REPORT

2023 State of Operational Technology and Cybersecurity Report

FORTINET

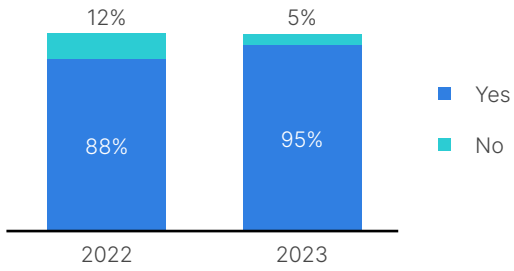
Table of Contents

Key Takeaways

People

In nearly all organizations surveyed, CISOs are now or will soon be responsible for OT cybersecurity. Also noteworthy, more OT cybersecurity professionals now come from IT security leadership rather than the operations team.

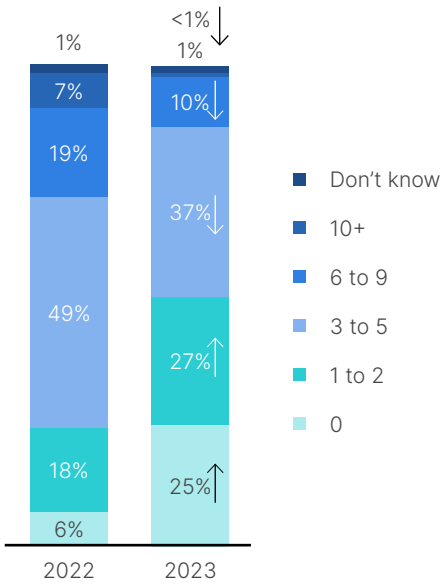
Cybersecurity to Be Under CISO in Next 12 Months



Cybersecurity Incidents

While the number of organizations that did not incur a cybersecurity intrusion improved dramatically YoY (from 6% in 2022 to **25% in 2023**), there is still significant room for improvement. In fact, three-fourths of OT organizations reported at least one intrusion in the last year, and nearly one-third of respondents reported being victims of a ransomware attack (**32%**, unchanged from 2022). Intrusions from malware and phishing increased **12%** and **9%**, respectively.

Number of Intrusions in Past Year

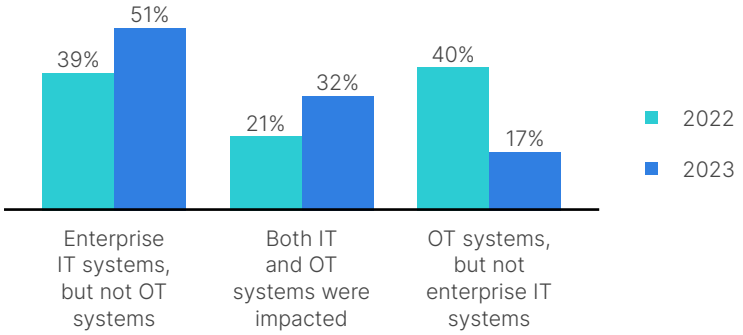


# By Cybersecurity Maturity			
	Level 0–2	Level 3	Level 4
Don't know	1%	0%	0%
10+	1%	2%	0%
6 to 9	11%	11%	6%
3 to 5	38%	35%	40%
1 to 2	36%[B]	21%	25%
0	14%	31%[A]	29%[A]

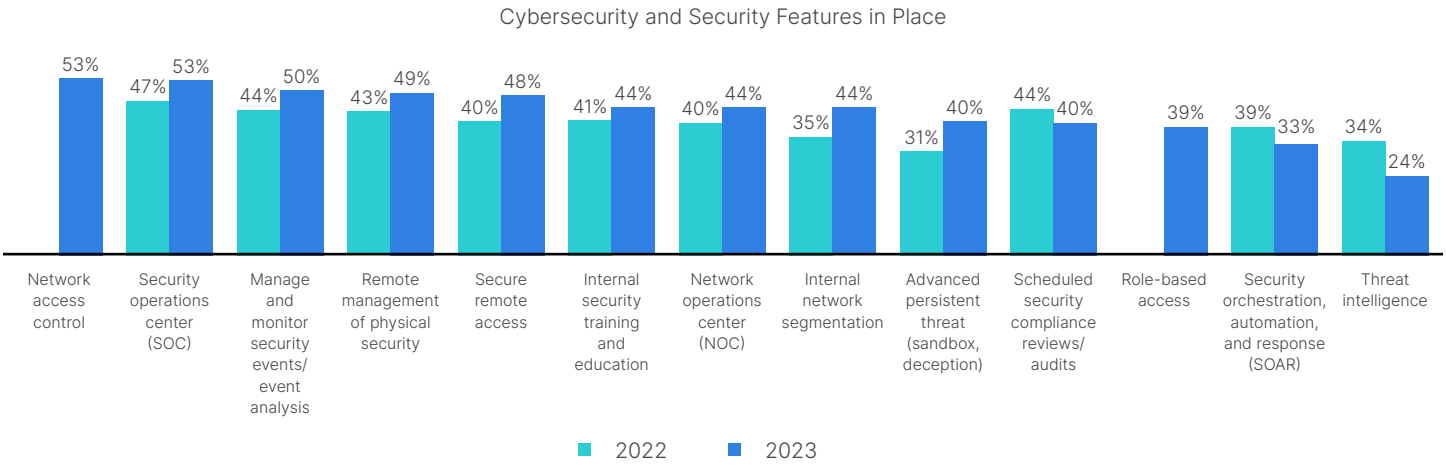
The Impact of Intrusions

When a cyberattack occurred earlier this year, nearly one-third **(32%)** of respondents indicated both IT and OT systems were impacted—up from only 21% last year. To combat intrusions, OT professionals are increasing cybersecurity solutions in their industrial networks.

