Publication date:
November 2023

Author:
Anna Ahrens
Hollie Hennessy

Secure Industrial OT and IIoT Cybersecurity Networks

Navigating the challenges of OT-IT integration

OMDIA
Brought to you by Informa Tech

Contents

Introduction

Digital transformation in industrial environments helps to increase efficiency and productivity, overcome human resource gaps, and improve sustainable production. However, digital opportunities bring digital dependence and a need for digital resilience. A core component of digital resilience is cyber-resilience to ensure operational continuity despite security incidents and breaches.

To reap the benefits of change, industrial organizations need to integrate what were, historically, the separate environments of IT and operational technology (OT). OT networks are inherently more complex to secure than their IT counterparts – comprising different assets, processes, software, and teams, they were never designed to run traditional IT or security software.

Integrating IT-based technologies with OT systems can add complexity and bring new challenges in the OT space. According to Omdia's IT Enterprise Insights: Manufacturing 2023 Survey, one of the most notable aspects is the increased cybersecurity threat.

OT and IIoT networks are particularly complex to secure thanks to the volume and age of legacy devices, combined with proprietary, customized, and complex ecosystems – as well as the crucial need to prioritize continuous operations and safety. Integrating IP-based connectivity with what historically were isolated systems and unconnected environments adds another dimension to the threat landscape and the potential for IT-based threats to cross into the OT realm.

While the drive toward automated, preventative response is strong, implementing this in practice brings real challenges. IT and operations must find a way to balance effectively securing industrial systems with maintaining continuity and safety of production, operational efficiency, business continuity, product integrity, and compliance. Another crucial factor (to successful deployment) is the convergence of IT and OT teams that historically have different skillsets, experiences, objectives, and KPIs.

To better understand how OT and IT teams view and approach cybersecurity, and explore the challenges, pain points, and vendor preferences that industrial firms face, Omdia, in partnership with TXOne Networks, undertook the Secure Industrial OT and IIoT Cybersecurity Networks Survey (2023).

Report key findings

- The drive toward automated, preventative response is strong. However, most organizations acknowledge that challenges exist that slow down progress. Organizations appreciate that connecting IT/OT can deliver real business benefits, but the friction between knowing and realizing these benefits is still a big issue.

- The survey found that almost half of the respondents are connected with advanced or significant network security controls—however, this leaves the other half that are connected without adequate security controls—presenting a very real threat scenario.

- Current approaches toward OT/IIoT networks security combine both active and passive cybersecurity methods, but there is a shift in the market toward a more active approach.

- Only a few organizations have a dedicated OT cybersecurity budget, with most businesses drawing investment from either the IT or a dedicated IT cybersecurity budget.

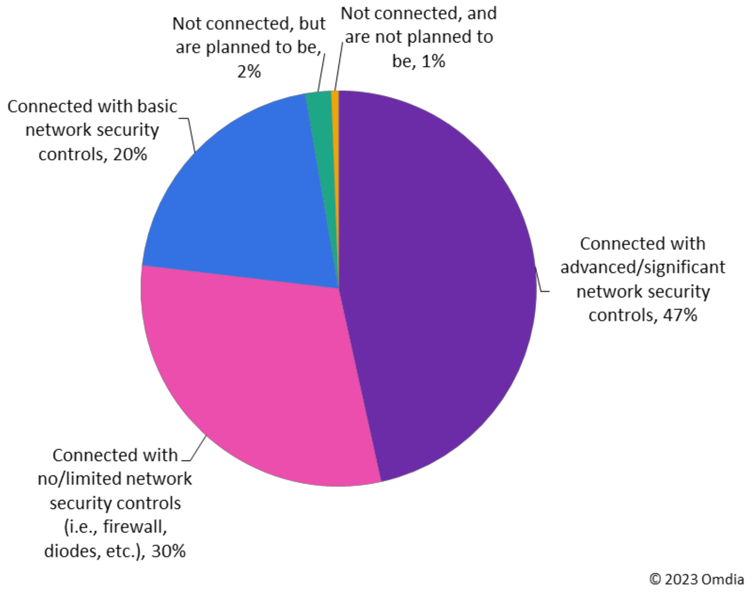
- The top priority for manufacturing operations or maintenance people is managing devices.

- OT/IIoT devices and systems have a considerably longer lifecycle than IT assets. Therefore, legacy and older devices, and software/operating systems, are commonplace within most operations. Managing the increased risk of these devices is not as simple as swapping them out for a new version.

