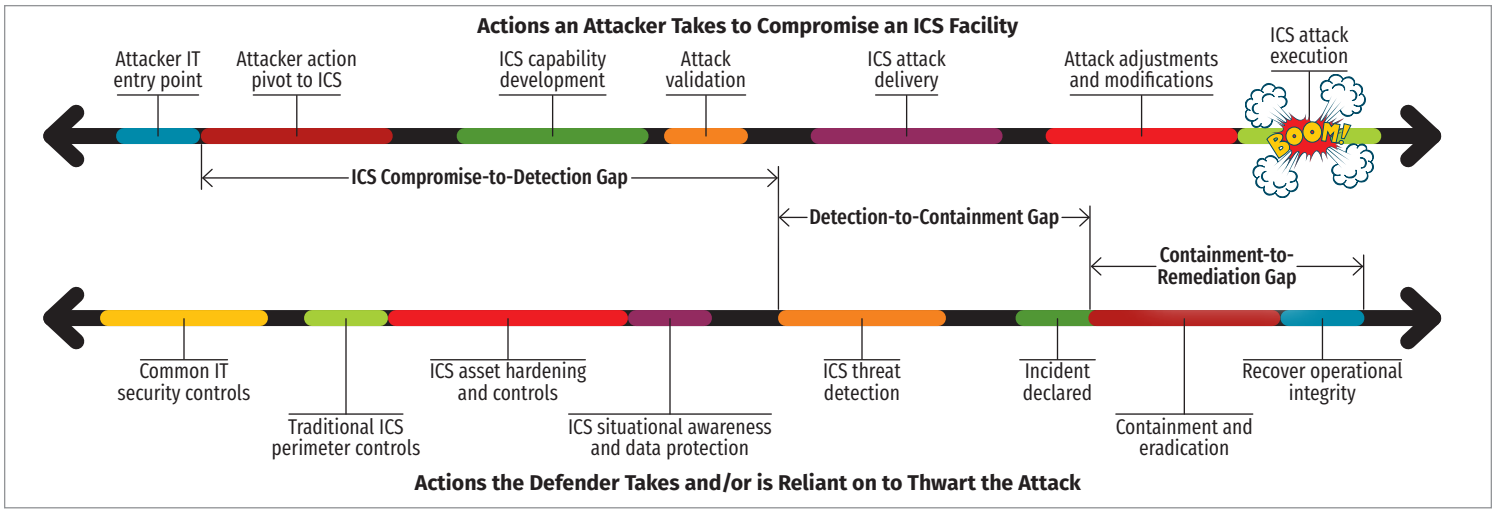


Figure 13. ICS Cyber Incident Timeline

Speaking of detection, our industry has historically had difficulty with how long it takes to detect a compromise and remediate. This is partially due to the lack of visibility in the ICS environment, as well as the skillsets required to recover from an ICS cyber incident, which is a blend of IT and OT knowledge and experience. Consider the timelines in Figure 13 for a traditional IT cyber incident that pivots to OT environments.

The top timeline identifies the steps required by an attacker to execute an ICS cyber attack; the bottom highlights the potential defender activities that can be used to detect, deter, prevent, and recover from such an attack. Based on the 2024 survey data, detection occurs relatively quickly (often less than 24 hours), but the later stages of the incident response lifecycle take considerable effort—with some remediation times stretching to a year or more, as seen in Figure 14.

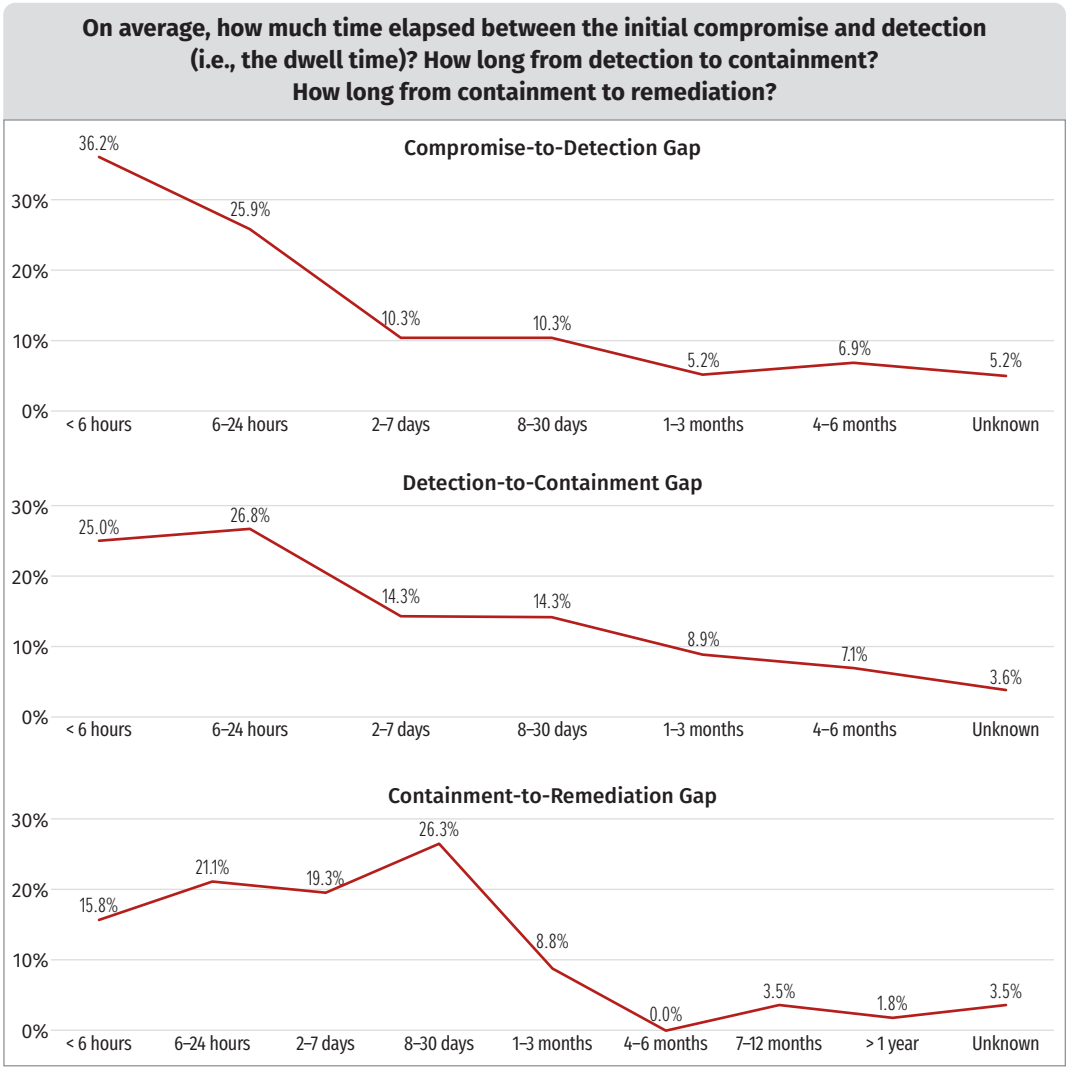


Figure 14. Detection, Containment, and Remediation Gaps for ICS Incidents

ICS-specific incident response still proves to be a challenge for industry. Although many organizations are making progress, a significant portion still lack adequate preparedness, testing, and integration across IT and OT functions. For ICS environments, where the stakes are exceptionally high, improving incident response capabilities should be a top priority, guided by industry standards and tailored to the specific risks to safety and reliability.

We're Getting Quicker...

Over half of respondents that had an incident reported a compromise-to-detection gap of *less than 24 hours*. In 2019, the same number had a compromise-to-detection gap of *2–7 days*.

SANS ICS Cybersecurity Critical Control #2: 2024 Defensible Architecture Trends

As mentioned earlier, technology is the largest budget category for ICS security programs. After establishing an ICS-specific incident response program based on scenarios and safety/reliability risks, organizations should deploy defensible architecture technologies and strategies tailored to the incidents that could affect the industrial process and human safety.

When asked about defensible architecture priorities, respondents clearly pointed toward network segmentation between IT and OT as the top concern. Compromised IT systems were the top vector for ICS/OT incidents in 2024, so it makes sense to see network protections ranked so high. Other priorities can be seen in Figure 15.

Rank the following ICS/OT cybersecurity architecture priorities for your organization.

