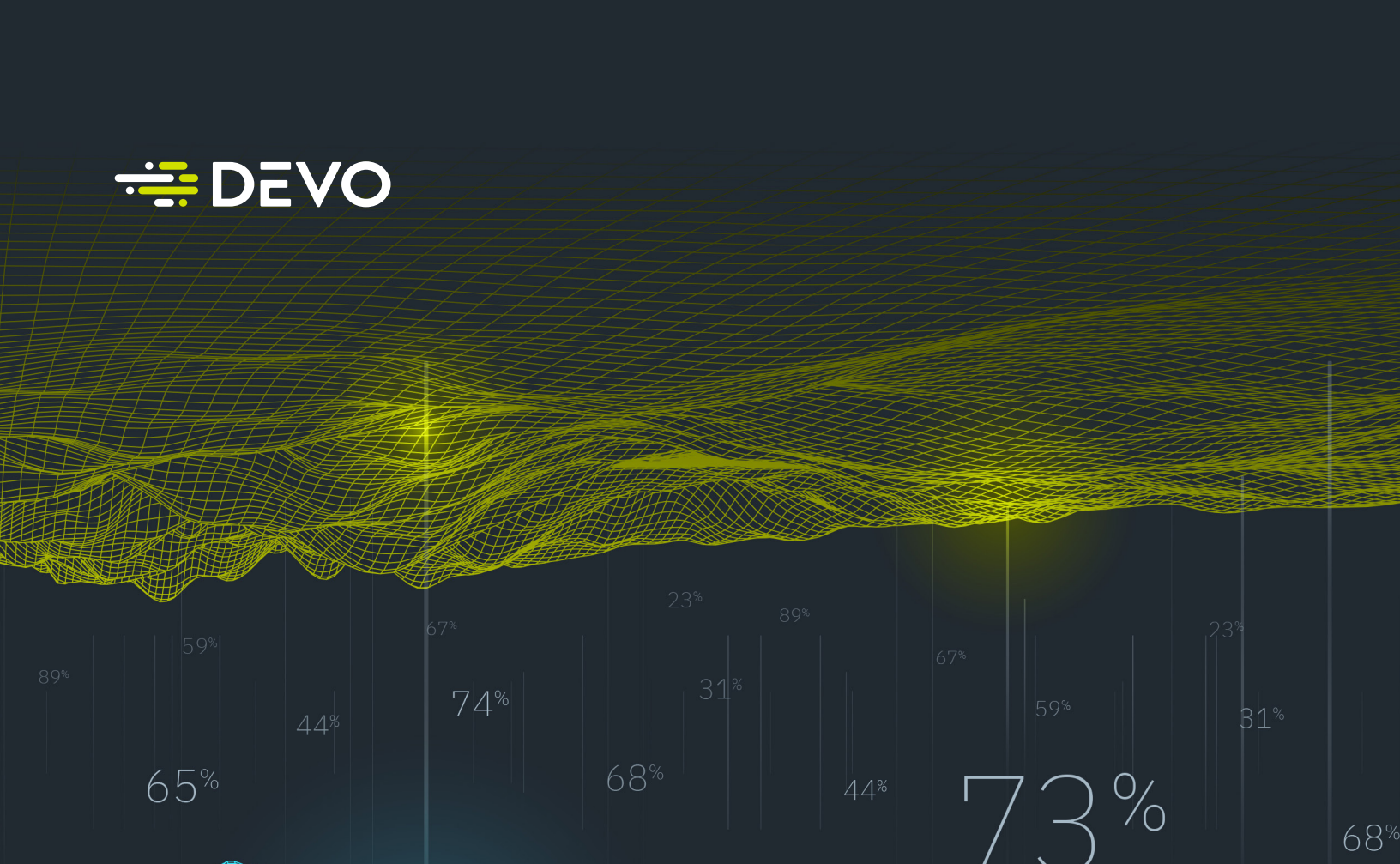


2020 Devo SOC Performance Report™

A Tale of Two SOCs

Survey independently conducted by Ponemon INSTITUTE

Table of Contents

What separates a highly effective SOC from a poor-performing SOC?

In the following study we examine exactly that.

Part 1.

INTRODUCTION

The *2020 Devo SOC Performance Report™* tells a tale of two SOCs. Based on the results of an independent survey of IT and IT security practitioners, the second annual report looks at the latest trends in security operations centers (SOC), both positive and negative. The report presents an unvarnished view of the current state of SOC performance and effectiveness based on responses from people with first-hand knowledge of SOC operations, identifies areas of change from the prior year's survey, and highlights the challenges that continue to hinder many SOCs from achieving their performance goals.

Devo commissioned Ponemon Institute to conduct a comprehensive, independent survey in March and April 2020 of professionals working in IT and security.

The survey posed a broad range of questions designed to elicit insights into several key aspects of SOC operations, including:

- The perceived value of SOCs to organizations
- Areas of effectiveness and ineffectiveness
- The ongoing challenge of SOC analyst burnout, its causes, and effects

The picture painted by the data from nearly 600 respondents shows that while some aspects of SOC performance show modest year-over-year improvement, major problems persist that continue to adversely affect organizational cybersecurity efforts and the well-being of SOC analysts.

A Tale of Two SOCs

Overall, the survey results tell a tale of two SOCs. One is a group of high-performing SOCs that are, for the most part, doing reasonably well in delivering business value. This group generally enjoys sufficient talent, tools, and technology to have a fighting chance of overcoming the relentless challenges that commonly afflict many SOCs.

Sharply contrasting with the high performers are the low-performing SOCs. This group struggles greatly because they are unable to overcome the myriad problems hindering their ability to deliver better performance. These SOCs generally lack the people, technology, and budget resources to conquer these challenges, resulting in them sinking even lower in effectiveness, putting their organizations at ever-greater risk of cyberattacks.

This report examines the specific areas where high- and low-performing SOCs most diverge, while also shining a light on the challenges with which both groups struggle. By identifying the differences and similarities between the two classes of SOCs, it illuminates the variable return on investment these SOCs are delivering to their organizations.

The Good(-ish) News

Before delving into the most significant—and in many cases, disturbing—findings from the survey, let's start by looking at how organizations rate the value their SOC provides. This year, 72% of respondents said the SOC is a key component of their cybersecurity strategy. That's up from 67% in 2019. This increase reflects more respondents feeling their SOC plays an important role in helping the organization understand the external threat landscape.

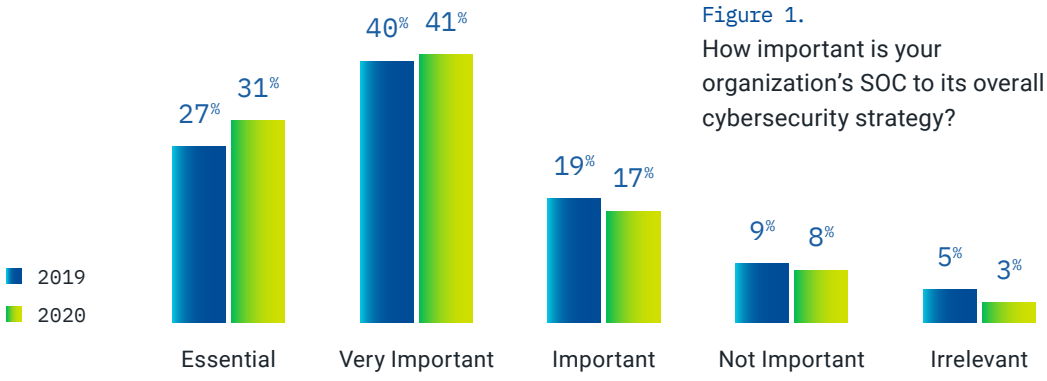


Figure 1.
How important is your organization's SOC to its overall cybersecurity strategy?

Other findings with a somewhat positive take on SOC performance include:

There is an eight-percentage-point increase among respondents who say their SOC is highly effective in gathering evidence, investigating, and identifying the source of threats. So far, so good. However, when you realize that last year only 42% of respondents felt that way, this year's "jump" to 50% means that half of those surveyed still don't believe their SOC is performing particularly well.

Respondents see improvements in their SOC's ability to mitigate risks. This is another example of good news/bad news. Last year only 40% of respondents felt their SOC was doing a good job reducing risks. In 2020, a still-modest 51% say their SOC is getting the job done in this area. That's a nice increase, but it still means that almost half of all respondents find their SOC lacking in this important capability.

Contributing to this rise, more SOCs (50%, up from 42% in 2019) are providing incident-response capabilities including attack mitigation and forensic services. The brightest spot in this aspect of SOC performance is that in 2020, 63% of respondents say SOCs are helpful in understanding the external threat environment by collecting and analyzing information on attackers and their tactics, techniques, and procedures (TTP), up from 56% last year.

There was a slight bump in the alignment between the SOC and the objectives and needs of the business. This year 55% of respondents say their SOCs are fully aligned (21%) or partially aligned (34%) with business needs, a slight increase from 51% in 2019. One possible reason for the improved alignment is that more lines of business are leading the SOC team (27% this year vs. 18% in 2019). But that practice also could be contributing to the rise in turf battles and silo issues. More on that later.

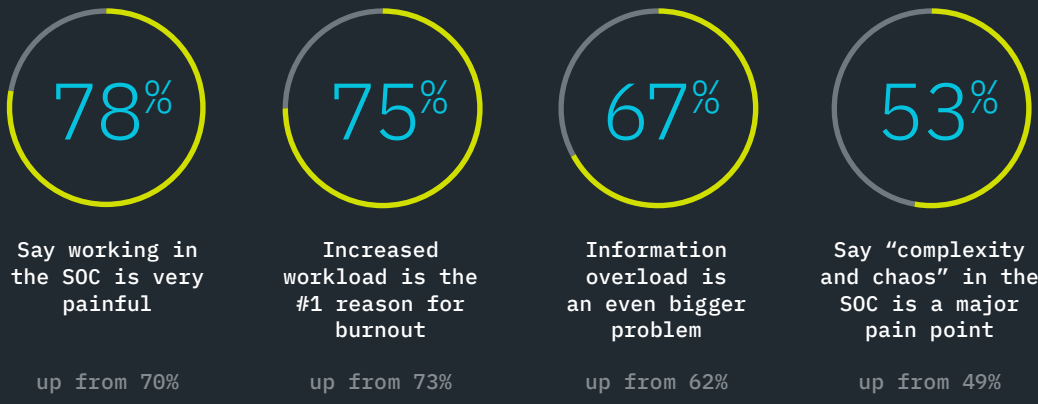
Organizations are investing in SOC technologies. Seventy percent of respondents say it is very likely (34%) or likely (36%) that their organization will open up their wallets to introduce new tools designed to improve SOC operations.

The SOC forecast is cloudy. A majority of organizations, 60%, now operate their SOC mostly (34%) or partly (26%) in the cloud. In 2019, only 53% of organizations identified as mostly cloud (29%) or operating a hybrid environment (24%). SOCs with limited cloud presence are declining, with only 40% of organizations identifying as mostly on-premises, down from 47% in 2019. This trend toward more cloud-based SOC operations reflects the overall move of IT and other business operations technologies taking advantage of the scale and cost benefits of cloud deployments.

The Really-Not-So-Good News

The first Devo SOC Performance Report in 2019 showed that the issue of analyst turnover due to stress-related burnout was significant.

Unfortunately, it's become an even bigger problem in 2020:



For all of these reasons, and many more as you'll see in the charts that follow, organizations must find ways to reduce the stress of working in the SOC—now.

Respondents are concerned that frustrated, stressed, and burnt-out analysts will vote with their feet and quit their jobs. An appalling 60% say the stress of working in the SOC has caused them to consider changing careers or leaving their jobs. Even worse, 69% of respondents say it is very likely or likely that experienced security analysts would quit the SOC, more discouraging than the 66% who felt that way last year.