Current approaches

OT networks are inherently more complex to secure than their IT counterparts – comprising different assets, processes, software, and teams, they were never designed to run traditional IT or security software. In addition, as networks converge and more assets are incorporated, the attack surface broadens, which can increase risks to businesses if not mitigated. In the survey, we asked organizations how their IT and OT networks are connected (see **Figure 1**), with almost half responding that they are connected with advanced or significant network security controls (47%). While this number may seem promising, this leaves half of organizations that are connected without adequate security controls in place across IT/OT networks. This is not sufficient, given that laterally moving from the IT realm into the OT realm or IT attacks impacting OT networks are a very real threat scenario that needs to be considered.

Figure 1: Which best describes how your organization's IT and OT networks are connected?



Source: Omdia

Something important to note here is the distinction between an OT attack and an IT attack. The May 2021 Colonial Pipeline ransomware attack is often mistakenly referenced as an OT attack – as operations were shut down. However, the reality is that the attack originated in the IT domain, with operations being shut down as a precaution to avoid the risks of infecting the complete OT environment.

The key takeaway, however, is that the Colonial Pipeline attack remains a good example of IT attacks *impacting* the OT network. The attack was not on the OT network, but the risk of this happening was high enough to stall operations. Colonial Pipeline was uncertain that the OT network would be protected during this incident, hence the preventative shutdowns, and there are many other organizations that have done similar.

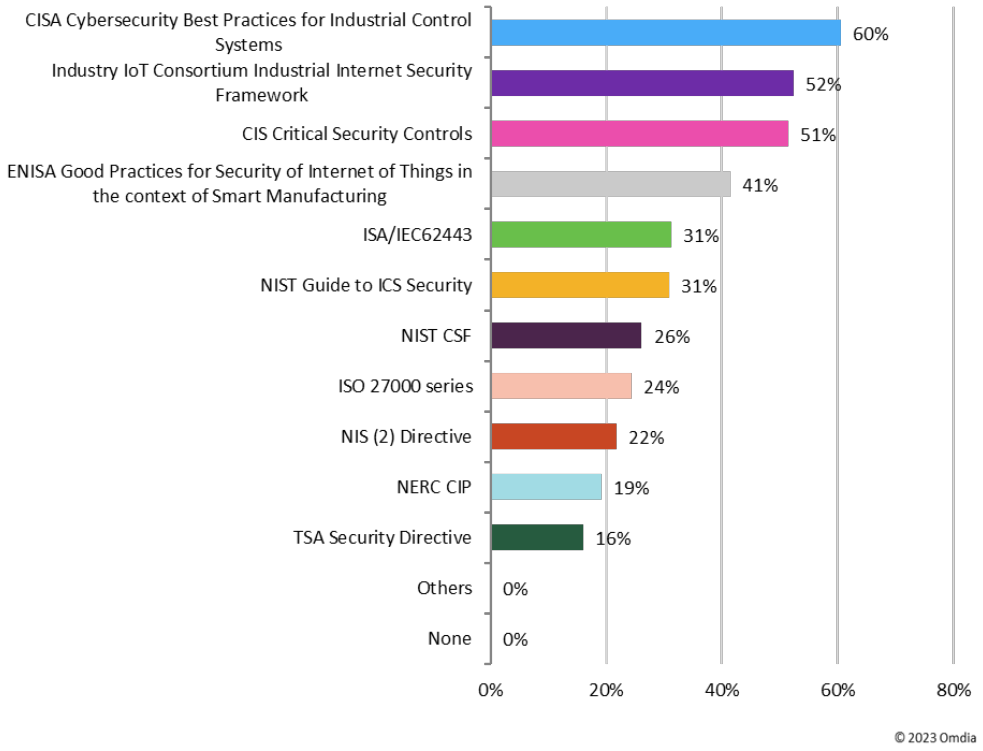
Other IT attacks that have similarly impacted operations include an April 2022 attack on German wind turbine operator, Deutsche Windtechnik, following which the company shut down remote data monitoring connections to many turbines. In November 2023, DP World Australia found data had been accessed and/or exfiltrated from the Australian corporate network and decided to take multiple ports offline in an effort to limit any further unauthorized access.

Many organizations with inadequate security controls across IT/OT may find themselves in a similar situation. Designing robust segmentation, applying preventative controls, and mitigating risk in the OT domain can give organizations that certainty that their OT networks will be protected, and remain operational in the event of an IT attack.

That said, thanks to the increasingly audacious and potential damage of cyberattacks, many organizations are on the journey to raising the bar when it comes to OT cybersecurity.

All respondents are adopting cybersecurity standards, frameworks, and regulations to help them secure their OT operations. The most adopted standard in all regions is the CISA Cybersecurity Best Practices, although organizations in Asia are more likely to use the NIST guide (see **Figure 2**).

Figure 2: Which standards, frameworks, and regulations are used by your organization for OT cybersecurity?