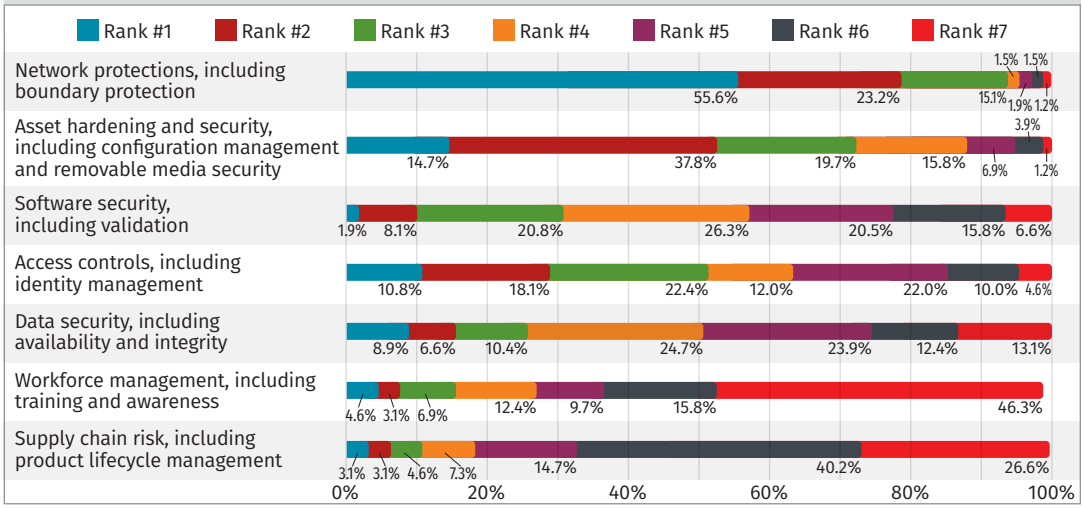


Figure 15. Defensible Architecture Ranked Priorities

Most respondents (64%) based their architecture on standards, threats, trends, and scenarios with safety and reliability impacts. A large majority (74%) documented the IT–OT boundary for industrial networks. However, nearly a quarter (22%) had some ICS/OT systems dual-homed with IT networks or on the enterprise IT network, exposing them to greater risks. Alarmingly, 34% of these respondents also had their safety instrumented systems (SISs) on the same IT network. SIS is the last defense during both a physical safety event and a potential ICS cyber incident, and should not be connected to enterprise IT networks due to the potentially disastrous impacts associated with an SIS failure.

22% of respondents had one or more ICS/OT assets dual-homed with IT networks or residing directly on the enterprise IT network.

Luckily, despite these fringe cases, industry understands the importance of separating the SIS, as seen in Figure 16.

Please describe your method of connectivity between your internal OT/control system network and safety instrumented systems (SIS) and/or functional safety systems.

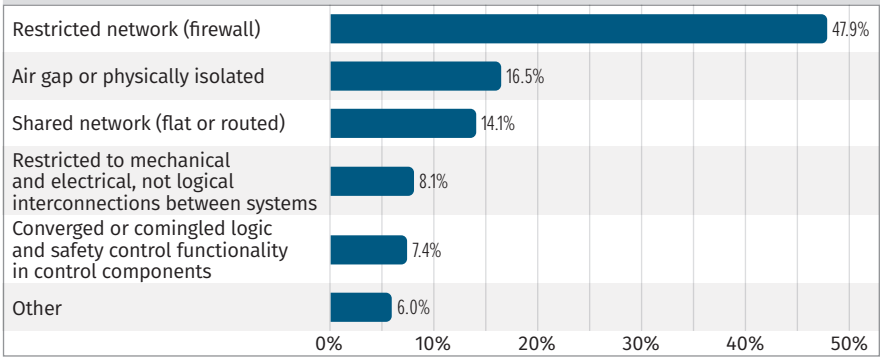


Figure 16. SIS Connectivity

Boundary protection is just one element of building a defensible ICS architecture. In the 2024 survey, we asked respondents to outline which technologies they have in place and which they are planning to implement over the next 18 months. The full list can be found in the Appendix. Of the nearly 40 technologies outlined in the survey, we captured the top five *currently implemented* in Figure 17.

Over the past five years, several of these categories have seen massive jumps in implementation across industry. For example, in 2019, 72% of respondents had access controls in place for ICS, compared to 81% today. Similarly, endpoint detection and response (EDR) was reported as being used by 53% of respondents in 2019; however, by 2024 there was a 20% jump to 73% using EDR. Interestingly, due to the larger penetration of the technologies in the top five, most of the planned rates are relatively low in relation to other technologies being deployed in ICS/OT environments. In comparison, the most-planned technologies in Figure 18 tell an interesting story for what the next 18 months in ICS security may look like.

Figure 18 shows the most-planned ICS security technologies. Except for ICS-specific cybersecurity metrics and dashboards, these technologies are already in use by nearly half of respondents, but over 30% more plan to use them. This suggests a possible shift toward non-technology spending, like training and tabletops. ICS network security monitoring stands out as the only highly planned technology, with over 50% current deployment.

Finally, three technology categories for defensible ICS architecture stood out for being the least deployed—but with a surprisingly large number of respondents planning to use them over the next 18 months, as seen in Figure 19.

What security technologies or solutions do you currently have in use in your OT environment? What new technologies or solutions would you most want to add for control system security in the next 18 months? *Select all that apply or indicate not applicable (N/A).*

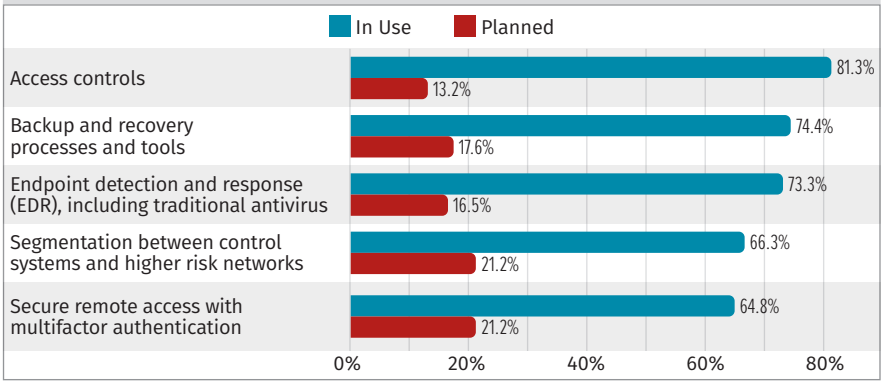


Figure 17. Top Five In-Use ICS Security Technologies

What security technologies or solutions do you currently have in use in your OT environment? What new technologies or solutions would you most want to add for control system security in the next 18 months? *Select all that apply or indicate not applicable (N/A).*

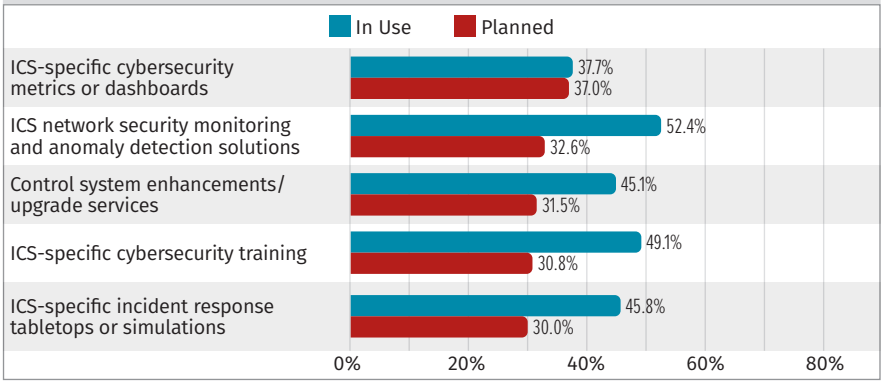


Figure 18. Most-Planned ICS Security Technologies

> **In 2019, OT-specific monitoring was used by only 33% of respondents (compared to 52% in 2024), demonstrating a massive growth across this technology category in only five years.**

What security technologies or solutions do you currently have in use in your OT environment? What new technologies or solutions would you most want to add for control system security in the next 18 months? *Select all that apply or indicate not applicable (N/A).*

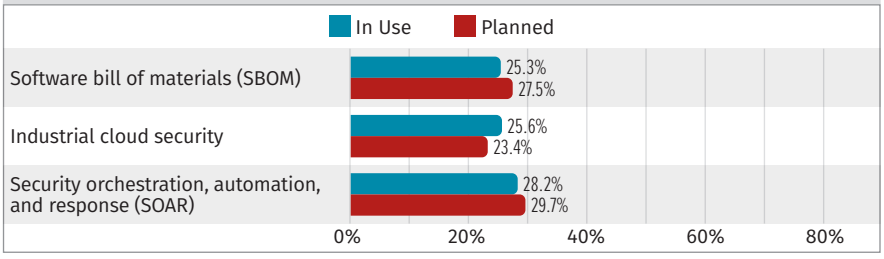


Figure 19. Least Used ICS Security Technologies with High Planned Rates

Software bill of materials (SBOM), industrial cloud security, and security orchestration, automation, and response (SOAR) were the least used technologies within the 2024 survey—but each has higher-than-average planned implementations for the next 18 months, indicating that these technologies may become more common across ICS security programs soon.

