SANS

Analyst Program

Survey

SANS ICS/OT Cybersecurity Survey: 2023's Challenges and Tomorrow's Defenses

Written by **Dean Parsons**

September 2023

OPSWAT.

Executive Summary

The ICS threat landscape continues to change, influenced by increased targeting of critical infrastructure with ransomware and by the discovery of an ICS-specific scalable attack framework in recent times.[1] Mature facilities are embracing the differences between IT and ICS/OT, then deploying specific ICS-aware technology, pursuing trained defenders, and focusing on dedicated ICS security efforts.

The evolution of targeted threats against critical infrastructure and ransomware events affecting ancillary ICS services send a clear message to the community. That message is: Proactive control system defense is required to preserve safety of operations. What's more, a well-designed, ICS-specific, defense-in-depth security program is not a nice-to-have, it is essential.

A well-designed, ICS-specific, defense-in-depth security program is not a nice-to-have, it is essential. But ICS facilities must go beyond preventive controls to be proactive.

Reactive-only organizations, that is, organizations waiting for already deployed preventive controls to be compromised or to fail, are at a disadvantage from the outset because adversaries have the means, methods, and motives to cause disruptive and destructive consequences to engineering systems that could negatively impact the safety of people (when adversaries use living-off-the-land attack techniques, for example). ICS cybersecurity defenders and leaders must be proactive. That is, they should assume defense-in-depth controls will fail, and push their team toward ICS threat hunting and making changes that reduce the ability of adversaries to living-off-the-land.

This 2023 ICS/OT Cybersecurity Survey addresses key questions, trends, and challenges, and puts forth best practices for practical control system cybersecurity appliable to all ICS sectors. This year's datasets reveal several changes in important areas and, most strikingly, a lack of effort in some key and increasingly risky areas.

This year's survey also maps key areas to the SANS Five ICS Cybersecurity Critical Controls,[2] setting forth the five controls most necessary to implement, given the state of the ICS threat landscape. The controls form an ICS/OT cybersecurity strategy flexible enough to be tailored to an organization's specific risk model, and they can be mapped to existing standards and frameworks such as IEC 62443[3] and NIST Cybersecurity Framework.[4]

---

[1] "Pipedream (toolkit)," https://en.wikipedia.org/wiki/Pipedream_(toolkit)

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

[3] "The World's Only Consensus-Based Automation and Control Systems Cybersecurity Standards," www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards

[4] "Cybersecurity Framework," www.nist.gov/cyberframework

Some insights from this year's survey include:

- Mature facilities realize the requirements for specific hands-on skillsets and training for ICS.
- ICS environments are using cloud services in a common way, and trending in a risky direction.
- Facilities can take an "implement now" strategy using the five ICS cybersecurity critical controls.
- Those knowledgeable in ICS skills are those chosen to perform ICS security assessments.
- A new approach to ICS security awareness helps all roles in the organization and changes culture.
- There is a pattern on where ICS penetration testing is being performed.
- Facilities are struggling with budgets, but there are several ways forward.

The 2023 SANS ICS/OT Cybersecurity Survey received over 700 responses representing a wide range of industrial verticals[5] from energy, chemical, critical manufacturing, and nuclear to water management and several others. Of the more than 60 subcategories across these verticals, many respondents sub-classified in electricity, oil and gas, equipment manufacturing, specialty chemicals, transportation equipment manufacturing, drinking water, and engineering services. Figure 1 provides a summary of key survey demographics.

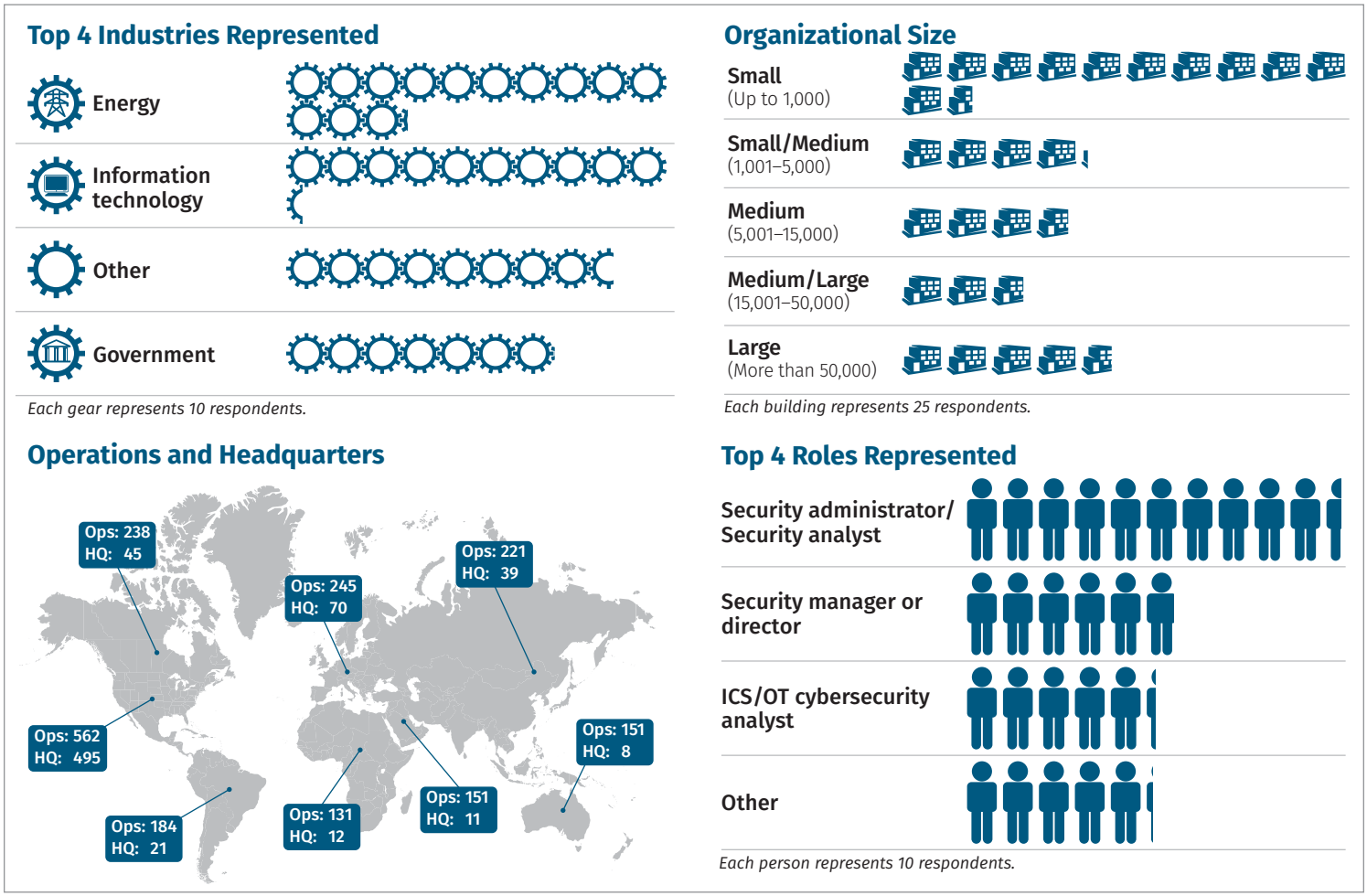

Figure 1. Survey Demographics

[5] CISA's critical infrastructure definitions with some modifications can be found at www.cisa.gov/critical-infrastructure-sectors

Introduction

This year, 25% of survey respondents consider the current cybersecurity threats against ICS as severe/critical. See Figure 2. The trend continues upward with a steady increase year over year—those who considered threats to ICS as "high" were 38% in 2019, 40% in 2021, 41% in 2022, and 44% in 2023.