Environments Impacted

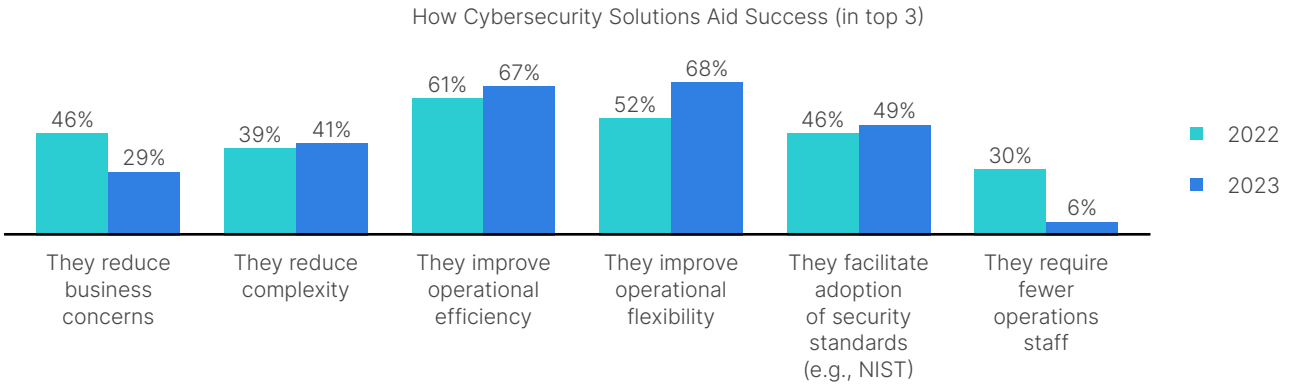


Advanced persistent threats, internal network segmentation, and secure remote access have increased the most, while threat intelligence has declined as a solution.



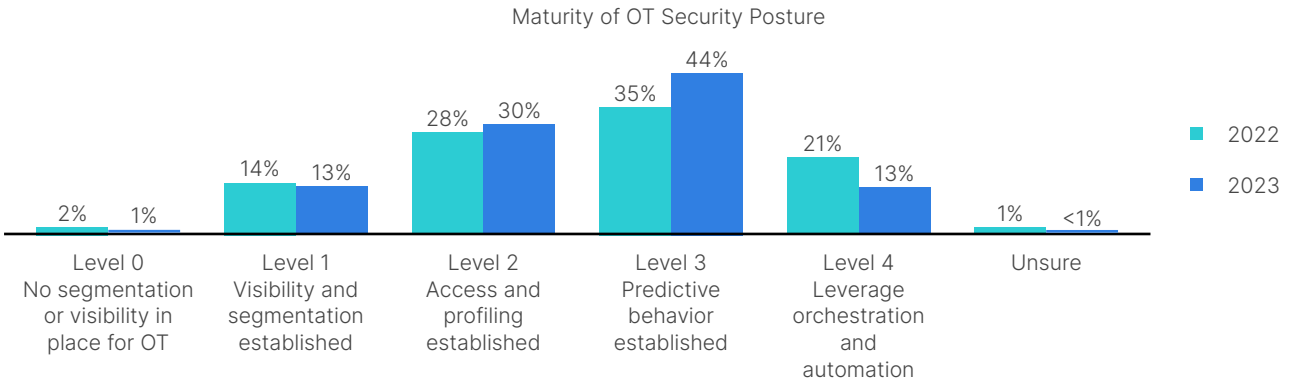
How Cybersecurity Helps

While survey findings reveal that cybersecurity solutions continue to aid in the success of most **(76%)** OT professionals, particularly by improving efficiency **(67%)** and flexibility **(68%)**, the data also shows that solution sprawl makes it more difficult to consistently protect their converged IT/OT landscape.

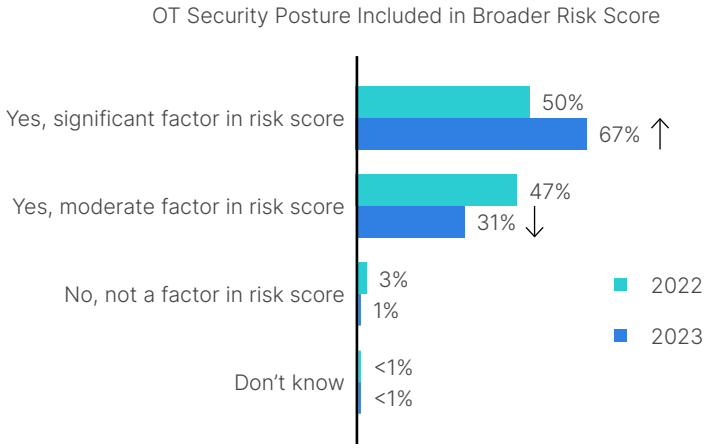


Cybersecurity Posture

While fewer individuals characterize their companies' OT cybersecurity posture as Level 4 ("highly mature") this year as compared to 2022 (down to **13% from 21%**), **44%** of all organizations now rate themselves at Level 3, up from last year's 35%. This may reflect a maturing approach to assessing capabilities, resulting in a more realistic view of the state of their posture.



Almost every organization (98%) now includes its OT cybersecurity posture in the broader risk score shared with executive leadership and boards of directors.

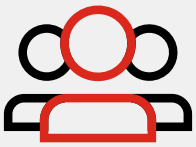


Executive Summary

The Fortinet 2023 State of Operational Technology and Cybersecurity Report is our fifth annual study based on data from an in-depth worldwide survey of 570 OT professionals conducted by a respected third-party research company.

Protecting OT systems is now more critical than ever as more organizations connect their OT environments to the internet. Although IT/OT convergence has many benefits, it is being hampered and handicapped by advanced and destructive cyberthreats. The spillover of these attacks is increasingly targeted at OT environments. For these reasons, this year's survey data indicates that OT cybersecurity is now more central and crucial in an organization's risk portfolio than ever.

An analysis of the 2023 data reveals that there are currently four prominent global trends:



2023's report finds that 95% of organizations have made their CISOs responsible for OT cybersecurity.

- There has been an overall decline in intrusions due to fewer insider breaches, though ransomware and phishing are still major threats. Rather than a decrease in cyber risk, however, this may be due to cybercriminals adopting a more targeted approach.
- Nearly all organizations have placed the responsibility for OT cybersecurity under a chief information security officer (CISO) rather than an operations executive or team.
- Organizations and OT professionals rely on a wide range of cybersecurity solutions to combat intrusions. There are indications that point products and solution sprawl may make it more challenging to apply policies and enforce them consistently across the converged IT/OT landscape.
- The number of respondents who consider their organization's cybersecurity maturity to be at Level 4 fell from 21% a year ago to 13% today, while those who see their cybersecurity to be at Level 3 are up from 35% to 44%. This data swing seems to indicate that OT professionals now have a more realistic self-assessment of their organization's OT cybersecurity capabilities.

After five years of surveying OT professionals, the most encouraging news is that cybersecurity now appears to be finally out of the shadows. Operational technology cybersecurity now has the full and frequent attention of enterprise leadership and C-suites. However, most organizations still have much work to do, and there is never time to "rest on one's laurels" regarding cybersecurity.