We often describe ICS/OT as the "M&M" model: hard shell, gooey center. This is why we focus a lot on IT–OT boundaries (i.e., the hard shell). However, security professionals need to also focus on toughening up that gooey center. Recall, for example, that replication through removable media was a top attack vector in 2024. To combat this, 69% of respondents have a formal program for removable media risks, and 70% have threat detections enabled for removable media in their ICS/OT environments.

SANS ICS Cybersecurity Critical Control #3: 2024 ICS Network Monitoring Trends

Industrial cybersecurity is evolving rapidly, and so are the capabilities of security operations centers (SOCs) that monitor and respond to threats in ICS environments. This year's survey reveals how organizations are integrating IT and OT SOCs, enhancing ICS-specific network monitoring, and correlating data for comprehensive analysis.

Establishing and Integrating OT-Specific SOCs

Nearly 30% of respondents have integrated their IT and OT SOCs, a sign of convergence between these domains. This allows for a unified and efficient response to threats, leveraging both IT and OT strengths. Most merged IT–OT SOCs report to a CISO (58%), map to standards (84%), and have a shared IT–OT budget (54%).

Many organizations have recognized the importance of a dedicated SOC, with 63% having one. That said, 45% have no OT SOC capabilities, leaving a significant gap in threat detection and response for ICS/OT environments, as shown in Figure 20.

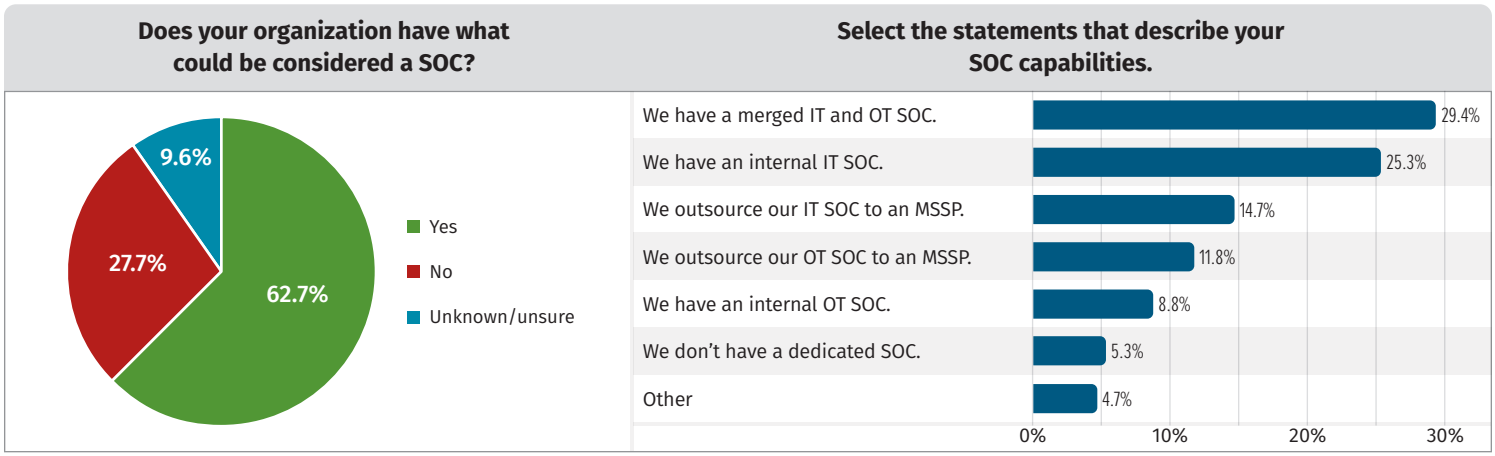


Figure 20. SOC Trends and Capabilities

Building SOC Capabilities with ICS-Specific Monitoring

Establishing a SOC is a potential first step for industrial organizations, but expanding capabilities with ICS-specific network monitoring is crucial. The survey reveals a wide range of monitoring capabilities across organizations. Although 52% of respondents have limited ICS/OT network monitoring, 26% have extensive monitoring solutions, reflecting a growing awareness of the need for ICS visibility.

However, Figure 21 shows that 12% of organizations have no ICS/OT network monitoring capabilities, exposing them to significant risk of undetected cyber threats and severe disruptions. For organizations with established SOCs, enhancing network monitoring capabilities is a natural and necessary progression.

Correlating Data for Comprehensive Analysis

Data collection and correlation across various ICS components is key for effective ICS/OT SOCs. The survey shows that most organizations (70%) collect and correlate data from ICS server assets, and 64% from network devices like firewalls and routers.

However, as Figure 22 shows, industrial organizations should also include less obvious components, such as serial/non-routable networks and embedded controllers, to gain deeper visibility and identify potentially hidden threats in high-impact facilities.

Deploying ICS-specific network monitoring appears to have a real impact on incident response. Respondents that had extensive ICS/OT network monitoring capabilities reported faster-than-average compromise-to-detection times, with over 50% detecting within *6 hours!*

Select the statement that best describes your ICS/OT network monitoring capabilities.

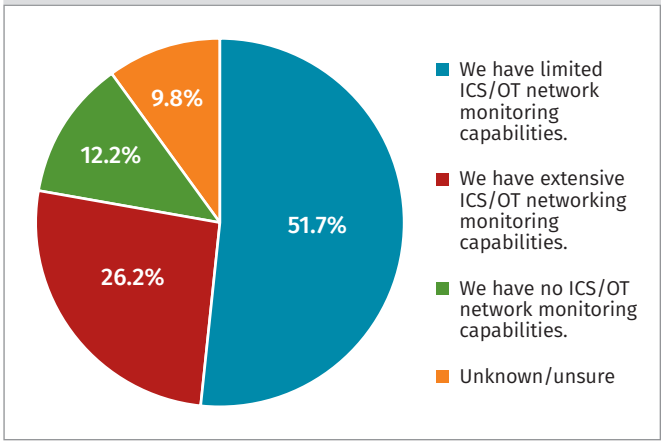


Figure 21. ICS-Specific Network Monitoring Coverage

From which control system components are you collecting and correlating data? ***Select all that apply.***

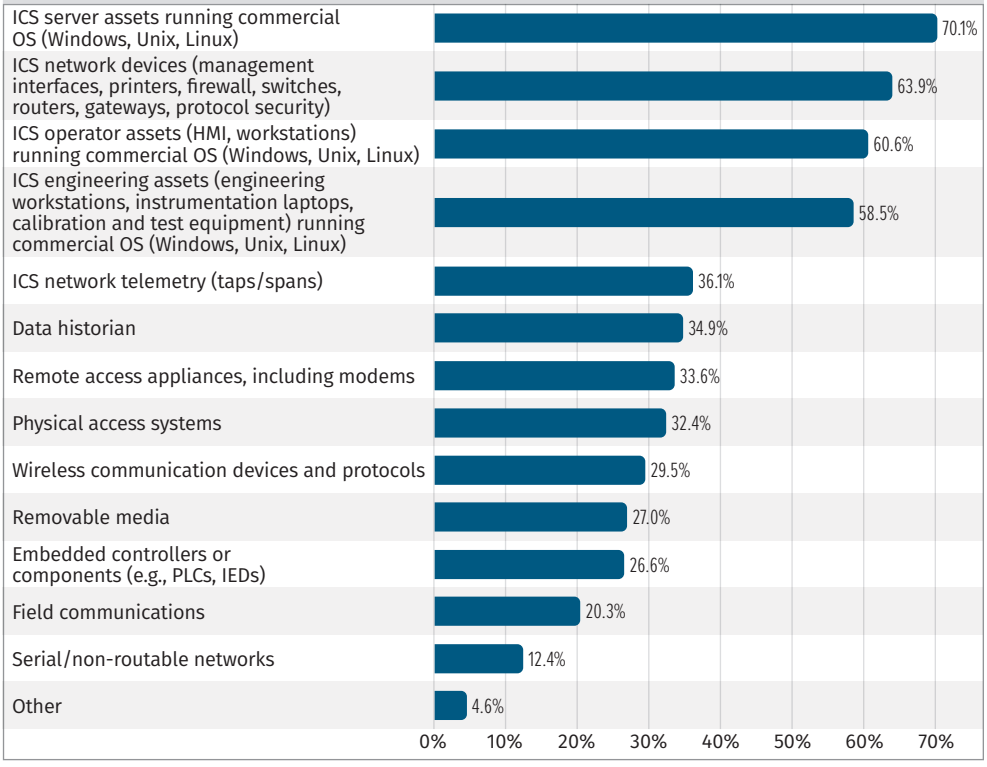


Figure 22. Data Collection and Correlation Across ICS/OT Components

Leveraging Threat Intelligence for Active Defense

With monitoring and data correlation in place, the next step is to leverage threat intelligence to make sense of the data and preemptively address potential threats. To do so, 56% of organizations use ICS-specific threat intelligence, relying mostly on external sources, with vendor-provided intelligence being the most common (79%).