Respondents identified the top three items of most importance for an ICS security program in 2023 as:

- **Obtaining network visibility:** ICS/OT-specific network visibility for ICS/OT protocols
- **Risk assessments:** Being able to conduct assessments to understand the risk to ICS environments
- **Detection of threats entering the ICS through a common vector:** Transient device threat detection

In contrast, the three items in order of least importance are secure file transfer, unidirectional gateways, and in last position, engineering software assessments.

How serious does your organization consider the current threats to control systems cybersecurity to be?

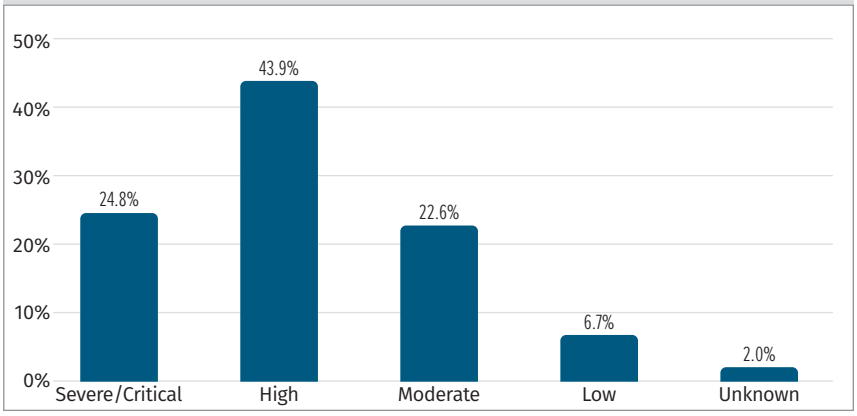

Figure 2. Current Threats to Control Systems

Transient Devices: A Multi-Sector ICS Risk

Transient devices can be described as portable devices that do not permanently reside in the ICS environment (such as but not limited to operational laptops or engineering system calibration tools). Transient cyber assets have specialized engineering software used to perform common control system tasks such as engineering troubleshooting, reprogramming or reconfiguring field devices, performing device updates, or other engineering system maintenance. Used for these purposes, a transient device operated by internal engineering teams, integrators, and external contractors could unintentionally introduce a contaminant into the control network. Similarly, an adversary targeting a specific ICS sector, or specific targeted organization, can attempt to introduce a contaminant onto a transient cyber asset with the hopes it will be brought into the target control network for further nefarious purposes and follow-on malicious actions.

ICS Threat Intel

When asked about consuming and leveraging ICS-specific threat intelligence, this year's respondents identify the No. 1 type of threat intelligence consumed as publicly available threat intel (see Figure 3). Generally, this is a no- or low-cost source. However, this may be a case of "you get what you pay for." Although a helpful place to start, publicly available threat intel could be limited in its value in the categories of timeliness and accuracy. Having less timely and accurate, and thus less applicable threat intel could leave facilities chasing more low-value, highly volatile indicators of compromise that could lead to higher volumes of false positives.

Are you leveraging ICS-specific threat intelligence in your OT defensive posture? ***Select all that apply.***

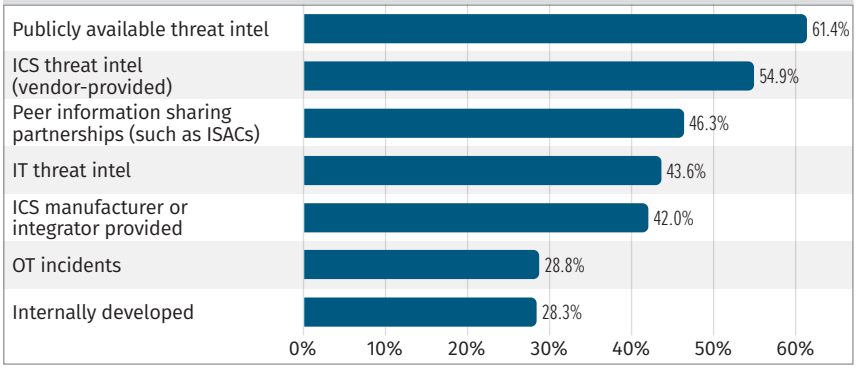

Figure 3. ICS Threat Intelligence Usage

Less timely, less accurate, and nonspecific ICS threat intel will keep ICS defenders in reactive-only mode. Responding to incidents and always just "putting out fires" can potentially burn out a team quickly. Instead, a better approach is working proactively to prevent an incident through making control system environment changes before impacts can occur to the engineering processes. Proactive defense is what makes a mature ICS security team and enables modern ICS threat hunting, which is a realistic and fruitful goal for any ICS today. Mature facilities realize IT threat intelligence fails to protect the control system due to differences in attack and defense techniques in ICS vs. IT environments. Fortunately, survey results showed specific ICS threat intel (vendor-provided) holding a spot in the top three sources for intel consumption the past three years in a row.

When asked about leveraging ICS threat intelligence, 45% of organizations in the survey indicate they are leveraging the MITRE ATT&CK® ICS framework with 57% of these organizations leveraging the defense framework to complete an ATT&CK ICS Attack Techniques coverage assessment. For those using the MITRE ATT&CK ICS for the betterment of the control system assets and networks protection, 37% are using it to understand ICS attack techniques and targeting activity, while 22% are using it to gain an understanding of ICS-specific threat detection capabilities.

The datasets also reveal that those who are leveraging it are working proactively to detect threats attempting to evade security technology, obtain initial access, perform lateral movement, obtain persistence in networks, and perform attack execution techniques.

It's encouraging to see low- or no-cost ICS defense tools become more pervasive in the security community to help both growing and established ICS defense teams. MITRE updates its ATT&CK Navigator[7] and related repositories on data sources, threat groups, etc., on a regular basis to assist both the enterprise (IT) and the ICS spaces. Additionally, MITRE has updated Caldera[8] to further assist ICS defenders. Caldera is MITRE's cybersecurity framework that empowers cyber practitioners to automate security assessments through autonomous adversary emulation and the testing and evaluation of threat detection.