Turf tussles and silo skirmishes are killing SOC effectiveness. This is another problem that's getting worse. This year, 64% of respondents say these internal battles over who is in charge of what are a huge obstacle to their SOC's success, a disheartening increase from 57% in 2019. Twenty-seven percent of respondents say lines of business are in charge of the SOC, an increase from 18% in 2019. However, 17% of respondents say no single function has clear authority and accountability for the SOC. And it's not a stretch to connect the dots and realize that an organization infected with in-fighting among its technology teams is likely to be more vulnerable to the potentially devastating effects of a successful cyberattack.

Budgets are not adequate to support a more effective SOC. SOC budgets increased slightly year over year, but not enough to close the gaps in effectiveness and performance. The average annual cybersecurity budget for the survey respondents' organizations rose to $31 million this year, a slight bump from $26 million. The average funding allocation for the SOC is 32% of the total cybersecurity budget or $9.9 million, a slight increase from 30% or $7.8 million in 2019. These figures are heading in the right direction, but they're still insufficient to fund the important work of an effective SOC team.

You can't stop what you can't see. SOC teams are handcuffed by limited visibility into the attack surface, which 69% of respondents cite as one of the primary causes of SOC analyst pain.

The mean time to resolution remains unacceptably high. MTTR is one of the benchmark metrics for SOC performance, and the responses to the survey show it is another significant problem area. According to 39% of respondents, MTTR can take months or even… years! Less than a quarter of respondents, 24%, say their SOC can resolve security incidents within hours or days. Compare these unsettling metrics with the industry estimate that it takes skilled hackers less than 19 minutes to move laterally after compromising the first machine in an organization. This points to a significant gap for the vast majority of SOCs, as only 8% have an estimated MTTR that is "within hours," which is even worse than the 9% of organizations in 2019.

Is it time for the rise of the machines? It's obvious from these survey results that the trend of SOC analyst stress, burnout, and turnover is getting worse. The question is what can organizations do to turn the tide? Well, if you listen to 71% of those surveyed, a big step in the right direction would be to introduce automation to the analyst workflow, and 63% state that implementing advanced analytics/machine learning would help. Respondents feel organizations should invest in technologies that would reduce analyst workloads. They believe automation and machine learning are even more important than a normalized work schedule in reducing SOC pain. The idea is to automate many of the repetitive, pressure-packed tasks typically performed by Tier-1 analysts who often have had enough of SOC work before they ever make it to Tier-2.

Spotlight on High-Performing SOCs

Thus far, we've focused on general trends, challenges, and significant problem areas affecting the performance of most SOCs. Now it's time to dig deeper into the specific differences in performance and effectiveness that distinguish high-performing SOCs from their even more-challenged brethren.

Let's start by answering the question:

What is a high-performing SOC? High-performing SOCs are those rated by survey respondents as a 7 or above on a 10-point scale in terms of SOC effectiveness.

High-performing SOCs are defined by their effectiveness, but even highly effective SOCs suffer from analyst pain and burnout. While these better-performing SOCs typically have the organizational support and resources to fuel a successfully operating SOC, there remain unaddressed pain points for the analysts in the trenches.

The most prominent attributes of high-performing SOCs include:

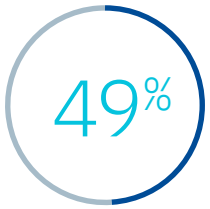
Not surprisingly, even highly effective SOCs have their work cut out for them when it comes to job-related stress afflicting analysts. When rating the pain of SOC security personnel in meeting their daily job requirements, 55% of respondents from high-performing SOCs still rated their pain as a 9 or 10 on a 10-point scale.

While high-performing SOCs, for the most part, deliver real business value, they continue to fight an ongoing battle in terms of attracting and retaining talent, preventing analyst burnout from overwork and stress, and navigating turf wars within their organization between IT and security. Among this group, organizations with larger budgets may be able to spend their way to solving some of these ongoing challenges. However, increasing spending as a means of overcoming persistent problems would deliver a less robust ROI.

The top three areas most in need of improvement, according to respondents from highly effective SOCs, are:

Lack of visibility into IT security infrastructure

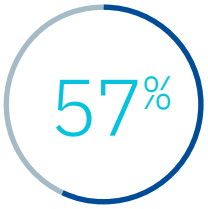
Turf or silo issues between IT operations and SOC teams



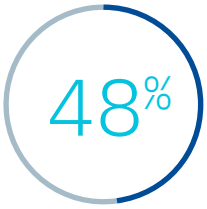
Compliance with privacy and data protection requirements

The most time-consuming tasks in high-performing SOCs include:

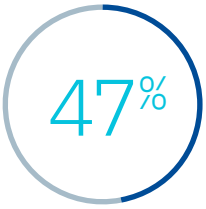
Managing threat intelligence



Malware protection and defense



Waiting on tools to respond to operations



Tool maintenance

Low Performers Feel the Pain

By contrast, low-performing SOCs suffer because they lack the talent, budget, technology, and other resources needed to successfully manage the barrage of cyberthreats faced by modern organizations. For example, better-resourced SOCs can deploy automation to help alleviate analyst burnout from the stress of performing repetitive, often mind-numbing work. This may be beyond the reach of asset-starved SOCs.

What are the most significant differences between high- and low-performing SOCs? When comparing responses, the areas of improvement for lower-performing SOCs are clear—acquisition and development of technology and talent are the best places to start to close some very large performance gaps.

THE PEOPLE GAP

Only 34% of highly effective SOCs identify the lack of available analyst talent as the main barrier to successfully operating the SOC. Whereas 72% of lower-performing SOCs identify the lack of available analyst talent as their main barrier.

THE PROCESS GAP

The most time-consuming task for less-effective SOCs, compared to SOCs that are highly effective, is data acquisition (33% vs 13%). Second is triaging alerts (39% vs 21%). These discrepancies are largely attributable to both technology and talent shortcomings, as well as processes that require additional resources if they are to improve.

THE TECHNOLOGY GAP

While 80% of high-performing SOCs are likely or very likely to add or change technologies to improve SOC operations and adapt to the always-evolving threat landscape, only 60% of lower-performing SOCs are likely to do the same. The greater willingness of high-performing SOCs to incorporate new or enhanced technology to improve their performance exemplifies an overall focus on making strategic investments and being more forward-thinking in their approach to technology.

Part 2.

KEY FINDINGS

In this section, we provide a deeper dive into the findings of the survey. The report also compares the 2019 survey to the 2020 results. The complete audited findings are presented in the Appendix of the report located on the Devo website at www.devo.com/wp-content/uploads/2020/06/The-2020-Devo-SPR-Appendix.pdf.

We have organized the research into the following topics:

- Progress in achieving a more effective SOC
- SOC analysts *still* feel the pain
- Lessons learned from highly effective SOCs
- Trends in infrastructure and security practices of today's SOC
- *Special section:*
  Why organization do not have a SOC

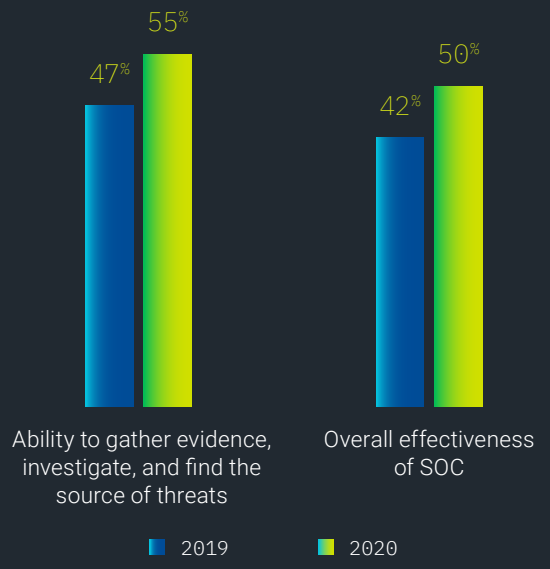
PROGRESS IN ACHIEVING A MORE EFFECTIVE SOC

Only 50% rate their SOCs as effective, although SOC effectiveness is improving, including the ability to gather evidence, investigate, and find the source of threats. Respondents were asked to rate the effectiveness of their organizations' SOC on a scale from 1 = not effective to 10 = highly effective. Only 50% of respondents (an increase from 42% in 2019) say their SOC is highly effective (responses of 7+). Fifty-five percent rate their SOC's ability to gather evidence, investigate, and find the source of threats as very high, a significant increase from 47% of respondents in 2019.

Figure 2.

How effective is your SOC and its ability to gather evidence, investigate, and find the source of threats?

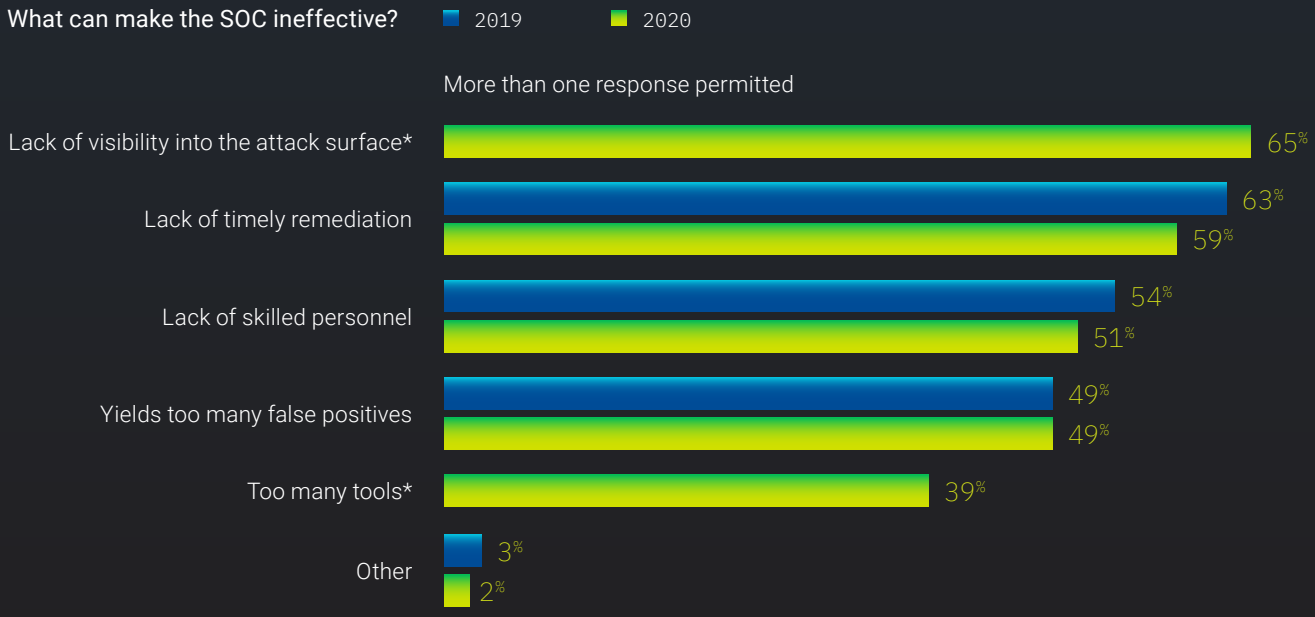
7+ responses on a scale of 1=not effective to 10=highly effective



Twenty-two percent of respondents rate their SOC as ineffective (responses of 1 to 4 on the 10-point scale). The primary reasons cited by these respondents are the lack of visibility into the attack surface, and lack of timely remediation (66% and 59% of respondents, respectively).

Figure 3.

What can make the SOC ineffective?