Source: Omdia

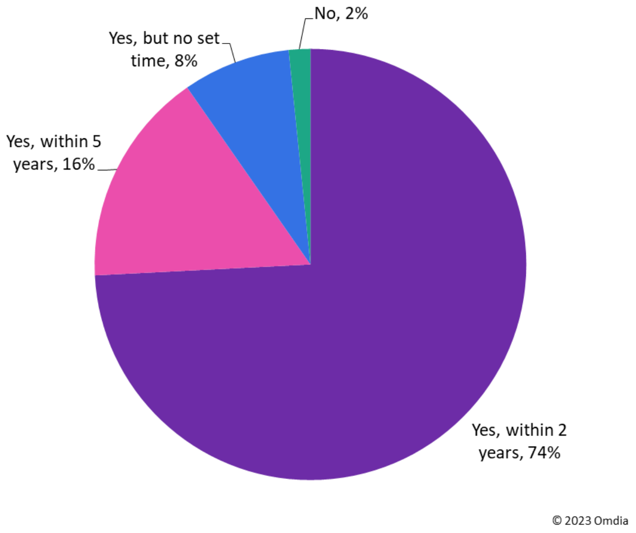
Challenges of implementing cybersecurity tooling and processes

Organizations appreciate that connecting IT/OT systems can deliver genuine business benefits, but friction exists between knowing and realizing these benefits.

The convergence and integration of OT and IT networks is more than a matter of just blending technologies – IT security teams and processes must incorporate the diverse real-time demands of the industrial environments. The infrastructure of each business is so unique that a "one size approach" does not fit all – security solutions must be tailored.

Industrial control system (ICS) environments can be highly customized and complex, with proprietary technologies, SCADA systems, human-machine interfaces, PLCs, and legacy or obsolete subsystems.

Figure 3: Is there a plan to remove, replace, or upgrade the legacy OS devices?



Source: Omdia

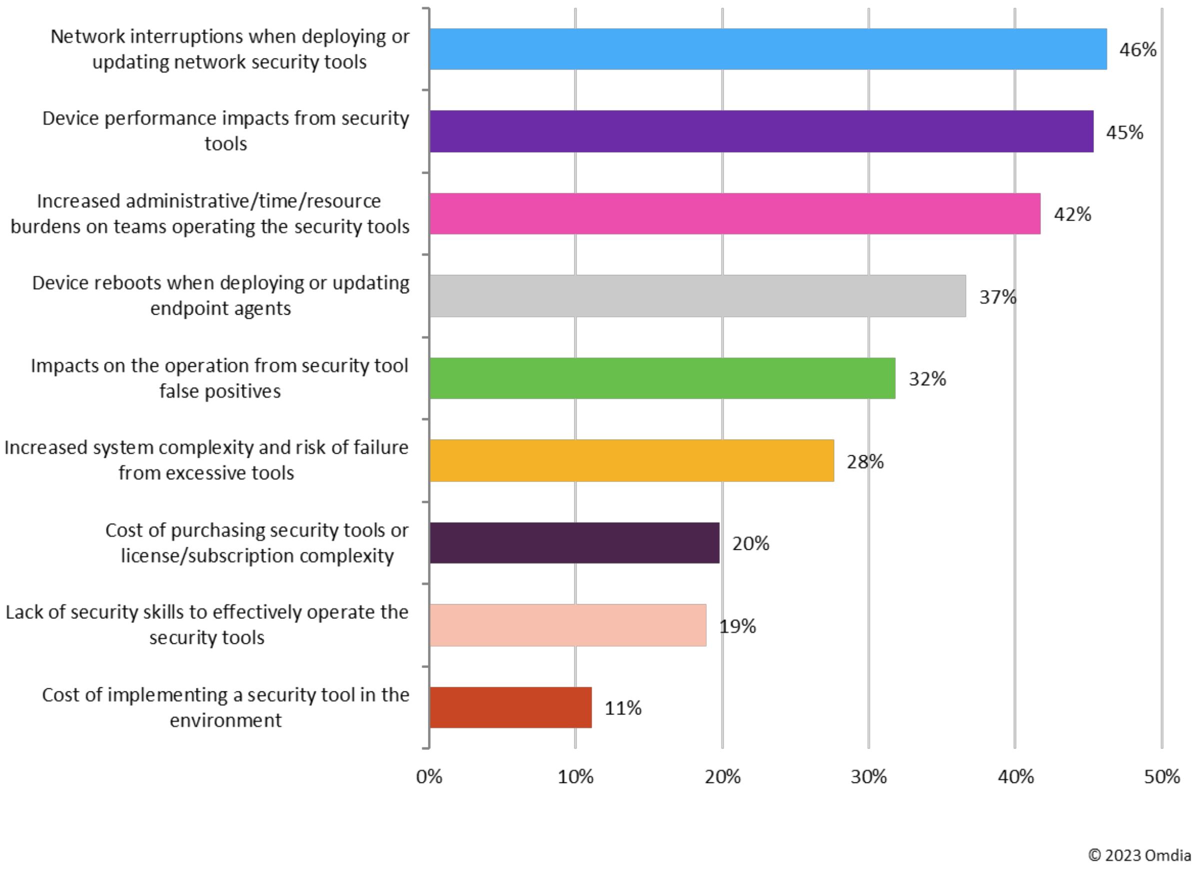
> As OT environments have long lifecycles, legacy assets are everywhere. But, as the survey reflects, these are being replaced.