MITRE Assessment

A MITRE ATT&CK ICS Techniques[6] coverage assessment can help identify important data sources in the control system environment for detecting adversaries that execute common attack techniques. This assessment can even be used to prioritize ICS SIEM rule creation, create ICS threat hunt hypotheses, and identify types of risk mitigations and related defense controls.

[6] "ICS Techniques," https://attack.mitre.org/techniques/ics/

[7] "MITRE ATT&CK Navigator," https://mitre-attack.github.io/attack-navigator/

[8] https://caldera.mitre.org/

Today's Top Vectors and Challenges

Rightfully, organizations governance bodies, standards, and frameworks are primarily focused on attack and infection prevention. However, prevention-only controls, while a critical part of a robust ICS specific defense-in-depth strategy, should never be at the cost of displacing the constant development, training, and execution of appropriate industrial incident response and recovery steps. ICS cyber incidents continue to happen. We must be prepared for a proper engineering response, with engineering recovery skills to meet ICS recovery point objectives (RPOs) and recovery time objectives (RTOs).

Those respondents concerned about attack prevention were asked to rank the common initial attack vectors based on incidents they have already experienced and responded to in their own ICS environment(s). See Figure 4.

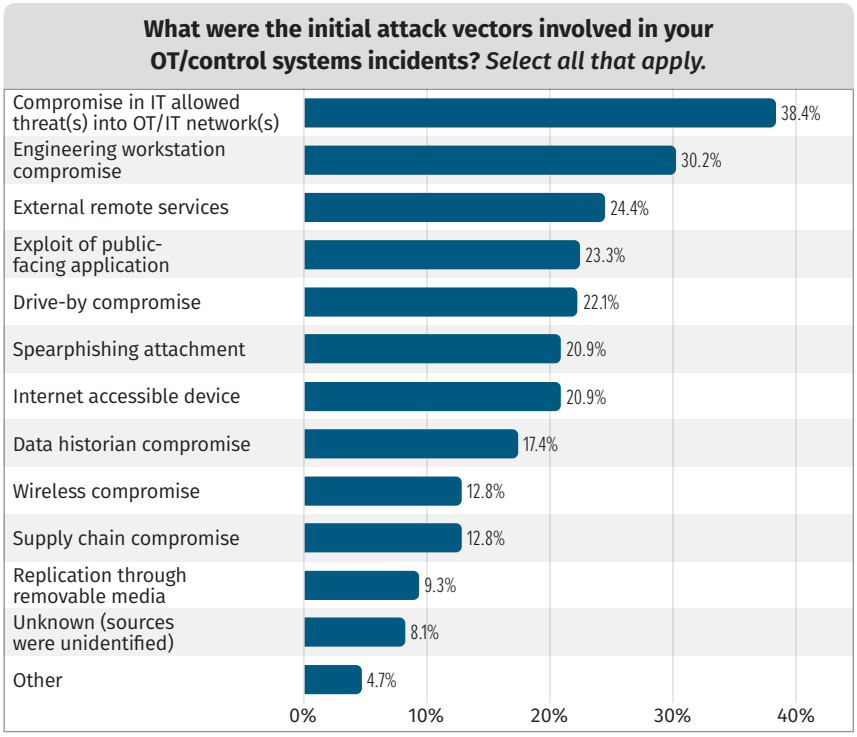

Figure 4. ICS Initial Attack Vectors

It is clear that most respondents are concerned about and have experienced ICS incidents where malware threats or attackers breached the IT business network, which in turn allowed the threats to access and pivot into the ICS/OT environment(s). Respondents ranked compromises in IT that allowed threat(s) into OT/IT network(s) first, followed by engineering workstation compromise, then external remote services.

Additional realistic ICS risks from this year's respondents include risks associated with adversary lateral movement and pivoting through compromised active directory infrastructure, a breach of IT and ICS network boundary devices putting sensitive ICS networks and engineering operations at risk, and third-party contractors onsite that could unintentionally deliver a contaminant via a transient device or through contaminated remote access pathways leaving the ICS vulnerable to remote attacks.

ICS Cybersecurity Roles and Responsibilities

The top three roles providing input to the survey this year are:

1. Security administrator/security analyst
2. Security manager or director
3. ICS/OT cybersecurity analyst

Of all respondents, 38% are focusing on both ICS and IT in their role, suggesting an increased responsibility in 2023, where those responsible for both ICS and IT security made up only 20% in 2022. Both IT and ICS teams are being asked to take on more, yet they might not understand the differences, additional skills, and experience needed to manage or perform effectively in both roles. This could be a result of resourcing struggles we all face.

IT security knowledge is certainly needed in an ICS cybersecurity role, but for effectiveness of control system defense and safety, defenders must not stop at traditional IT security skills. They must have additional crucial skillsets. Appropriate cybersecurity staff responsible for control system assets and networks must understand the nuances between traditional IT and ICS security. They must prioritize safety while understanding the engineering process and effects on the engineering equipment and the physical world when a cyber-to-physical incident occurs.

At a technical level, those responsible for ICS security must have a solid understanding of how engineering systems use industrial control system protocols and respective expected traffic flows. They also need to understand ICS-specific attack techniques, apply threat intelligence, and know at a deep packet level how ICS network protocols are used (and potentially abused, as seen in several recent attacks).

Maturing security analysts, architects, and incident responders are turning to the ICS ACDC (Active Cyber Defense Cycle[9]), which excels in network visibility, threat detection, industrial incident response, and engineering recovery in industrial control system environments. This cycle must be staffed with the aforementioned skills to be effective.

There is continued effort and investment into ICS-specific security assessments with 22% of organizations planning ICS assessments in the next 18 months. Nearly 70% of organizations already have ICS assessments as part of their already-deployed ICS security program for the protection of their control system environments in some capacity. For example, 23% have deployed continuous assessments in ICS, 19% have conducted ICS assessment within the past three months, and 16% within the last four to six months.

In 2023, those responsible for the implementation of security controls on industrial control systems are 1) ICS/OT security consultancy (25%), internal ICS/OT team (24%), and internal IT team (22%).

Mature organizations are realizing the value of ICS-specific security assessments and see the value in having those trained with ICS-specific knowledge bringing in the field-specific experience and insights needed for ICS-specific control implementation and protection.

[9] "The Sliding Scale of Cyber Security," September 2015, www.sans.org/white-papers/36240/

ICS Cybersecurity Awareness

For some facilities in 2023, a dedicated ICS security awareness program for internal engineering staff, vendors, and contractors is on their plan for implementation. Such programs yield clear benefits: ICS security awareness bridges gaps between IT and ICS; enables convergence of skillsets; and considers legacy assets, unique control system risks, threats, and specific incident response (IR) steps unlike what is expected in IT. ICS organizations can empower staff in all roles, and quicky. Short ICS security-specific awareness training modules, with knowledge checks, can help and provide a great metric to measure a positive change in culture to reduce ICS-specific risk.