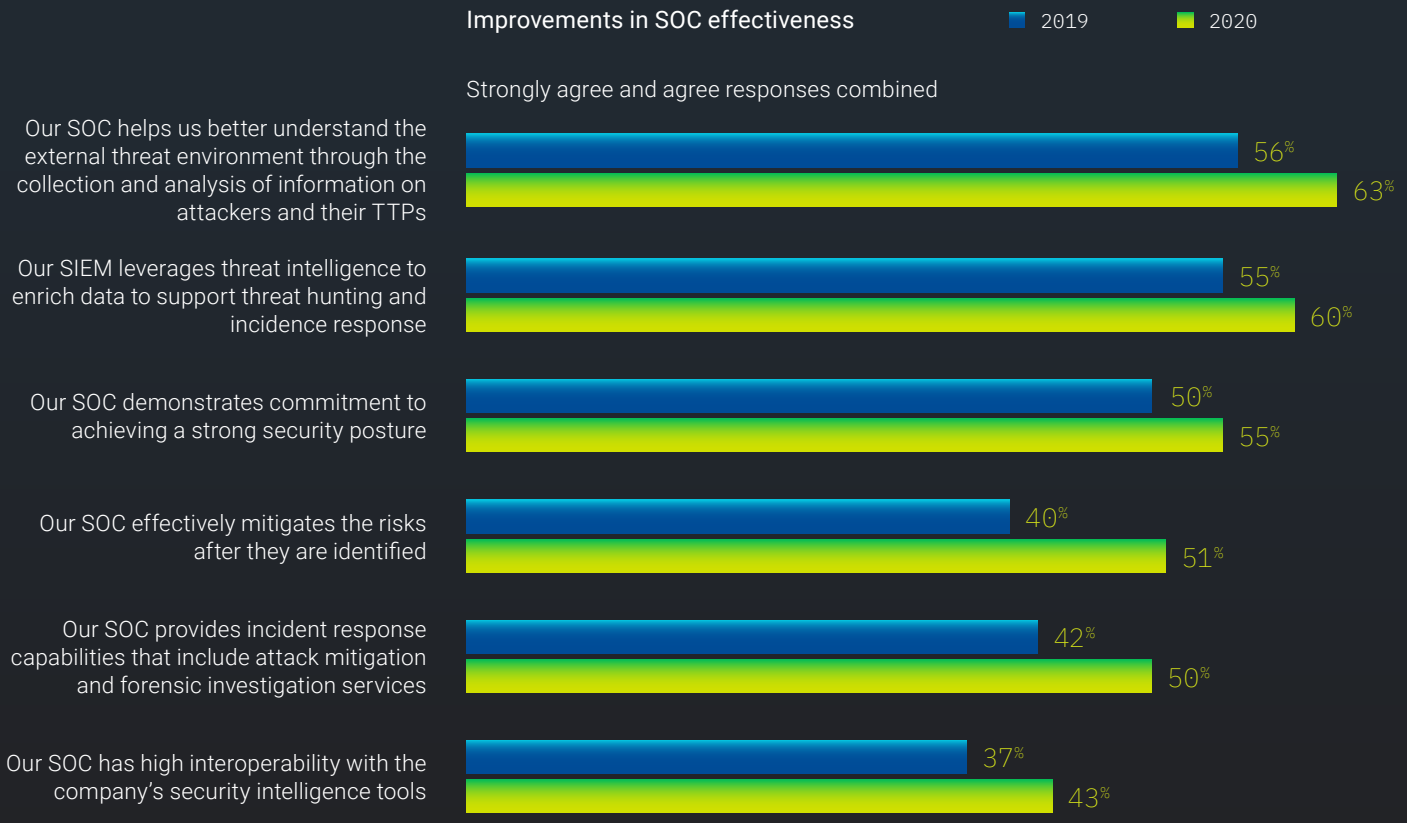
*New response option in 2020 survey

SOCs still have difficulty mitigating risks.

Despite improvements, challenges remain with the SOC's ability to mitigate risks. Figure 4 shows the most significant improvement since 2019 is the ability of the SOC to effectively mitigate risks after they are identified, an increase from 40% to 51% of respondents.

More SOCs provide incident response capabilities that include attack mitigation and forensic services, an increase from 42% of respondents in 2019 to 50% in 2020. And more respondents say SOCs are helpful in understanding the external threat environment through the collection and analysis of information on attackers and their tactics, techniques, and procedures (TTP), an increase from 56% to 63% of respondents.

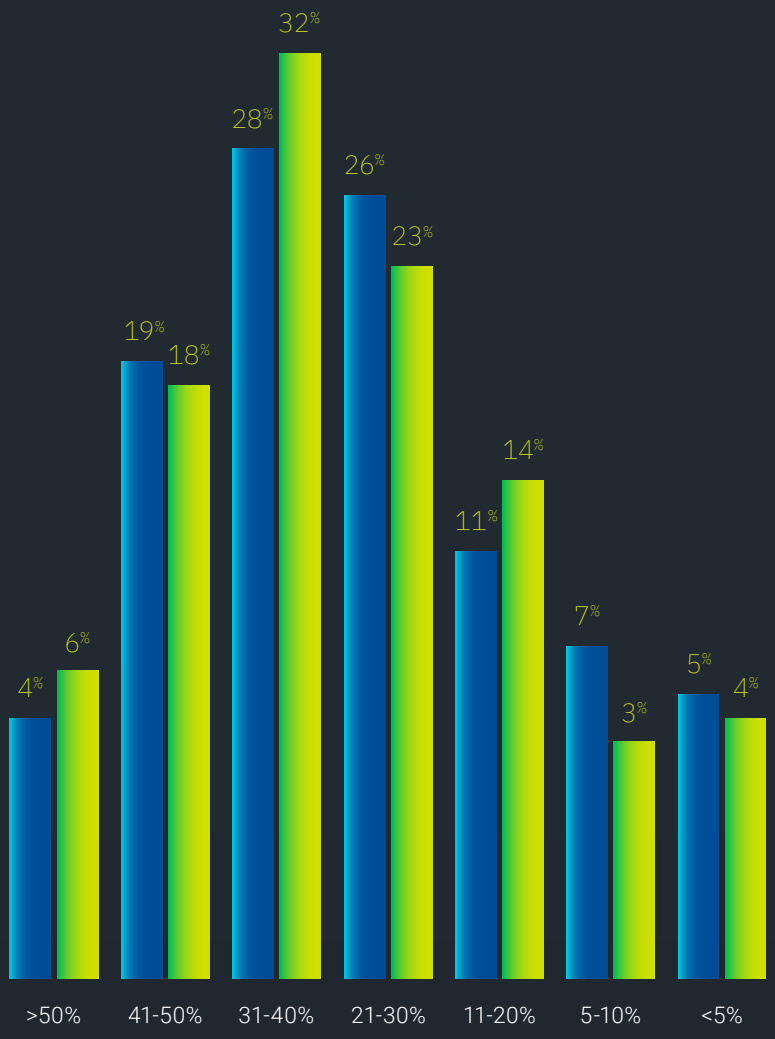
Figure 4.
Improvements in SOC effectiveness



The SOC budget increases, but only slightly.

The average annual cybersecurity budget for organizations represented in this study is $31 million, a slight increase from $26 million. As shown in Figure 5, the average funding allocation for the SOC is 32 percent of the total cybersecurity budget or $7.8 million, a slight increase from 30 percent or $9.9 million in 2019.

Figure 5.
What percentage of your cybersecurity budget will fund the SOC this year?

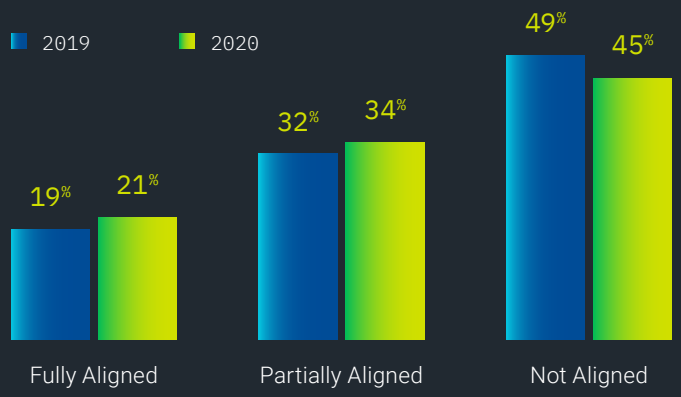


Extrapolated value = 32% (2020) 30% (2019)

Aligning SOCs with business proves challenging.

Only 55% of respondents say their SOCs are fully or partially aligned with their business, although there is slightly improved alignment from 2019 to 2020. In this year's research, only 21% of respondents say their SOCs are fully aligned and 34% are partially aligned, a slight increase from the combined 51% in 2019.

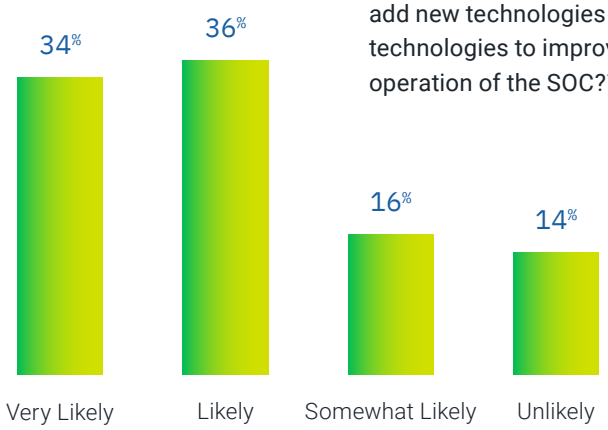
Figure 6.
Within your organization, are SOC objectives aligned with business needs?



SOCs are investing in new technology.

Seventy percent of respondents say it is very likely (34%) or likely (36%) they would add new technologies or change technologies to improve SOC operations.

Figure 7.
How likely is your organization to add new technologies or change technologies to improve the operation of the SOC?*

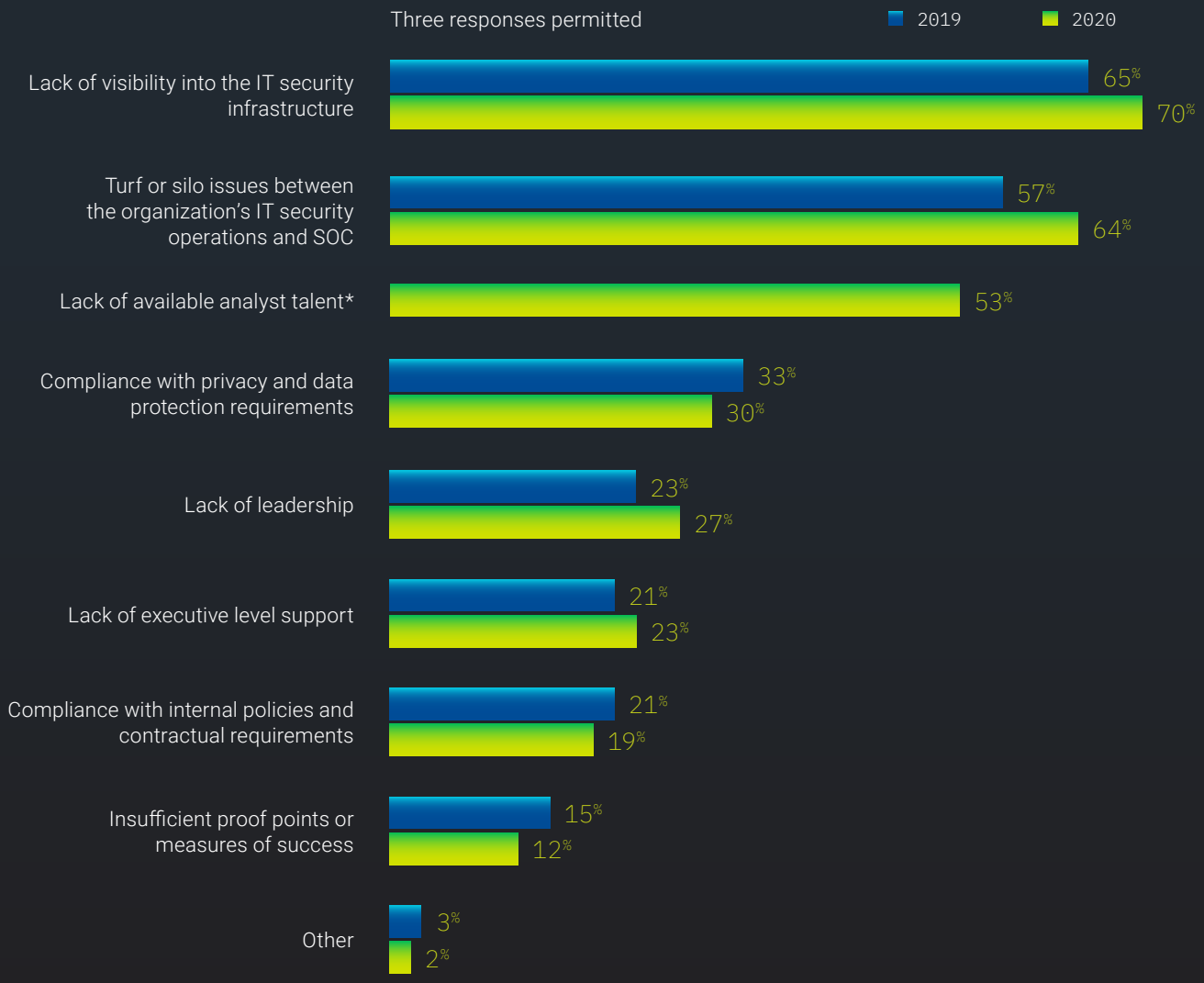


*New question in 2020 survey

Lack of visibility along with turf issues continue to be the biggest barriers to SOC effectiveness—and they are getting worse.