To assist your organization with improving its OT security posture, this year's State of Operational Technology and Cybersecurity Report concludes with a list of common best practices that top-tier organizations employ to keep their OT systems secure.

Introduction

Today, no one can doubt the importance of protecting OT systems. Operational technology controls the critical infrastructures that we all rely on—from managing the electrical grid to operating water and sewage systems, running transportation networks, manufacturing essential goods, and enabling global supply chains. And lest anyone forget, OT is also a key component of many industrial organizations' digital acceleration efforts.

Today's market conditions have made the adoption of Industry 4.0 methodologies and technologies an "era of connectivity, advanced analytics, automation, and advanced-manufacturing technology"[1] essential for manufacturers and other industries to remain competitive.

Cybersecurity Threats to OT

The convergence of IT and OT networks has not occurred without drawing the attention of cybercriminals and aggressive nation-states. Recent FortiGuard Labs Global Threat Landscape Reports point out the increased detection of malware and malicious activity in OT systems.[2]

Several high-profile cybersecurity attacks highlight this challenge and act as wake-up calls for all those responsible for protecting OT systems. One prime example is Russia's continuous aggression against Ukraine's critical infrastructure,[3] which escalated into a physical "hot war" over a year ago.[4] But these attacks are not limited to open aggression between nation-states. Operational technology systems worldwide continue to be the targets of cybercriminals, especially manufacturing, which continues to see many targeted ransomware attacks against their OT systems.[5]

Unfortunately, the percentage of organizations in this year's survey that experienced a ransomware intrusion (32%) is the same as last year's group (also 32%). Progress must be made in defending against these types of attacks. Given the evolution and growing sophistication of ransomware operations, it's not surprising that 84% of organizations represented in this year's Fortinet 2023 Global Ransomware Report survey remain "very" or "extremely" concerned about this threat.[6]

Although intentional and unintentional insider breaches have dropped considerably this year, according to survey respondents, intrusions from malware and phishing increased significantly—12% and 9%, respectively. These survey results are supported by the most recent FortiGuard Labs Global Threat Report, which states, "Malware has a way of dominating headlines and keeping businesses on their toes."[7]

No Longer Air-Gapped

Now that the infrastructures of IT and OT have almost universally been integrated, the air gap that previously kept OT systems nearly invulnerable to cyberattacks is gone. Consequently, the attack surfaces of industrial organizations have greatly expanded. Add to this the increased deployment of Industrial-Internet-of-Things (IIoT) devices with OT's new susceptibility to the IT threat landscape and the high value of targeting production environments that increase an organization's motivation to pay a ransom, and it is clear why protecting OT has become vital.

OT Cybersecurity in the Spotlight

Last year's State of Operational Technology and Cybersecurity Report[8] stated that the increased focus and investment in OT cybersecurity is an excellent development. However, as revealed in this year's survey, many organizations still have a long way to go to adequately protect their OT systems.

Let's take a deep dive into this year's survey data and see what we can learn about the current state of OT cybersecurity. Hopefully, one of the headlines in our report next year will be about the significant progress made to protect OT systems.

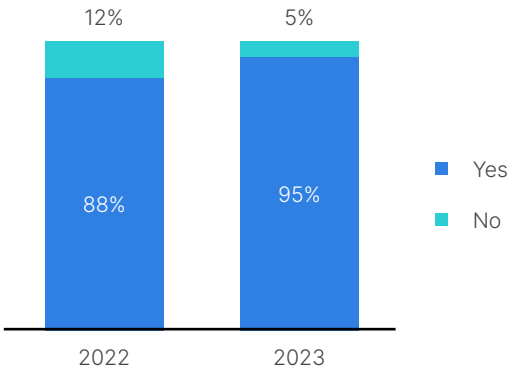
Critical Insights

Critical Insight #1: OT Cybersecurity Responsibility Is Moving from OT Personnel to Cybersecurity Experts

People who work in OT can be found in almost every major industry: manufacturing, transportation, logistics, healthcare, pharmaceutical, oil, gas, energy, utilities, chemical, water, wastewater, and others. And traditionally, these OT professionals have also been deeply involved in cybersecurity purchase decisions for their OT environments.

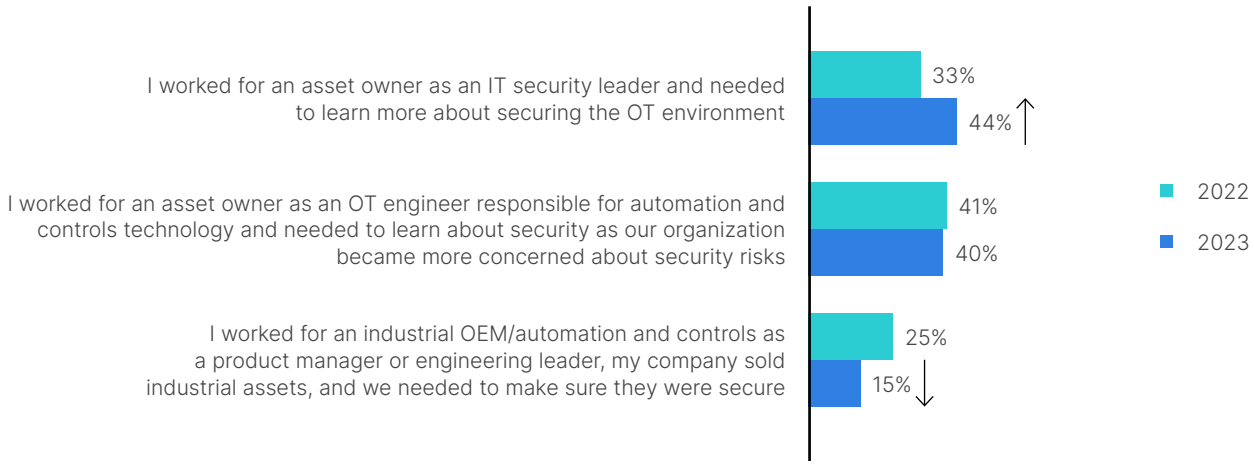
However, it appears that the continued vulnerability of OT networks to cyberattacks has led to moving OT cybersecurity decisions under the CISO. The data also shows that OT security professionals are coming from the ranks of the IT team rather than those with product management work experience. As a result, and as the survey data indicates, the C-suite and traditional security leaders, especially the CISO/CSO, are becoming more involved and invested in cybersecurity decision-making.

Q: Does your organization plan to roll OT cybersecurity underneath the CISO in the next 12 months?



Cybersecurity to Be Under CISO in Next 12 Months

Q: What career background led you to OT security?