The SANS Institute recently released a new series of Industrial Control System and Operational Technology cybersecurity awareness modules[10] that can help build or augment an existing cybersecurity awareness program. In the new series, more than 20 new training modules have been specifically developed to highlight the unique risks and defense capabilities for individuals working in critical infrastructure environments. The videos can be added to an existing security awareness program and address ICS-specific challenges, risks, and related control system defenses for many engineering-specific roles, such as IT, engineering staff, operators, administration staff, physical and safety staff, and ICS leadership.

ICS Connections and Risk

On a scale of zero to 10 (zero being not at all confident, 10 being very confident), facilities have a widely differing confidence level about whether their ICS and process control operations are separated from assumed hostile networks such as the IT enterprise network and the internet. By far, most facilities indicate a confidence level of an eight out of 10.

This survey result is favorable, given that one of the five ICS cybersecurity critical controls mentioned earlier in this paper is a properly architected and defensible network that separates risky zones from the engineering process zones. For example, such a network could include and assume properly designed access-control rules for industrial grade and ICS protocol-aware firewalls, or even data diodes where feasible.

We can reasonably assume facilities would have had to perform security assessments on remote access and network controls in and out of the ICS network to technically verify such a confidence level of network segregation. However, we would advise not only the completion of such an assessment with recurring verification, but also the monitoring of even trusted ingress and egress network paths.

[10] "ICS Engineer Security Awareness Training," www.sans.org/security-awareness-training/products/specialized-training/ics-engineer/

Regardless of confidence level, the ICS security should continue logging and reviewing remote access (including vendor remote access) and network boundary logs to ensure that any potential abuse of trusted zones or assets is investigated and acted upon immediately. Still today, a common vector for pivoting through trusted network zones is through the IT enterprise network into the control system network. This is an observable attack path for an adversary and can be mapped to both Stage 1 and Stage 2 of the ICS Cyber Kill Chain.[11]

Across the verticals, the data continues to reveal industrial control system security training and certification is sought after. Facilities and ICS/OT leadership recognize and highly value ICS/OT-specific certifications when they or their teams are responsible for control systems operation and security. Most respondents hold ICS/OT-specific certifications. The top three are: 1) Global Industrial Cyber Security Professional (GICSP) (47%)[12], 2) the Global Response and Industrial Defense (GRID)[13] certifications (28%), and 3) Critical Infrastructure Protection Certification (GCIP)[14] certification (22%).

Resources in the ICS security workforce are in higher demand. In fact, respondents of the survey indicate one of the biggest challenges facilities face is insufficient labor resources to implement existing ICS security plans. Hiring managers may be looking for specific ICS certifications. Existing employees may look for options to increase their knowledge or solidify their career path by obtaining accreditation in ICS security specifically. ICS/OT cybersecurity leaders can consider the two-day ICS418: ICS Security Essentials for Managers[15] course offered by SANS to sharpen the skills needed to build and lead an ICS/OT cybersecurity team.

A Variation on the Security Triad

In ICS, there is a misconception that the IT security triad of CIA (confidentiality, integrity, availability) is reversed in priority for ICS (availability, integrity, confidentiality). However, as SANS teaches in ICS418: ICS Security Essentials for Managers,[16] an effective and prioritized approach can be considered as:

Safety of system and people first—ICS Security supports safety where safety is the main goal and mission.

Integrity—Ensure control system operators' commands are getting to the field, and field devices are responding as expected without manipulation.

Availability—There is little use for a control system if it is available but in the control of an adversary.

Confidentially—Although important, confidentially would be at a lower position than the others mentioned. Additionally, the position of confidentiality may vary among ICS sectors.

[11] "The Industrial Control System Cyber Kill Chain," October 2015, www.sans.org/white-papers/36297/

[12] GIAC GICSP Certification: www.giac.org/gicsp

[13] GIAC GRID Certification: www.giac.org/certifications/response-industrial-defense-grid/

[14] GIAC GCIP Certification: www.giac.org/certifications/critical-infrastructure-protection-gcip/

[15] ICS418: ICS Security Essentials for Managers: www.sans.org/ics418

[16] ICS418: ICS Security Essentials for Managers

Control Systems and Cloud

Given the trends, benefits, and accessibility of cloud services, this year's survey increased focus on cloud service offerings, their applicability, and possible use-cases in ICS. Figure 5 shows the order in which organizations are using cloud-based services for ICS/OT systems.

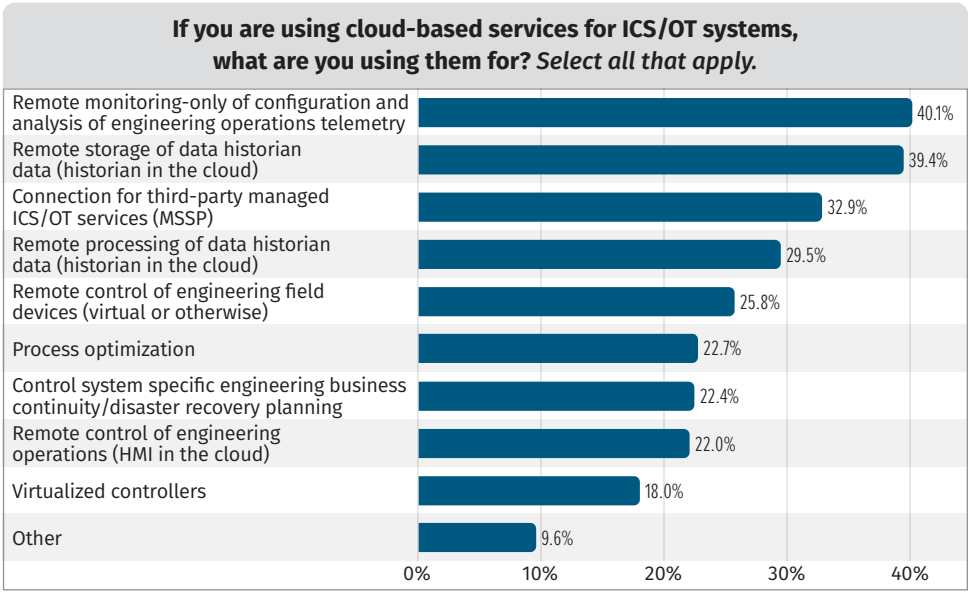

Figure 5. Cloud-based Services Used in ICS/OT Systems

A common ICS attack technique entails pivoting from IT into the ICS through trusted access paths or assets. As seen through threat intelligence, the data historian is one of those assets, trusted and residing between the IT and ICS networks with possible access to both networks.

Some vendors already provide a data historian solution in the cloud that comes with clear benefits. Done properly, and securely, a data historian implementation in secured cloud infrastructure may be effective for the business and could simultaneously reduce risk to the ICS network in some ways. If the data historian is truly removed from this traditional architecture, this pivoting path could be reduced or removed but could possibly open the ICS to other risks. It is important to note that this approach does not remove other non-data historian trusted pathways.

There is a growing concern about how some facilities may be using cloud for ICS. For example, facilities may allow HMI in the cloud, thereby allowing remote access for the capability to control engineering field devices.