Internal data can further refine this threat intelligence, as seen in Figure 23, which can include a mix of automated and human-driven processes, with 71% of respondents using threat detection across their ICS/OT security program. Of those, 70% use automated means, such as asset-based EDR, to detect threats within OT networks. Additionally, 40% utilize ICS protocol-aware network monitoring solutions, and 48% rely on anomaly-based detection engines. These tools, combined with trained ICS staff conducting threat hunting (38%), create a layered defense that can significantly improve threat detection and response capabilities.

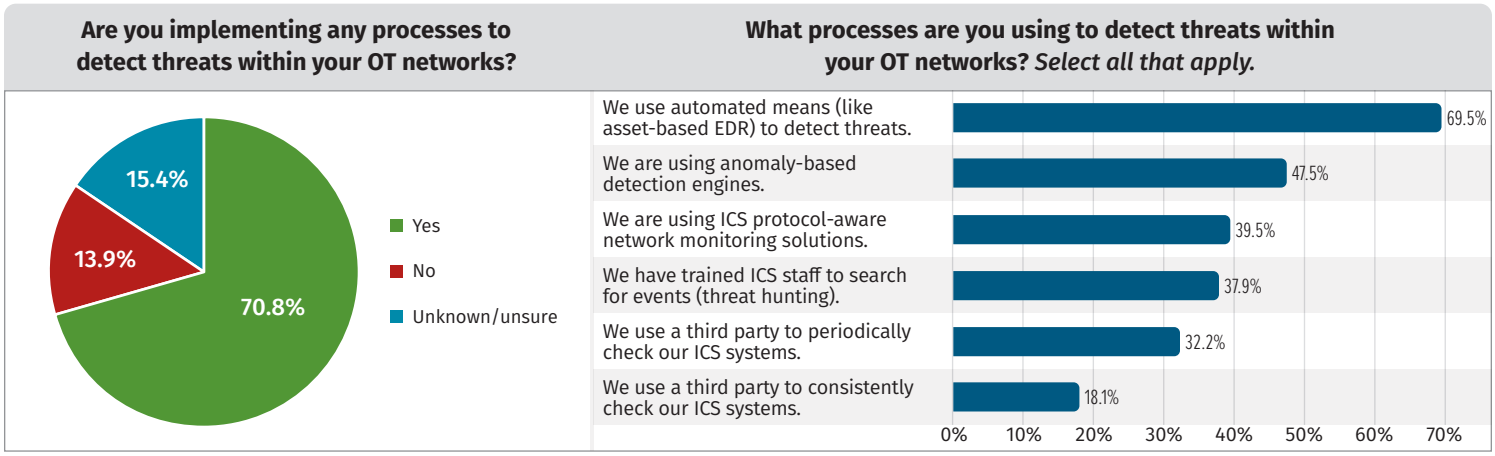


Figure 23. ICS/OT Threat Detection Capabilities

Third parties can be used to either consistently or periodically check ICS/OT systems, and this year's survey data shows a healthy use of those opportunities. Even respondents with extensive monitoring capabilities and a merged IT–OT SOC use these third parties, implying that there is a benefit in either additional coverage, external expertise, or both when examining ICS/OT threats.

This year's survey shows consistent advancements in the monitoring of ICS networks, with SOCs playing a central role in this evolution. Organizations are fostering stronger cybersecurity defenses by creating ICS-enabled SOCs, improving monitoring tailored to industrial environments, broadening data correlation, and utilizing threat intelligence. Nevertheless, the survey identifies that there is room for improvement, especially in terms of extending monitoring abilities.

Even respondents that said they have extensive capabilities and a merged IT–OT SOC report using third parties for help detecting threats, implying that there is a benefit in either additional coverage, external expertise, or both when examining ICS/OT threats.

SANS ICS Cybersecurity Critical Control #4: 2024 Secure Remote Access Trends

Remote access has been a difficult topic across ICS/OT security programs. Unlike IT networks, ICS/OT environments must balance access requirements with potential reliability and safety impacts. These extra considerations are exacerbated by the isolated locations of many industrial sites, where support is often limited. Remote access by vendors, contractors, and internal staff has increased over the past few years. COVID lockdowns did not help the situation when, for example, many vendors urgently provided their remote access tools for free. Temporary solutions, however, can create permanent risks. What was once a carefully planned activity became reactionary, making the need for secure remote access a top critical control.

Understanding remote access issues begins with recognizing the existing connectivity in industrial settings. A little over half (53%) of those surveyed have documented *all* of their connectivity outside the ICS/OT perimeter. Such documentation increases to 63% if the ICS program is mapped to cybersecurity standards, and increases even further (79%) if the organization also has extensive ICS network monitoring capabilities (as covered in Figure 21). This highlights how both governance and technology can aid organizations in their maturity across multiple security capabilities, as well as the importance of knowing your industrial assets and how/why they have external connectivity.

Once the network connectivity has been evaluated, organizations typically invest in a formal remote access policy or program. As highlighted in Figure 24, 84% of respondents have either an informal or formal policy in place for remote access.

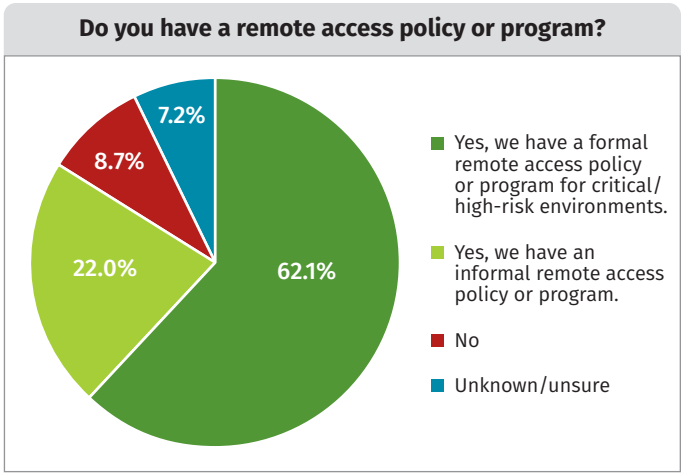


Figure 24. Remote Access Policy and Program Implementation

Policies can only go so far—where the rubber meets the road is when specific technical capabilities of the remote access are secure. As seen in Figure 25, multifactor authentication (MFA) is the most popular security control for remote access, followed by using a jump box to establish a trusted path to the ICS/OT environment. These approaches are largely driven by external factors, including ICS security standards, cyber insurance, and regulation—and, architecturally, are recommended best practices.

If an organization maps its ICS cybersecurity program to standards and has extensive ICS monitoring capabilities, it is 53% more likely to have documented *all* external connections to its industrial environment.

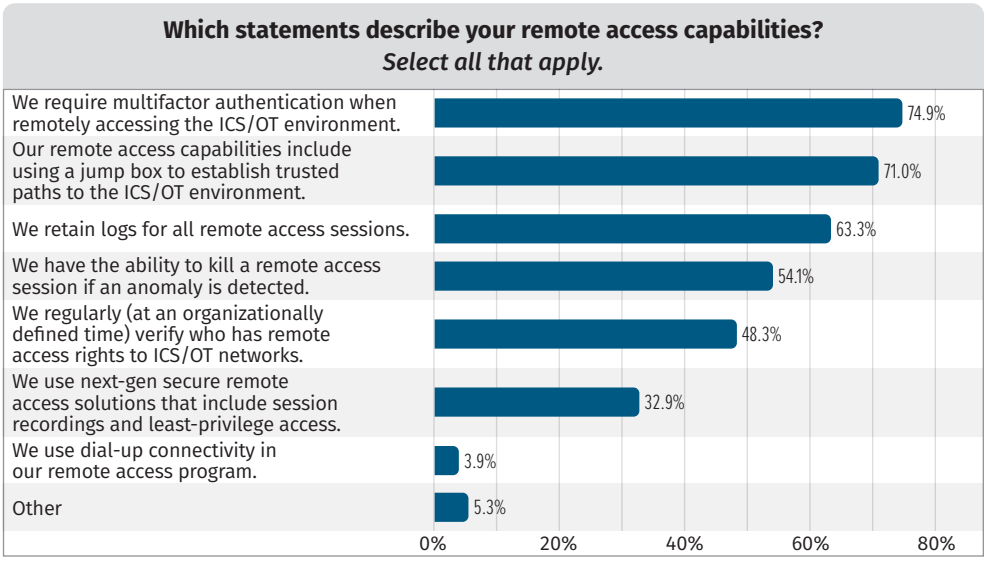


Figure 25. Secure Remote Access Capabilities

Interestingly, one-third (33%) of those surveyed reported having a next-gen secure remote access platform, and just over half (54%) could terminate a remote access session if an anomaly were detected. Compared to the technology plans in the Appendix, where a significant majority of those questioned utilize secure remote access (65%), a moderate share (21%) plan to deploy it over the next 18 months. This could indicate a potentially interesting shift as industry evaluates older, legacy remote access platforms for newer technology with enhanced security capabilities.