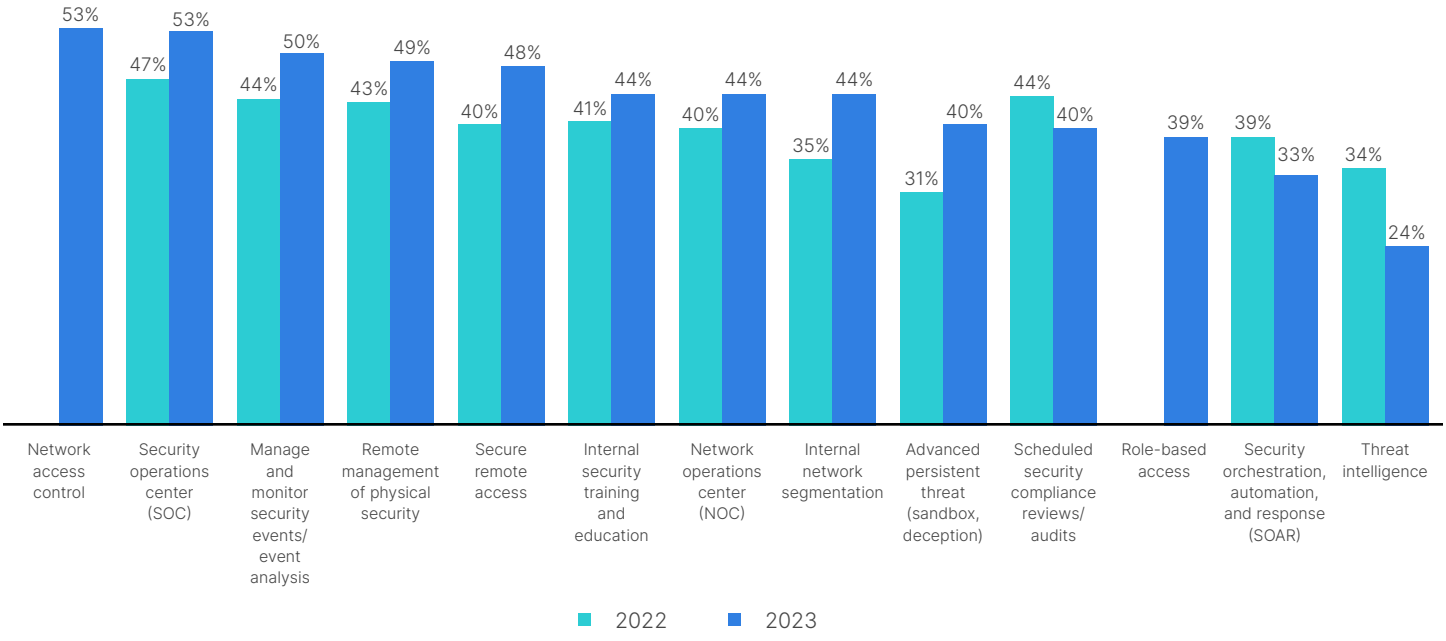


Career Background That Led to OT Security

Critical Insight #2: OT Professionals Rely on a Range of Solutions

This year's surveyed OT professionals are looking for cybersecurity solutions that, first and foremost, detect known vulnerabilities. One unique challenge OT teams face is that downtime is often far more critical than in IT environments. As a result, success in an OT network is measured less by maintaining the confidentiality and integrity of data and more by the availability of critical systems. This places a premium on response time to attacks, as illustrated by an across-the-board increase in the implementation of OT network and cybersecurity solutions.

However, as with IT networks, just having solutions in place is insufficient to prevent all attacks on OT networks. Part of the challenge may be linked to solution and vendor sprawl, making it more difficult to detect a threat and prevent a coordinated response.



Cybersecurity and Security Features in Place

Critical Insight #3: The Number of Intrusions Is Still Troublesome

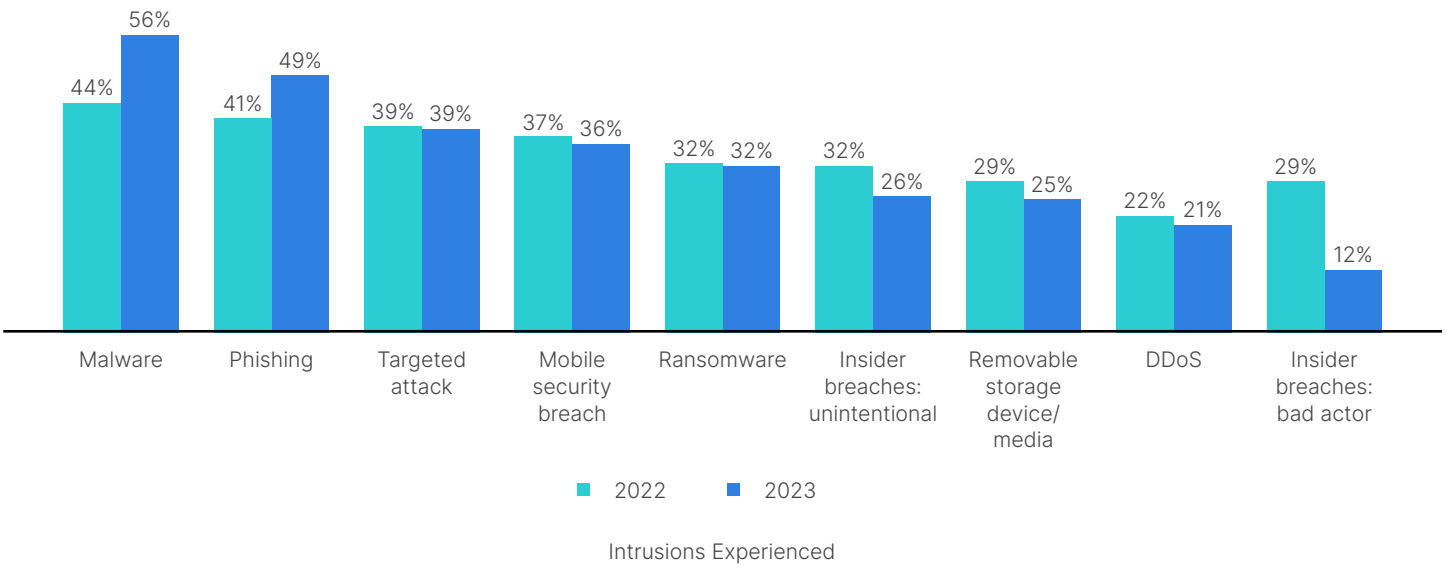
The number of intrusions experienced is declining, but still 75% of the surveyed organizations reported they experienced at least one intrusion in the last 12 months. The overall decline is attributed to fewer insider breaches, not to fewer cybercriminal attacks.