To help manage these related risks, before deploying cloud services for any part of the ICS/OT systems/processes/assets/data, 61% of organizations Indicated that they complete a risk analysis and security evaluation of the cloud service provider for the secure administration and management of the data, connections, and access.

There are pros and cons here that could vary between the different critical infrastructure sectors and designs. Having a data historian in the cloud for monitoring could remove one common pathway into the ICS from IT while making the data available to authorized business users. However, access controls and data would be housed externally to the control system. If an HMI with control capabilities was housed in an external cloud, and was compromised, remote adversaries could directly control the engineering process with possibly less detection from internal ICS defense in depth controls on adversary pre-positioning. Facilities should proceed with care here. To ensure proper due diligence, business, safety, security risk, data storage compliance, and cloud infrastructure security assessments should be performed, and the results considered prior to architectural changes.

Penetration Testing the ICS

With the industry's increased interest in adopting penetration testing in ICS, we asked whether facilities are conducting penetration testing of their ICS/OT assets and networks. The survey was specifically designed to discover at which levels of the Purdue Model the penetration testing is being performed.[17] The results revealed a general pattern of more penetration testing at higher levels and less penetration testing at lower levels. Figure 6 shows the levels targeted for pen testing.

If you are conducting penetrating testing of your ICS/OT assets and networks, at which levels of the Purdue Model is the penetration testing being performed against? ***Select all that apply.***

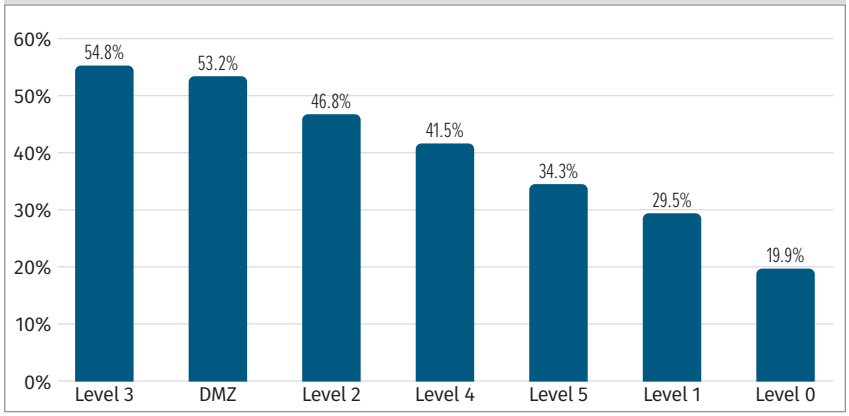

Figure 6. Penetration Testing in ICS/OT Environments

It is important to note that although there is value in penetration testing mature ICS programs and technical control system network architectures, penetration testers should fully understand the engineering systems being tested, what their purpose is for the control system, and the impact to engineering process if compromised or disrupted. The testing must be done with a high degree of caution and should include planning with engineering staff and associated leadership. It should be performed in a maintenance window to ensure utmost safety. If a higher risk level is acceptable, penetration testing could be performed cautiously in production in some cases, always with engineering knowledge. Testing will vary among ICS sectors.

Penetration testing does bring the inherent risk of introducing unintentional systems inconsistences during scanning or active system interaction. This holds true especially for legacy engineering devices.

A practical penetration test of a real-world scenario could be to emulate TTPs across IT into ICS, starting the test with an established IT foothold such as in Level 4 then attempting to move into the ICS network DMZ or lower (such as Level 3) toward traditional operating system-based HMIs or toward engineering workstations.

[17] "Introduction to ICS Security Part 2," July 2021, www.sans.org/blog/introduction-to-ics-security-part-2/

An overview of the Purdue Levels and the associated control system assets categorization follows.

Level 5: Enterprise Networks/Cloud

Corporate-level services supporting individual business units and users. These systems are usually located in corporate data centers.

Level 4: Business Networks

IT networks for business users at local sites. Connectivity to enterprise wide area network (WAN) and possibly local internet access. Direct internet access should not extend below this level.

Level 3: Site-Wide Supervisory

Monitoring, supervisory, and operational support for a site or region.

Level 2: Local Supervisory

Monitoring and supervisory control for a single process, cell, line, or distributed control system (DCS) solution. Isolate processes from one another, grouping by function, type, or risk.

Level 1: Local Controllers

Devices and systems to provide automated control of a process, cell, line, or DCS solution. Modern ICS solutions often combine Levels 1 and 0.

Level 0: Field Devices

Sensors and actuators for the cell, line, process, or DCS solution. Often combined with Level 1.

Facilities are urged to review the ROI on penetration testing based on currently deployed ICS controls to consider which practices are currently used as well as where the organization stands in its ICS-specific security maturity. This also will help assess a facility's risk appetite for impacting production or safety systems. For example, expect low ROI from an ICS penetration test against a facility that does not yet have a defensible ICS network architecture, has ICS passive technologies, or does not have active trained ICS defenders in place.

ICS Incident Response: Gaps and Wins

We asked who would be consulted when there are signs of an infection or infiltration of control system cyber assets or networks. The survey results showed that a non-specific cybersecurity solution provider (43%) would be the leading resource, followed by internal resources (38%), then control system vendors (36%). See Figure 7.

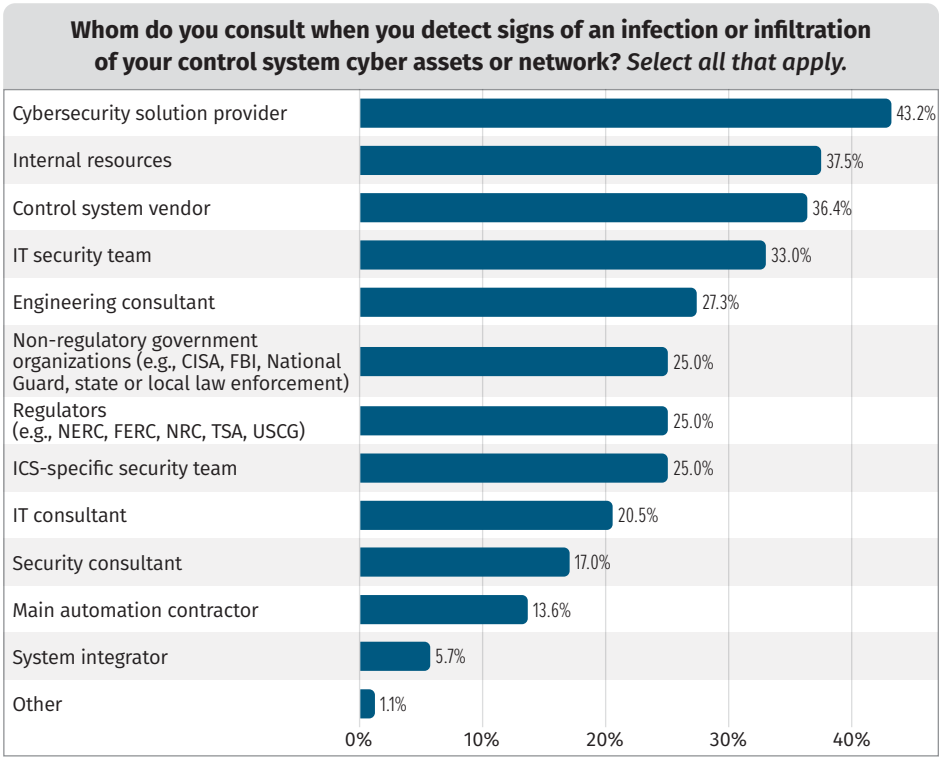

Figure 7. Who Assists When an Incident Occurs

ICS Incident Response Challenges

Although internal resources are frequently called to assist, these resources may not include any internal ICS-specific security teams. The ICS-specific security team category ranks in eighth place—making up only 25%, which is concerning.