SANS ICS Cybersecurity Critical Control #5: 2024 Risk-Based Vulnerability Management Trends

ICS/OT vulnerabilities vary in their severity and exploitability. Vulnerability management does not mean "patch management" for many industrial organizations; each vulnerability needs to be assessed for its potential impact and the attack vector required for exploitation.

To understand these impacts and risks, industrial organizations typically start with some sort of security assessment. Most organizations (71%) reported having conducted security assessments of their control systems, aiding their understanding of system vulnerabilities. Of those that have performed security assessments, about 75% had performed the assessment in the past year. This is on par with previous annual surveys, as seen in Figure 26.

Percentage of Respondents Performing an ICS/OT Cybersecurity Assessment in the Previous 12-Month Period

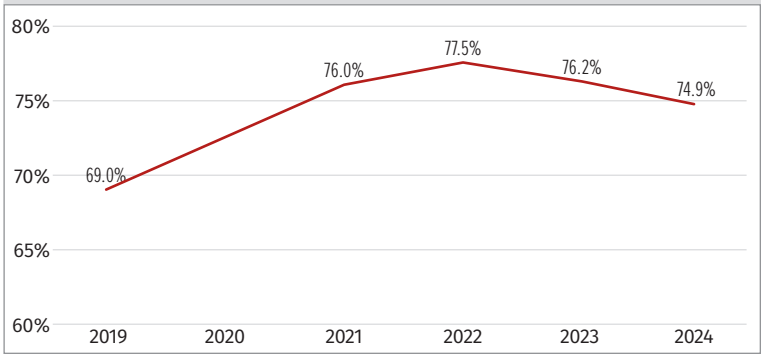


Figure 26. 2019–2024 Trend of ICS/OT Cybersecurity Assessments

Annual ICS/OT cybersecurity assessments appear to be "table stakes" for any industrial organization; the past five years of data shows about 75% of respondents regularly perform one.

Who performs the assessments has shifted somewhat, however. ICS/OT cybersecurity consultants performed more assessments in 2024, increasing by 7% from 25% in 2019–2023 to 32% in 2024. Internal ICS security teams saw a moderate 3% increase from previous years, implying that both IT consultants and internal IT teams are performing fewer ICS/OT assessments, offset by more subject-matter experts specific to industrial security. That said, the most popular assessment type is a paper-based vulnerability assessment (as seen in Figure 27), with fewer respondents leveraging more technical active vulnerability assessments (in test or production) and fewer still performing ICS-specific penetration testing.

What types of security assessments has your organization performed in the past 36 months in your ICS/OT environment? *Select all that apply.*

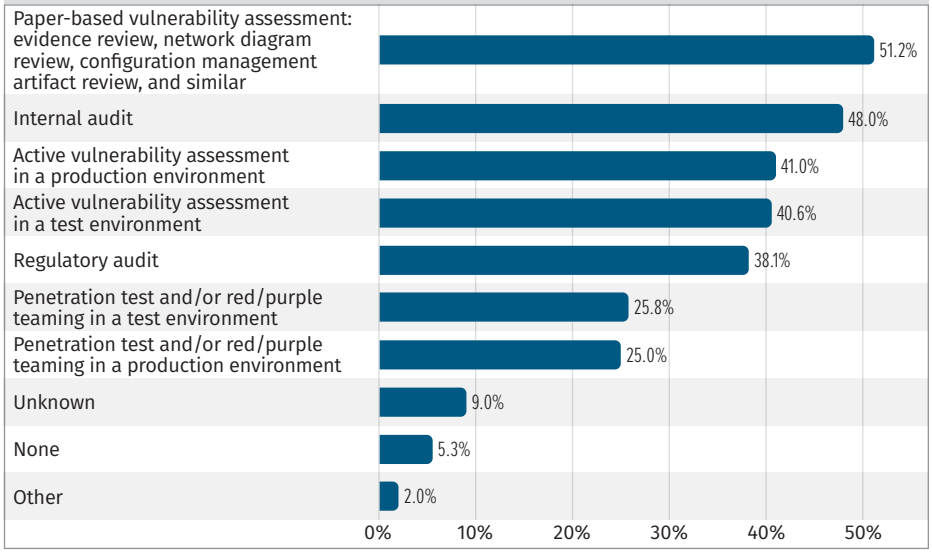


Figure 27. ICS/OT Cybersecurity Assessment Types and Popularity

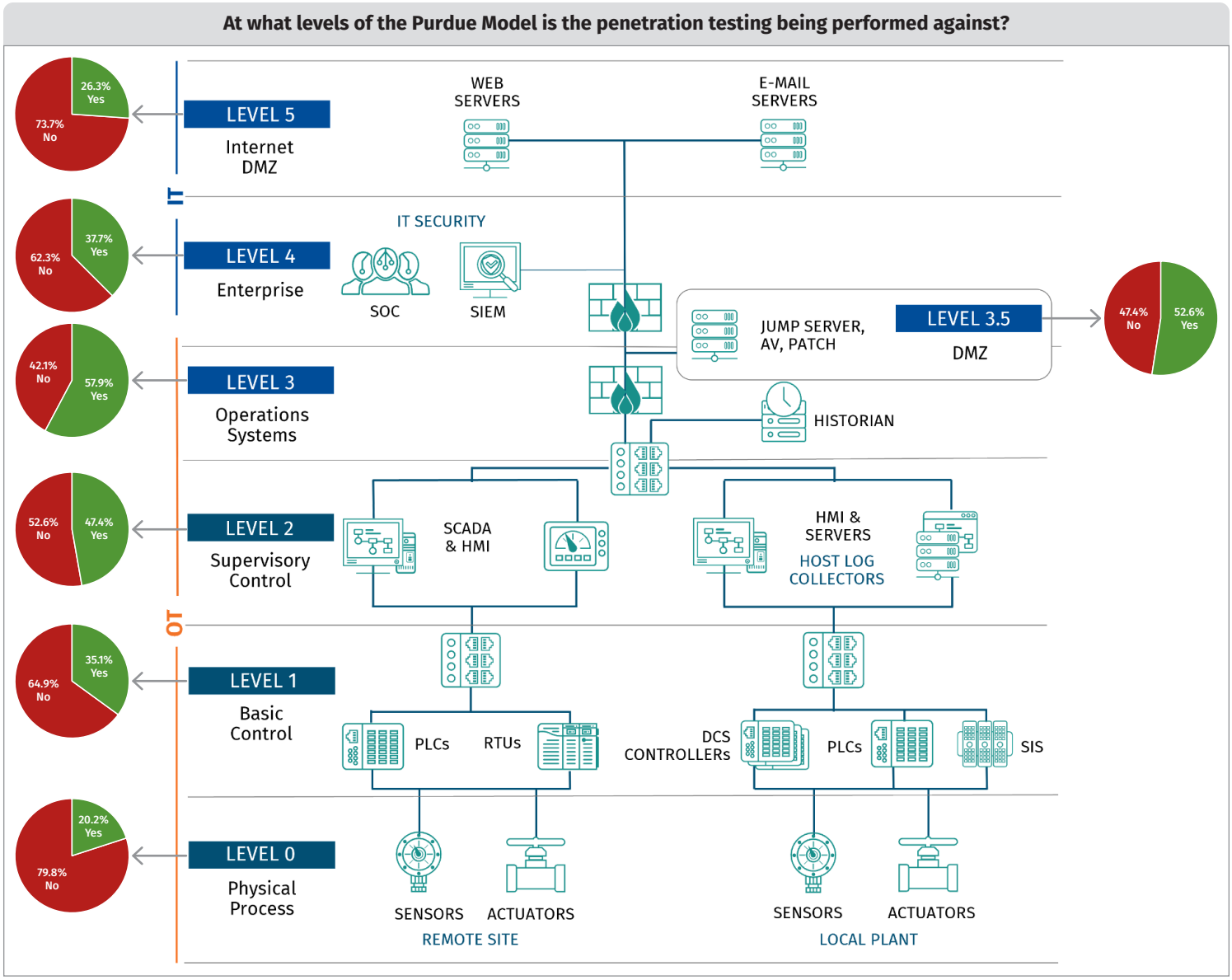


Figure 28. Penetration Testing Across the Purdue Model

When penetration tests are performed, they are mostly performed across the DMZ or Level 3 of the Purdue Model, as seen in Figure 28. Although difficult (and requiring ICS-specific skill sets and knowledge), penetration tests can be performed at lower levels of the Purdue Model when safety and reliability concerns are taken into consideration.