However, malware and phishing incidents are still the most common threats and increased since last year, but ransomware remains the highest concern, and incidents continue to grow. The impacts were broad, increasingly affecting IT and OT systems, but they tended to be resolved within hours (increasingly in minutes).

Some of the intrusion decreases may result from a shift in cybercriminal tactics. However, attackers' approaches are still effective based on the increases we've seen in malware and phishing. Still, given the high value of OT systems, we can foresee a shift to more highly targeted attacks.

It is important to note that overconfidence about readiness harms organizations every bit as much as having the wrong tech in place, which, according to our latest ransomware report,[9] is another problem most organizations face. Although defending against ransomware, for example, is a high priority for most organizations, many solutions they identify as key to their cybersecurity strategy provide little protection against ransomware attacks.

Q: What types of intrusions were experienced? (check all that apply)



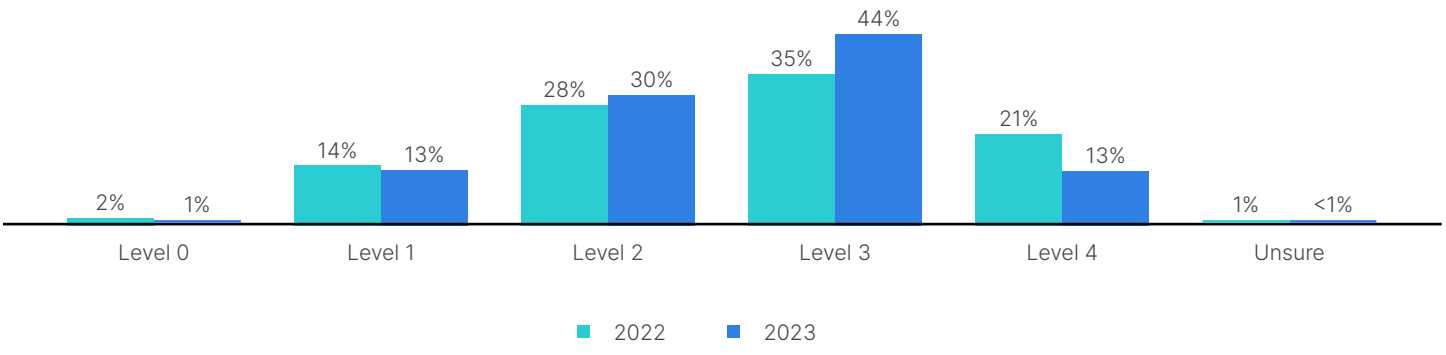
Intrusions Experienced

Critical Insight #4: The Average Cybersecurity Maturity Level Is Improving

Accurate self-assessment of one's cybersecurity capabilities and posture maturity is a critical first step in improving cyber defenses and properly securing OT environments. Globally, fewer companies characterize their OT security posture as highly mature this year, down from 21% in 2022 to 13% this year. At the same time, 44% of organizations now characterize their OT cybersecurity posture maturity at Level 3, up from 35% a year ago. This data indicates that this year's respondents may have a more realistic self-assessment of their OT cybersecurity capabilities.

The Maturity Scale	
Level 0	No segmentation or visibility in place for OT
Level 1	Visibility and segmentation established
Level 2	Access and profiling established
Level 3	Predictive behavior established
Level 4	Leverage orchestration and automation

Q: How would you characterize the maturity of your OT security posture?

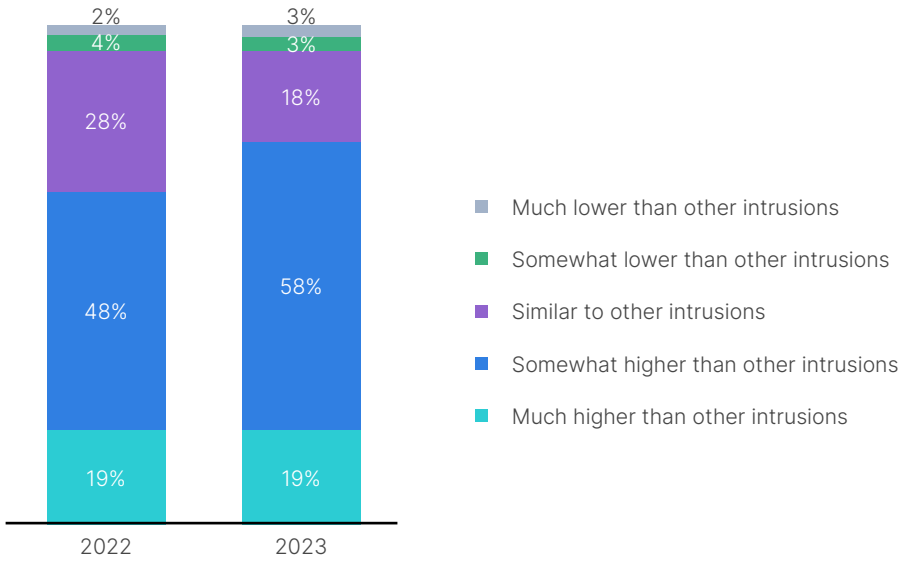


Maturity of OT Security Posture

A Deep Dive into the 2023 Survey

Q: Compared to other intrusions, how concerned are you about ransomware's impact on your OT environment?