Industrial systems prioritize safety and continuity above all else, so security that risks impacting processes is not an option. This poses difficulties for instituting and running cybersecurity solutions.

These challenges were clearly reflected in the concerns most organizations faced when implementing OT cybersecurity tools (see **Figure 4**). Business interruption and performance weighed almost equally alongside the added burden on teams having to operate the security tools.

The resource burden reflects a shortage of in-house security expertise, combined with a diminishing skilled workforce on the operational side.

Figure 4: Which best describes your organization's primary concerns when implementing OT cybersecurity tools?



Source: Omdia

Regarding the types of cybersecurity risks that are of concern, the increased threat of ransomware attacks topped the list, closely followed by theft of intellectual property and trade secrets. Organizations were also highly aware of the risk of IT-based threats traversing into the OT environment, where threats can be challenging to detect and prevent. This awareness is likely fueled by high-profile cases such as the Colonial Pipeline incident. Although the OT network was not attacked, the risk of the threat traversing into OT led to operational shutdown as a prevention, referenced above.

Adding to the overall complexity, the expansion of OT brings new stakeholders, considerations, and priorities to the security ecosystem. Instead of assuming IT tools can be replicated to OT, a different approach is needed to balance and mitigate risk.

Organizations need their solutions to bear in mind priorities of safety, availability, and reliability of devices in operational environments, as well as bring value to key stakeholders across the organizations, ensuring minimal impact and interruptions in deployment and use.

Crucially, neither side has all the answers. IT teams must adapt to the needs of OT and, conversely, a certain amount of give is needed from the OT side too. A balance needs to be struck so both teams can work together to understand the overall risk posture and collaboratively make decisions on the best overall reduction and mitigation techniques. By understanding and using their different perspectives in a positive way, the business can explore new and innovative solutions to problems in ways not previously considered.

> “Crucially, neither side has all the answers! By understanding and using their different perspectives in a positive way, the business can explore new and innovative solutions to problems in ways not previously considered.”

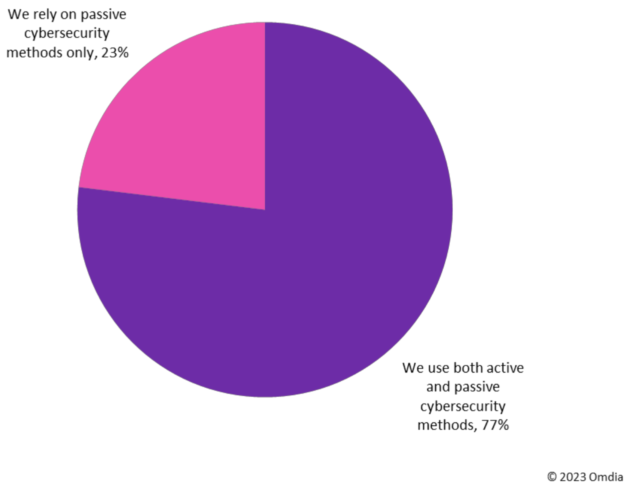
Shift toward a (more) active approach

Traditionally, the OT cybersecurity market has tended toward a “passive-only” approach – mainly to reduce the risk of disrupting operations. And rightly so! Taking a ham-fisted approach with tools available previously would, and often did, have a negative impact on the operation. But dynamics have changed with a growing understanding of the challenges and technologies.

Current approaches toward OT/IIoT networks security combine both active and passive cybersecurity methods, but there is a shift toward a more active approach (and by active we mean actively gaining information from the network or endpoint, such as active querying, probing, or polling).

One of the reasons for this shift is because OT cybersecurity offerings or technologies are maturing. As technology has developed over the last 10 or so years in this space, specialist security vendors have innovated and developed their technological capabilities to allow active approaches in industrial environments without impact to operations or network interruption. Active methods can also offer more granular detail and information about assets, allowing for more effective and rich discovery of devices connected to the network, while also reducing the manual effort or strain on security teams. Yet, although vendors are moving toward offering more active capabilities, so far the response from end users has been mixed with many still apprehensive or relying on passive measures (see **Figure 5**).