The main barrier to an effective SOC is a lack of visibility into the IT security infrastructure, according to 70% of respondents, increasing from 65% in 2019. Turf issues between IT and security operations also saw an increase from 2019, jumping to 64% from 57%. Fifty-three percent say the lack of analyst talent is a primary barrier to success.

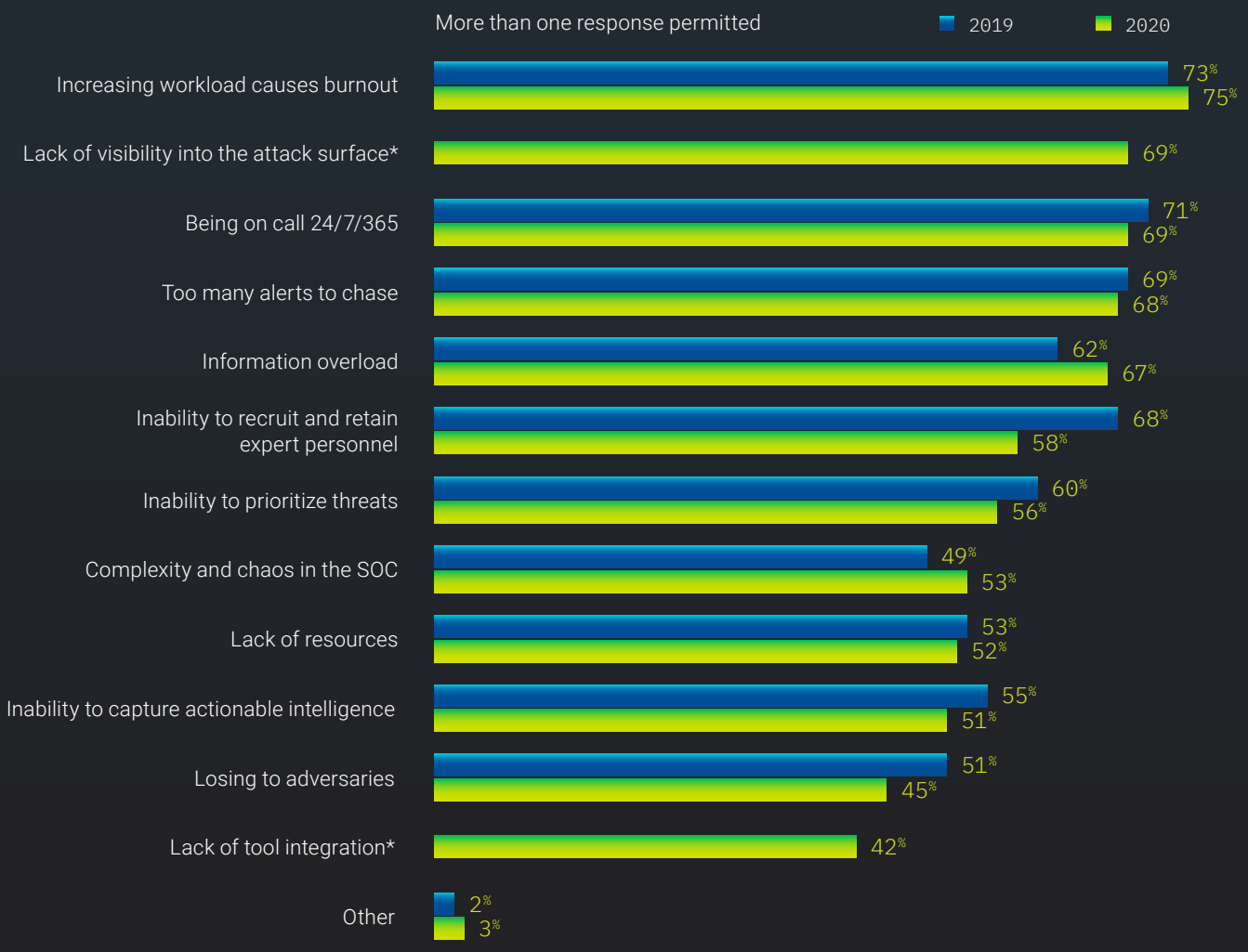
Figure 8.
What do you see as the main barriers to successfully operating the SOC?



SOC ANALYSTS *STILL* FEEL THE PAIN

Results shows that the pain of working in a SOC has increased. Respondents were asked to rate the "pain" of the SOC personnel's experience in meeting their daily job requirements from a scale of 1 = no pain to 10 = very painful. Seventy-eight percent of respondents say working in the SOC is very painful, an increase from 70% in last year's research. The number-one reason cited is burnout caused by increasing workload, followed by a lack of visibility into the attack surface. They also mention being on call 24/7/365 and having too many alerts to chase.

Figure 9.
What makes working in the SOC painful?

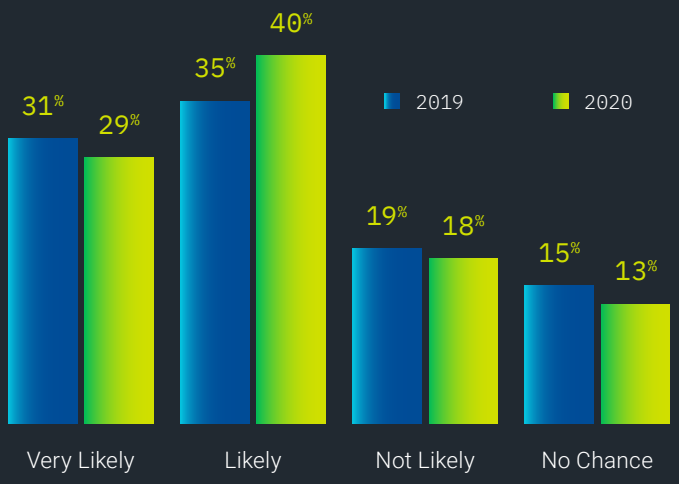


*New response option in 2020 survey

More than two-thirds of those surveyed believe experienced security analysts will quit.

Sixty-nine percent of respondents say it is very likely or likely that experienced security analysts would quit the SOC, up from 66% last year. Sixty percent of respondents say the stress of working in the SOC would cause experienced analysts to consider changing careers or leaving their jobs.

Figure 10.
What is the likelihood that the above pain factors would cause experienced security analysts to quit the SOC?

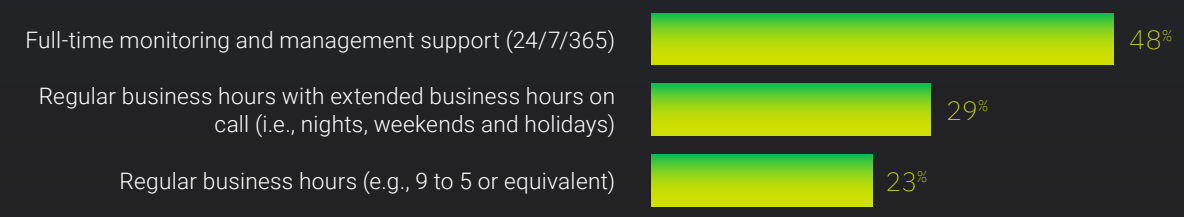


Most SOCs operate 24/7.

Being on call all day, every day is a main reason why working in the SOC is painful and almost half of respondents say their SOCs conduct full-time monitoring and management support. Just 23% of respondents say their organizations operate only during regular business hours.

Forty-three percent of respondents say their organizations have Tier-1 analysts followed by 40% of respondents who say their organizations have generalists who cover any part of the lifecycle. Only 20% of respondents say they have Tier-3 and 17% of respondents say they have Tier-2 analysts. These results indicate that many SOCs rely on less-experienced, less-skilled analysts, to protect their organization from cyberattacks, as well requiring them to cover a wide spectrum of responsibilities without the specialized skills that would make them more effective.

Figure 11.
What best describes the coverage model of your organization's SOC? *



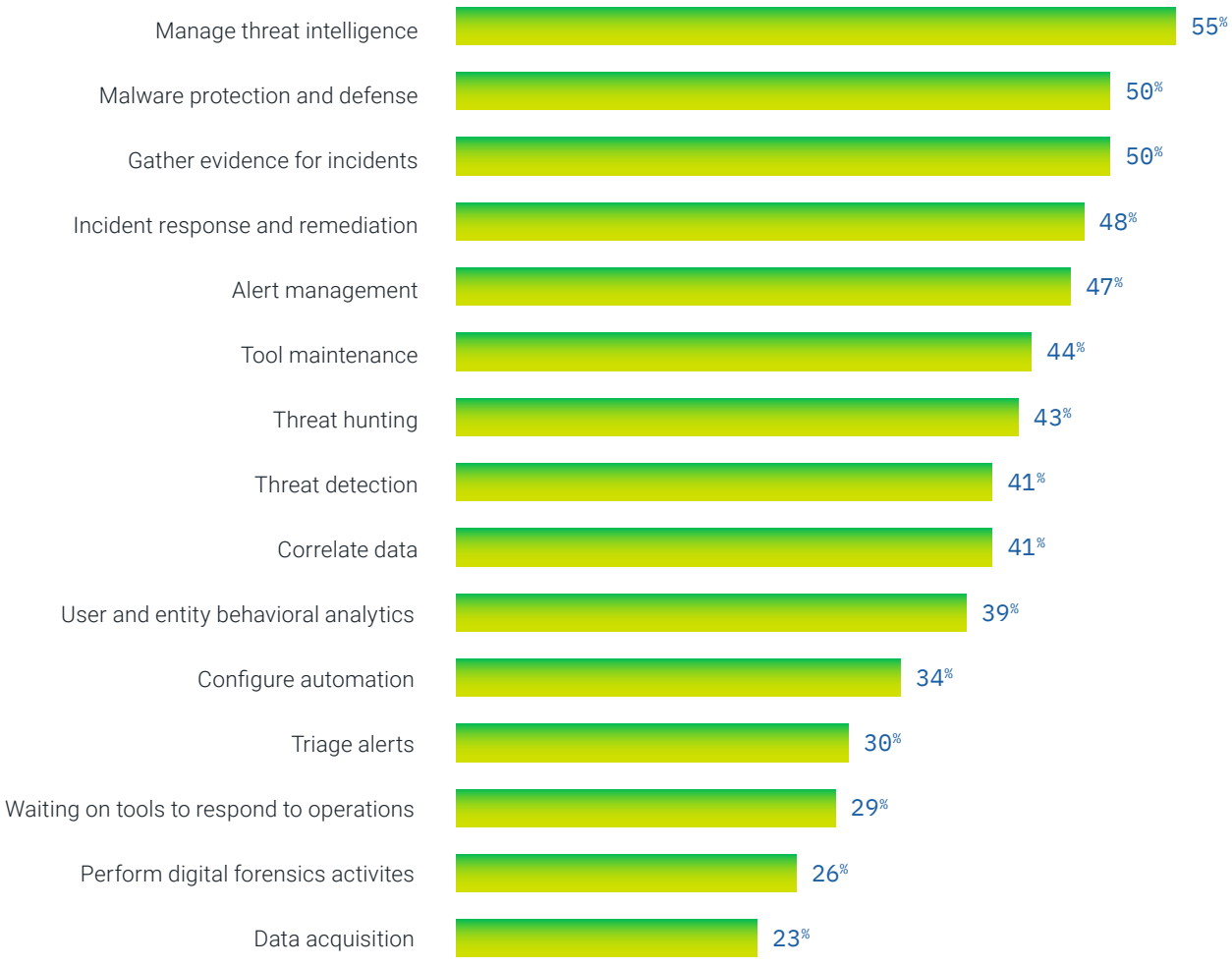
*New question in 2020 survey

Organizations should consider investing in technologies that would reduce analysts' workloads.