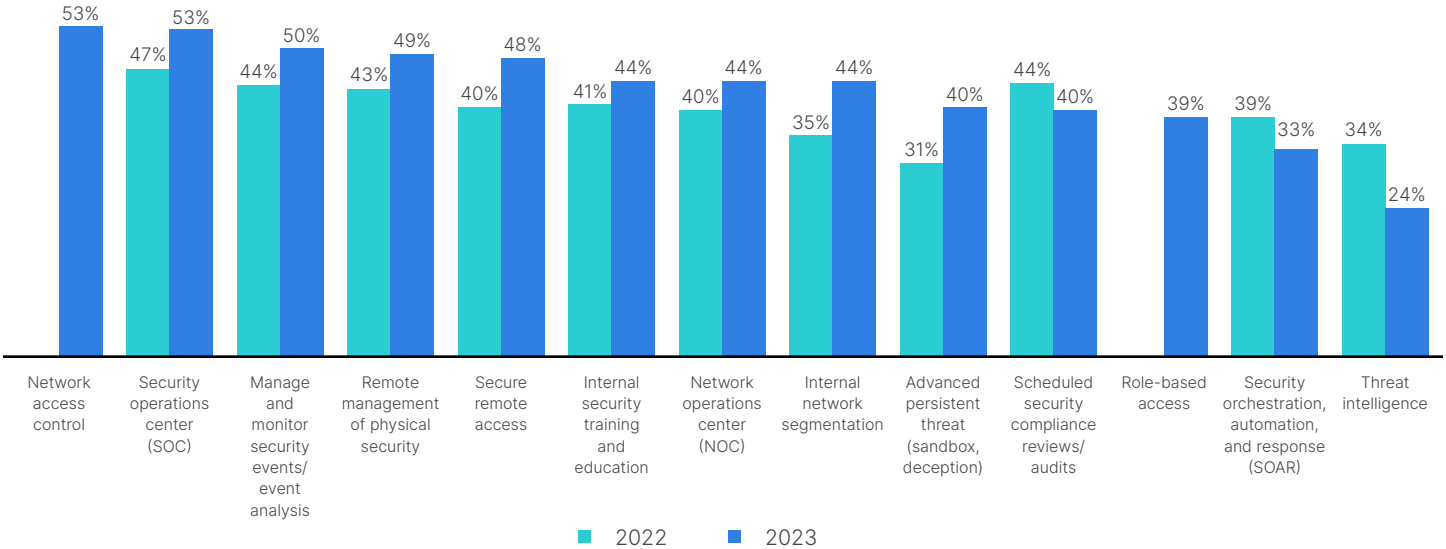
Ransomware incidents occurring in the enterprise or IT network can directly or indirectly impact production. Organizations are increasingly more concerned about it than other intrusions (despite phishing and malware being more common). Thus, ransomware remains a top concern because of production and financial implications.



Concern About Impact from Ransomware

Q: What cybersecurity and security features do you have in place today?

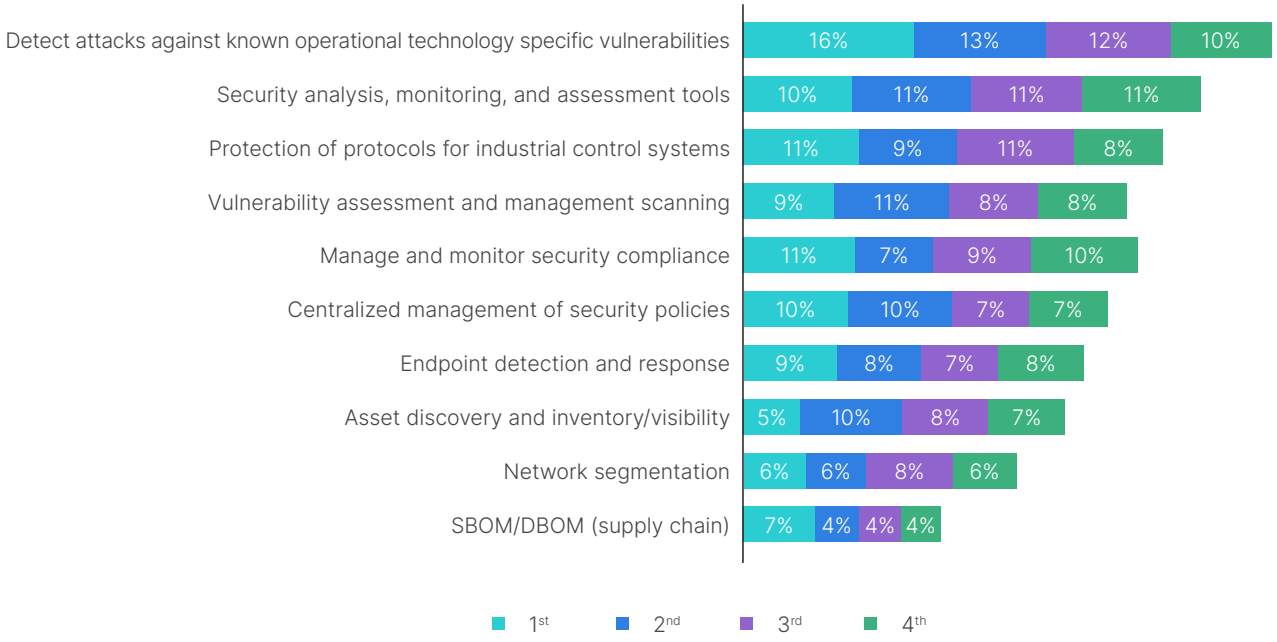
To combat intrusions, OT professionals are fortifying the many cybersecurity and defensive features they have in place. With the increase in features, we suspect that security audits are in decline due to the proliferation of these additional features and the more advanced solutions, such as SOAR and threat intelligence. Once these new features are firmly operational, audits will likely increase to pre-existing levels.



Cybersecurity and Security Features in Place

Q: What features are most important in OT cybersecurity solutions? (rank up to four)

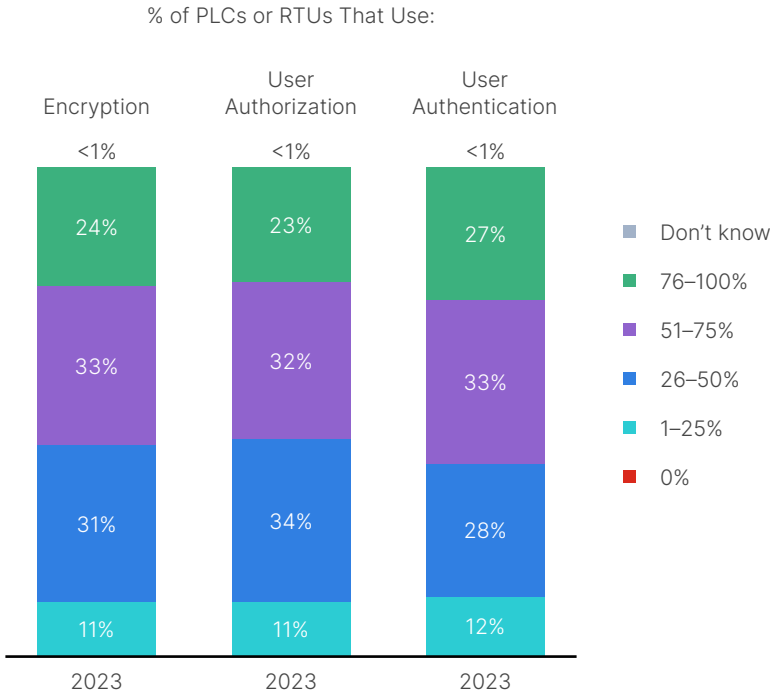
Detecting attacks against known vulnerabilities is now the most essential cybersecurity solution feature, increasing in importance over the past year. Another indication of increasing maturity in OT security is the lower priority in asset discovery and segmentation. What we've seen in the industry and consistent with the CIS Critical Security Controls ICS Companion Guide,[10] is that most customers have taken these basic steps and are moving on to more advanced foundational and organizational solutions.