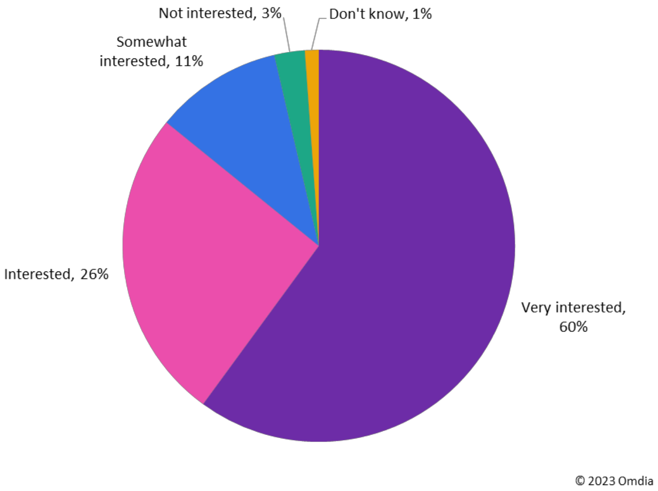
Figure 5: Which best describes your organization’s approach to security for OT/IIoT networks?



Source: Omdia

However, the survey suggests that this mindset is beginning to shift with organizations becoming more open to exploring active cybersecurity options (see **Figure 6**). It was also interesting to see that currently over three quarters of companies are using automated response actions. These range from actions throughout the environment to response actions in non-critical areas of the operations.

Figure 6: How interested is your organization in using active cybersecurity methods for your OT/IIoT networks?

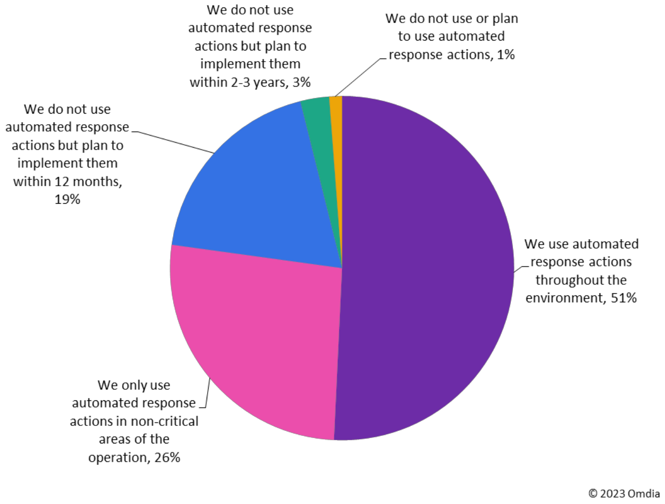


Source: Omdia

Given that key concerns center on avoiding network interruptions, alongside safety, reliability, and availability priorities, automated response functions (as found in the IT world) traditionally were not offered in OT – the focus was on protective and mitigating controls. However, specialist vendors in the OT security space, as with active discovery, have developed methods to offer automated response in industrial networks while satisfying these OT priorities.

Those not yet using automated response clearly see the value in the technology and are planning to implement some form of response in the future (see **Figure 7**). Only a small number of respondents told us they are not using, or planning to use, the technology – interestingly, it was higher in the production (OT) infrastructure or networking roles, which may be due to more apprehension around keeping the network running and KPIs around continuity that these roles must hit.

Figure 7: Which best describes your organization’s automated security response appetite in OT?



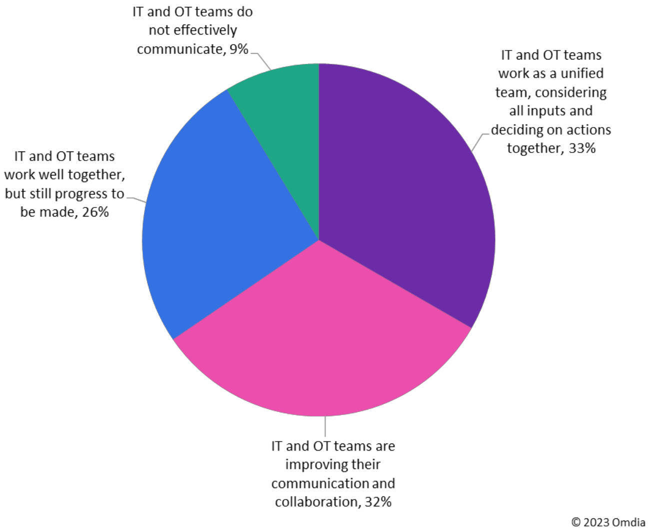
Source: Omdia

Inter-team frictions

As already discussed, integrating what historically were separate systems can create challenges. The same applies to the teams. Although the idea is that IT and OT teams work harmoniously together, most acknowledge that challenges exist. It is not uncommon to find internal tensions within organizations when introducing digital projects due to different expectations, expertise and priorities, a lack of communication, coordination, and mutual understanding across teams, especially where there is no shared or common goal. People convergence and collaboration are crucial for successful projects deployment.