Figure 12 presents 15 tasks analysts regularly perform, with the most time-consuming tasks identified as managing threat intelligence, protecting and defending against malware, and gathering evidence for incidents. By targeting these tasks with technology efficiencies, organizations will reduce analysts' workload and pain, which would potentially improve talent retention.

Figure 12.
What are the most time-consuming tasks for your organization's security analysts?*

Six responses permitted

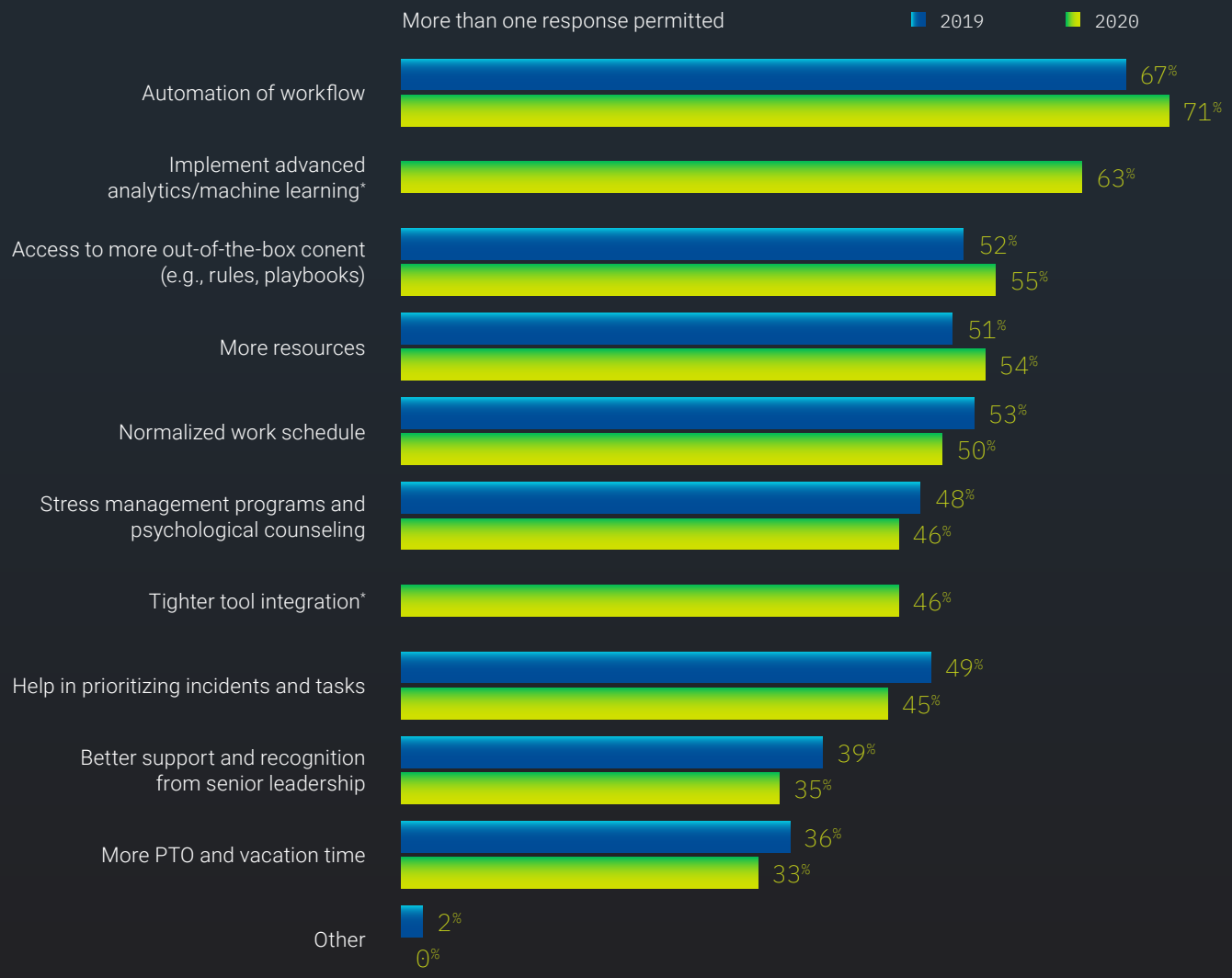


*New question in 2020 survey

Automation and machine learning are more important than a normalized work schedule in reducing SOC pain.

To help manage analysts' workload and avoid burnout, organizations should consider investments in automation and advanced analytics/ machine learning.

Figure 13.
What is the likelihood that the above pain factors would cause experienced security analysts to quit the SOC?

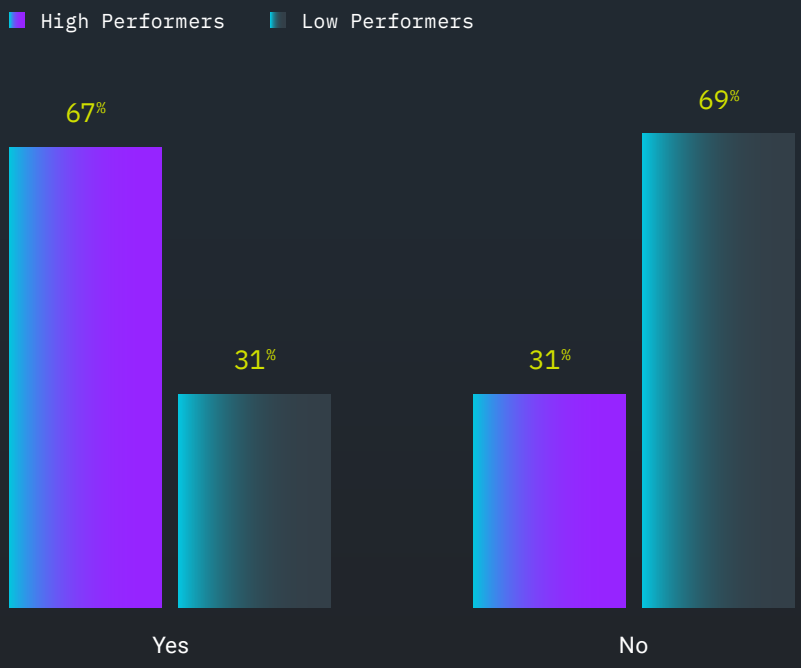


*New response option in 2020 survey

Programs to train and retain analysts are critical to easing their pain, reducing turnover, and improving overall SOC effectiveness.

Seventy-six percent of all respondents say a defined program to train and retain analysts is very important. But only 47% of respondents say they have a defined training program. Among high- and low-performing organizations, the differences are even more stark. Aligning with the clear need to reduce analyst pain, implementing these types of programs is one way to help solve the analyst-pain issue.

Figure 14.
Do you have a defined program to train/retain analysts?*



*New question in 2020 survey

LESSONS LEARNED FROM HIGHLY EFFECTIVE SOCs

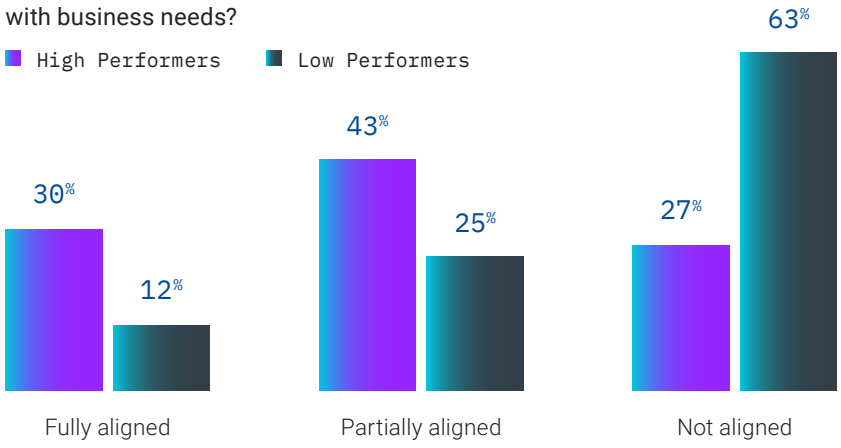
We identified certain organizations represented in this study that self-reported as having achieved a highly effective SOC. These organizations are better able to mitigate risks, vulnerabilities, and attacks.

Of the 585 organizations represented in this survey, 290 respondents (50% of the total sample) self-reported a rating of 7+ on a scale of 1 to 10 that their SOC is highly effective. Eighty percent of respondents from these organizations, referred to as high performers, say the SOC is essential or very important to their overall cybersecurity posture. In contrast, only 64% of the lower performers say the SOC is essential or very important.

High-performing SOCs are more likely to be aligned with their organization's business needs.

Seventy-three percent of high-performer respondents say their SOC is either fully or partially aligned with business needs. In contrast, 63% of respondents in the low-performer group say their SOC is not aligned with business needs.

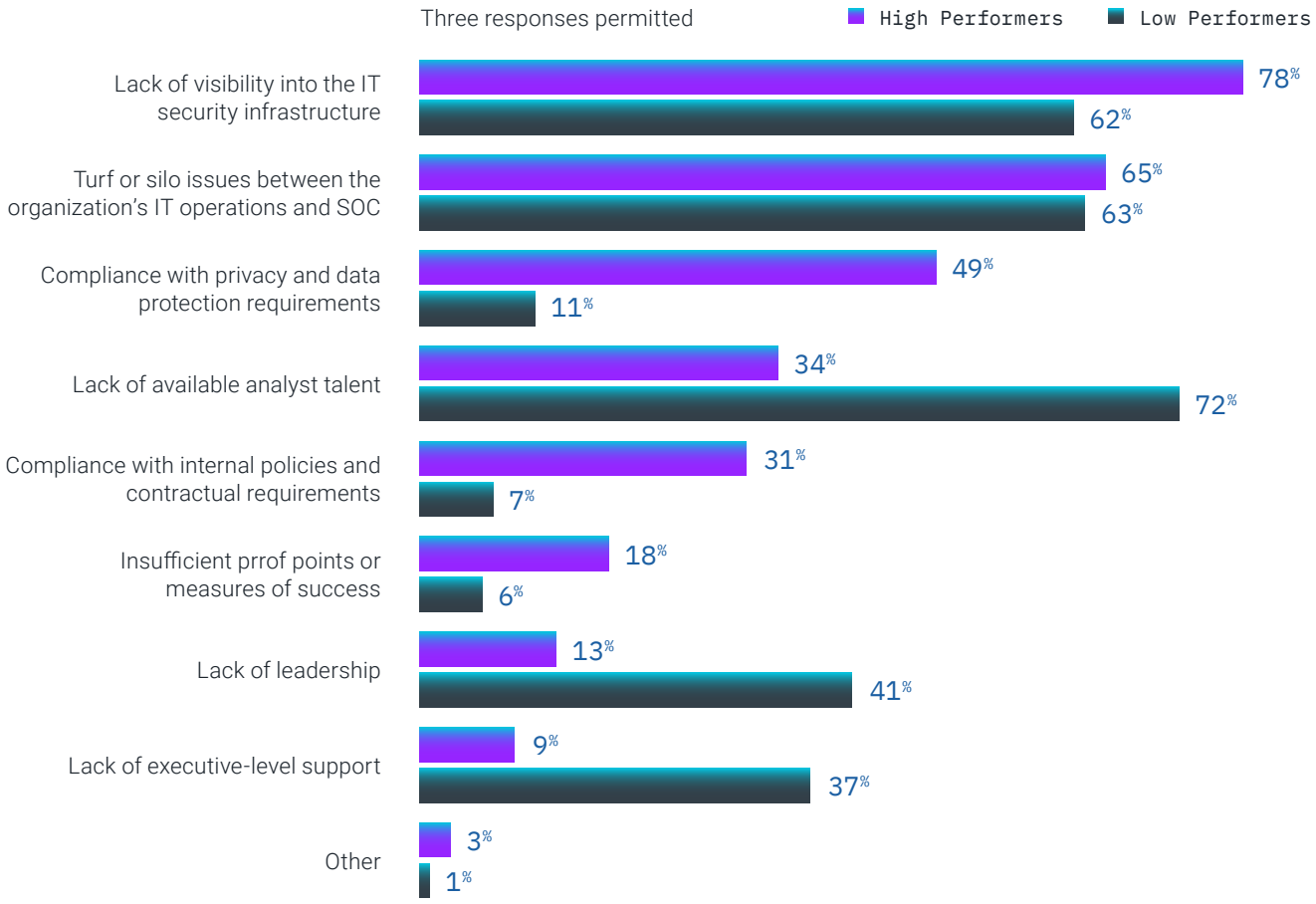
Figure 15.
Within your organization, are SOC objectives aligned with business needs?