Most Important Security Solutions Features (Ranking)

Q: What percentage of your PLCs or RTUs use each of the following security capabilities?

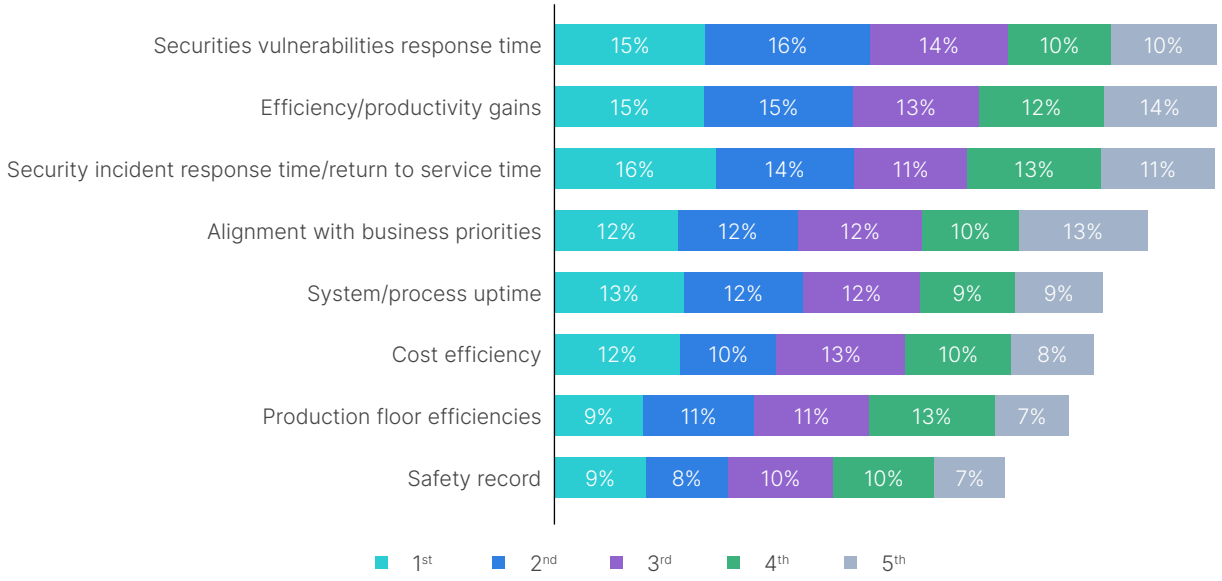
Encryption, user authorization, and user authentication tend to be used in over 50% of PLCs or RTUs.



Global Impact

Q: How is your success measured? (rank up to five)

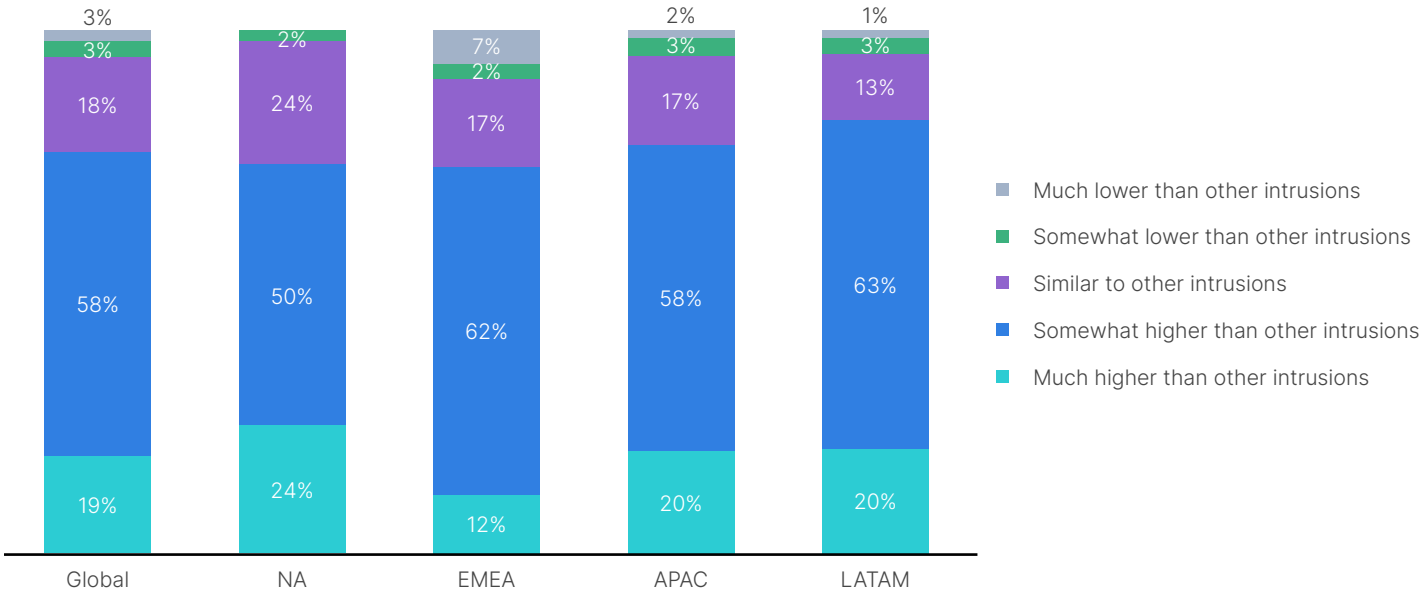
Interestingly, there is no single definition of OT success, which indicates the immaturity of the OT security space. Though, as expected for OT environments, response time and productivity gains have risen to the top.



How Success Is Measured (Ranking)

Q: Compared to other intrusions, how concerned are you about ransomware's impact on your OT environment?

Although ransomware attacks aren't the most common intrusions, they are the top concern of most organizations globally (more than any other threats), likely because of their notoriety and the high cost of restoring affected systems.



