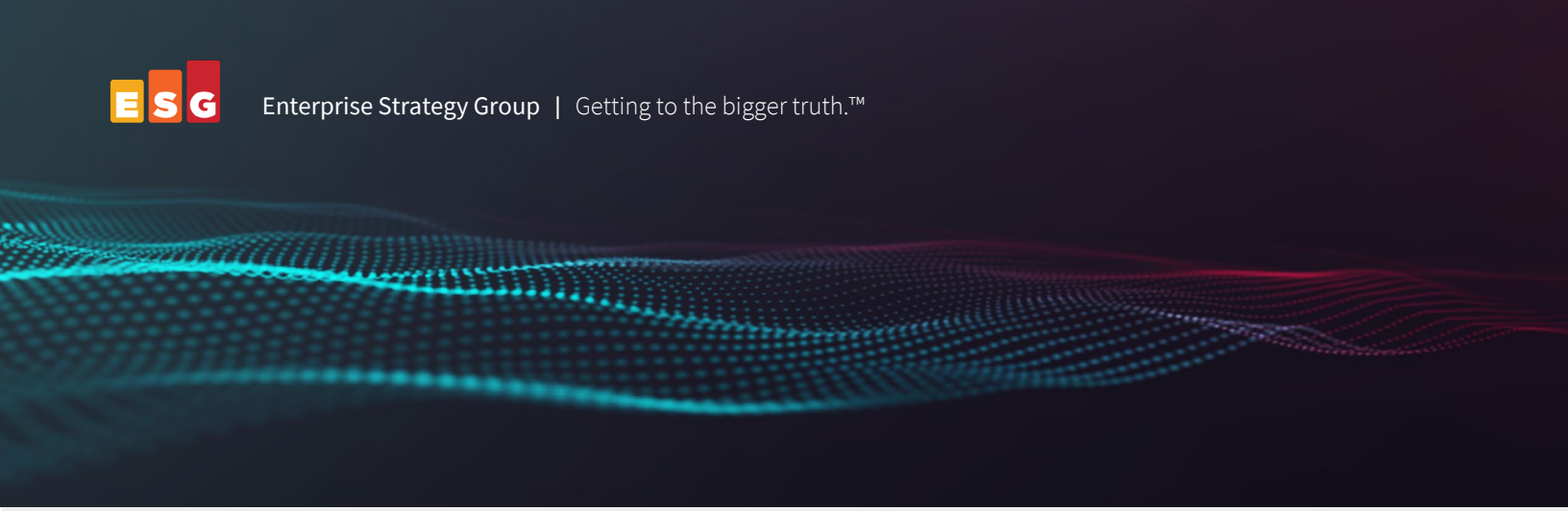



ESG RESEARCH INSIGHTS PAPER

# Threat Detection and Response in Manufacturing

## Current and Future Use Cases for Deception Technology

By Jon Oltsik, ESG Senior Principal Analyst and Fellow

October 2020

This ESG Research Insights Paper was commissioned by TrapX and is distributed under license from ESG.

## Contents

## Executive Summary

In August 2020, TrapX, in partnership with the Enterprise Strategy Group (ESG), completed a research survey of 150 cybersecurity and IT professionals who are directly involved with their organization's cybersecurity strategies, controls, and operations. Twenty-nine percent of respondents came from mid-market organizations (i.e., 100 to 999 employees) while the remaining 71% came from enterprise organizations (i.e., more than 1,000 employees), and all respondents worked at organizations in the manufacturing industry. Further descriptions of the research methodology and survey demographics are presented in the appendix of this report.

Based upon the research collected for this project, TrapX and ESG reached the following conclusions:

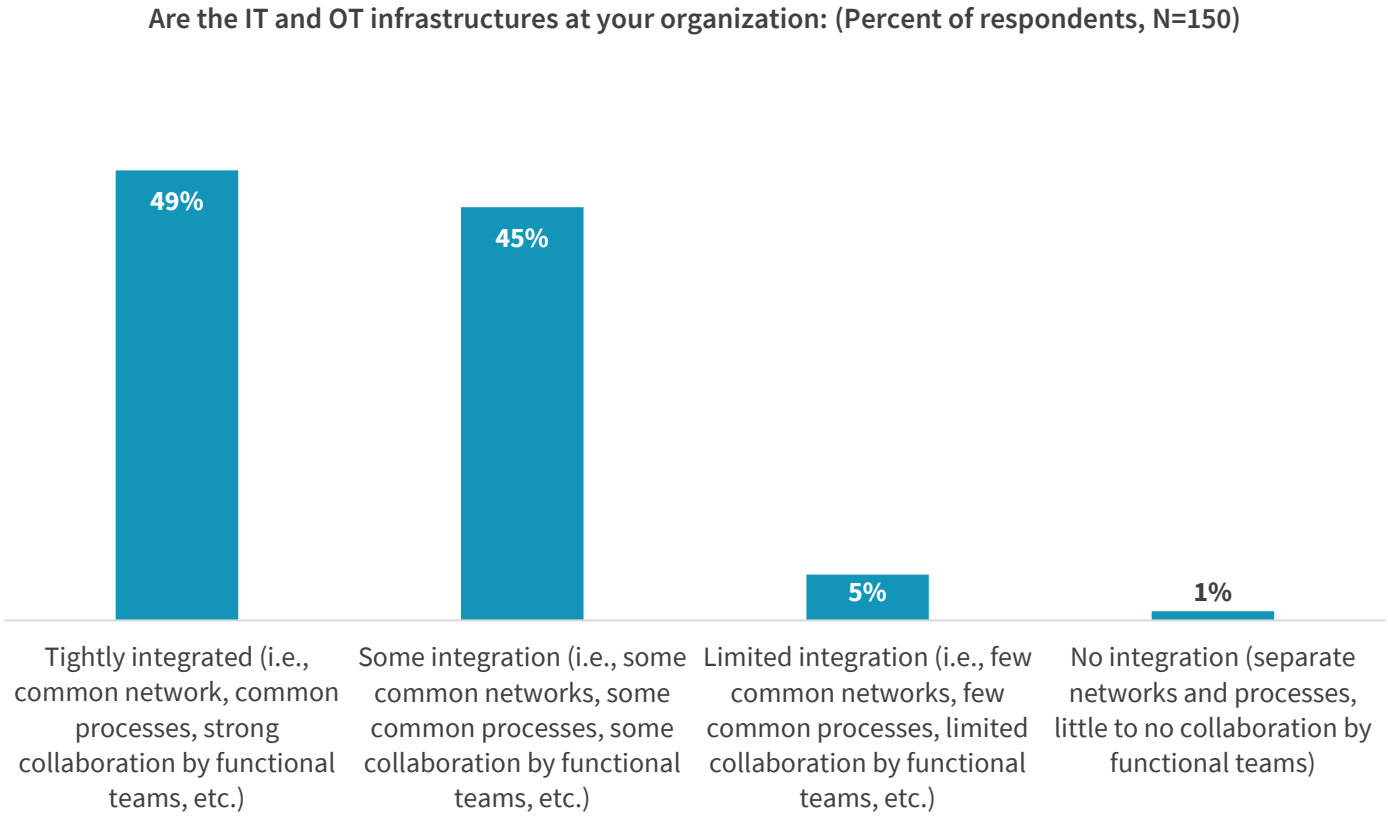
- Manufacturing organizations are consolidating IT and OT infrastructure. Most organizations have already brought these two environments together to some extent and expect further convergence moving forward. Organizations are also consolidating IT and OT security using common tools, processes, and staff.
- Threat detection and response remains difficult. While IT/OT convergence makes business sense, the data indicates that many manufacturing organizations are struggling to safeguard OT assets, especially as the attack surface expands. Security teams can't keep up with growing volumes of security data or the increasing number of security alerts. They lack the right level of visibility and threat intelligence analysis and don't have the right staff and skills to handle the cybersecurity workload. Consequently, more than half of the manufacturing organizations surveyed have experienced some type of cybersecurity incident on their OT systems and these incidents can take weeks or months to remediate. This disrupts business operations while increasing cyber-risk.
- Manufacturing organizations are beginning to look toward deception technology for help. Just over half of manufacturing organizations deploy detection technology while others remain confused or misinformed about deception technology use cases and value. Even some of the organizations using deception technology aren't using it to its full potential. The research does point toward increasing use of deception technology moving forward as suppliers educate the market and manufacturing companies use deception technology as part of comprehensive threat detection and response strategies.

## IT and OT Security Are Merging

Manufacturing organizations have large and growing investments in information and operational technology (OT). As the research reveals, most organizations operate these assets through collective efforts using common networks, common processes, and strong collaboration by functional teams. Nearly half (49%) of organizations say that IT and OT infrastructure are tightly integrated while another 45% claim that there is some integration between IT and OT (see Figure 1). IT and OT integration will only increase as 77% of respondents expect further infrastructure convergence in the future.

These data points seem to indicate that IT and OT integration is a best practice. Therefore, organizations must build expertise in understanding each environment and create a shared infrastructure that meets demands for IT/OT availability, performance, and security.

**Figure 1. IT/OT Integration Efforts**




*Source: Enterprise Strategy Group*

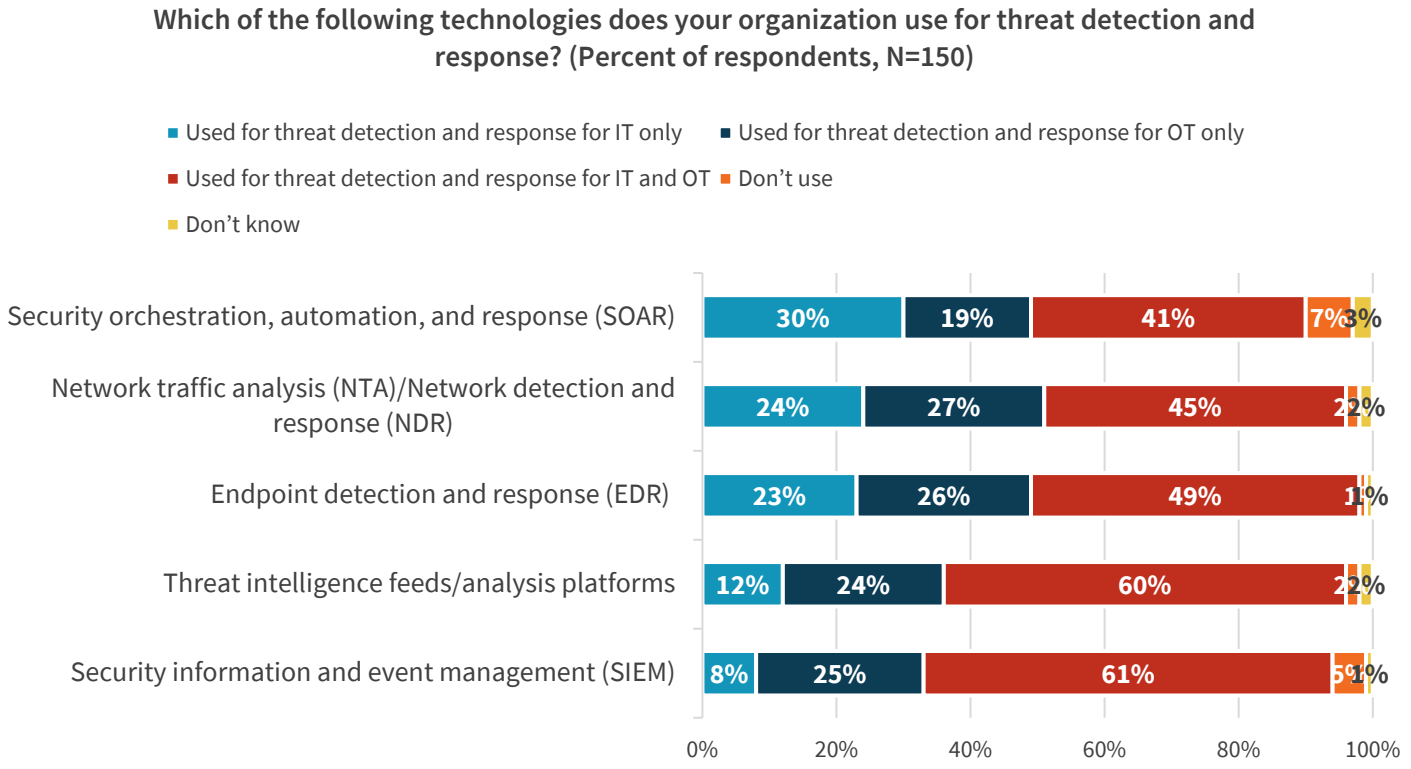
Beyond infrastructure integration, organizations are also consolidating their efforts around IT and OT security through a common cybersecurity staff. Forty-one percent of organizations employ an IT security team with dedicated OT specialists, while 32% rely on their IT security team alone to protect OT assets. This means that security teams must develop an acute understanding of normal operational technology behavior to be able to identify threats in real time.

As part of a secure IT/OT infrastructure, some organizations (17%) employ air-gapped networks, physically separating IT and OT assets, but most firms (58%) use network technology tactics like IP ranges, VLANs, or microsegmentation to segment IT and OT network traffic. Almost one-quarter (24%) of organizations simply use one common network for IT and OT communications.

While OT threats may be specialized, the research also reveals that most organizations continue to use standard IT security technologies like SIEM platforms, threat intelligence feeds, and EDR software for threat detection in IT and OT infrastructure (see Figure 2).

Common tools and staff may make operational sense, but this strategy assumes that security teams understand the nuances of OT assets while threat detection and response technologies are tuned for OT-focused attacks. As this research reveals, however, these assumptions aren't always accurate.

## Figure 2. Technologies Used for Threat Detection and Response




*Source: Enterprise Strategy Group*

### IT/OT Security Convergence: Situational Analysis

While organizations are on a path toward network convergence, 58% of survey respondents claim that detecting and responding to IT and OT threats has become more difficult over the past 2 years for several reasons (see Figure 3). Why the growing difficulties? Security professionals point to factors like:

**45% of organizations are collecting and processing more security data, while 43% say that the volume of alerts has increased over the past 2 years.**

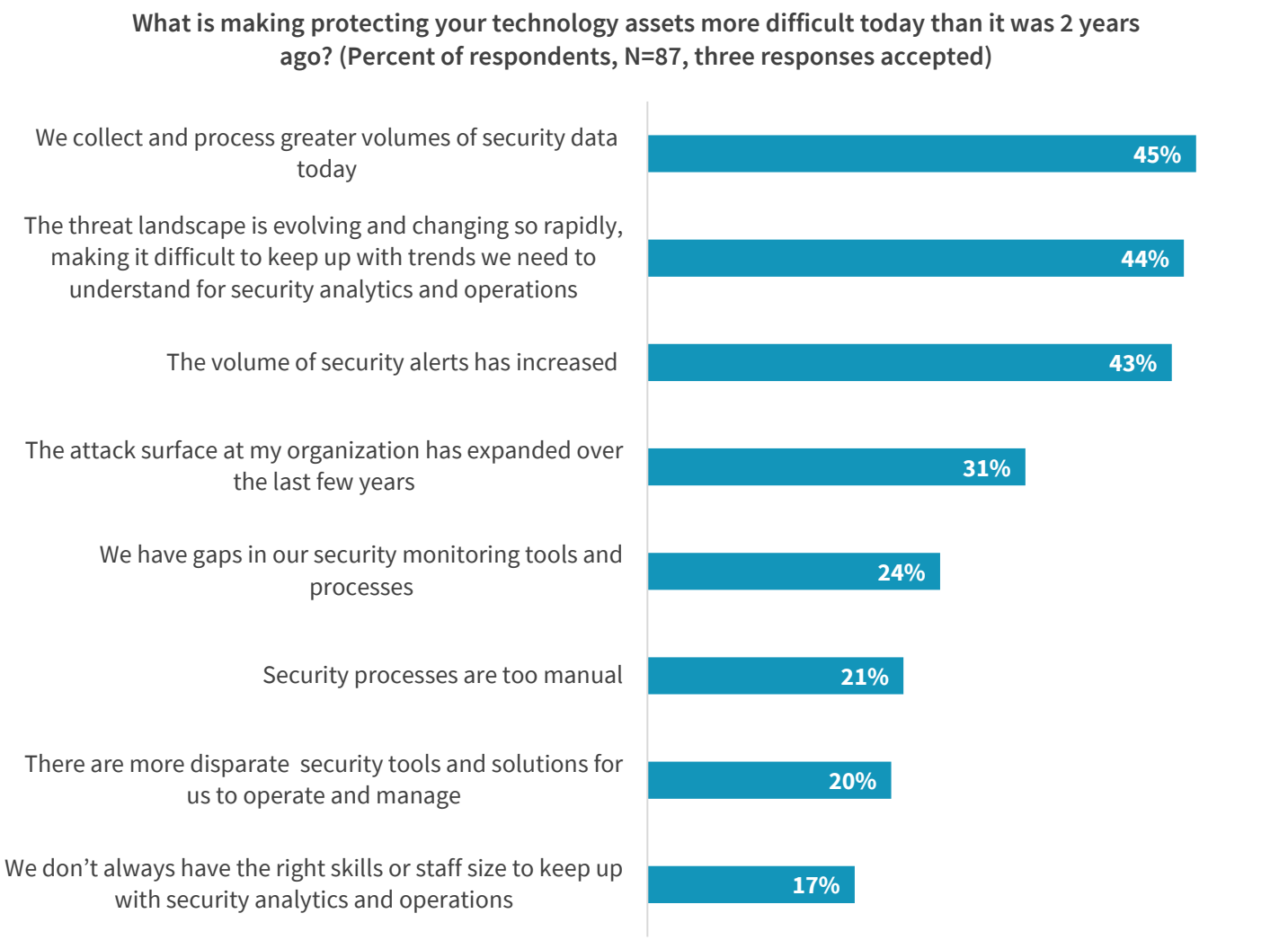
- Data and alert volume. Nearly half (45%) of organizations say that they are collecting and processing more security telemetry, making threat detection and response more difficult. Similarly, 43% of firms say that the volume of security alerts has increased, making threat detection and response more difficult. Since these trends aren't dissipating, it's safe to assume that threat detection and response difficulties will continue.

- Emerging threats. Just under half (44%) of organizations claim that evolving and changing threats are making threat detection and response more difficult. This has been particularly true as threat actors take advantage of the "fog" of COVID-19. As OT and IT infrastructures merge, OT threat volume and sophistication will increase, exacerbating this situation.

- Visibility gaps. Nearly one-quarter (24%) of security professionals say that their organization has gaps in their security monitoring and processes, making threat detection and response more difficult. ESG has noted that these gaps are often related to specialized OT assets, protocols, and traffic patterns.

CISOs at manufacturing organizations should view the ESG/TrapX data with some concern. Security teams are being overwhelmed with security data on one hand while lacking comprehensive visibility on the other. This likely leads to undetected attacks and long dwell times.

**Figure 3. Why Protecting IT and OT Assets Is More Difficult than 2 Years Ago**

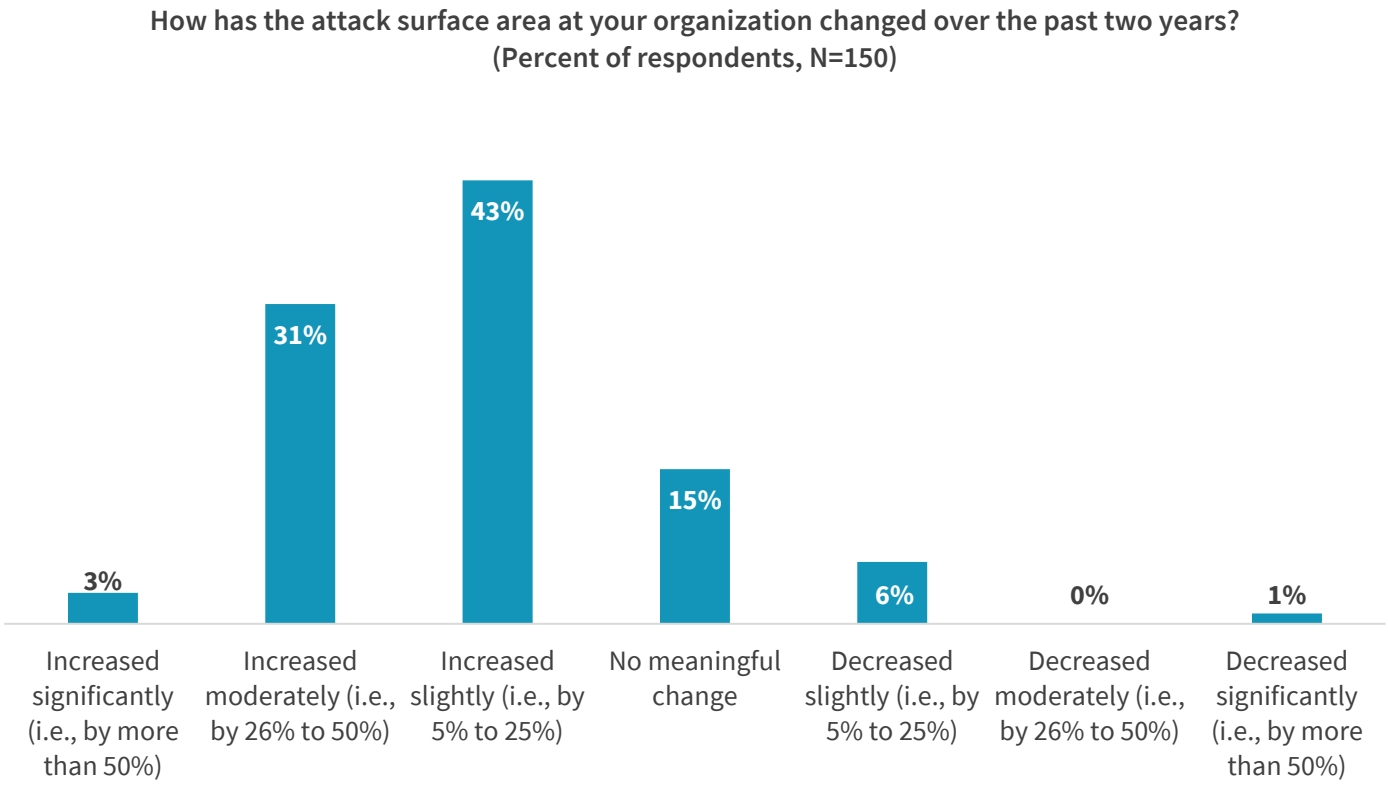



*Source: Enterprise Strategy Group*

Note that almost one-third (31%) of organizations indicate that attack surface growth is driving threat detection and response difficulties. This is understandable, since 77% of organizations surveyed admit to attack surface growth over the past two years (see Figure 4).

Attack surface growth is a predictable outcome of other ongoing IT trends. Firms are embracing SaaS applications like Office365, Salesforce, and ServiceNow as replacements for on-premises alternatives. At the same time, many organizations are moving workloads to, and developing new applications on, public cloud infrastructure. As part of digital transformation, companies are also deploying specialized IoT devices in industries like healthcare, logistics, and transportation. As the IT/OT attack surface grows, security teams are spread thinner as they try to keep up with security operations tasks such as threat detection, investigations, incident response, and risk mitigation.

## Figure 4. Changes in the Attack Surface



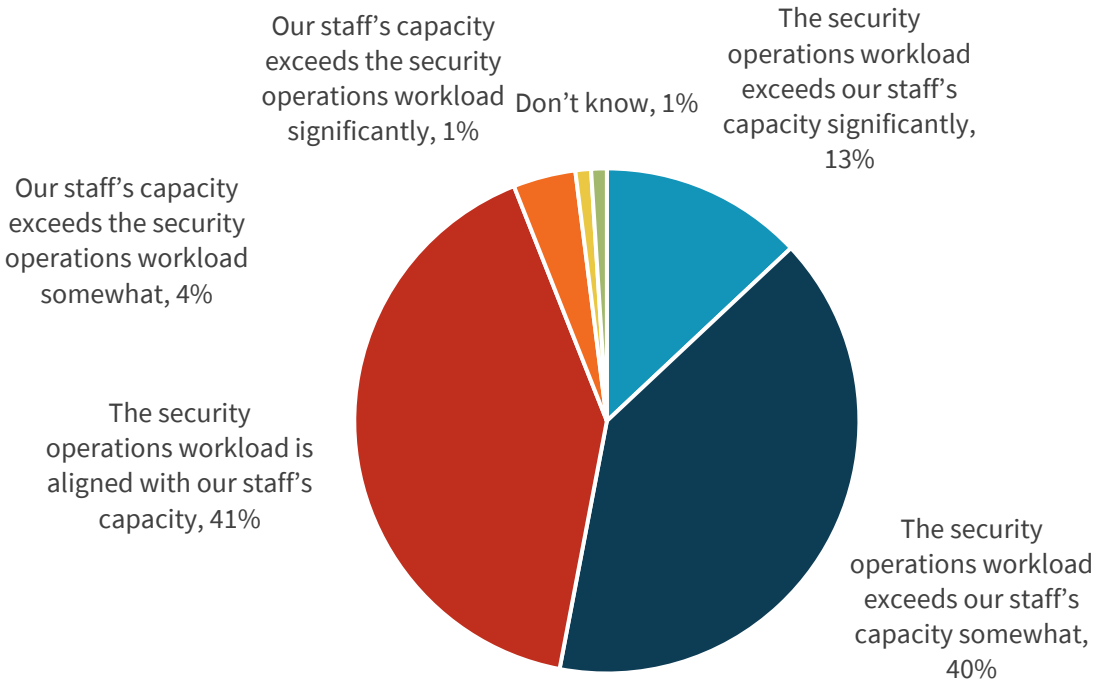

*Source: Enterprise Strategy Group*

As if threat detection and response challenges weren't enough, they are often exacerbated by the global cybersecurity skills shortage. Many organizations don't have enough staff members or the right skills to meet their cybersecurity requirements. Unfortunately, this issue is impacting the manufacturing companies surveyed for this research report. More than half (53%) of manufacturing organizations say that the security operations workload exceeds their staff's capacity "significantly" or "somewhat" (see Figure 5). Since CISOs can't hire their way out of this situation, they will need to make their people more efficient and productive—somehow.

**53% of manufacturing organizations say that the security operations workload exceeds their staff's capacity.**

**Figure 5. Staffing Capacity Versus Security Operations Workload**

**When comparing your organization's security operations workload to its staff size and capabilities, which of these statements is most accurate? (Percent of respondents, N=150)**

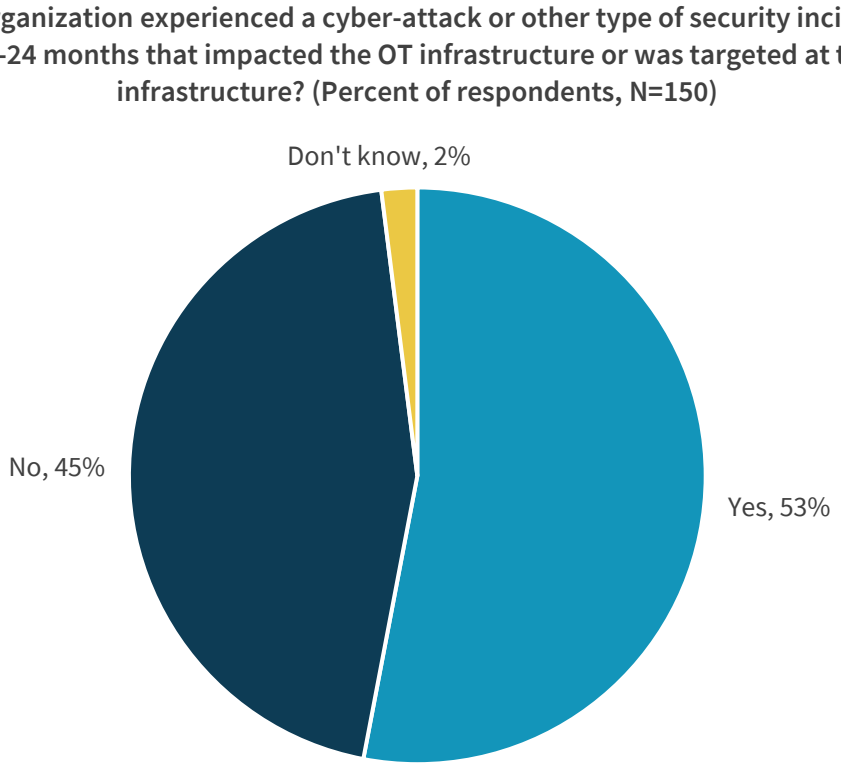



*Source: Enterprise Strategy Group*

The combination of threat detection/response challenges and staff/skills shortage leads to predictable results—53% of manufacturing organizations surveyed claim that they have experienced a cyber-attack or other type of security incident in the last 12-24 months that impacted the OT infrastructure or was targeted at the OT infrastructure (see Figure 6).

Those organizations that experienced a cyber-attack on OT infrastructure were then asked the following question: How long does it typically take your organization to fully remediate and recover from an attack on its OT systems? Twenty-eight percent said it takes less than one week to fully remediate and recover from an OT attack, but recovery and remediation took longer at most organizations—47% said a week to one month, 19% said one month to less than one quarter (i.e., 3 months), 5% said one quarter to less than 6 months, and 1% said more than 6 months. Clearly, OT attacks and long remediation cycles can cause unplanned downtime, leading to business disruption and higher costs.

**Figure 6. Security Incidents Impacting OT**




*Source: Enterprise Strategy Group*

Based upon the research presented in this research report, business, IT, and security managers have cause for concern. Manufacturing companies are integrating IT and OT infrastructure and organizations to gain efficiencies and scale, but they remain behind in preventing, detecting, and responding to security events. This can lead to security incidents and data breaches that can require lots of time and resources for full recovery. Of course, downtime in a manufacturing environment leads to production disruptions, customer service issues, and higher costs. Executives should analyze this data to answer an obvious question: What can our organization do to mitigate cyber-risks to OT assets?

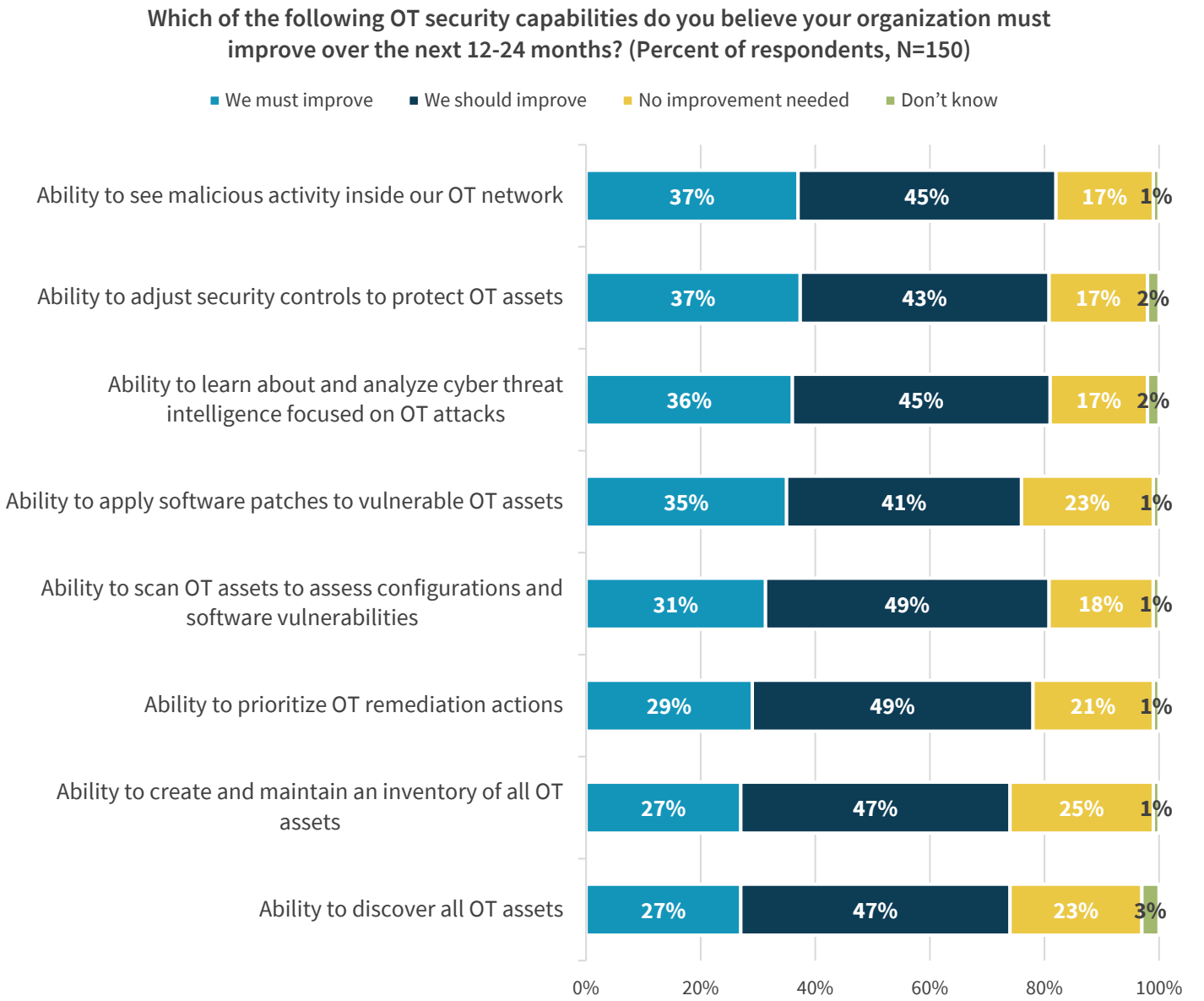
## Areas for Improvement

Survey respondents were then presented with a number of security capabilities and asked whether their organization needed to improve in each area (see Figure 7). Four "must improve" categories stood out:

- 37% of organizations say they must improve their ability to see malicious OT activity. This speaks to the lack of visibility and blind spots identified previously. Organizations need more timely, granular, and accurate data so they can quickly assess risk and make data-driven risk mitigation decisions, especially regarding OT assets, protocols, and data.
- 37% of organizations say they must improve their ability to adjust security controls. This fits under the response side of threat detection and response. CISOs want to fine-tune security controls based upon new threat intelligence or discovered vulnerabilities. This demands better technology integration and process automation.

- **36% of organizations say they must improve their ability to understand OT-focused threat intelligence.** Security teams want to know more about the tactics, techniques, and procedures (TTPs) used in cyber-attacks on actuators, industrial controls systems (ICSs), SCADA systems, and sensors. Armed with this knowledge, security teams can implement compensating controls while monitoring their networks for signs of attacks.
- **35% of organizations say they must improve their ability to patch vulnerable OT assets.** In this case, security teams want to improve vulnerability scanning, asset classification, and patch management as a closed-loop lifecycle. This will require better tooling, threat intelligence analysis, and process improvements between security and IT operations teams.

**Figure 7. Organizations Believe They Must Improve OT Security Capabilities**




*Source: Enterprise Strategy Group*

## The Case for Deception Technology

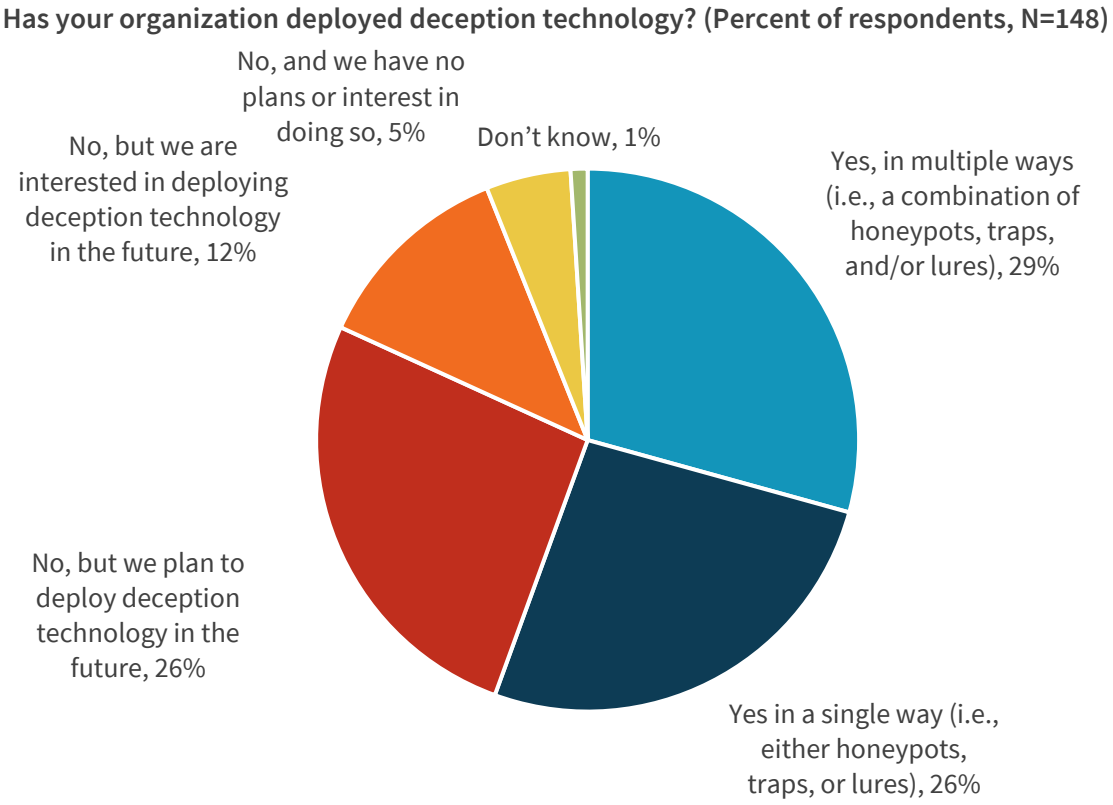
The research presented previously indicates that manufacturing organizations lack the right visibility for threat detection and response, especially regarding OT assets. Consequently, additional security complexity is unacceptable—any new security technologies they adopt must help them get more out of existing tools, processes, and staff.

Some manufacturing firms are bridging the security gap through extended use of deception technology. In cybersecurity terms, ESG defines deception technology as:

*A cybersecurity defense strategy designed to emulate real assets in order to deceive attackers as they proceed through the lifecycle (kill chain) of a targeted attack (on IT or OT assets).*

According to the ESG/TrapX research, more than half of the manufacturing organizations (55%) surveyed use deception technology today (see Figure 8).

**Figure 8. Limited Deployment of Deception Technology**




*Source: Enterprise Strategy Group*

Why deception technology? Manufacturers are implementing it for several reasons, including:

- To emulate the OT environment. Deception technology can assess an organization's network and then create realistic lures, decoys, and traps that mimic real OT assets, networks, and data. These deception assets can confuse hackers who may be overwhelmed by the size and complexity of the network. In this way, deception technology can deter cyber-adversaries from the start, immediately reducing malicious activities and filtering out cybersecurity noise.

- To provide high fidelity alerts. When more sophisticated cyber-adversaries compromise a system, they move laterally through the network and escalate privileges, pursuing an end goal of disrupting operations or stealing data. In this case, deception technology tilts the balance of power in favor of network defenders. Since all decoys and lures are invisible to legitimate users, any interaction with deception assets can only indicate malicious activity. When this occurs, deception technologies generate high-fidelity alerts with specific details of what happened. These high-fidelity alerts can help eliminate the useless work associated with false positives while supplementing other telemetry from EDR, NDR, SIEM, and threat intelligence systems. The result? An accurate picture of what happened and when it happened.

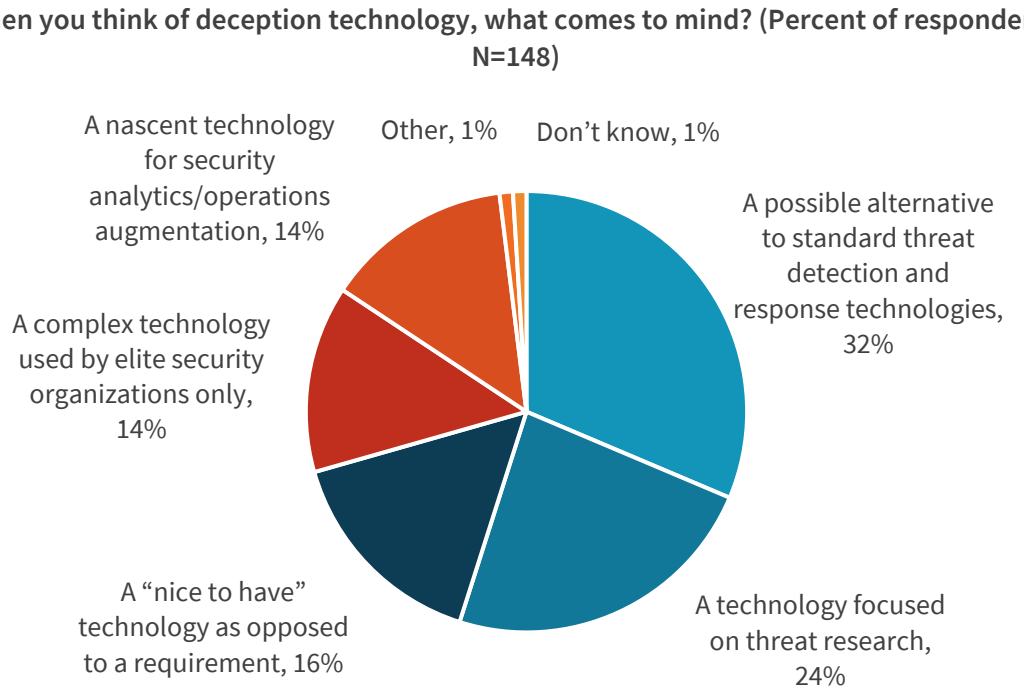
- For advanced use cases. Some organizations use deception technology more traditionally as a way to collect intelligence about specific threat actors and campaigns. Armed with this intelligence, security teams can fine-tune controls as well as deception assets. Mature organizations can also use deception technology for proactive threat hunting by seeding their networks with enticing fake assets that may be especially attractive to particular threat actors. These traps can be used to expose attacks in their formative stages.

Given these use cases, it's not surprising that deception technology is slowly gaining a foothold in manufacturing organizations. At the same time, however, the research also suggests confusion about deception technology (see Figure 9).

As described, modern deception technologies can be used as part of a threat detection and response strategy and even serve as an alternative to other layers of defense. This use case is understood by almost one-third (32%) of respondents. Unfortunately, two-thirds of security professionals remain confused, viewing deception technology as focused on threat research (24%), as a "nice to have" technology (16%), as a complex technology used by elite organizations (14%), or as a nascent technology for security analytics/operations augmentation (14%).

Manufacturing companies have ideas about deception technology but lack a true understanding of how it can be used strategically as part of an enterprise cybersecurity program.

**Figure 9. Deception Technology Is Misunderstood**




*Source: Enterprise Strategy Group*

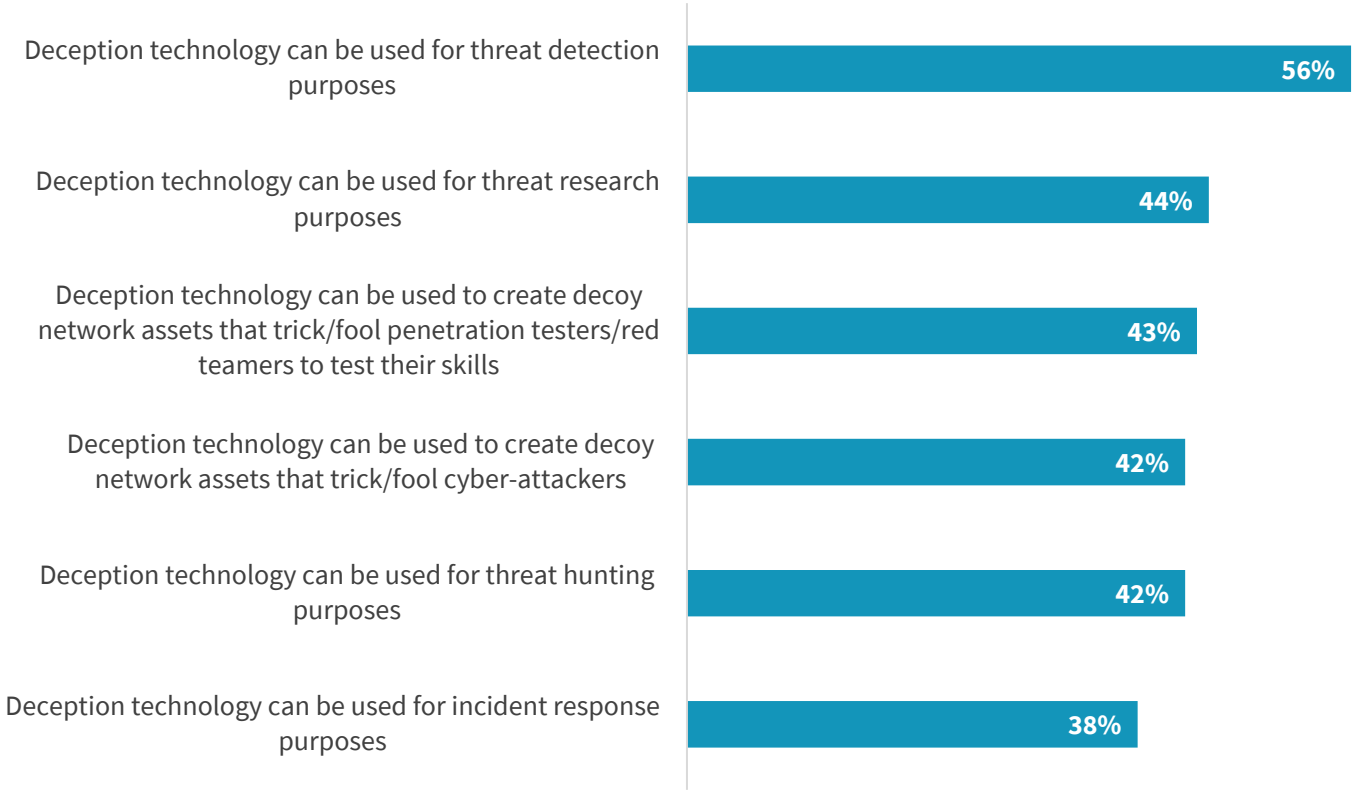
To further flesh out deception technology, organizations using, planning to use, or interested in using deception technology were asked for further details about their use cases (see Figure 10). More than half (56%) said that deception technology can be used for threat detection purposes, clearly recognizing its value here. Respondents also recognized deception technology's roles in threat research (44%), as a decoy (43%), or for threat hunting purposes (42%).

**56% of manufacturing organizations using deception technology do so for threat detection purposes.**

The data in Figure 10 reveals some of the confusion around deception technology. Most security technologies perform a single function—they detect malware, block network connections, or monitor specific activities. Rather than having a fixed function, however, deception technology can be used in numerous proactive and reactive ways. Furthermore, deception technology can be used to supplement existing security technologies like SIEM by helping to provide accurate and actionable alerts. When a cyber-adversary accesses a deception decoy, there is no doubt that malicious activities are happening. This can help organizations not only improve threat detection and response but also streamline security operations. Manufacturing organizations using deception technology can achieve these results, but only if they take the time to learn the technology and use it to its full potential.

**Figure 10. Deception Technology Use Cases**

**You indicated that your organization has deployed deception technology, plans to deploy deception technology, or is interested in doing so. What are the primary reasons for this decision? (Percent of respondents, N=139, multiple responses accepted)**




*Source: Enterprise Strategy Group*

In summary, deception technology seems to be at an inflection point with manufacturing organizations. While some firms are taking advantage of deception technology, most are using it tactically, and others remain confused or ignorant of its

potential value. This is a classic example of an emerging technology and immature market. As deception technology advances and the market matures, manufacturing companies are likely to recognize its value and add deception technology as another layer of defense.

## The Bigger Truth

The research presented in this report illustrates an imbalance between business initiatives and security protection. Manufacturing organizations are consolidating their IT and OT environments to achieve economies of scale and enable new types of business processes. Unfortunately, this advancement carries the growing risk of disruptive cyber-attacks. While organizations have deployed numerous technologies for threat detection and response, they seem overwhelmed by growing volumes of security data, visibility gaps, and a lack of staff and skills.

How can manufacturing organizations address these issues? They can start by using this report to help CISOs assess their current security status and address specific weaknesses. For example, the research indicates that organizations need:

1. Better visibility into their OT networks and assets.
2. Quicker reactions to anomalous, suspicious, and malicious activities.
3. Help for their security staff.

Using deception technology strategically can help here as follows:

1. Better visibility into their OT networks and assets. Deception technology can emulate assets and force cyber-adversaries to access a decoy and trigger an alert. These alerts will be accurate and detailed, providing a new level of visibility detail.
2. Quicker reactions to anomalous, suspicious, and malicious activities. Deception technology offers high-fidelity alerts that can speed investigations, incident response, and risk mitigation actions.
3. Help for their security staff. By reducing false positives and overall "noise" in the system, deception technology can address much of the complexity that often overwhelms security staff.

In aggregate, manufacturing companies need to work smarter, and not harder, on protecting valuable OT assets that drive the business. Deception technology is a bit of a different approach to security and it's clear that many organizations remain confused about what it is and what it can do. Nevertheless, deception technology seems to be catching on with manufacturing companies, as it can help improve security efficacy and operational efficiency. Given its potential value, deception technology is likely to gain popularity with manufacturing companies moving forward.

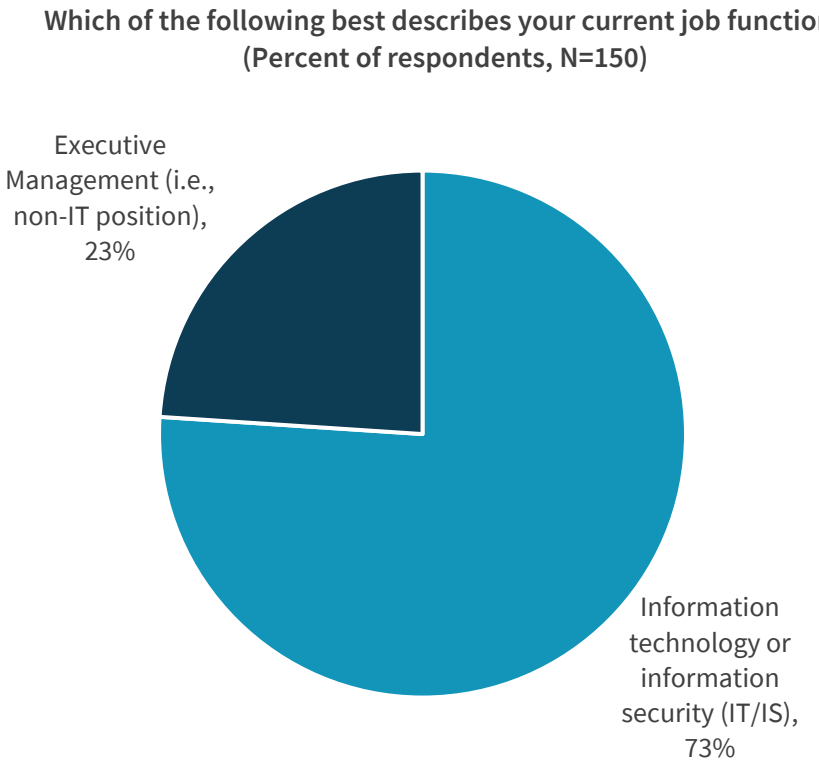
## Research Methodology

To gather data for this report, ESG conducted a comprehensive survey of security decision makers employed at midmarket organizations (29%, 100 to 99 employees) and enterprise organizations (71%, 1,000+ employees) in North America between August 17th and August 31st, 2020. Key sectors of the manufacturing industry were represented, including discrete manufacturers, process manufacturers, life sciences, oil and gas, and consumer packaged goods. All respondents were provided an incentive to complete the survey in the form of cash awards and/or cash equivalents.

After filtering out unqualified respondents, removing duplicate responses, and screening the remaining completed responses (on several criteria) for data integrity, a final sample of 150 respondents remained. The figures that follow detail the demographics of the respondent base discussed in this report.

Note: Totals in figures and tables throughout this report may not add up to 100% due to rounding.

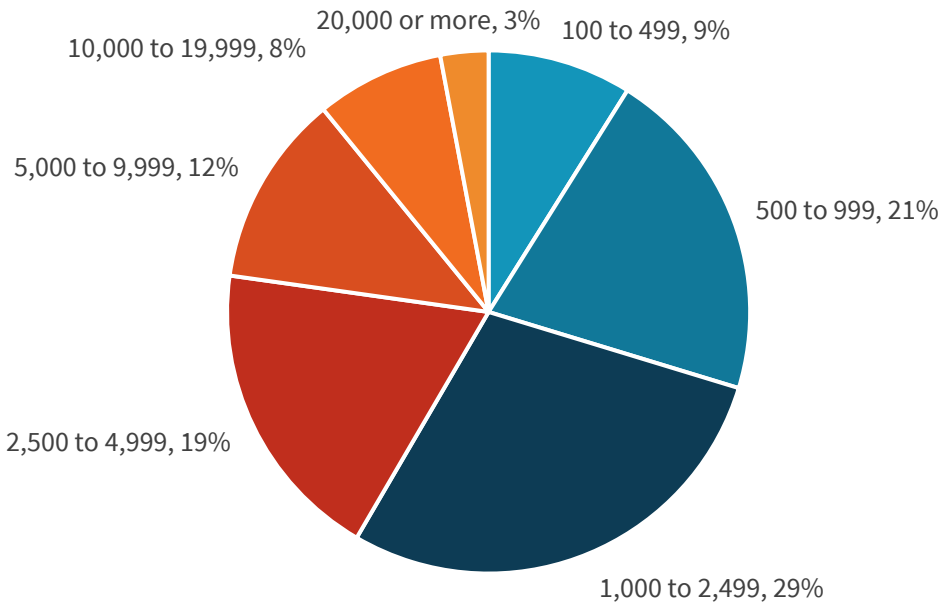
**Figure 11. Survey Respondents, by Job Responsibility**




*Source: Enterprise Strategy Group*

## Figure 12. Survey Respondents, by Company Size

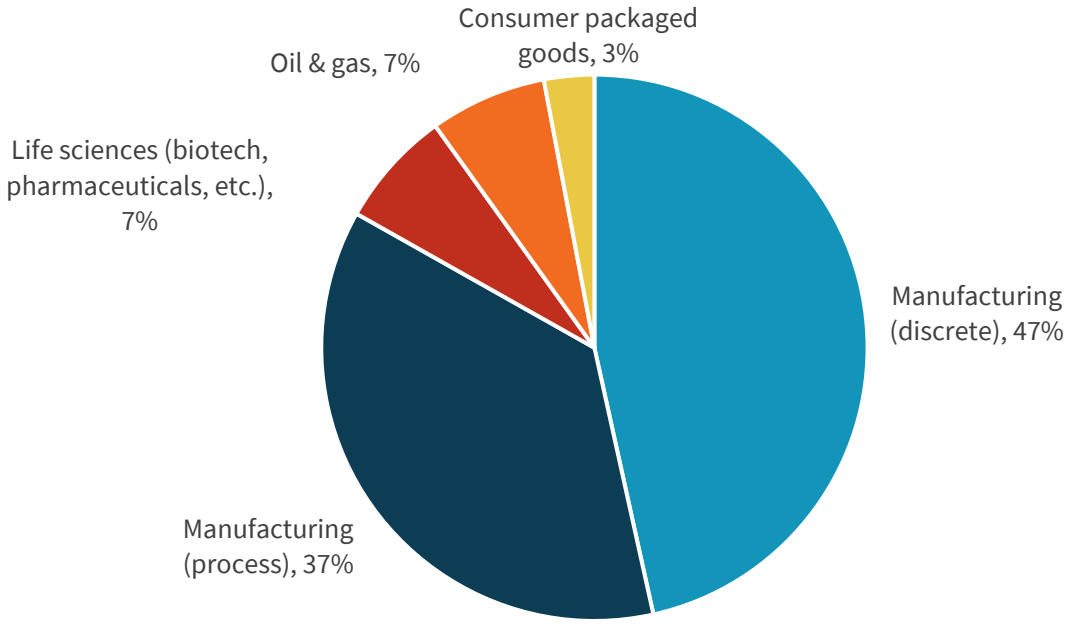
**How many total employees does your organization have worldwide? (Percent of respondents, N=150)**




*Source: Enterprise Strategy Group*

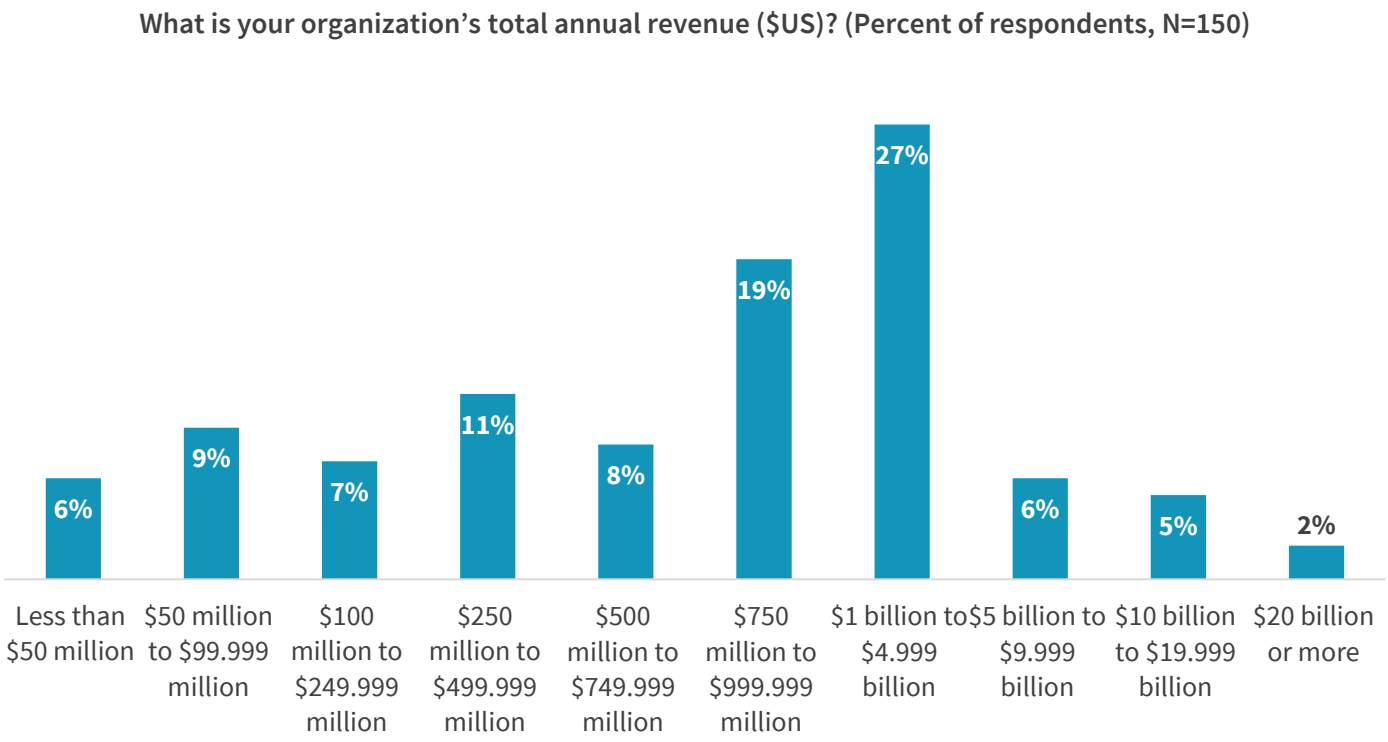
## Figure 13. Survey Respondents, by Industry

**What is your company's primary industry? (Percent of respondents, N=150)**




*Source: Enterprise Strategy Group*

## Figure 14. Survey Respondents, by Annual Revenue




*Source: Enterprise Strategy Group*