High performers are more likely to have analysts with expertise.

Yet, 34% of high performers still cite the lack of available analyst talent as a main barrier to successfully operating the SOC. In the low-performer sample, 72% of respondents say the number-one barrier is a shortage of analyst talent. For both the high- and low-performing groups, lack of visibility into the IT security infrastructure as well as turf and silo issues are significant barriers to success.

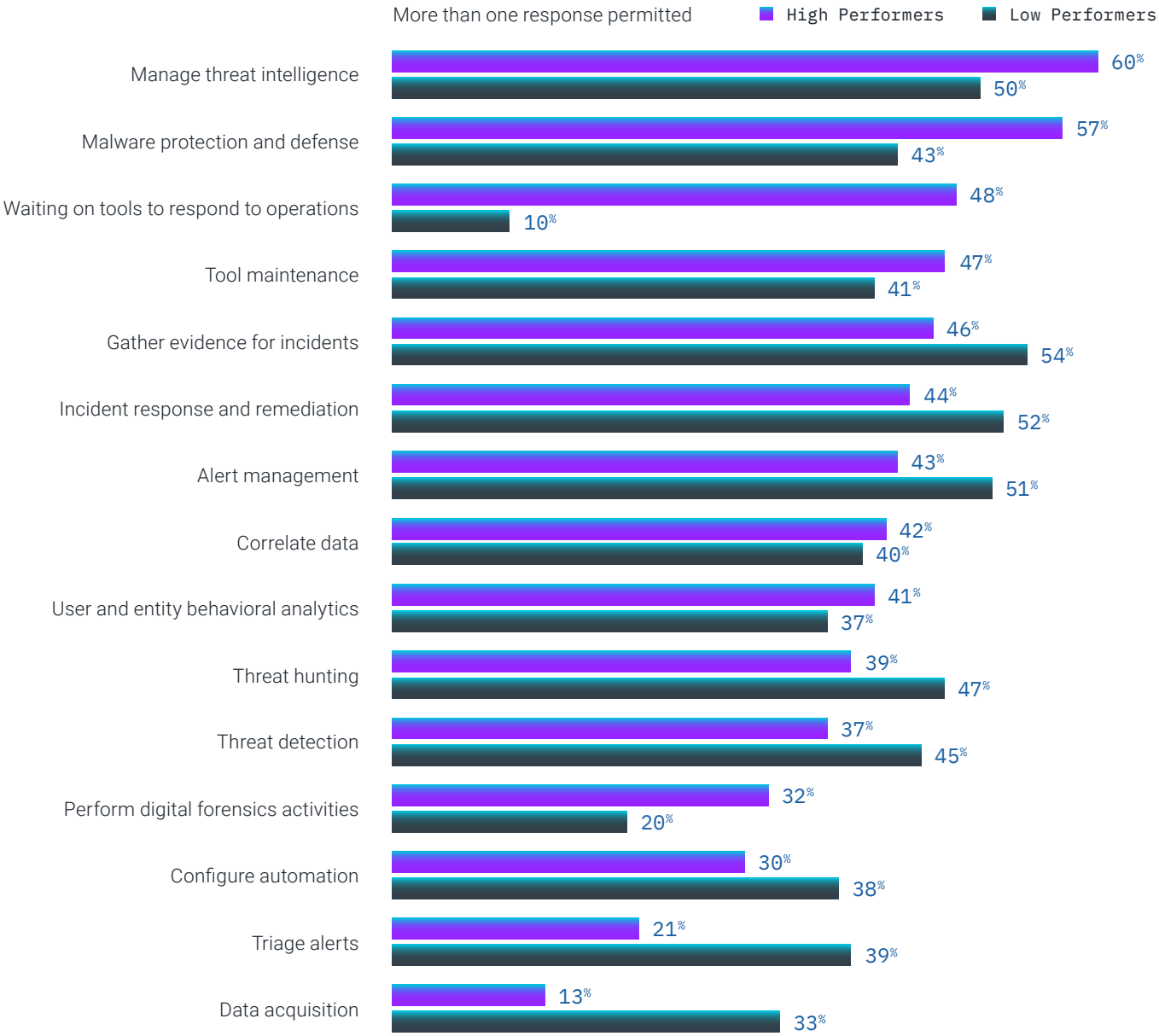
Figure 16.
What are the main barriers to successfully operating the SOC?



High performers say the most time-consuming tasks for security analysts are management of threat intelligence and malware protection and defense.

Respondents in the low-performing sample say the most time-consuming tasks are gathering evidence for incidents, incident response and remediation, and alert management.

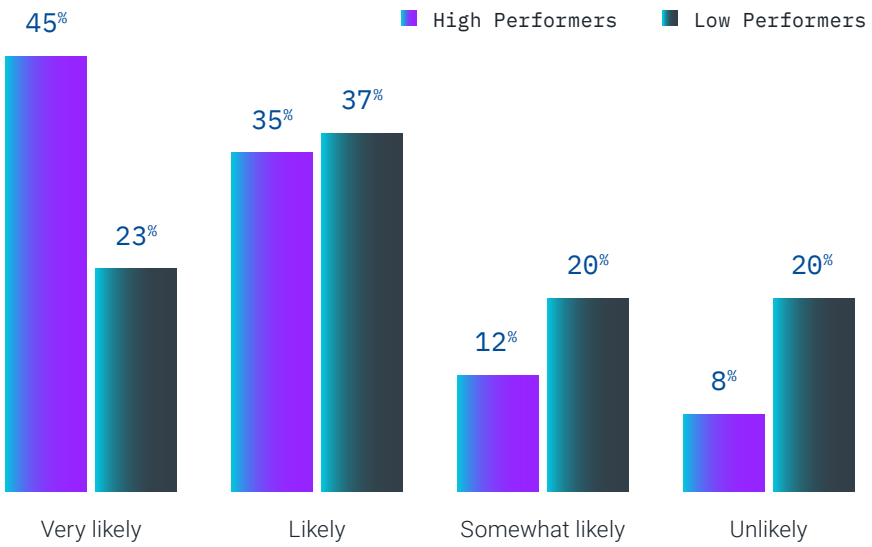
Figure 17.
What are the most time-consuming tasks for your organization's security analysts?



High performers are more likely to add or change technologies to improve SOC operation.

Eighty percent of respondents in high-performing organizations say it is very likely or likely their organization will invest in technologies. Just 60% of respondents in the low-performing group say their organizations are adding or changing technologies.

Figure 18.
How likely is your organization to add new technologies or change technologies to improve the operation of the SOC?



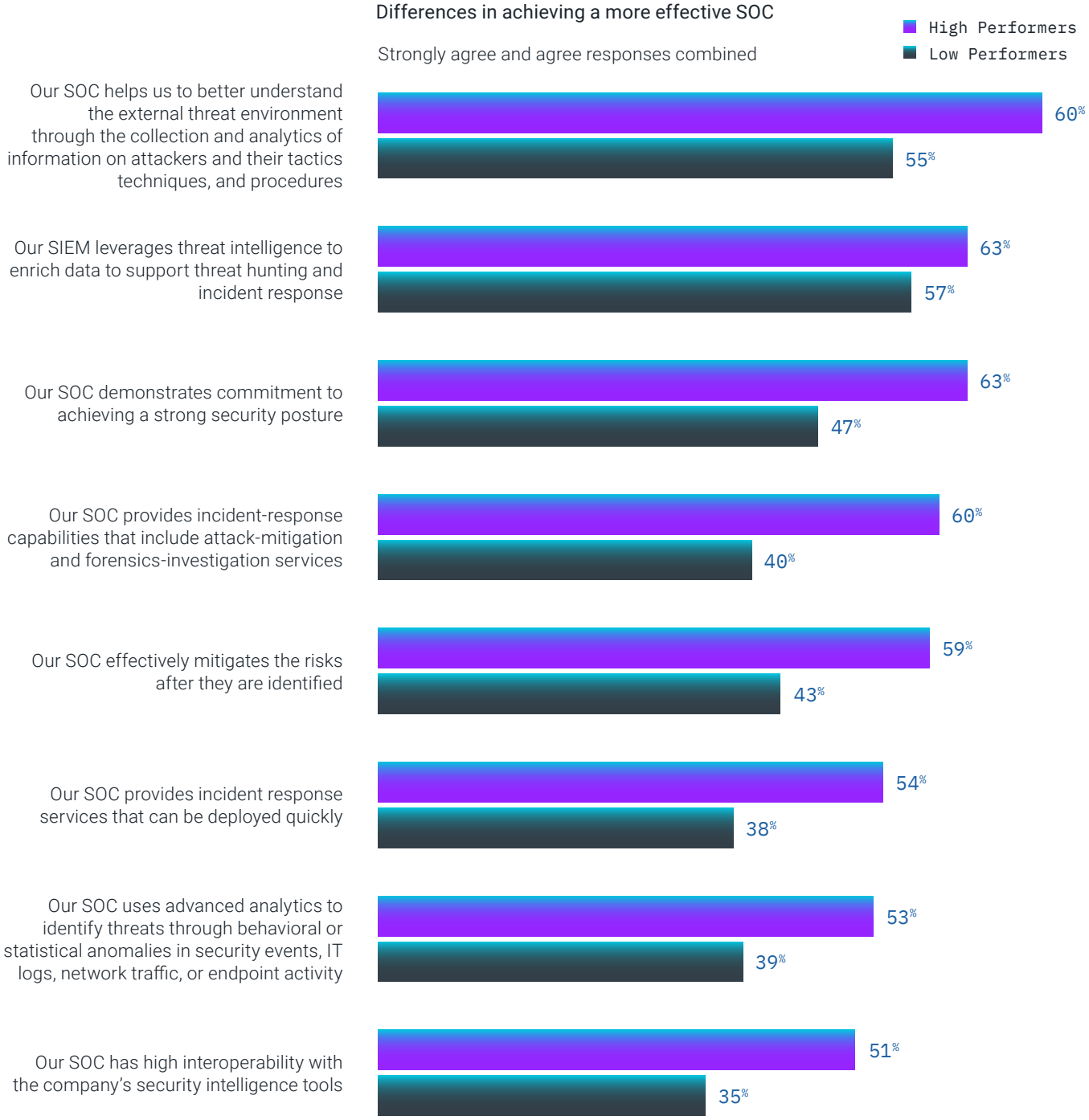
Why do some organizations have high-performing SOCs?

Specifically, high performers are more likely to have incident response capabilities that include attack mitigation and forensic investigation services (60% of high performers vs. 40% of low performers). The SOC helps in understanding the external threat environment (71% of high performers vs. 55% of low performers), effectively mitigating the risks after they are identified (59% of high performers vs. 43% of low performers), having incident-response services that can be deployed quickly (54% of high performers vs. 38% of low performers) and having high interoperability with the company's security intelligence tools (51% of high performers vs. 35% of low performers).

Figure 19 shows significant differences in attributes between high- and low-performing SOCs, with high performers ranked better in each category.