Risk managers and IT teams may appreciate, and agree, that preventative security can reduce risk. However, when it comes to implementing solutions, it is not cut and dry. While the IT environment may be able to implement tools such as endpoint detection and response (EDR)/extended detection and response (XDR), the OT environment may not always be able to do so as their requirements may differ and many IoT and OT devices will not be able to work with IT-based agents. As another example, legacy OS devices cannot simply be replaced or altered, as doing so might increase business risks, cause significant interruptions, and ultimately impact the bottom line. It is also important to remember that (cybersecurity) technology is not always the only or best option for risk reduction. Security teams may not be aware of, for example, a mechanical control that could better mitigate a risk. Again, this reinforces the fact that close collaboration between teams is essential to explore new solutions and deliver the best overall outcomes for the operation, security, and business as a whole (see **Figure 8**).

Figure 8: Which best describes how well aligned various OT cybersecurity stakeholders are within your organization?



Source: Omdia

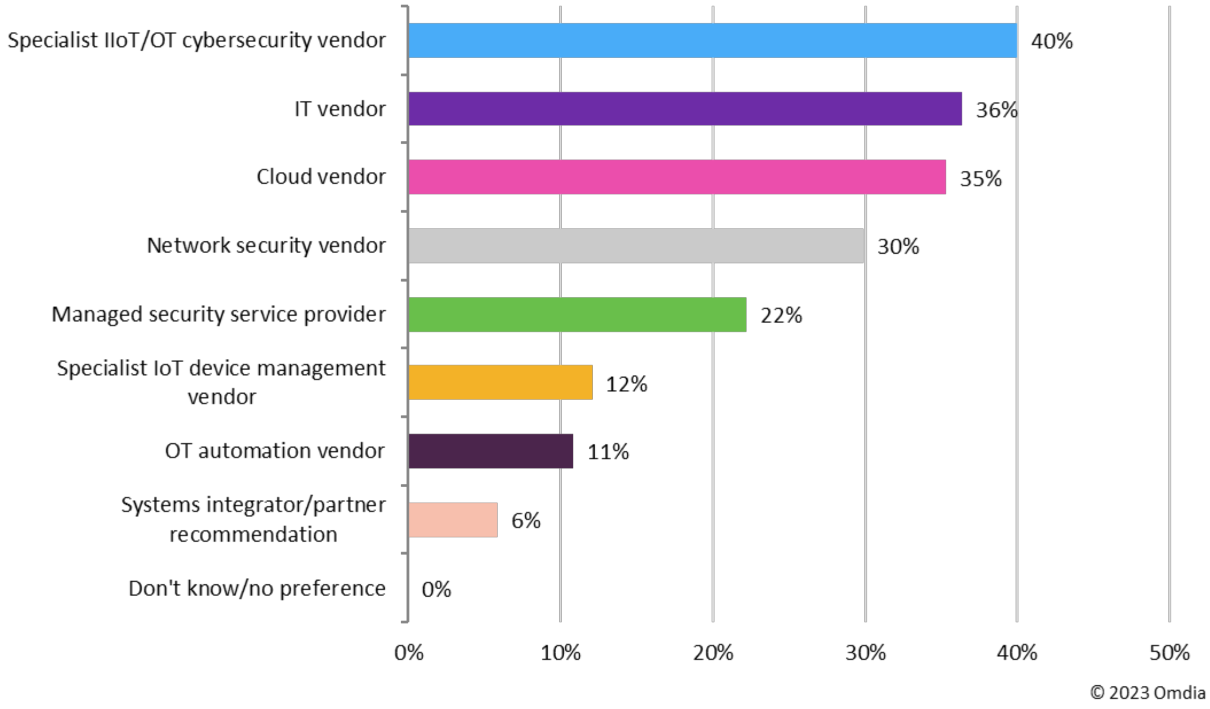
Most organizations are taking proactive steps to address these issues but, overall, operational managers and corporate leadership have a higher perception (over the reality for those in security roles) that these teams are working in a unified way.

Importance of selecting the right vendor and partner

Thus far, we have explored practices, attitudes, and approaches, but what about working with vendors and partners? This is a fast-changing and fast-growing market landscape, with multiple vendors and service providers presenting an extensive range of solutions and services.