The fourth resource that would get called to assist with industrial incident response is IT security. The risk here is related to the types of devices and those that require ICS knowledge during an active response. It does vary, but in general, 70–80% of assets in most ICS environments run non-traditional operating systems that IT security teams would likely not natively have skills to assess ICS threats on. Even the 20–30% of ICS assets that are running traditional operating systems inside the ICS environment have differences when it comes to ICS threat detection, forensic data sources, and response techniques.

We must not assume handling incidents in IT and ICS/OT environments are the same. Nor should we assume IT security skills alone (which are necessary for ICS incident response) are adequate for threat detection, adversary tracking, attack techniques, or industrial response and recovery in ICS. IT security skills must be, and can easily be, augmented for an effective ICS incident response.

Developing ICS Cyber Defense Teams[18]

Effective ICS cybersecurity staff understand the nuances among traditional IT and ICS security; the ICS mission; safety; the engineering process; ICS protocols and active defense strategies that excel inside control environments; and impacts of incidents in ICS to equipment, the environment, and people. A recipe to help us obtain, train, and retain the top ICS security defenders includes these ingredients: IT security knowledge augmented with ICS engineering and ICS attack knowledge, with an understanding of cyber-to-physical impacts while prioritizing safety at every step.

A recipe to help us obtain, train, and retain the top ICS security defenders includes these ingredients: IT security knowledge augmented with ICS engineering and ICS attack knowledge, with an understanding of cyber-to-physical impacts while prioritizing safety at every step.

Incidents in ICS environments range from the loss of visibility or control of a physical process to the manipulation of the physical process by unauthorized users, which can ultimately lead to serious personnel safety risks, injury, or death. The Department of Homeland Security states: "Standard cyber incident remediation actions deployed in IT business systems may result in ineffective and even disastrous results when applied to ICS cyber incidents, if prior thought and planning specific to operational ICS is not done."[19]

The ICS Defensible Cyber Position

More important now than ever, as taught in ICS515: ICS Visibility, Detection and Response,[20] is the Defensible Cyber Position as part of a practical ICS-specific incident response process. The Defensible Cyber Position can allow the control system to be functional (but in a limited capacity) in the event of an incident while fighting through an incident response, keeping systems up and safely operating. In many cases, it involves limiting or further restricting remote connectivity or disabling non-critical services. Some organizations may refer to this position as running in "manual mode" and it may consist of actions depicted in Figure 8.

Survey results show 56% of respondents have an exercised and documented plan to operate ICS engineering systems in a reduced capacity if some electronic systems in the control network are unavailable due to a cyber incident.

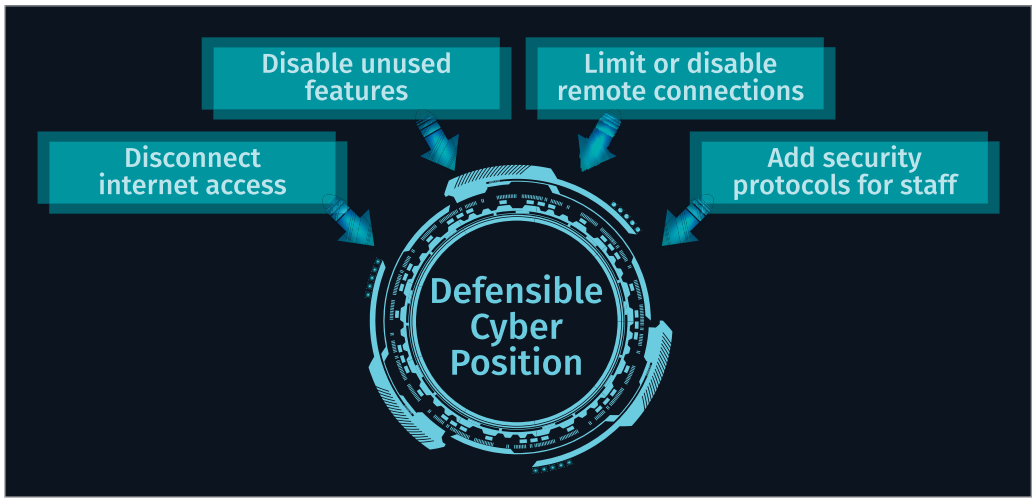

Figure 8. The ICS Defensible Cyber Position

A quarter of respondents are unable to answer whether they have an exercised and documented plan to operate ICS engineering systems in a reduced capacity, such as in manual operations. This is an area of opportunity to practically improve ICS incident response, at no or low cost, and can easily be discovered during an internal or externally facilitated ICS incident response table exercise.

[18] "Developing ICS/OT Engineering Cyber Defense Teams," August 2022, www.sans.org/blog/developing-ics-ot-engineering-cyber-defense-teams/

[19] "Recommended Practice: Developing an Industrial Control Systems Cybersecurity Incident Response Capability," www.cisa.gov/uscert/sites/default/files/recommended_practices/final-RP_ics_cybersecurity_incident_response_100609.pdf

[20] ICS515: ICS Visibility, Detection, and Response, www.sans.org/cyber-security-courses/ics-visibility-detection-response/

Beyond satisfying security compliance obligations, here are some other benefits of regularly conducting ICS IR tabletop exercises:[21]

Validation—ICS IR tabletop exercises validate readiness by comparing defense, response, and recovery controls against existing threats without introducing risk to the control environment. Areas of improvement will be identified in industrial cyber incident response plans, security technologies, and safety playbooks. Simultaneously, tabletops help train new and established team members on the industrial process, the ICS-specific security landscape, and related modern practical defenses.

ICS security awareness and team building—Creating ICS IR tabletop scenarios considers the most recent threat intelligence teams. This involves situational awareness and educating the right staff about adversary capabilities, attack techniques, and prioritized defenses. Regularly performing tabletops will establish and strengthen cross-departmental relationships needed for incident response events that could span multiple industrial sites across large geographic regions, where not one small team can manage an incident.

Practical defense actions—Tabletop exercises can identify gaps in threat detection, data source collection, log correlation, network segmentation, access control, security and safety processes, and work as a vehicle for the communication of roles and responsibilities.