Figure 19.
Differences in achieving a more effective SOC

Strongly agree and agree responses combined

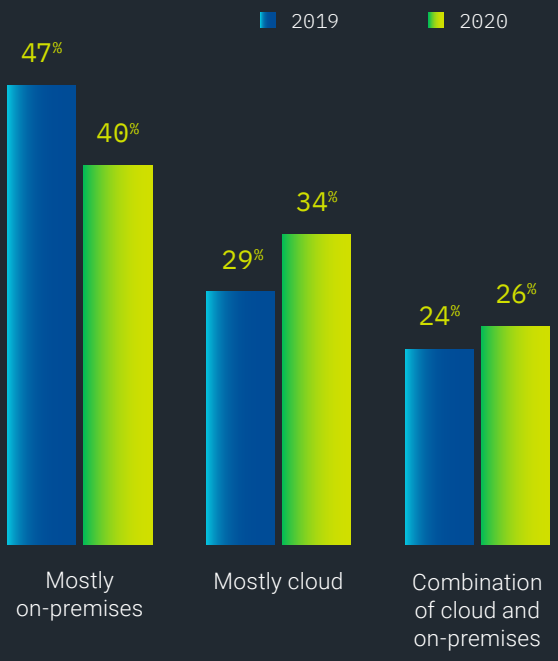


TRENDS IN THE INFRASTRUCTURE AND SECURITY PRACTICES OF TODAY'S SOC

Organizations continue to move the SOC to the cloud.

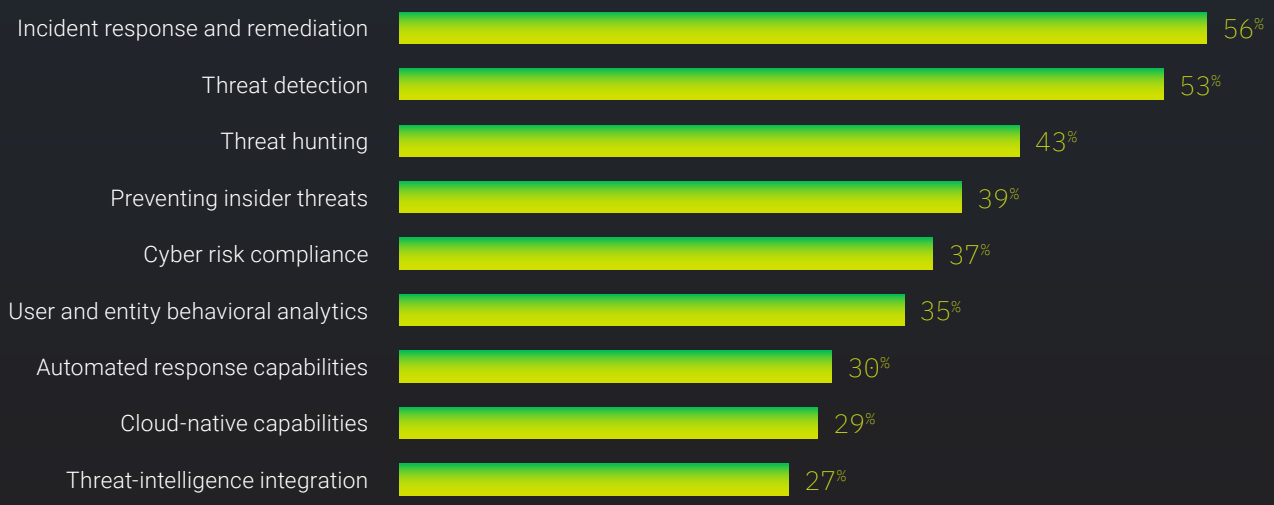
Sixty percent of respondents in the overall sample define the IT infrastructure that houses the SOC as mostly cloud (34%) or a combination of cloud and on-premises (26%), an increase from 53% of respondents in 2019. Since last year, respondents who say their SOCs are mostly on-premises has declined from 47% to 40%.

Figure 20.
What best defines the IT infrastructure that houses your SOC?



The majority of organizations deploy incident response and remediation, and threat detection (56% and 53% of respondents, respectively). Least deployed are cloud-native capabilities and threat-intelligence integration, 29% and 27% of respondents, respectively.

Figure 21.
Core services deployed today* More than one response permitted



*New question in 2020 survey

The most likely investments in the next year will be in threat detection, automated response capabilities, and threat hunting.

Figure 22.
Services to be added within the next 12 months*

More than one response permitted

*New question in 2020 survey

More lines of business are leading the SOC team.

Twenty-seven percent of respondents say lines of business are in charge of the SOC, an increase from 18% of respondents in 2019. However, 17% of respondents say no single function has clear authority and accountability for the SOC. Without clear processes and leadership in place, it can be more difficult to make decisions that could lead to SOC improvements.

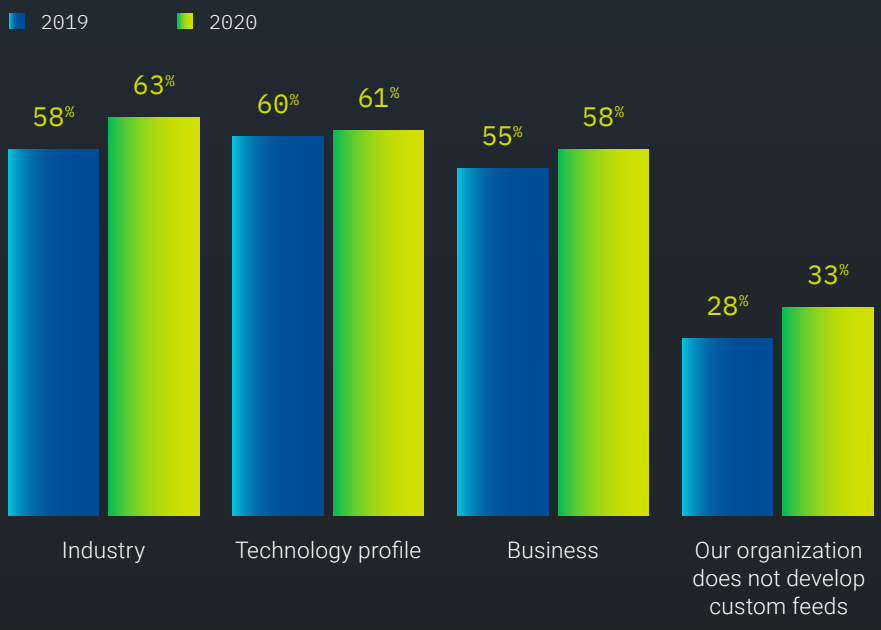
Figure 23.
Who leads your organization's SOC team?

Organizations are increasing their investment in threat-intelligence feeds.

Fifty-five percent of respondents say their organizations invest in threat-intelligence feeds. Of these organizations, 60% of respondents say the threat-intelligence feeds combine open-source and paid feeds, an increase from 54% of respondents in last year's survey.

Sixty-three percent of respondents say their organizations develop custom feeds based on the industry they are in, and 61% of respondents develop internal custom feeds based on a technology profile. Thirty-three percent of respondents say their organizations do not develop custom feeds, which could adversely affect the SOC's performance.

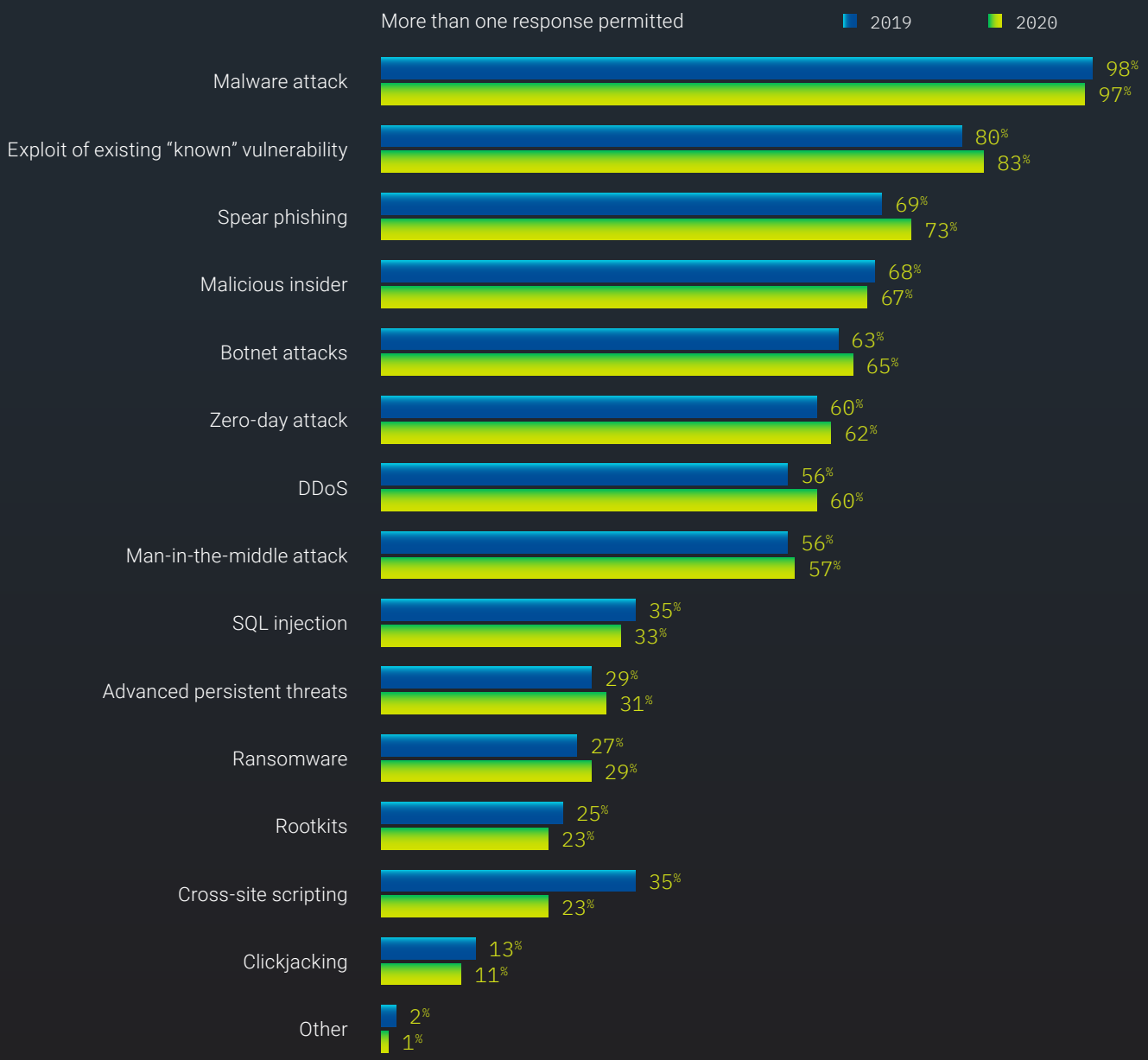
Figure 24.
Does your organization develop custom threat-intelligence feeds?



The SOC most commonly identifies malware attacks and exploits of existing “known” vulnerabilities.

Figure 25 presents a list of security exploits identified by SOCs. As shown, the most commonly identified are malware attacks, exploits of existing “known” vulnerabilities, spear phishing, malicious insider, botnet attacks, zero-day attacks, DDoS, and man-in-the-middle attacks.