The benefits of a standards-based ICS/OT cybersecurity program are clear: organizations that follow *any* security standard are 15% more likely to conduct a security assessment *and* penetration test. The best results, however, come from combining both a standards-based approach and ICS-specific threat intelligence; this boosts the rates of security assessments to 88% (a 1.2x increase) and penetration tests to 74% (a 1.5x increase).

Organizations that both use a standards-based approach to their ICS/OT cybersecurity program and ingest ICS-specific threat intel perform more in-depth cybersecurity assessments.

There are, of course, other ways to detect vulnerabilities. As outlined in Figure 29, the most common technique is continuous monitoring across ICS/OT assets (52% of respondents), followed closely by passive network monitoring (47%). These methods reflect a shift toward more proactive and continuous forms of vulnerability management, leveraging both automated tools and collaborative efforts with vendors.

Assessing and tracking detected vulnerabilities can take many forms; 46% of respondents use configuration management artifacts for such purposes. When asked about coverage across their ICS/OT environments, 53% of respondents claimed that their configuration baselines could be leveraged for at least half of their assets.

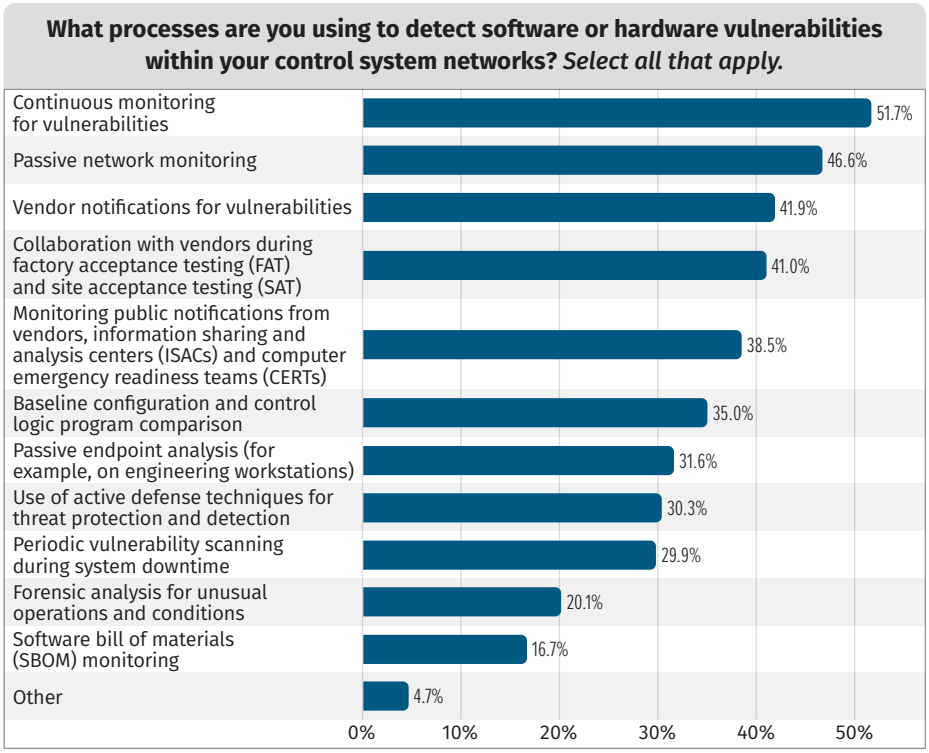


Figure 29. Vulnerability Detection Techniques

Once detected, organizations have several available options for implementing patches or finding a workaround, as outlined in Figure 30 from the U.S. Department of Homeland Security.

If patching is ultimately pursued, the most popular method used by respondents (34%) is to pretest and apply vendor-validated patches on a defined schedule.

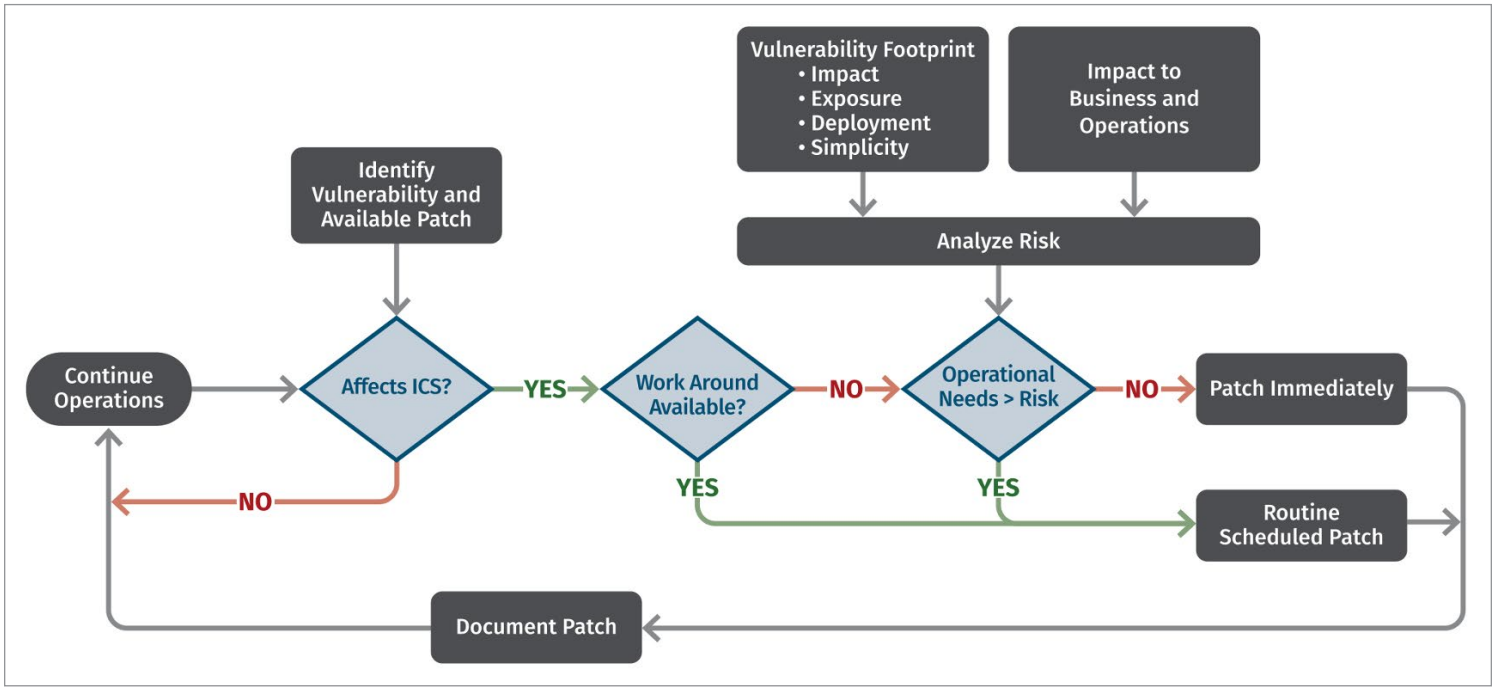


Figure 30. DHS Patch Urgency Decision Tree[7]

[7] "Recommended Practice for Patch Management of Control Systems," www.cisa.gov/uscert/sites/default/files/recommended_practices/RP_Patch_Management_S508C.pdf

Next Steps for Industry

This year's SANS State of ICS/OT Cybersecurity report highlights both progress and ongoing challenges in the field. The insights provided should be used to drive tangible improvements in cybersecurity programs. Organizations are encouraged to benchmark their own efforts against these findings to inform their strategies for 2025 and beyond—whether in budgeting, workforce development, or technology adoption.

Adopt a Standards-Based Program with Centralized Governance and ICS-Specific Threat Intelligence

Data shows that ICS/OT programs that integrate standards-based frameworks, centralized governance, and ICS-specific threat intelligence are more mature and capable of managing cybersecurity risks. These programs are better positioned to anticipate, detect, and respond to threats, leading to a more secure and resilient environment. Organizations should prioritize adopting these approaches to strengthen their security posture and address the unique risks within industrial environments.