ICS IR Tabletops – Ransomware Impacting ICS

Remaining in the top recommended ICS incident response tabletop scenarios is ransomware on IT impacting the control system processes, or ransomware directly on the ICS/OT network. Details on how to prepare for a run a ransomware scenario impacting ICS, and other tabletop scenarios, please review a recent SANS blog on this subject: "Top 5 ICS Incident Response Tabletops and How to Run Them."[22]

ICS Cybersecurity Investment Areas and Budgets

As we looked toward budgets for this year and the trends over the past three years, some interesting points were revealed. Essentially, budgets are down in just about every category we analyzed. Except for facilities having a budget of less than $100,000 USD, the data indicating facilities that have no budget for ICS/OT security drastically jumped from 2022 (8%) to 2023 (22%). See Figure 9.

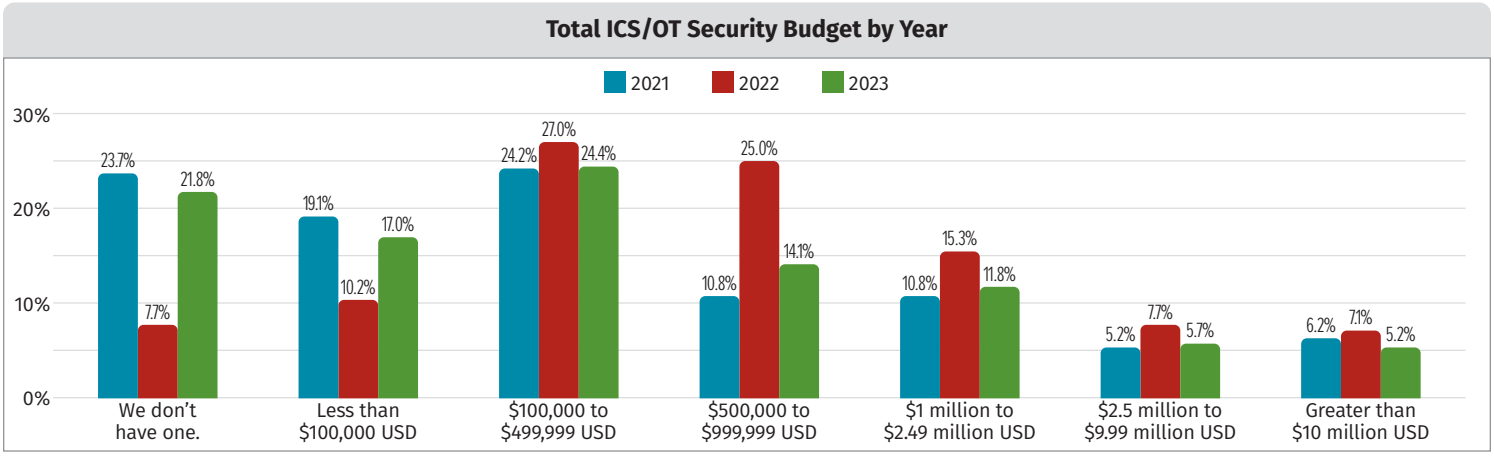

Figure 9. ICS/OT Cybersecurity Budget Comparisons 2021–2023

[21] "Top 5 Incident Response Tabletops and How to Run Them," June 2021, www.sans.org/blog/top-5-ics-incident-response-tabletops-and-how-to-run-them

[22] "Top 5 Incident Response Tabletops and How to Run Them"

Although some facilities may be in a low budget cycle for 2023, it's imperative that they continue focusing on their ICS cybersecurity roadmap. This means spending on what will provide the highest return to reduce the highest known risks. Security awareness, leveraging ICS tools from trusted sources for assessments (such as from MITRE), a risk-based approach to vulnerability management, and alignment with the five ICS cybersecurity critical controls, are solid places to shift the strategy for 2023.

Figure 10 shows the top three initiatives ICS facilities with solid budgets are investing in over the next 18 months.

As a top investment category, ICS visibility continues to be a top priority for facilities focusing on practical ways to improve their ICS security program, while the lowest investment category is in engineering sensor/actuator, Purdue Level 0 security.[23]

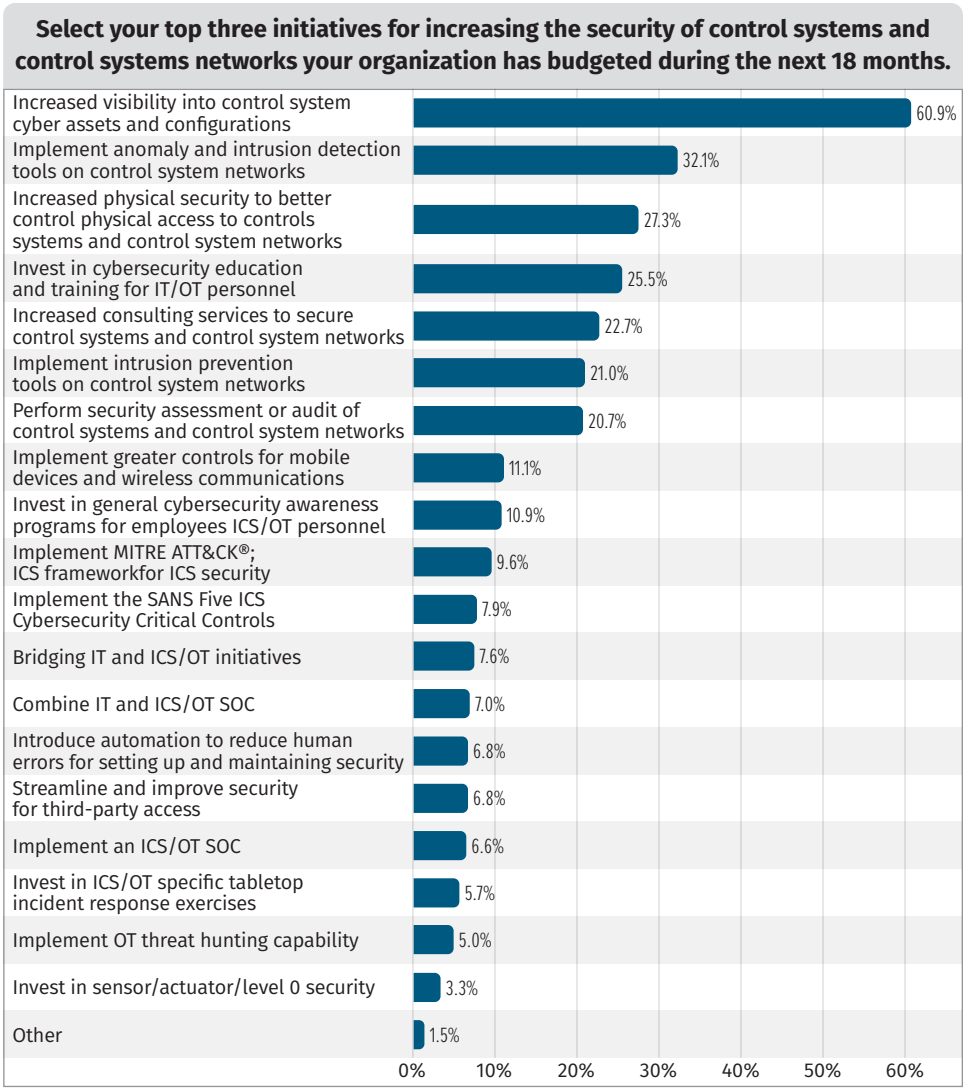

Figure 10. ICS Cybersecurity Investments in the Next 18 Months

Implement Now: The Five ICS Cybersecurity Critical Controls

SANS authors and instructors Robert M. Lee and Tim Conway have been working with the community to analyze all the known ICS cyberattacks for the purpose of creating the most important cybersecurity controls for organizations to implement with high priority, regardless of ICS sector.