Yet, when it came to vendor selection, the preference was toward working with a combination of specialist IIoT/OT cybersecurity vendors, IT vendors, and cloud vendors (see **Figure 9**).

Figure 9: Which type of organization would you prefer to purchase OT/IIoT cybersecurity solutions from?



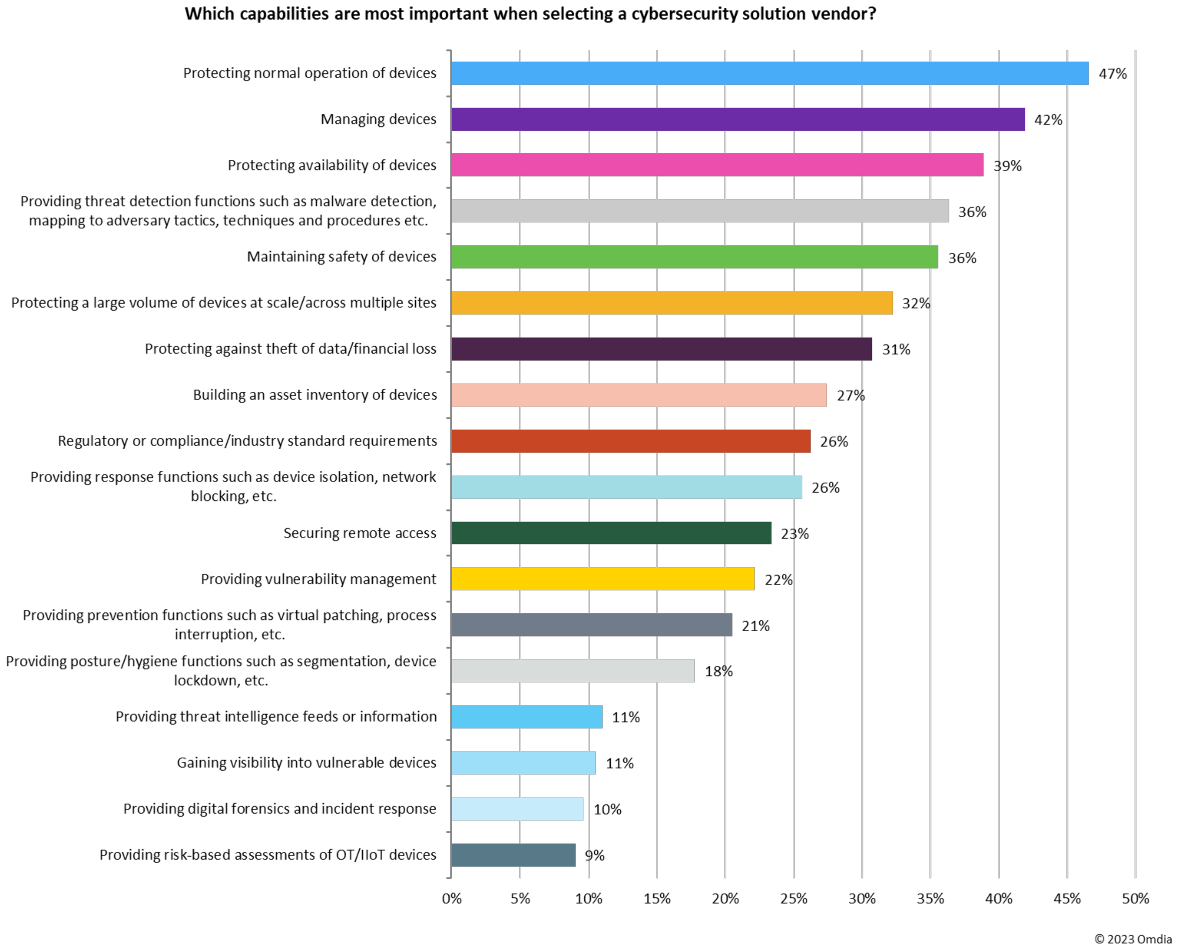
Source: Omdia

Industrial organizations understand the importance of partnering with a provider that brings a deep understanding of their specific operational and business needs. Such specialists are ideally placed to advise and help organizations evaluate and identify the best options to meet their specific business's target outcomes and offer OT-tailored tooling and controls – rather than simply replicating IT tools to OT environments.

It is also important to remember that, while vendors provide powerful products and services, those vendors offering a strong partner ecosystem (i.e., partners/SIs with an OT focus and understanding of the operations mindset) will bring additional value.

When it comes to selecting a cybersecurity solution vendor, OT prefers the capabilities to protect normal device operation, manage devices, and protect availability of devices over the threat detection or other security-related capabilities (see **Figure 10**). Clearly, this reflects their priorities to prevent downtime and maintain operations. Interestingly, and in contrast to their IT counterparts where risk-based vulnerability management is key, the least important capabilities for OT were the ability to gain visibility into vulnerable devices, providing digital forensics and incident response, and providing risk-based assessments of OT/IIoT devices. Visibility has long been a priority for those deploying OT and IoT networks. In Omdia's experience, however, the fact that this is now finding itself further down the priority list may suggest that organizations on the whole now have this visibility in place and are looking for more from the OT cybersecurity market.

Figure 10: Which capabilities are most important when selecting a cybersecurity vendor?



Source: Omdia

Conclusions

- Organizations understand that there are benefits in connecting IT/OT, but to realize these benefits they need to overcome the challenges of integrating what historically were separate systems and teams. While most organizations are taking proactive steps to address the challenges, operational managers and corporate leadership have a higher perception that IT/OT teams are working in a unified way over the reality.

- The benefits of automated active response are acknowledged but organizations must balance the benefits of implementation against the risks, concerns, and limitations of the OT/ICS devices and systems. Cross-team collaborative approaches and centralized cybersecurity management are indispensable in delivering a successful cybersecurity strategy.

- Different teams in the business are looking for ways to reap the benefits through different lenses, based on what is possible from their perspective and understanding of the systems. Instead of assuming IT tools can be replicated to OT, a different approach is needed to balance and mitigate risk. Crucially, neither IT nor OT has all the answers. A balance needs to be struck between teams as they work together to understand the overall risk posture and collaboratively explore options.

- Industrial organizations understand the importance of partnering with a provider that brings a deep understanding of their specific operational and business needs. Also important is working with vendors that offer a strong partner ecosystem. Such specialists are ideally placed to advise and help businesses identify and evaluate all the options. It is so important to thoroughly evaluate the vendor landscape and explore the partnerships available, then leverage this expertise. Working with such expertise will help organizations to shape the best fitting solution for the operational environments and business needs in order to ensure long-term success.

Appendix

Methodology

In 2023, Omdia conducted an online buyer survey on Industrial OT and IIoT Cybersecurity to look at topics such as investment trends, managed services, supplier preferences, inventory management, perceived gaps, and IT/IoT training.

The survey comprised 300 decision-makers with a focus on IT, OT, technology, networking, security, and operations in medium and large industrial companies across North America, Europe, and Asia Pacific.

Authors

Anna Ahrens
Principal Analyst, Industrial IoT
customersuccess@omdia.com

Hollie Hennessy
Senior Analyst, IoT Cybersecurity
customersuccess@omdia.com

Get in touch

www.omdia.com
askananalyst@omdia.com

Omdia consulting

Omdia is a market-leading data, research, and consulting business focused on helping digital service providers, technology companies, and enterprise decision-makers thrive in the connected digital economy. Through our global base of analysts, we offer expert analysis and strategic insight across the IT, telecoms, and media industries.

We create business advantage for our customers by providing actionable insight to support business planning, product development, and go-to-market initiatives.

Our unique combination of authoritative data, market analysis, and vertical industry expertise is designed to empower decision-making, helping our clients profit from new technologies and capitalize on evolving business models.

Omdia is part of Informa Tech, a B2B information services business serving the technology, media, and telecoms sector. The Informa group is listed on the London Stock Exchange.

We hope that this analysis will help you make informed and imaginative business decisions. If you have further requirements, Omdia's consulting team may be able to help your company identify future trends and opportunities.

Copyright notice and disclaimer

The Omdia research, data and information referenced herein (the "Omdia Materials") are the copyrighted property of Informa Tech and its subsidiaries or affiliates (together "Informa Tech") or its third party data providers and represent data, research, opinions, or viewpoints published by Informa Tech, and are not representations of fact.

The Omdia Materials reflect information and opinions from the original publication date and not from the date of this document. The information and opinions expressed in the Omdia Materials are subject to change without notice and Informa Tech does not have any duty or responsibility to update the Omdia Materials or this publication as a result.

Omdia Materials are delivered on an "as-is" and "as-available" basis. No representation or warranty, express or implied, is made as to the fairness, accuracy, completeness, or correctness of the information, opinions, and conclusions contained in Omdia Materials.

To the maximum extent permitted by law, Informa Tech and its affiliates, officers, directors, employees, agents, and third party data providers disclaim any liability (including, without limitation, any liability arising from fault or negligence) as to the accuracy or completeness or use of the Omdia Materials. Informa Tech will not, under any circumstance whatsoever, be liable for any trading, investment, commercial, or other decisions based on or made in reliance of the Omdia Materials.