Prioritize Workforce Development

The maturing ICS/OT cybersecurity workforce requires active leadership to continue its growth. Leaders must focus on attracting and retaining talent, investing in professional development, and facilitating knowledge transfer from experienced professionals to newer team members. This is crucial for building a workforce that is not only technically skilled but also deeply knowledgeable about the specific challenges of ICS/OT security.

Evaluating Technology Adoption

The pace of technology adoption in the ICS/OT space is another interesting trend identified in this report. The past five years have seen substantial growth in the implementation of ICS/OT-specific network monitoring, endpoint protection, and access control technologies. Although considered slower than traditional IT deployments, there are not only metrics showing some considerable growth, but also plans to continue to leverage new technologies for ICS/OT cybersecurity. The rapid evolution of the ICS/OT cybersecurity landscape demands that organizations remain agile and proactive in adopting advanced technologies.

Final Thoughts

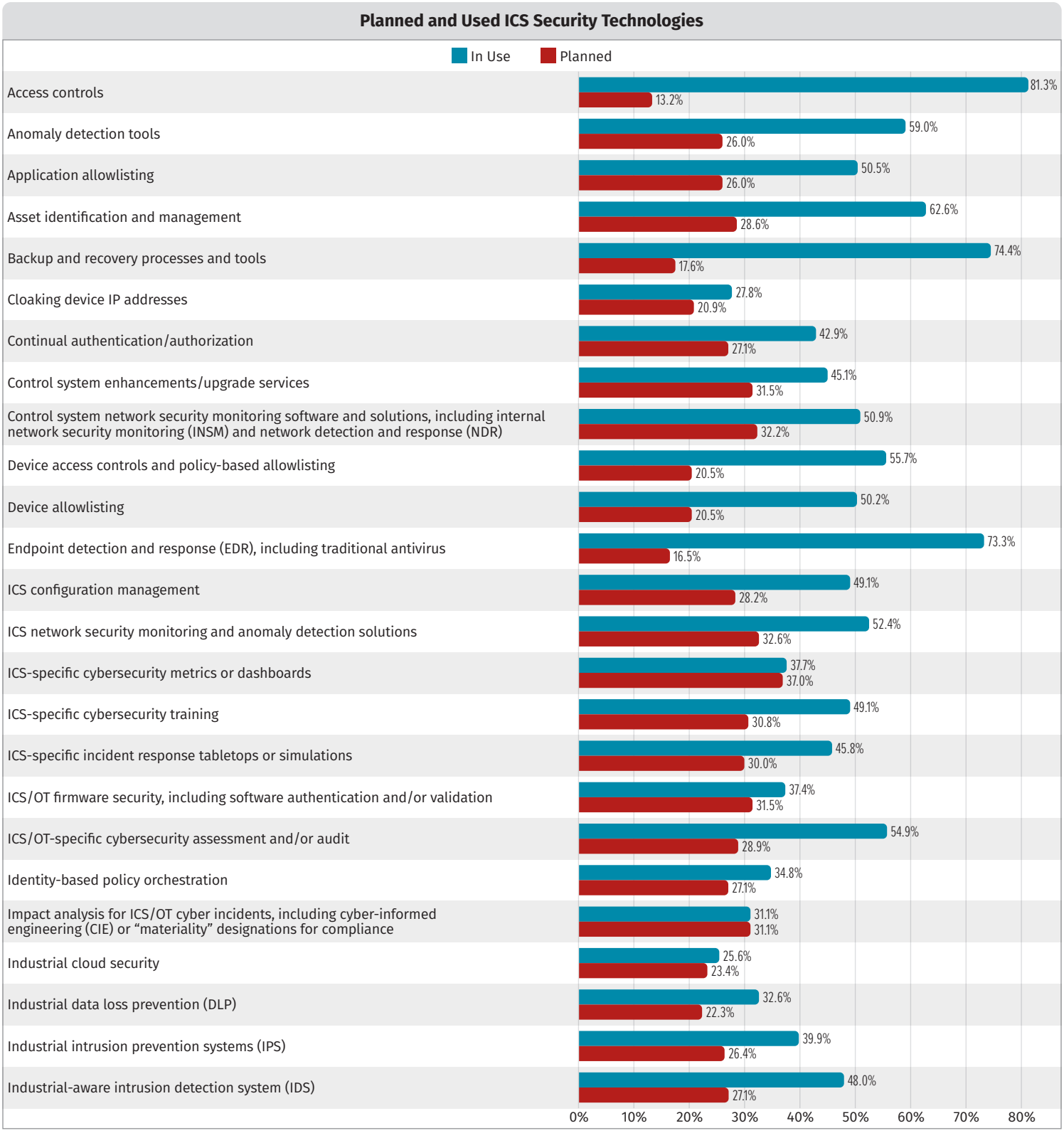
The insights from this report should serve as a catalyst for action, not just as data points to be filed away. Organizations must critically assess their security postures and use these findings to shape strategic plans for the future. By adopting standards-based governance, prioritizing workforce development, and embracing advanced technologies, organizations can effectively manage the complex risks facing critical infrastructure.

The path forward is clear: proactive, informed, and strategic actions are essential to ensuring the security and resilience of our ICS/OT environments. With the right focus and resources, organizations can meet today's challenges and be well-prepared for the threats of tomorrow.

Sponsor

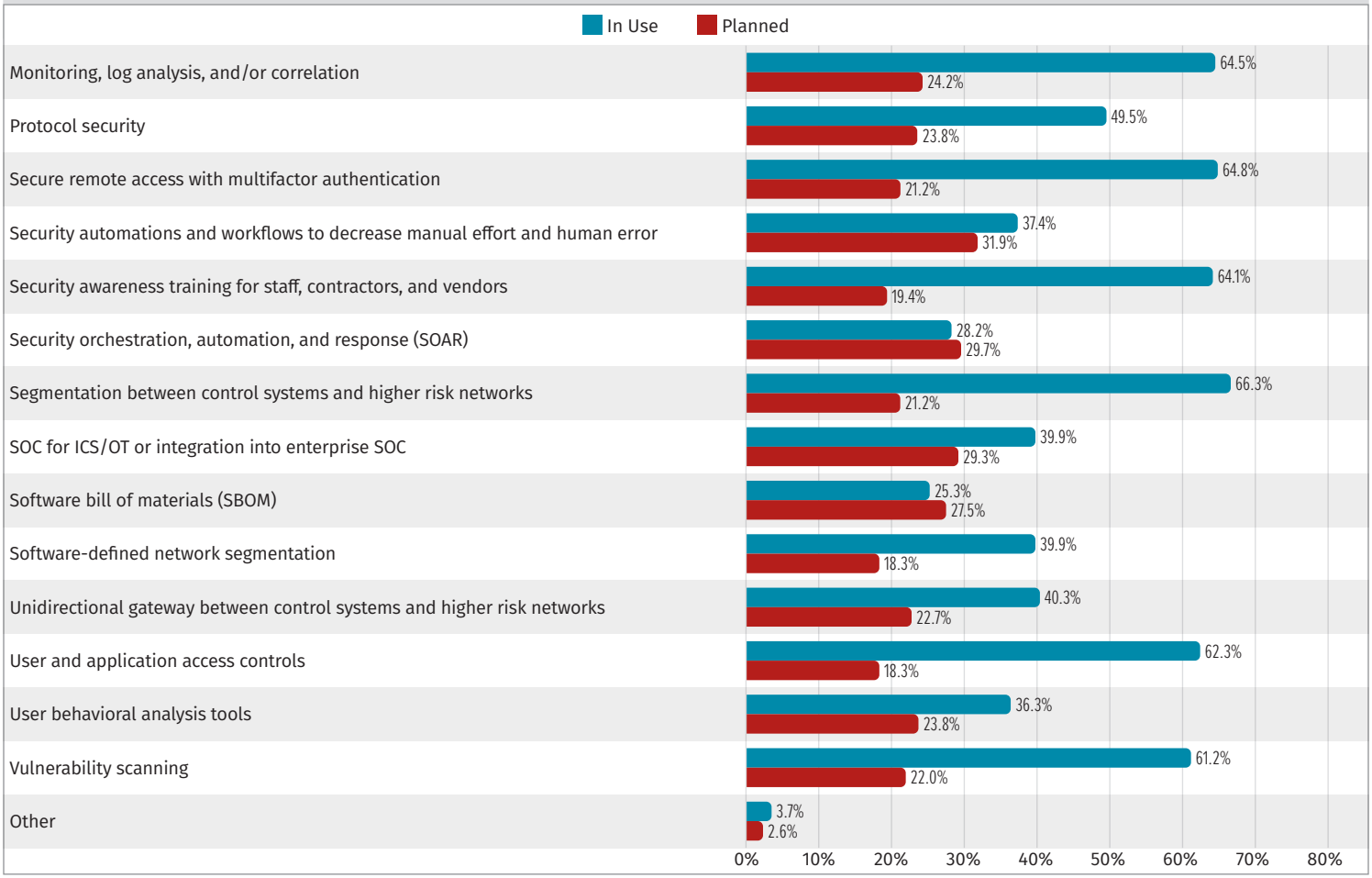
SANS would like to thank this survey's sponsor:

Appendix: 2024 Defensible Architecture Technology



CONTINUED ▶

Planned and Used ICS Security Technologies (continued)



Cyolo

SANS | Research Program

Product Briefing

ICS/OT with Cyolo PRO:

The Evolution of Remote Access in ICS/OT Environments

October 2024

In recent years, organizations have increasingly opened their Industrial Control Systems (ICS) and Operational Technology (OT) environments to remote access by employees and internal staff as well as third-party vendors and contractors. As a result of the pandemic and changing work practices, many industrial organizations rapidly deployed new remote access tools. These stopgap solutions kept operations running but also introduced ongoing security risks, as carefully controlled access management practices became ad hoc and reactive. Recognizing this, the SANS Institute identified remote access security as a critical cybersecurity control in 2022. The latest *2024 SANS State of ICS/OT Cybersecurity* report underscores the importance of secure remote access in defending critical systems against evolving threats.

Cyolo PRO: Redefining Secure Remote Access for ICS/OT Environments

Traditional Secure Remote Access (SRA) tools—such as VPNs, Virtual Desktop Infrastructure (VDI), and jump servers—fail to meet the complex needs of today's OT environments. These tools often lack real-time visibility, are difficult to manage, and expose organizations to security risks by granting overly broad access.

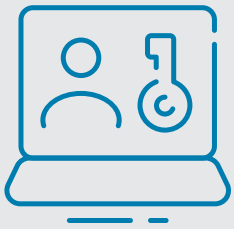
Cyolo PRO (Privileged Remote Operations) is an advanced SRA platform purpose-built for critical industries like manufacturing, energy, and oil & gas. Cyolo PRO secures remote access for employees, third-party vendors, and privileged staff, combining an innovative decentralized architecture with enhanced security, operational agility, and user experience.

Key Findings

Historically, ICS/OT environments were secured primarily through isolation. The recent shift toward connectivity and remote access has necessitated new approaches to security:

Multi-Factor Authentication (MFA)
74.9% of organizations now employ MFA as their primary security measure for remote access.

Jump Boxes
71% use jump boxes to create a secure path into OT systems.



Access Verification and Supervised Access
Less than half (48.3%) regularly verify remote access rights, while only a third (32.9%) employ next-generation solutions for session recording and least-privilege access.

Cyolo PRO Architecture and Key Capabilities

1. **Decentralized, Trustless (Zero Trust) Architecture—** Cyolo PRO operates within the user's own infrastructure, offering organizations full control over their security perimeter. It uses a reverse-proxy model, requiring no inbound network connections and minimizing network changes.
2. **Seamless Integration with Legacy Systems—**Cyolo PRO wraps OT assets in a secure layer that provides MFA, Single Sign-On (SSO), and session recording, allowing organizations to maintain security across diverse devices, from modern PLCs to legacy Windows hosts.
3. **Agentless Access for Third-Party Users—**Cyolo PRO enables secure remote access without the need for agents, eliminating compatibility issues for third-party users and allowing them direct access via a web browser.
4. **Zero Trust and Just-In-Time Access—**Adopting a zero-trust approach, Cyolo PRO uses digital identities with just-in-time creation, granular access policies, and restricted visibility for high-risk environments.
5. **Operational Agility—**Cyolo PRO can be deployed in under 15 minutes, making it easy to integrate into existing network topologies without asset modifications.

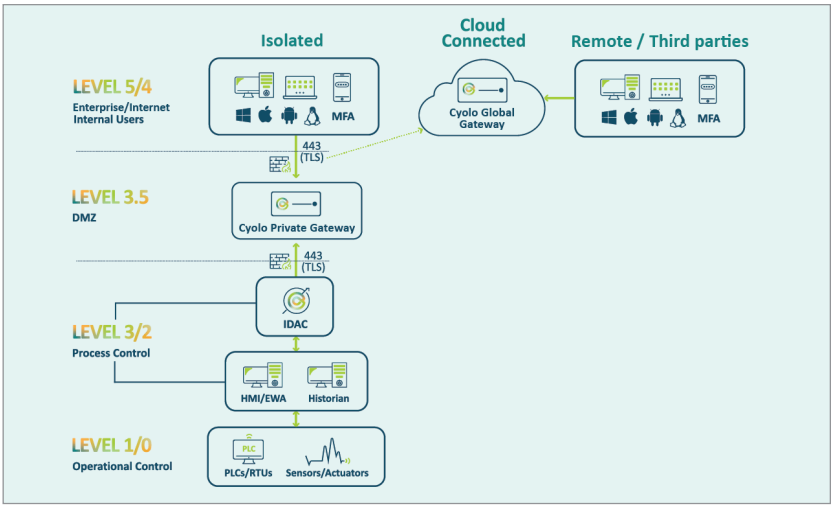


Figure 1. Its unique decentralized architecture allows Cyolo PRO to integrate seamlessly into any environment

Cyolo PRO Solves Major ICS/OT Security Challenges

The 2024 SANS survey highlights pressing challenges in ICS/OT environments, including:

- **Technical Integration of Aging Systems—**65% of organizations report difficulties integrating legacy OT systems with modern IT. Cyolo PRO's agentless architecture addresses these concerns by securely integrating legacy systems without requiring modifications.
- **Knowledge Gaps among IT Staff—**Half of surveyed organizations struggle in the face of IT staff's limited understanding of OT needs. Cyolo PRO simplifies management and offers secure, supervised access tailored to the unique requirements of OT.
- **Skilled Labor Shortages—**As 46% of organizations cope with labor shortages, Cyolo PRO's intuitive and agentless-first approach eases the burden on security teams, making secure remote access efficient and straightforward for all users.

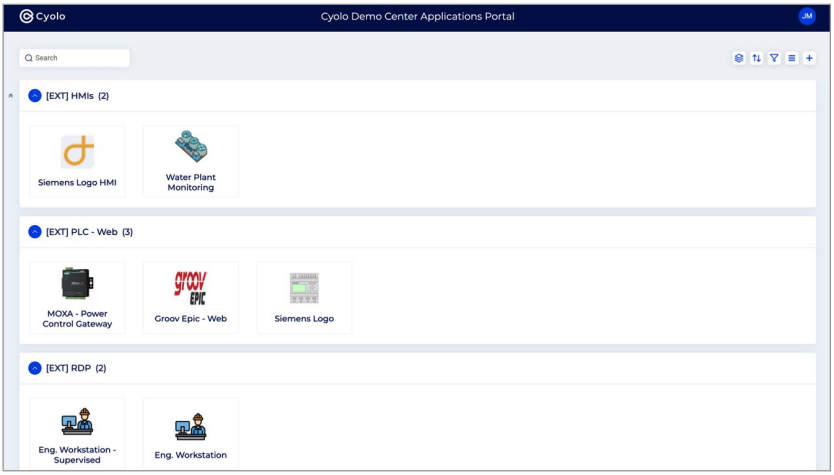


Figure 2. Verified users access authorized assets via the Cyolo PRO applications portal

Operational Benefits of Cyolo PRO

1. **Enhanced Visibility and Security Controls—**Cyolo PRO offers in-depth session monitoring, with granular policies for specific users, times, and geographic locations. It also includes access limitations and real-time supervision, so internal staff and OEMs can receive tailored security controls.
2. **Fast, Reliable Connections for Critical Situations—**Built without reliance on cloud processing, Cyolo PRO delivers rapid connections and low latency, ensuring that critical situations can be managed efficiently, regardless of location.
3. **On-Prem Security for OT Safety—**The on-prem nature of Cyolo PRO allows engineers to remotely access OT assets without compromising safety. This approach supports safe and secure operations, even for remote users handling sensitive ICS/OT assets.

Scan here to get a demo of the Cyolo PRO solution.

Cyolo.io/demo

Conclusion: Why Cyolo PRO is the Future of Secure Remote Access

Cyolo PRO addresses the urgent need for an effective, user-friendly, and highly secure remote access solution in ICS/OT environments. Its unique architecture, zero-trust approach, and agentless deployment enable organizations to overcome the traditional challenges of remote access, especially in environments with aging systems, third-party integrations, and labor shortages. With Cyolo PRO, industrial organizations can achieve the security, agility, and efficiency required to stay resilient in an evolving threat landscape.