Concern About Impact from Ransomware

Best Practices

Seventy-five percent of the organizations in this year's survey reported at least one intrusion in the past 12 months. Believe it or not, this is improvement over 2022, when over 90% reported at least one intrusion. And this year, only 11% of the respondents reported six or more intrusions. Last year, 27% reported six or more intrusions.

While cybersecurity solutions continue to aid in the success of most (76%) OT professionals, particularly by improving efficiency (67%) and flexibility (68%), report data also indicates that solution sprawl still makes it difficult to consistently incorporate, employ, and enforce policies across their increasingly converged IT/OT landscape. And the problem is compounded by aging systems, with the majority (74%) of organizations reporting that the average age of the ICS systems deployed across their organization is between six and ten years. No doubt there's been some progress made in global OT cybersecurity, but organizations need to keep pressing forward.

Below are some of the best practices we have surmised are behind the small but significant improvement found in this year's survey results.

Develop a vendor and OT cybersecurity platform strategy.

Consolidation reduces complexity and accelerates outcomes. The first step is to begin building a platform over time by partnering with vendors that engineer their products with integration and automation in mind. The right vendor will enable organizations to consistently incorporate and enforce policies across an increasingly converged IT/OT landscape. Also, seek to engage with vendors with a wide portfolio of solutions that can provide the basic solutions of asset inventory and segmentation and more advanced solutions, such as an OT SOC or the ability to support a joint IT/OT SOC.

Deploy network access control (NAC) technology.

Solving challenges associated with securing industrial control systems (ICS), supervisory control and data acquisition (SCADA), Internet of Things (IoT), bring your own device (BYOD), and other endpoints requires advanced NAC to be part of a comprehensive security architecture. An effective NAC solution also helps to maintain complete control of an organization's network by managing new devices that want to connect or communicate with other parts of the organization's infrastructure.

Employ a zero-trust approach.

Implement the basic steps of asset inventory and segmentation. Zero-trust access provides continuous verification of all users, applications, and devices seeking access to critical assets, regardless of where they reside.

Incorporate cybersecurity awareness education and training.

Cybersecurity training remains critical because the battle against cybercriminals will require the collective empowerment of all employees to have the knowledge and awareness to work together to protect themselves and their organization's data. Organizations should consider including nontechnical training targeted toward anyone who uses a computer or mobile device, from teleworkers to their families.

Top Tips

1. Continue to implement the basic steps of asset inventory and segmentation and then employ more advanced microsegmentation and virtual patching solutions to protect devices against known vulnerabilities to provide sufficient time to patch devices properly.
2. Collaborate across IT, OT, and production teams to adequately assess cyber and production risks, specifically ransomware incidents, and inform the CISO to ensure proper awareness, prioritization, budget, and personnel allocations.
3. Develop a vendor and OT cybersecurity platform strategy. Many new security solutions are being introduced, yet the personnel gap widens. Also, as your security posture matures, seek to engage with vendors with a wide portfolio of solutions that can provide the basic solutions of asset inventory and segmentation to more advanced solutions such as an OT SOC or the ability to support a joint IT/OT SOC.

Methodology for this Study

Most survey respondents have “plant operations” or “manufacturing operations” titles, with nearly one-third being vice presidents or directors of plant operations. Most of those surveyed, no matter their title, are deeply involved in cybersecurity purchase decisions. And these individuals increasingly have the final say in OT purchase decisions. This year’s survey found that 91% of respondents are regularly involved in their organization’s cybersecurity purchase decisions.

All those who participated in this year’s survey worked in one of the following industries:

- Manufacturing
- Transportation, logistics
- Healthcare, pharma
- Oil, gas, refining
- Energy, utilities
- Chemical, petrochemical
- Water, wastewater

Study Objectives

Fortinet retained InMoment, a third-party company with research expertise, to help us develop the persona of an OT professional.

The survey they helped us create is intended to understand the following better:

- How the persona fits in organizations
- How security features are utilized
- How information is tracked and reported
- Influences and success factors

Approach

A panel sample was used to obtain 570 completes with the following respondent type from a business in:

- Manufacturing
- Transportation, logistics
- Healthcare, pharma
- Oil, gas, refining
- Energy, utilities
- Chemical, petrochemical
- Water, wastewater
  - with more than 1,000 employees with select exceptions
- Operations technology is within functional responsibility
- Has reporting responsibility for manufacturing or plant operations

- Involved in cybersecurity purchase decisions
- Expanded to global reach in 2022 and 2023:
  - Survey respondents were from different locations around the world, including: Australia, New Zealand, Brazil, Canada, Egypt, France, Germany, India, Japan, Mexico, South Africa, United Kingdom, and United States, among others.

Conclusion

The 2023 State of Operational Technology and Cybersecurity Report finds that organizations are making cybersecurity for OT environments a priority. This is an important and necessary trend because 75% of the surveyed organizations have had to deal with at least one cyberattack in the last 12 months. The survey data suggests that OT cybersecurity is improving or maturing, and incidents appear to be declining. Likewise, the risks associated with OT incidents are becoming more apparent through world events. Also, corporations are now more aggressive in their OT security posture, and IT teams are becoming more involved in the industrial networks.

Our survey data demonstrates an across-the-board increase in various OT cybersecurity solutions. Operational technology cybersecurity, the ownership, and the risk and implementation of security solutions are maturing and making an impact. But there's still a long way for most organizations to go in adequately protecting against the most common malware, such as ransomware.

[1] "What are Industry 4.0, the Fourth Industrial Revolution, and 4IR?," McKinsey and Company, August 17, 2022.

[2] 2022 Global Threat Landscape Report, FortiGuard Labs, February 22, 2023.

[3] "Cyber-Attack Against Ukrainian Critical Infrastructure," CISA, July 20, 2021.

[4] "Ukraine: Russian attacks on critical energy infrastructure amount to war crimes," Amnesty International, October 22, 2022.

[5] Jonathan Reed, Pipedream Malware Can Disrupt or Destroy Industrial Systems, Security Intelligence, April 19, 2023.

[6] The 2023 Global Ransomware Report, Fortinet, April 24, 2023.

[7] 2022 Global Threat Landscape Report, FortiGuard Labs, February 22, 2023.

[8] 2022 State of Operational Technology and Cybersecurity Report, Fortinet, June 21, 2022.

[9] The 2023 Global Ransomware Report, Fortinet, April 24, 2023.

[10] CIS Critical Security Controls ICS Companion Guide, Center for Internet Security, Version 7.

FORTINET

www.fortinet.com

May 24, 2023 10:13 AM

2101968-0-0-EN