The recent publication of the previously referenced whitepaper, *The Five ICS Cybersecurity Critical Controls*, sets forth the top five controls that are also designed to be an ICS/OT cybersecurity strategy that can scale to an organization's risk model. These controls can be mapped to existing standards and frameworks such as IEC62443 and the NIST Cybersecurity Framework. Each of the five ICS cybersecurity critical controls are described on the next page.

[23] "Control Systems Are a Target," October 2021, www.sans.org/posters/control-systems-are-a-target/

ICS-Specific Incident Response

This control is an operations-informed ICS incident response plan with focused control system integrity and engineering recovery capabilities enacted during an attack on an aspect of the engineering systems. ICS incident response-specific exercises must be designed to reinforce risk scenarios specific to ICS operations.

Survey results show only 52% of respondents currently have a dedicated ICS/OT incident response plan, with 17% unsure whether they have such a plan.

Defensible Control System Network Architecture

These are network architectures that support effective segmentation, visibility of control system traffic for analysis, log collection, asset identification, industrial DMZs, and enforcement for process communication integrity and reliability.

In this survey, most facilities indicate an 80% confidence level, meaning they are highly confident that their ICS networks are well segregated and secured from the IT network and the internet.

ICS Network Visibility and Monitoring

This control is characterized by continuous network security monitoring of the ICS environment with protocol-aware toolsets and system-to-system interaction analysis capabilities used to inform engineering of potential risks to the control, view, and safety of operations.

Sixty-one percent of respondents indicate that the top initiative for increasing the security of control systems and control system networks budgeted to be implemented within the next 18 months is increasing visibility into control system cyber assets and configurations.

Secure Remote Access

This control addresses identification and inventory of all remote access points and allowed destination environments, on-demand access, and MFA where possible, jump host platforms to provide control, and monitoring points within secure segments.

The data shows only 25% of facilities are collecting and correlating remote access event data, remote security access logs, and data transfer over remote access connections.

Risk-Based Vulnerability Management

This control requires an understanding of cyber digital controls deployed and device operating conditions that aid in risk-based vulnerability management decisions to patch vulnerabilities, enable appropriate safety-informed mitigations to impact, or monitor for possible attack exploitation internal to the control network. When it comes to patching vulnerabilities, less than 30% of facilities are deploying patches that are pre-tested, vendor-validated, and applied on a defined schedule in the ICS environment while 15% of facilities are applying all outstanding patches and updates during routine maintenance windows. See Figure 11.

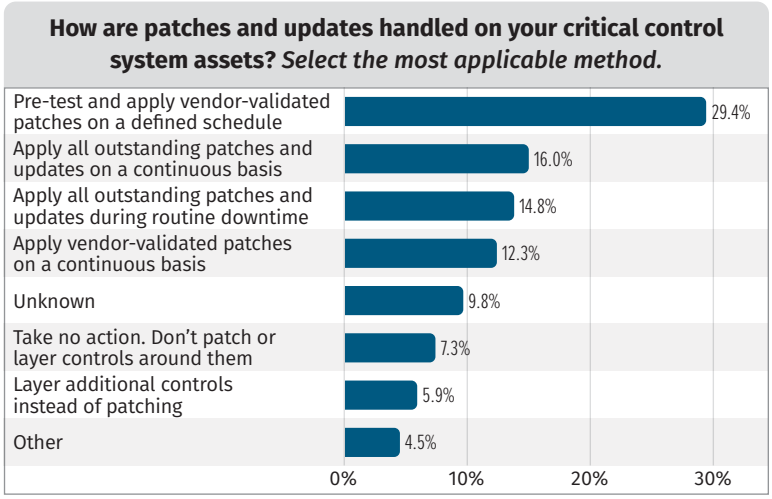

Figure 11. ICS Patch Management Approaches

Conclusion

Clear defense improvements continue for inventorying assets, strengthening access controls between IT and ICS networks boundaries, deploying ICS-specific network detection systems, and training and retaining staff with specific ICS security skillsets.

A combination of preventive and detective controls is part of any robust ICS cybersecurity defense strategy and will continue to provide value. Proceed with care when using controls that automatically block or prevent ICS network communications or endpoint engineering application commands that could introduce false positives and impeded operations.

Modern ICS defense programs must include ICS-aware technologies yet be prepared for industrial responses focused on engineering system integrity and engineering recovery capabilities. This means assuming some security controls will fail at some point, where trained ICS cyber defenders with knowledge of the engineering process, commands, and protocols will appropriately respond, prioritizing the safety and reliability of operations at every step. Safety is the No. 1 goal in control systems.

Those responsible for ICS/OT security at facilities would do well to consider these top takeaways to kick-start or continue maturing their ICS cybersecurity program:

The five ICS cybersecurity critical controls—The related whitepaper described earlier in this paper detail the controls that will help prioritize implementation and map to several standards and frameworks that may already be in place.

ICS security awareness—Short-format ICS-specific awareness modules with knowledge checks will strengthen the culture and reduce risk across many roles. ICS practitioners will further enhance defense, response, and recovery capabilities, and administrative and non-technical employees will gain the knowledge to better understand their crucial role and contribution to critical infrastructure protection. Corporate leadership will examine best practices in critical skills such as incident handling, information assurance, and supply chain risk.

ICS IR plan and exercises—ICS facilities will benefit from performing ICS-specific tabletop exercises. The exercise scenarios should be derived from sector threat intel with a focus on control system integrity and engineering recovery capabilities during a cyberattack. ICS IR-specific exercises must be designed to reinforce risk scenarios specific to engineering operations.

ICS network visibility—Visibility into ICS networks using ICS-aware network detection systems continues to be a top priority. However, this control must be powered with specifically trained ICS security defenders. Only then can the return on investment be high.

ICS in the cloud—The benefits are clear where cloud services could be leveraged for some monitoring capabilities for ICS. However, exercise caution when faced with putting an HMI or similar control elements into external cloud infrastructure without first performing the proper risk, safety, compliance, and security assessments.

Sponsor

SANS Would like to thank this survey's sponsor: