2020 STATE OF SECURITY OPERATIONS

A Survey of International IT Security Operations Professionals on the Challenges They Face and the Best Practices and Technologies They Embrace to Meet These Challenges

OCTOBER 2020

A CYBEREDGE RESEARCH STUDY SPONSORED BY:

Table of Contents

Introduction

The 2020 State of Security Operations Report takes a close look at the front lines of IT security: security operations. For our survey, we wanted to talk to the people who find and mitigate vulnerabilities, detect threats, perform security investigations, respond to incidents, and do countless other operational tasks on a daily basis. We also wanted to hear from security operations managers and executives about the challenges their teams are facing.

Our objective for this report is to take a snapshot of today's security operations and to indicate how things are likely to evolve in the coming months and years.

The survey at the heart of this report was conducted in August 2020. This was several months after the COVID-19 pandemic began, with many of the participants in locations that had not yet fully reopened. As you read this survey report, keep in mind that it reflects the viewpoints and opinions of IT security operations professionals roughly six months into the pandemic.

CyberEdge would like to thank our research sponsor, Micro Focus, who conceived this report and whose support has been essential to its success.

Top Five Insights for 2020

This report contains dozens of actionable insights on IT security operations. Here are our top five takeaways:

1. Threat detection is a major hurdle. There's clearly no shortage of threats, but there's definitely a shortage of personnel to detect and analyze them. Organizations are already using security information and event management (SIEM) solutions, tools with machine learning (ML) and artificial intelligence (AI) technology, and processes leveraging the MITRE ATT&CK Framework to try to improve threat detection, but it's not enough. Threat detection currently overshadows all other aspects of security operations in terms of across-the-board concern.

2. More and more tools are in use. All 11 common types of security operations tools we asked about are expected to exceed 80% adoption in 2021. For example, over 92% of organizations expect to be using SIEMs in 2021. Security operations is such a broad area that more and more tools are needed for complete coverage.

SURVEY DEMOGRAPHICS

- **Responses received from 410 qualified IT security operations executives, managers, and practitioners**
- **All from organizations with 500 or more employees**
- **Representing five countries: Germany, India, Japan, the United Kingdom, and the United States**
- **Representing 17 industries**

3. Reliance on external resources is rising. Over 96% of organizations use the cloud for IT security operations, and on average nearly two-thirds of their IT security operations software and services are already deployed in the cloud. Furthermore, over 87% of organizations already outsource some of their IT security functions to managed security service providers (MSSPs)—with an average of three functions outsourced.

4. Malware is still #1. Of all the security threat types out there, organizations are most concerned about malware, followed closely by phishing/spear-phishing attacks and ransomware. However, survey participants indicated that their organizations are at least moderately concerned about all common types of threats.

5. Cyberthreats and incidents related to COVID-19 are impacting security operations. The biggest challenge from COVID-19 to security operations teams has been the increased volume of cyberthreats and security incidents they've had to deal with.

About This Report

The findings of this report are divided into four sections:

Section 1: Technology

With the sheer volume and scale of technology needed to secure today's digital assets, it's no surprise that IT security operations teams must heavily rely on technology in order to do their jobs. This section of the survey provides insights on current tool use and planned acquisitions. It also looks at how some tools and technologies with multiple features are actually being used. Readers will be able to compare their organization's security operations technology against the broad sample surveyed and see where they may be ahead—or behind—of their peers.

Section 2: Processes

In this section, we look at the processes that organizations use in conjunction with their security operations tools and technologies. Survey participants told us what their toughest process challenges are, and how they are using industry-standard frameworks to help improve their processes. The data in this section can help readers to assess and compare the challenges in their own organizations with those of other organizations.

Section 3: People

To complement the first two sections on technology and processes, the third section looks at people. Skilled personnel are critical to security operations. We focus on personnel shortages and the areas of security operations where more staffing would help the most. Readers may want to compare their staffing with the snapshot depicted in this section and adjust their staffing plans, hiring expectations, and automation support needs.

Section 4: Perceptions

In the last section, we asked survey participants for their opinions on several subjects that cut across technology, processes, and people. For example, we asked about the effect of the COVID-19 pandemic on security operations teams. We also asked about where security operations software and services are located or if they are outsourced. The goal of this section is to get a better picture of the current state of security operations and how organizations are coping with modern challenges.

Navigating This Report

We encourage you to read this report from cover to cover so you don't miss any valuable tidbits. That said, there are three other ways to navigate through the report if you're looking for a particular topic:

- Table of Contents. Each topic in the Table of Contents pertains to specific survey questions. Click on any topic to jump to its corresponding page.
- Research Highlights. The Research Highlights page showcases the most significant headlines of the report. Page numbers are referenced with each highlight so you can quickly learn more.
- Navigation tabs. The tabs at the top of each page are clickable, enabling you to conveniently jump to different sections of the report.

Research Highlights

Technology

- **Tools galore.** Organizations are widely using 11 common types of security operations tools, with each type expected to exceed 80% adoption in 2021 (page 6).
- **Managing threats with SIEMs.** Organizations most often use SIEMs to detect and investigate threats, and to respond to successful attacks. Log management and compliance reporting features are less important within SIEM (page 7).
- **Widespread ML and AI usage.** Over 93% of organizations use security operations products with ML or AI technology (page 8).
- **Changing roles for ML and AI.** Although many vendors tout them for decreasing false positives, most organizations actually use ML and AI-based products to improve threat and attack detection (page 8).

Processes

- **MITRE ATT&CK Framework becoming ubiquitous.** Nearly 9 in 10 organizations use the MITRE ATT&CK Framework knowledge base of attack techniques (page 9).
- **Protect: the biggest NIST CSF challenge.** Of the five NIST Cybersecurity Framework functions, Protect—developing and implementing safeguards to ensure delivery of critical services—is the biggest challenge for IT security operations (page 10).
- **Tough times for security operations teams.** Asked to consider several challenges for security operations teams in 2020, organizations rated all of them as having moderate to moderate-high severity (page 11).

People

- **Wanted: more skilled people.** Over 90% of organizations have shortages in their security operations staffing, with the most shortages in India (over 98%) and in the education sector (100%) (page 12).
- **Wanted: attack detection talent.** Organizations would most benefit from having more staff skilled in attack detection and analysis (page 13).

Perceptions

- **Mostly cloudy.** Over 96% of organizations use the cloud for IT security operations, and on average nearly two-thirds of their IT security operations software and services are deployed in the cloud (page 15).
- **Discouraging news about threats.** Organizations are moderately concerned at a minimum about all common types of cyberthreats (page 16).
- **Just read the headlines.** Organizations are most concerned about malware, phishing/spear-phishing attacks, and ransomware (page 16).
- **COVID-19 challenges.** During the pandemic, security operations teams have faced many challenges. The biggest has been the increased volume of cyberthreats and security incidents, followed by higher risks due to workforce usage of unmanaged devices (page 17).
- **Reliance on MSSPs.** Globally, 87% of organizations outsource at least one IT security function to an MSSP, with individual organizations outsourcing three functions on average (page 18).

Security Operations Tools

Which of the following security operations tools are currently in use or planned for acquisition (within 12 months) by your organization?

	Currently in use	Planned for acquisition	No plans
Security configuration management (SCM)	71.1%	18.5%	10.4%
Security information and event management (SIEM)	65.7%	26.4%	7.9%
Network traffic analysis (NTA)	63.4%	26.5%	10.1%
Threat intelligence platform (TIP) or service	60.1%	28.1%	11.8%
Patch management	59.4%	27.4%	13.2%
Log management (without advanced SIEM capabilities)	59.1%	29.7%	11.2%
Vulnerability assessment/management (VA/VM)	58.5%	31.0%	10.5%
Security data lake	55.7%	27.5%	16.8%
Security orchestration, automation and response (SOAR)	55.2%	34.0%	10.8%
Threat hunting tool	54.2%	31.2%	14.6%
User and entity behavior analytics (UEBA)	52.6%	29.9%	17.5%

Figure 1: Percentage of security operations tools currently in use or planned for acquisition within 12 months.

Security operations includes many responsibilities, so it's no surprise that organizations use numerous tools to help carry out all of those duties. In this survey, we asked organizations about common security operations tools to find out if they were already using them or were planning on acquiring them in the next 12 months (see Figure 1).

All 11 categories of security operations tools are currently used by more than half the organizations. That includes newer technologies, like user and entity behavior analytics (UEBA) (52.6%) and threat hunting tools (54.2%), which we'd expected wouldn't be as widely used as more established technologies. Sure enough, the most widely used tools are security configuration management (SCM) (71.1%) and security information and event management (SIEM) (65.7%).

What surprised us was some of the tools in the middle of the pack. Conventional wisdom is that tools for patch management, log management, and vulnerability assessment/management are all fundamental and widely used, but less than 60% of organizations are actually using them.

Finally, many organizations are planning on adding security operations tools in the next 12 months, with the most popular being security orchestration, automation and response (SOAR) (34.0%), threat hunting tools (31.2%), and vulnerability assessment/vulnerability management (31.0%). Even the least popular categories of tools are expected to be used or acquired by over 80% of organizations within the next year. That's a lot of tools!

SIEM Use Cases

Which of the following are the primary use cases for your organization's usage of SIEM technology? Rank your top three in decreasing order of importance.

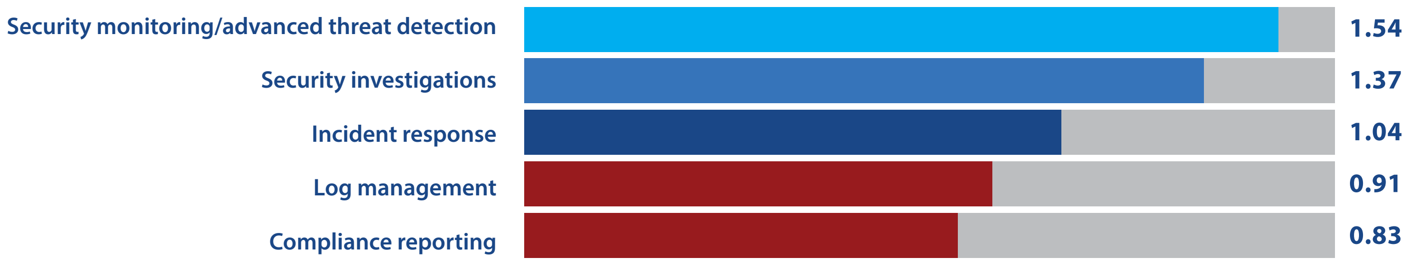

Figure 2: Primary use cases for SIEM.

We've already determined that SIEMs are expected to be in use or acquired by over 92% of organizations in the next 12 months (see Figure 1). When we extended the acquisition timeframe past 12 months, we found that the number rose to 95.1%! SIEM will be the most widely used of the security operations tools in 2021.

To better understand SIEM usage, we asked those respondents why their organizations use SIEM (see Figure 2). The graph shows the results as weighted averages on a scale of 0.0 to 3.0, where 3.0 would indicate everyone ranking the same use case as their top priority, and where 0.0 would indicate a use case not being included in anyone's rankings. Two use cases are by far the most common: security investigations are important for 69.5% of respondents, and security monitoring/advanced threat detection for 68.7%.

At the other end of the spectrum, less than half of the organizations cite compliance reporting (46.0%) or log management (46.5%) as one of their primary use cases for SIEM technology, and 54.5% select incident response.

These use cases indicate that most organizations are focused on using SIEM for threat-related objectives, like detecting threats, investigating threats, and responding to successful attacks. Non-threat-related objectives like compliance reporting and log management are generally not the main reasons for using SIEM.

ML and AI Technology Usage

What are the primary reasons your organization uses security operations products that feature machine learning (ML) and/or artificial intelligence (AI) technology? Rank your top three in decreasing order of importance.

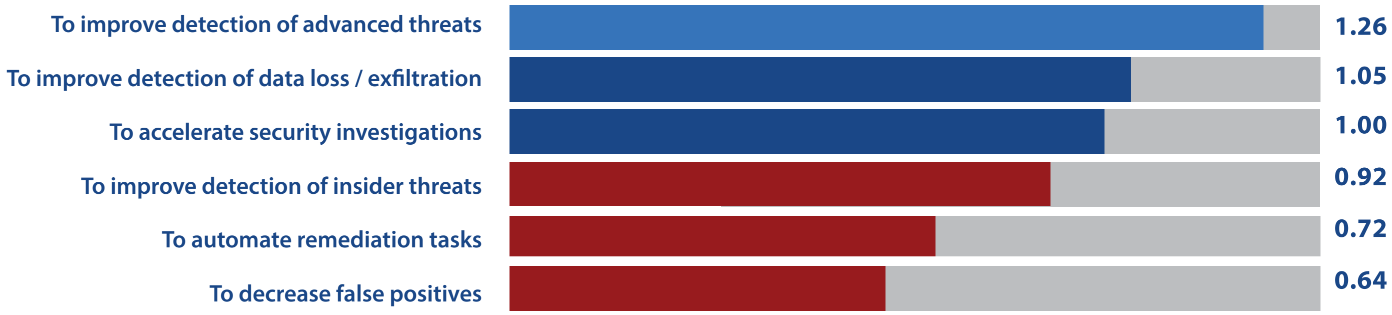

Figure 3: Primary reasons for using security operations products with ML and/or AI technology.

Many security operations products use machine learning (ML) and/or artificial intelligence (AI) technology. Now that these technologies have had some time to mature, we were curious as to how widely they were being used and why (see Figure 3). The graph shows the results as weighted averages on a scale of 0.0 to 3.0.

Over 93% of the respondents' organizations use ML and AI-based security operations products. These products are mainly being used to improve detection capabilities. Detecting advanced threats is the #1 reason for 25.2% of organizations, and a top three reason for 59.1% of organizations. Detecting data loss/exfiltration attempts, accelerating security investigations, and detecting insider threats are also common reasons.

What surprised us was that the least common reason was decreasing false positives. Many vendors tout ML and AI technologies as being able to decrease false positives—to stop erroneously reporting benign activity as malicious—but organizations seem far more interested in decreasing false negatives—to ensure they don't miss malicious activity.

It is unclear whether this means that false positives are less of a concern lately or if the improved detection capabilities that ML and AI can provide are simply more appealing to organizations at the moment. Either way, the results clearly indicate a shift in why organizations are using ML and AI in security operations.

The MITRE ATT&CK Framework

What are the primary reasons your organization uses the MITRE ATT&CK Framework? Rank your top three in decreasing order of importance.

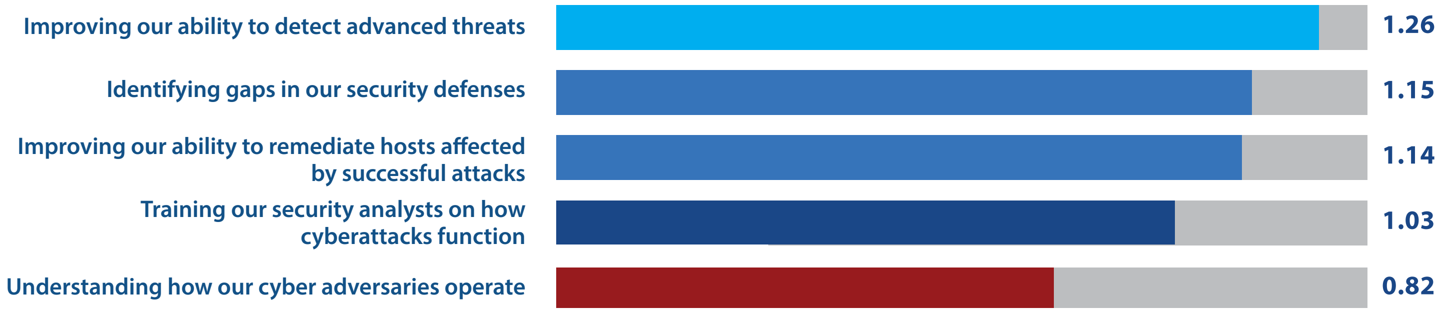

Figure 4: Primary reasons for using the MITRE ATT&CK Framework.

The MITRE ATT&CK Framework is a knowledge base that details hundreds of techniques used in cyberattacks. It is publicly available and offers a number of practical uses. We asked our survey participants how many of their organizations are using the MITRE ATT&CK Framework, and a resounding 89.8% said that they are.

To get more insights into how the MITRE ATT&CK Framework is being used for security operations purposes, we listed five possible reasons and asked participants to choose their top three (see Figure 4). The graph shows the results as weighted averages on a scale of 0.0 to 3.0. The most popular reasons are detecting advanced threats, identifying defensive gaps, and remediating hosts.

Looking at the top three reasons, each has a similar weighted average (see Figure 4). Detecting advanced threats has a slight advantage over the others, which is consistent with answers to other survey questions that indicate detecting advanced threats is of greatest concern.

The bottom two reasons, training security analysts and understanding how adversaries operate, are also common, with the latter the least popular at 42.5% of organizations. Still, it's clear that organizations seem more interested in using the MITRE ATT&CK Framework to immediately improve their security operations than to increase employee understanding of threats and attacks.

Toughest NIST Cybersecurity Framework Function

Which of the following NIST Cybersecurity Framework functions currently poses the toughest challenge for IT security operations at your organization?

	Global	USA	UK	India	Germany	Japan
Identify	29.9%	28.0%	20.0%	52.5%	21.2%	19.6%
Protect	35.4%	37.6%	46.0%	26.3%	36.5%	32.1%
Detect	19.2%	19.1%	24.0%	15.0%	25.0%	16.1%
Respond	8.9%	10.2%	6.0%	2.5%	11.5%	14.3%
Recover	6.6%	5.1%	4.0%	3.8%	5.8%	17.9%

Figure 5: Toughest challenge for IT security operations by NIST Cybersecurity Framework Function.

The National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) defines a set of activities that organizations can perform to manage their cybersecurity risks. At the highest level, the activities are grouped by five functions:

- **Identify –** Develop an organizational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities.
- **Protect –** Develop and implement appropriate safeguards to ensure delivery of critical services.
- **Detect –** Develop and implement appropriate activities to identify the occurrence of a cybersecurity event.
- **Respond –** Develop and implement appropriate activities to take action regarding a detected cyber-security incident.
- **Recover –** Develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident.

We asked survey participants to indicate which of the five functions currently poses the toughest challenge to their IT security operations. The functions focusing on preparation, Identify and Protect, are the most difficult for a majority of organizations in each of the five countries (see Figure 5). Across countries and industries, the Protect function is cited most often, with three exceptions: the country of India and the industries of Technology and Education cite Identify most often.

The post-detection functions, Respond and Recover, are the toughest for relatively few organizations. Taken together, they only total 15.5% globally, which is less than any of the other three functions.

The surprise is the Detect function not being considered the toughest challenge for IT security operations. With a global percentage of 19.2%, it's just about average. Because responses to other survey questions indicate that organizations are strongly concerned about detecting advanced threats, the relatively low selection of the Detect function indicates that organizations still face many unresolved challenges with Identify and Protect. Perhaps the Identify and Protect functions need to be improved first so that the Detect function becomes less challenging.

Challenges Facing IT Security Operations Teams

On a scale of 1 to 5, with 5 being highest, rate the severity of each of the challenges facing your IT security operations team.

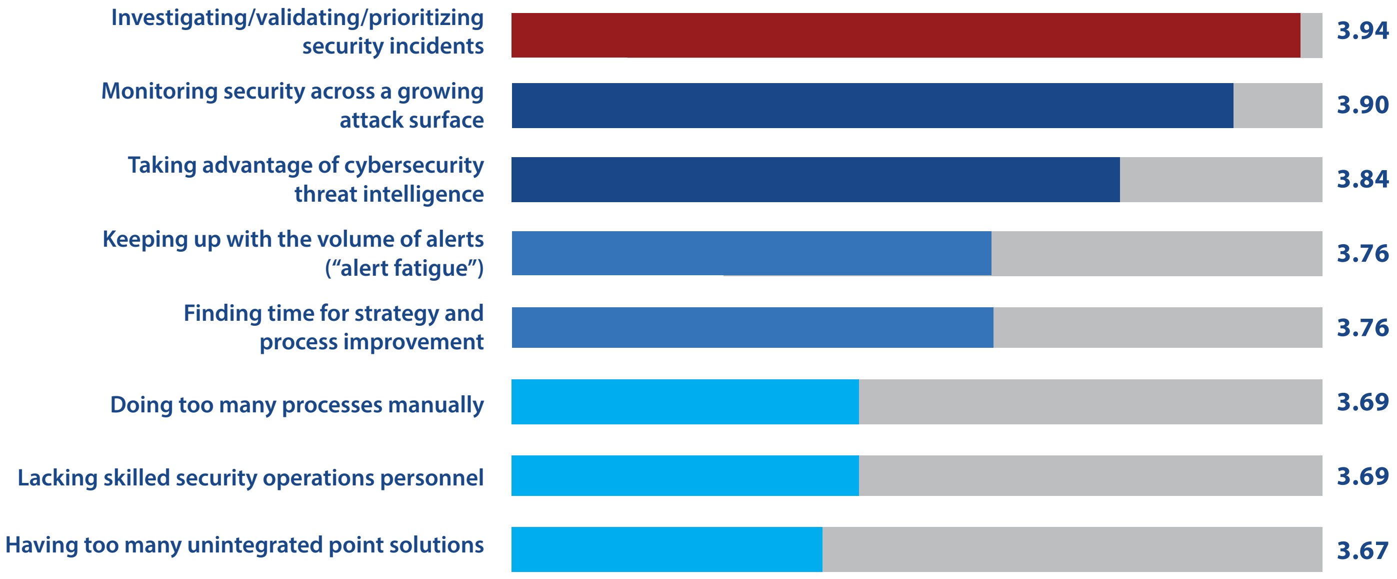

Figure 6: Severity of challenges that IT security operations teams are facing.

We asked respondents to rate the severity of several challenges that IT security operations teams are facing. Each rating uses the same five-point scale, where 1 is low severity and 5 is high severity (see Figure 6).

The two most severe challenges are investigating/validating/prioritizing security incidents (3.94) and monitoring security across a growing attack surface (3.90). Approximately one-third of all organizations say these two challenges are high severity for them.

However, what's most noteworthy is that organizations consider all of these challenges to have similar severity. The range of ratings is only 3.67 to 3.94, which means they are all moderate to moderate-high severity. Even the challenge with the lowest rating, having too many unintegrated point solutions, is still considered high severity by 27.2% of organizations.

The takeaway is that organizations overwhelmingly feel that their security operations teams are facing many daunting challenges at this time. These include point solutions not being integrated, a lack of skilled personnel, too many manual processes, a lack of time for strategy and process improvement, alert fatigue, and failing to take advantage of cybersecurity threat intelligence. Security operations teams need notable help and support in order to address these challenges.

Personnel Shortages by Role

Select the roles for which your organization is currently experiencing a shortage of skilled IT security operations personnel. Select all that apply.

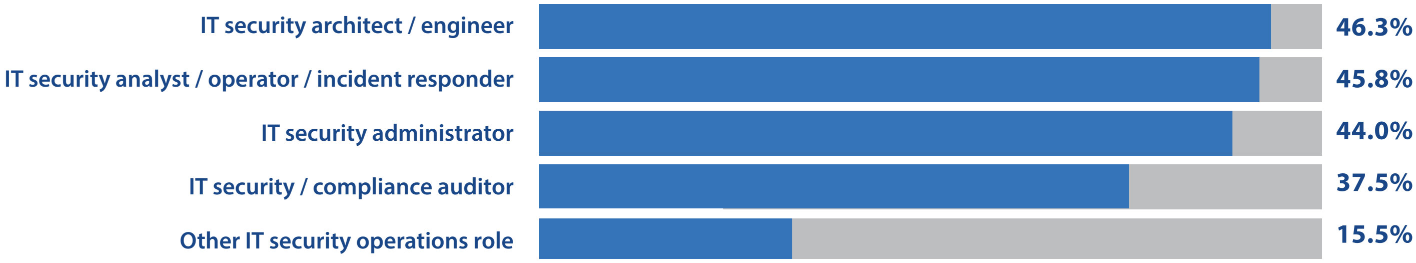

Figure 7: Percentage of organizations with IT security operations personnel shortages per role.

We all know already that IT security personnel in general are in short supply, but which roles are most challenging to fill? And where are those shortages most widespread? To answer these questions, we asked respondents to indicate if their organization is experiencing a shortage for several roles (see Figure 7).

Shortages are fairly similar for all the roles. Nearly half the organizations are experiencing shortages of IT security architects/engineers (46.3%), IT security analysts/operators/incident responders (45.8%), and IT security administrators (44.0%). IT security/compliance auditor shortages are slightly less severe (37.5%).

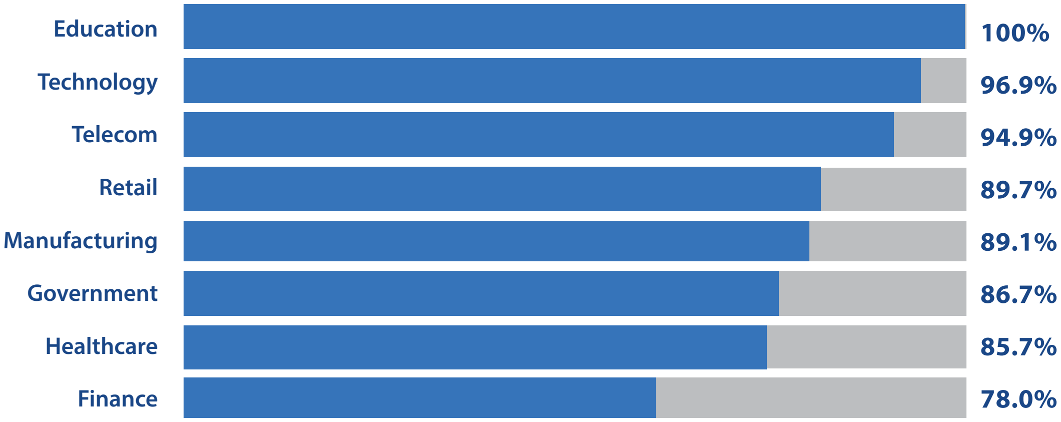

Figure 8: Percentage of organizations with IT security operations personnel shortages, by industry.

On average, each organization has shortages in more than one of the IT security operations roles.

Overall, 90.5% of organizations have a shortage of IT security personnel in at least one of the roles. Shortages are widespread in all surveyed countries, with India having the highest percentage of organizations with shortages (98.7%) and the UK having the lowest (84.9%).

There's more variation in the shortages when we look at the responses by industry (see Figure 8). Every educational institution surveyed has a shortage. Meanwhile, some of the most regulated industries in the survey—finance, healthcare, and government—have the lowest percentages of organizations with shortages (78.0% for finance, 85.7% for healthcare, 86.7% for government).

Staffing Needs by Skill

Which of the following aspects of your IT security operations would benefit the most from an increase in skilled staffing? Rank your top three in decreasing order of importance.

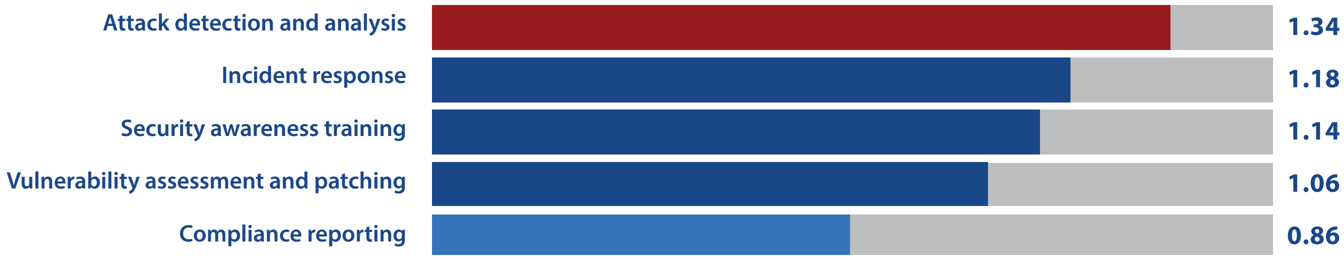

Figure 9: IT security operations areas where more skilled staffing would make the biggest difference.

We took a closer look at what areas of IT security operations would most benefit from additional skilled staffing (see Figure 9). Note that this doesn't necessarily correspond to personnel shortages; for example, an organization could significantly benefit from hiring a highly skilled person whether or not that role has a shortage. The graph shows the results as weighted averages on a scale of 0.0 to 3.0.

Not surprisingly, most organizations (93.1%) say they would benefit from an increase in skilled staffing. Attack detection and analysis is the area that would most benefit, with 63.4% of organizations including it in their top three. This is another instance where respondents made it clear that attack detection is an area of great concern for them.

Organizations chose the next three areas—incident response, security awareness training, and vulnerability assessment and patching—roughly as often as each other (57.3%, 56.8%, and 57.5%, respectively), but vulnerability assessment and patching was less likely to be given the #1 ranking (only 14.1% of the time compared to 19.2% for security awareness training and 21.0% for incident response).

The area chosen least often was compliance reporting. It was the only one selected by less than half of the organizations (44.2%). This correlates with other questions in the survey where organizations indicated relatively few challenges with compliance reporting.

Security Operations Software and Services in the Cloud

Approximately what percentage of your organization's IT security operations software and services are presently deployed in the cloud?

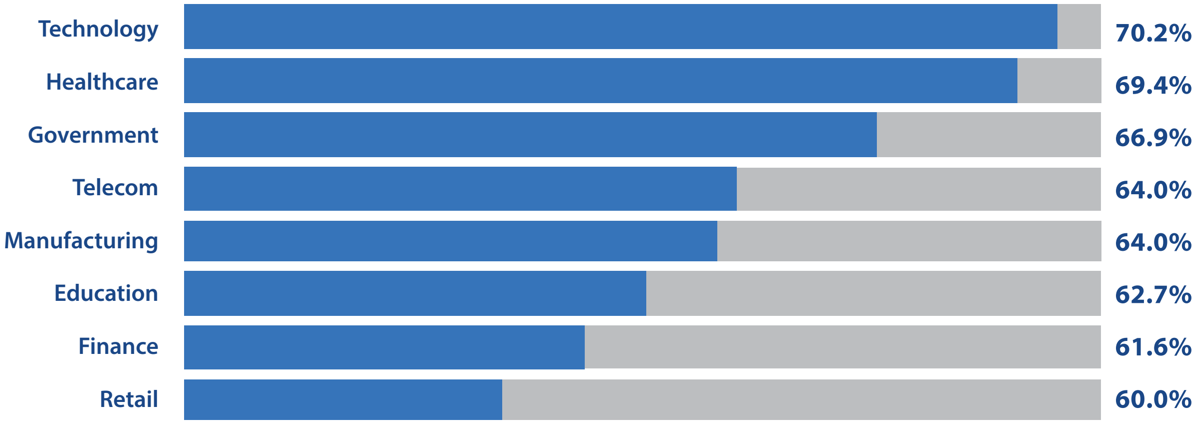

Figure 10: Percentage of IT security operations software and resources in the cloud, by industry.

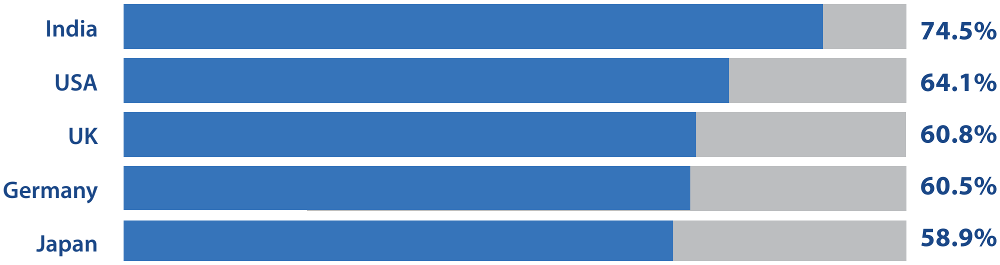

Figure 11: Percentage of IT security operations software and resources in the cloud, by country.

We all know that organizations have migrated many applications and services to the cloud, but what about their IT security operations software and services? We asked what percentage of organizations' IT security operations software and services are cloud implementations (see Figure 10). Nearly two-thirds of IT security operations software and services are deployed in the cloud (64.6%).

Of the surveyed countries (see Figure 11), India is making the most use of the cloud, with every surveyed organization having at least some cloud deployment, and with organizations on average having 74.5% of their IT security operations software and services in the cloud. Other countries ranged from having 58.9% to 64.1% of their software and services implemented in the cloud.

An overwhelming 96.3% of organizations have at least some IT security operations software and services deployed in the cloud. There's one sector that's much different from the others—government. 27.8% of government organizations have no IT security operations software and services deployed in the cloud. No other industry is close to that number, and for two industries, manufacturing and retail, every surveyed organization has some IT security operations implemented in the cloud.

Cyberthreat Concerns

On a scale of 1 to 5, with 5 being highest, rate your overall concern for each of the following types of cyberthreats targeting your organization.

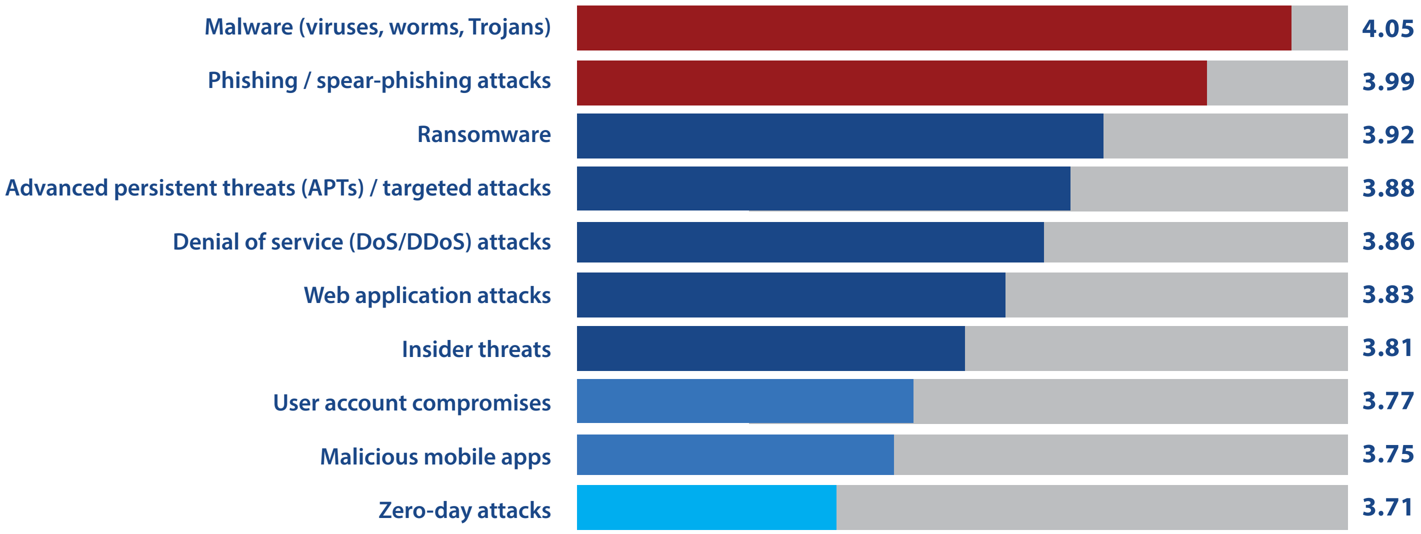

Figure 12: Concern that organizations have for types of cyberthreats.

We presented the survey participants with a list of 10 types of cyberthreats and asked them to rate their concern regarding each one on a five-point scale, with 1 being low and 5 high (see Figure 12).

The average score is 3.86, and the range of scores for all 10 cyberthreat types is narrow, with zero-day attacks the lowest at 3.71 and malware the highest at 4.05. This indicates that while there's some slight differences in which cyberthreats organizations are most concerned about, overall organizations are moderately concerned at a minimum about all types.

Organizations are most concerned about malware (4.05), phishing/spear-phishing attacks (3.99), and ransomware (3.91). None of those are surprising. Malware and phishing/spear-phishing have been major threats for many years. Ransomware has become far more prevalent in the last few years, with headlines and stories about organizations effectively shut down by ransomware.

At the other end of the scoring range, organizations are least concerned about zero-day attacks (3.71), malicious mobile apps (3.75), and user account compromises (3.77). However, "least" concerned still means concerned in this instance. Even the cyberthreat type least often rated as a high concern, user account compromise, is still a high concern for 25.2% of organizations.

COVID-19 Challenges

What have been the biggest challenges for your organization's security operations team during the COVID-19 pandemic? Select up to three.

	Global	USA	UK	India	Germany	Japan
Increased volume of cyberthreats / security incidents	45.3%	42.5%	41.2%	58.2%	37.0%	46.6%
Increased risks due to workforce usage of unmanaged devices	40.3%	39.9%	41.2%	40.5%	42.6%	37.9%
Increased challenge of investigating and/or remediating incidents	37.7%	36.6%	27.5%	50.6%	29.6%	39.7%
Insufficient access to on-premises IT security systems	35.7%	33.3%	37.3%	41.8%	31.5%	36.2%
Insufficient remote access / VPN capacity	28.4%	25.5%	31.4%	22.8%	33.3%	36.2%
Temporary hiring freeze / inability to fill open positions	24.8%	21.6%	35.3%	34.2%	27.8%	8.6%
Decreased budget for new security operations investments	24.8%	25.5%	21.6%	25.3%	25.9%	24.1%

Figure 13: Biggest challenges for security operations teams during the COVID-19 pandemic.

The COVID-19 pandemic has obviously affected organizations all over the world. In many places, lockdowns have prevented most or all employees from entering their typical workplaces. Once workplaces reopen, social distancing and other measures are used.

We asked survey participants to indicate what their security operation team's biggest challenges have been during the pandemic (see Figure 13). Each participant could select up to three challenges, and the average was 2.37, which indicates that many organizations are facing three of the challenges (and could be facing more than that).

The most common challenge has been the increased volume of cyberthreats/security incidents (45.3%). There have been many reports in the press and social media about malware, phishing, and other attacks specifically crafted to take advantage of the pandemic, so this result correlates that. The second most common challenge has been increased risks due to workforce usage of unmanaged devices (40.3%), which is also not unexpected, especially with some organizations switching to remote work with little or no warning.

The good news is that budget challenges and hiring challenges have both been relatively low (24.8% each) compared to the other categories. Also, only 28.4% of organizations cite insufficient remote access/VPN capacity as a challenge.

The industries with the most challenges per organization on average are technology (2.49), telecommunications (2.49), education (2.48), and manufacturing (2.47). Those with the fewest challenges are government (2.06), finance (2.23), retail (2.24), and healthcare (2.33).

Outsourcing IT Security Functions to MSSPs

Which of the following IT security functions does your organization outsource to a managed security service provider (MSSP)? Select all that apply.

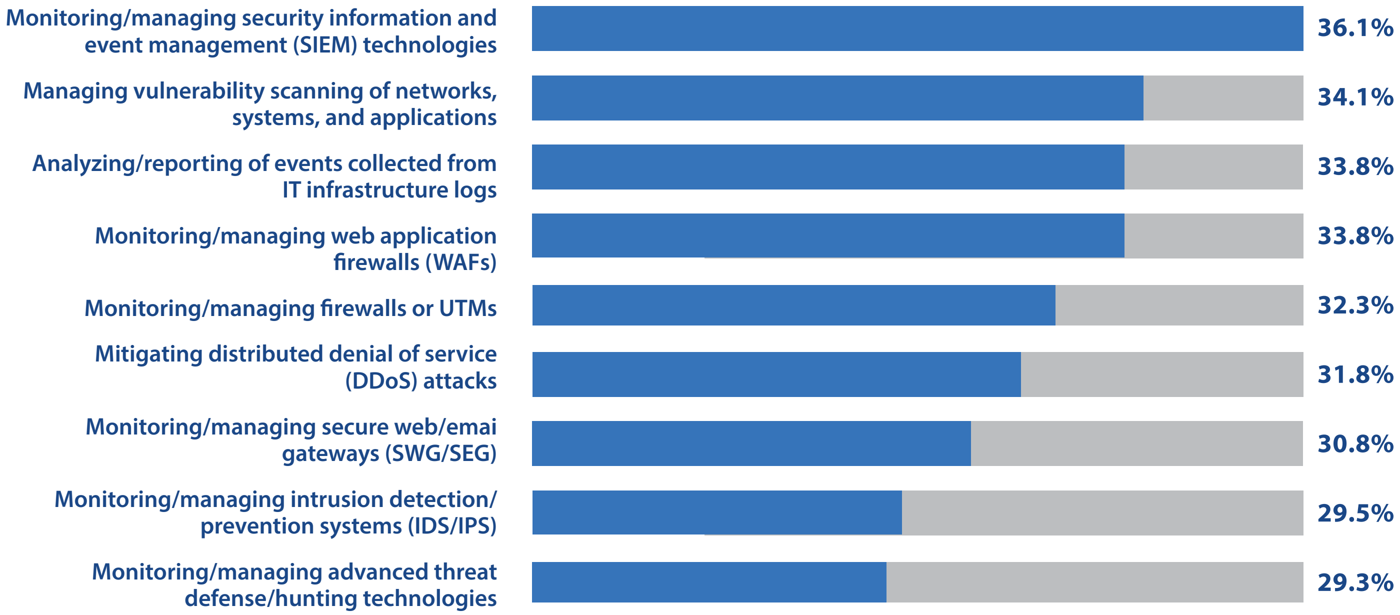

Figure 14: Percentage of organizations outsourcing each IT security function to an MSSP.

We asked survey participants if their organizations outsource several IT security functions to a managed security service provider (MSSP) (see Figure 14). Globally, 32.4% of these functions are currently outsourced, and there's not much variation in that among roles. The least-often outsourced of them is monitoring/managing advanced threat defense/ hunting technologies, which is outsourced 29.3% of the time. The most outsourced, monitoring/managing SIEM technologies, is outsourced only 36.1% of the time.

Globally, 87.6% of organizations outsource at least one IT security function to an MSSP. Organizations outsource three such functions to MSSPs on average. The extent of outsourcing varies by country, with India being the country most likely to outsource IT security functions (97.5% of organizations) and outsourcing the most functions per organizations on average (4.06).

Looking at the percentages of organizations in the surveyed industries that outsource (see Figure 15), organizations in government (62.5%) and finance (78.0%) are outsourcing less often than the others, and manufacturing is using MSSPs most often (98.4%). A possible reason for government and finance organizations having the lowest MSSP usage is that they are heavily regulated industries, so outsourcing may be more complex and cause considerable administrative overhead.

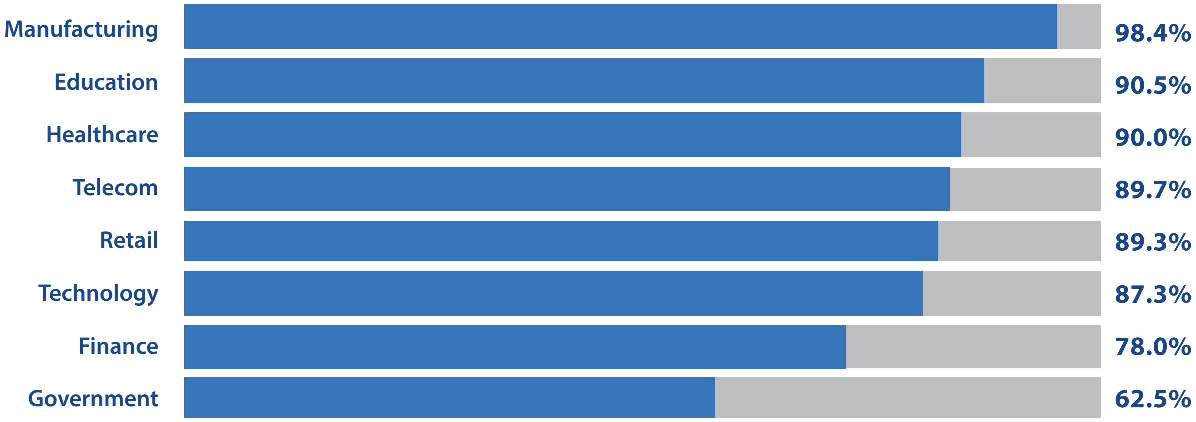

Figure 15: Percentage of organizations outsourcing an IT security function to an MSSP, by industry.

Conclusion

One thing is crystal clear from our survey: security operations, like the rest of the world in 2020, faces no shortage of challenges. Let's summarize some of the most significant ones:

- Handling the increased volume of cyberthreats and security incidents related to the COVID-19 pandemic
- Using and maintaining an increasingly large number of tools
- Having sufficient skilled personnel for all security operations roles
- Improving threat and attack detection and analysis capabilities
- Developing and implementing safeguards for critical services
- Investigating, validating, and prioritizing security incidents

But the news isn't all bad. Survey respondents also indicated several exciting new trends, including the following:

- Organizations are continuing to invest in security operations during the pandemic, including acquiring new tools to help automate processes.
- Organizations utilize the industry-standard MITRE ATT&CK Framework in their security operations.
- Most organizations use the cloud for the majority of their IT security operations software and resources.
- Most organizations outsource an average of three IT security functions to an MSSP.

So, what can we learn from these insights? To us, the main takeaway is the need for greater operational efficiency, especially since it seems the shortage of skilled security operations personnel won't be getting better any time soon. As a result, organizations should concentrate on reducing the burden on their teams by adopting solutions that enable them to intelligently adapt their resources to the areas where they're most needed.

Consider the following strategies for improving your organization's security operations and achieving greater cyber resilience.

Increase the use of automated tools.

Tools are a force multiplier. They can automate time-consuming, repetitive manual processes that people would otherwise have to do. Most organizations already have security configuration management (SCM), security information and event management (SIEM), and network traffic analysis (NTA) tools in use.

Security operations tools that your organization is most likely to want to acquire soon, if they aren't already in place, are the following:

- Security orchestration, automation, and response (SOAR)
- Threat hunting tools
- Vulnerability assessment/management (VA/VM)
- User and entity behavior analytics (UEBA)

Transfer security operations functions to cloud services and MSSPs.

Our results found that many more organizations are adopting MSSPs and cloud, although the reason for doing so wasn't explored. As such, we recommend that organizations look into the pros and cons of these options to determine if they would be beneficial. One benefit we see for migrating from data centers to the cloud is that it makes it easier for security operations teams to access security operations functions from anywhere. And that includes from their homes during the COVID-19 pandemic or other crisis. Using MSSPs could be especially helpful for organizations that can't afford their own around-the-clock staffing.

Organizations are currently most likely to outsource these IT security functions to MSSPs:

- Monitoring/managing SIEM technologies
- Managing vulnerability scanning of networks, systems, and applications
- Analyzing/reporting of events collected from IT infrastructure logs
- Monitoring/managing web application firewalls (WAFs)
- Monitoring/managing firewalls or UTMs

Shift personnel to critical areas like threat and attack detection and analysis.

If your organization can increase the use of automated security automation tools and outsource some security functions to MSSPs, that should free up some time for members of your security operations team. For most organizations, it seems this time will best be put to use in critical areas like threat detection and analysis. Tools can be invaluable to supporting these areas, but in most cases a person still needs to review the information from their tools to determine the best course of action.

Even with ML and AI technologies built into many tools, it’s clear that the lack of skilled personnel in critical areas is significantly hampering security operations, which in turn could expose organizations to threats that would keep them from achieving their missions. By shifting responsibilities, organizations can enable their security operations teams to more effectively reduce their risk while maximizing their efficiency.

Survey Demographics

This report is based on survey responses from 410 qualified participants from five countries (see Figure 16). Each respondent was required to have a role in some aspect of IT security operations (see Figure 17). Approximately two-thirds of them held management or executive positions.

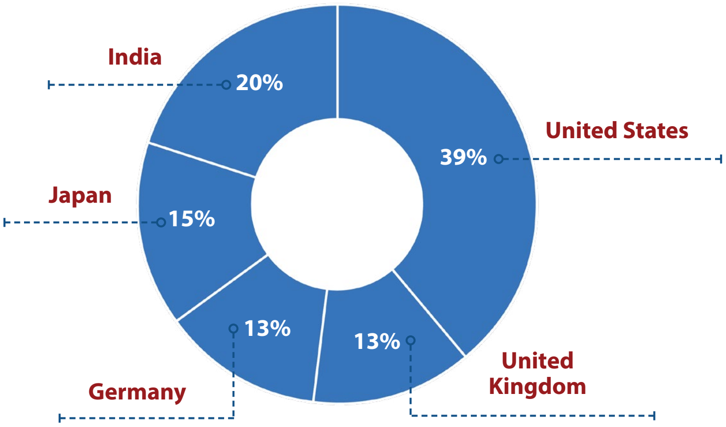

Figure 16: Survey respondents by country.

All participants in this survey were working for organizations with 500 or more employees (see Figure 18). They spanned 17 industries (plus "Other") with no single industry composing more than 16% of the total participants. For selected questions, additional analysis was conducted based on the industries with the largest number of respondents (see Figure 19). Those eight industries—technology, manufacturing, finance, telecommunications, retail, education, healthcare, and government—had almost three-fourths of all participants.

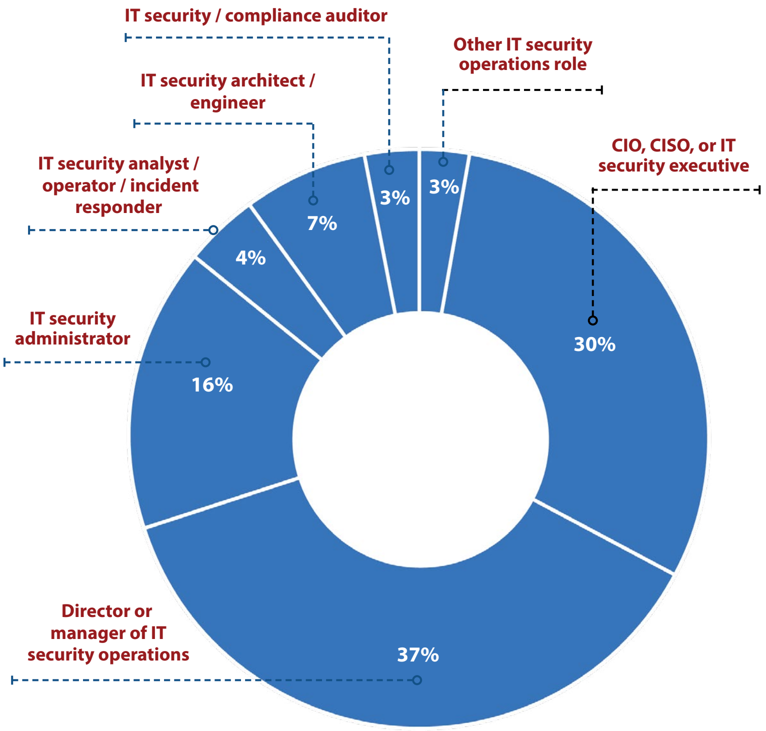

Figure 17: Survey respondents by IT security operations role.

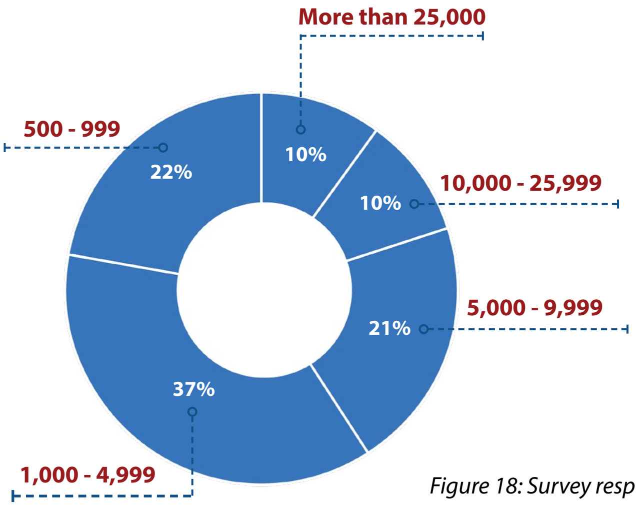

Figure 18: Survey respondents by organization employee count.

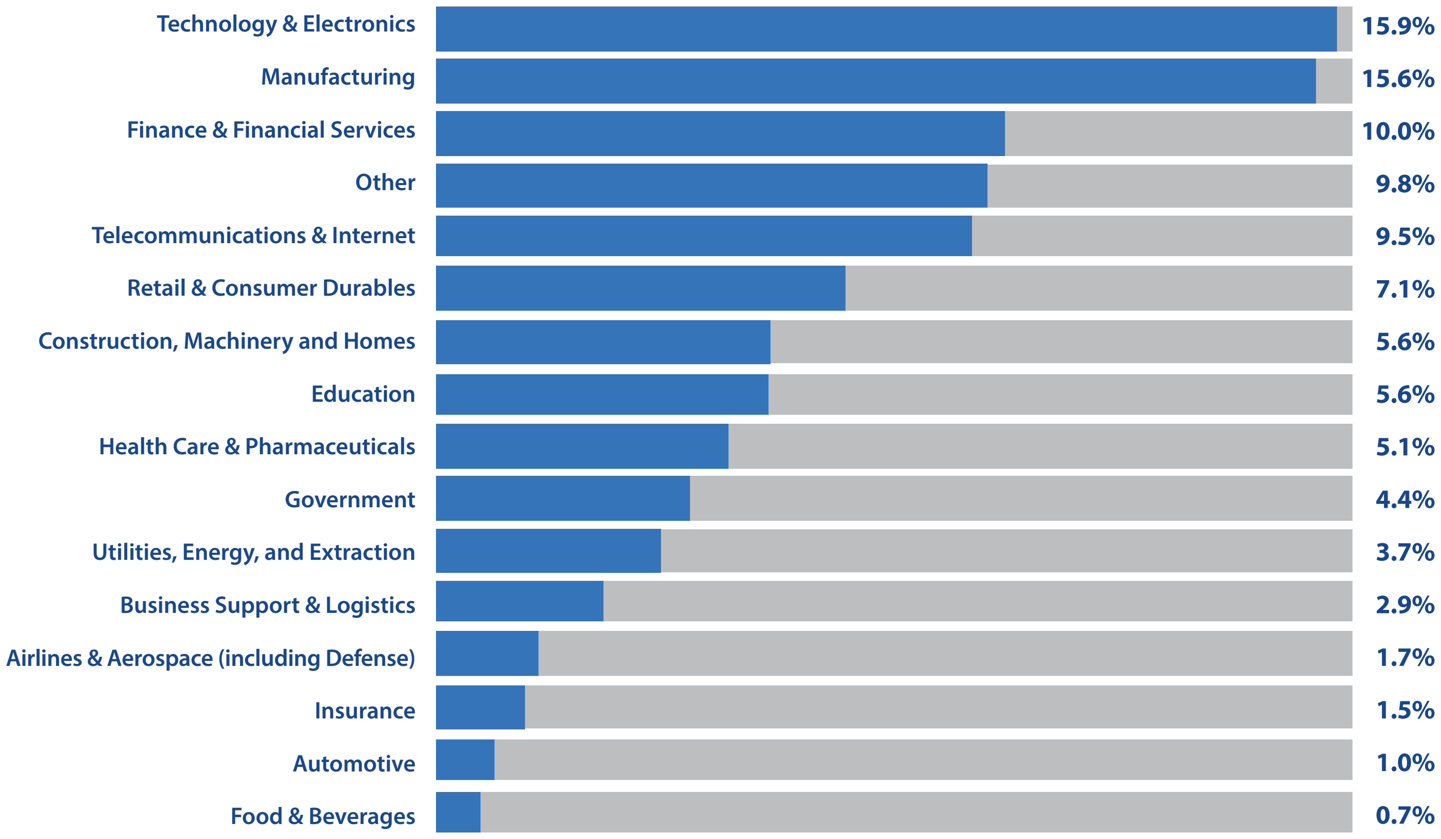

Figure 19: Survey respondents by industry.

Research Methodology

CyberEdge developed a 15-question web-based survey instrument in partnership with Micro Focus. The survey was promoted via email to 410 security operations professionals in the United States, United Kingdom, Germany, India, and Japan in August 2020. The global survey margin of error for this research study (at a standard 95% confidence level) is 5%. All results pertaining to individual countries and industries should be viewed as "anecdotal" as their sample sizes are much smaller. CyberEdge recommends making actionable decisions based on global data only.

All respondents must meet two filter criteria: (1) they must have a security operations role in their employer's IT department, and (2) they must be employed by a commercial or government organization with a minimum of 500 global employees.

At CyberEdge, survey dataquality is paramount. CyberEdge goes through extraordinary lengths to ensure its survey data is of the highest caliber by following these industry best practices:

- Ensuring that the "right" people are being surveyed by (politely) rejecting respondents that don't meet the respondent filter criteria of the survey (e.g., job role, job seniority, company size, industry)
- Ensuring that disqualified respondents (who do not meet respondent filter requirements) cannot restart the survey (from the same IP address) in an attempt to obtain the survey incentive
- Constructing survey questions in a way to eliminate survey bias and minimize the potential for survey fatigue
- Only accepting completed surveys after the respondent has provided answers to all of the survey questions
- Ensuring that survey respondents view the survey in their native language (e.g., English, German, French, Spanish, Japanese, Chinese)
- Randomizing survey responses when possible to prevent order bias
- Adding "Don't know" (or comparable) responses when possible so respondents aren't forced to guess at questions they don't know the answer to
- Eliminating responses from "speeders" who complete the survey in a fraction of the median completion time
- Eliminating responses from "cheaters" who apply consistent patterns to their responses (e.g., A,A,A,A and A,B,C,D,A,B,C,D)
- Ensuring the online survey is fully tested and easy-to-use on computers, tablets, and smartphones

CyberEdge would like to thank Micro Focus for making this survey report possible. We'd particularly like to thank Joe Leung, Preston Wheiler, Kevin Swan, and Fiona Ing for sharing their experience and security operations expertise with us.

About Our Sponsor

Micro Focus | www.microfocus.com
Micro Focus delivers enterprise software to empower our 40,000 customers worldwide to digitally transform. With a broad portfolio, underpinned by a robust analytics ecosystem, the company enables customers to address the four core pillars of digital transformation: Enterprise DevOps, Hybrid IT Management, Predictive Analytics, and Security, Risk & Governance. By design, these tools bridge the gap between existing and emerging technologies so customers can run and transform at the same time.

About CyberEdge Group

Founded in 2012, CyberEdge is the largest research, marketing, and publishing firm to serve the IT security vendor community. Today, approximately one in seven established IT security vendors (with $10 million or more in annual revenue) is a CyberEdge client.

CyberEdge's highly acclaimed Cyberthreat Defense Report (CDR) and other single- and multi-sponsor survey reports have garnered numerous awards and have been featured by both business and technology publications alike, including The Wall Street Journal, Forbes, Fortune, USA Today, NBC News, ABC News, SC Magazine, DarkReading, CISO Magazine, and others.

CyberEdge has cultivated its reputation for delivering the highest-quality survey reports, analyst reports, white papers, and custom books and eBooks in the IT security industry. To learn more about how we help our IT security vendor clients succeed, connect to our website at www.cyber-edge.com.

CYBEREDGE GROUP, LLC

1997 ANNAPOLIS EXCHANGE PKWY.
SUITE 300
ANNAPOLIS, MD 21401

☎ 800.327.8711

WWW.CYBER-EDGE.COM

✉ INFO@CYBER-EDGE.COM

Security with Smart Built In

A real-time approach to threat detection and response

Micro Focus believes that the best security posture comes from a strong human-machine team that leverages the strengths of each: faster-than-human analysis by machines to identify leads for investigation and the contextual understanding of SOC analysts and threat hunters.

Learn more ›

MICRO FOCUS