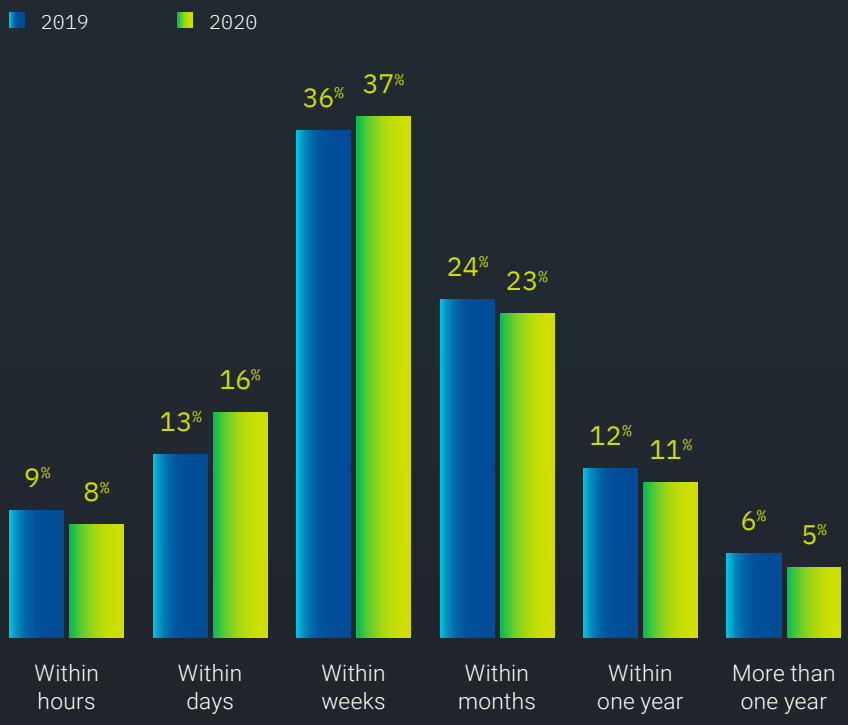
Figure 25.
The exploits or compromises the SOC has identified over the past 12 months



Mean time to resolution (MTTR) remains staggeringly high.

Respondents were asked to estimate the time it takes to resolve a security incident. Only 24% of respondents say resolution can occur within hours or days. Thirty-nine percent of respondents say the average time to resolve is months or even years.

Figure 26.
On average, what is the MTTR for a security incident in your SOC?



Special section:

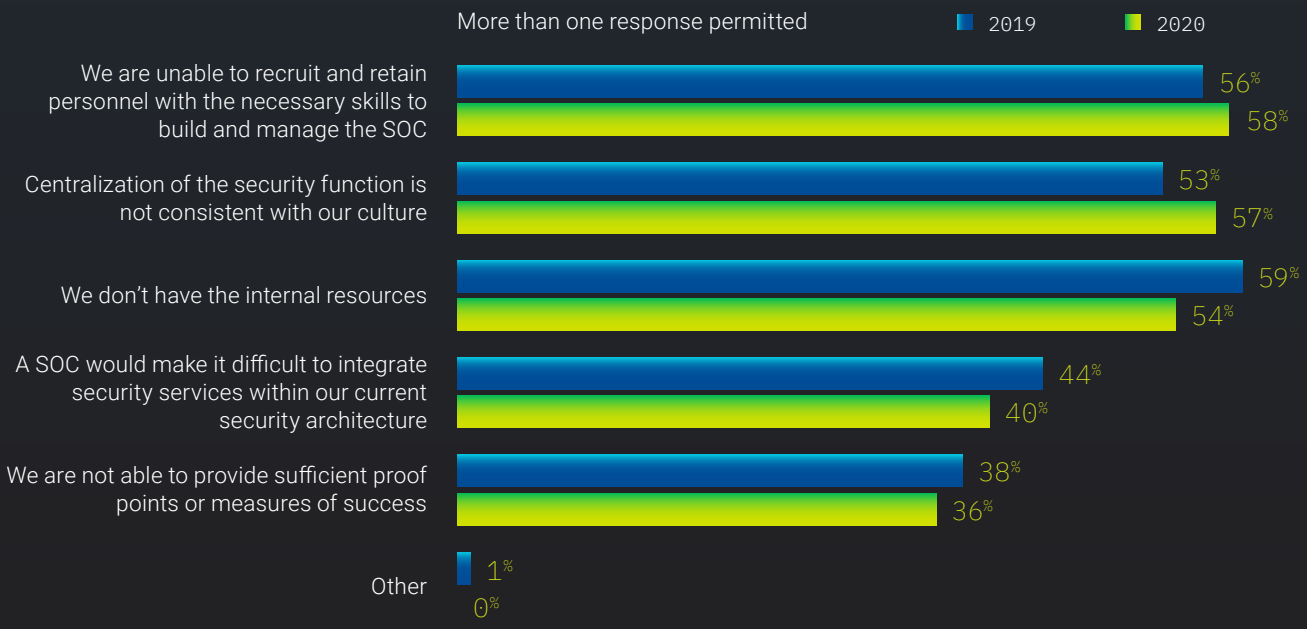
WHY ORGANIZATIONS DO NOT HAVE A SOC

In the previous sections of the report, all findings were based on organizations that have a SOC. However, we asked people who were screened out from completing the survey why they do not have a SOC, and what would motivate them to establish one. These respondents were not included in the overall study, but their responses to these questions are presented in this section.

Organizations without a SOC cite a lack of internal resources and difficulty recruiting and retaining people.

Reasons for not having a SOC are unchanged since last year. The primary reasons remain the inability to recruit and retain personnel with the necessary skills to build and manage the SOC, centralization of the security function is not consistent with their culture, and the lack of internal resources.

Figure 27.
Why does your organization not deploy or plan to deploy a SOC?



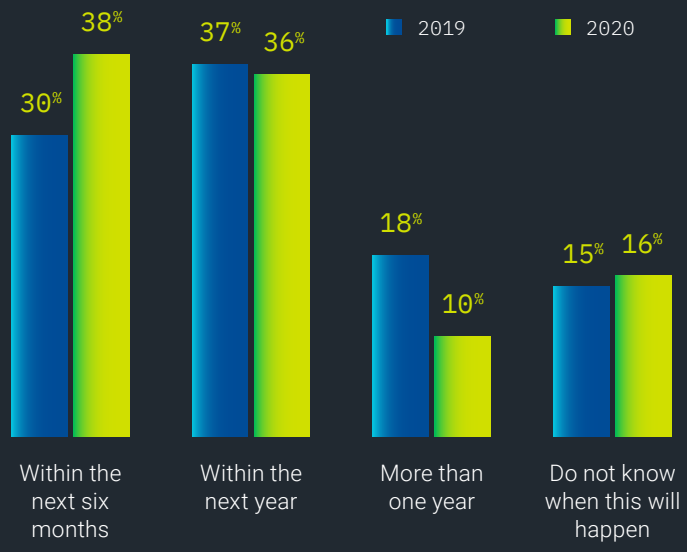
An adequate budget would encourage more organizations to deploy a SOC.

Respondents without a SOC recognize the importance of having adequate budget to ensure the success of a SOC. However, more respondents in this year's study say a security incident resulting in significant financial or data losses would motivate their organization to deploy a SOC.

Figure 28.
What would motivate your organization to deploy a SOC?

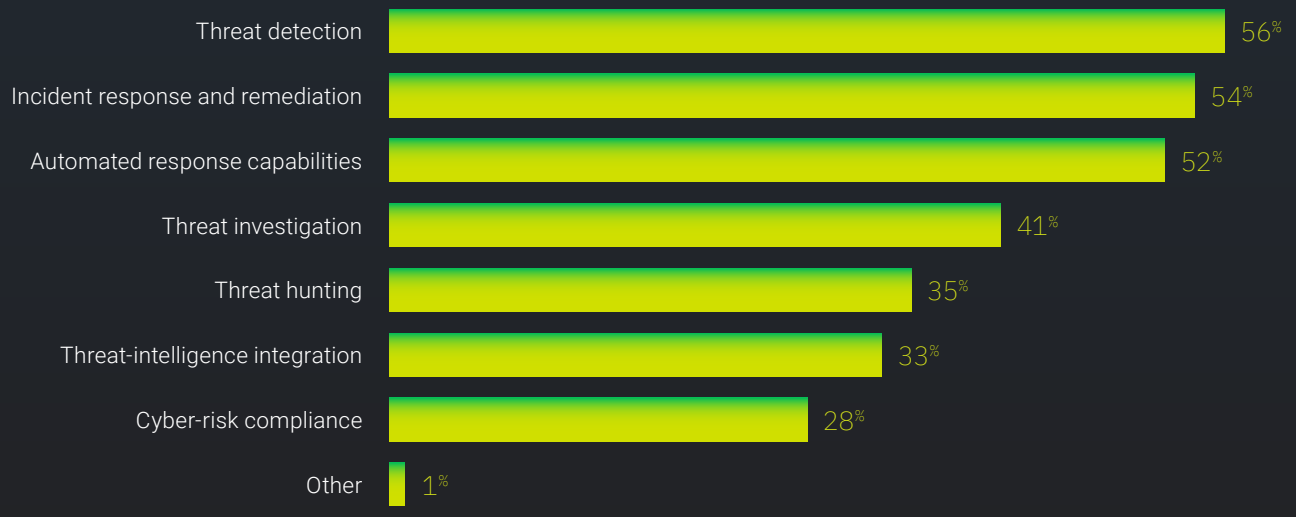
Seventeen percent of respondents in this group say they do plan to have a SOC and 38% say it will be within the next six months.

Figure 29.
When does your organization plan to deploy a SOC?



Once a SOC is established, threat detection, incident response and remediation, and automated response capabilities would be the top priorities.

Figure 30.
What would be the top two priorities when you deploy your organization's SOC?*



*New question in 2020 survey

Looking ahead.

As this report shows, SOC performance continues to be a critical element for the success of enterprise security operations, especially as SOCs must contend with new technologies and a rapidly evolving threat landscape. The 2020 data shows some meaningful improvements in SOC performance, but it is clear that many significant challenges across people, process, and technology persisted—and often increased—during the past year. We look forward to next year's report and gathering further insights into how IT and security practitioners can more successfully navigate the fast-moving security environment.

Part 3.

SURVEY METHODS

The sampling frame is composed of 16,343 IT and IT security practitioners in organizations that have a SOC. As shown in Table 1, 642 respondents completed the survey. Screening removed 57 surveys. The final sample was 585 surveys resulting in a 3.6% response rate.

TABLE 1. SAMPLE RESPONSE	FY2020	FY2019
Total sampling frame	16,343	15,495
Total returns	642	607
Rejected or screened surveys	57	53
Final sample	585	554
Response rate	3.6%	3.6%

Chart 1 reports the current position or organizational level of the respondents. More than half (57%) of respondents reported their current position as supervisory or above. Thirty-nine percent of respondents reported their current position as technician/staff.

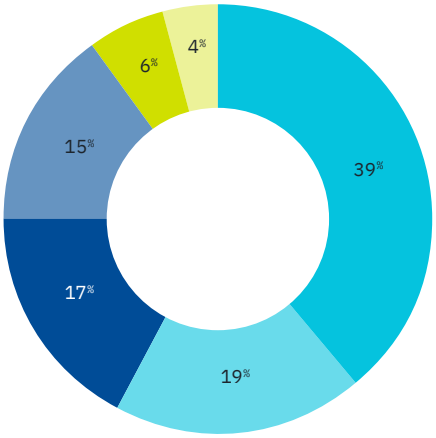


Chart 1.
Current position or organizational level

- Technician/Staff
- Manager
- Supervisor
- Director
- Senior Executive/VP
- Contractor

As shown in Chart 2, 33% of respondents report to the chief information officer, 20% of respondents report to the chief information security officer, 14% of respondents report to the line(s) of business management, and 9% of respondents indicated they report to the chief technology officer.

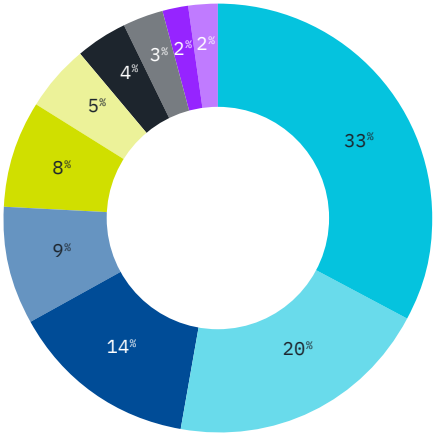


Chart 2.
Primary person you or your leader reports to

- Chief information officer
- Chief information security officer
- Lines of business management
- Chief technology officer
- Chief risk officer
- Compliance officer
- CEO/executive committee
- Chief security officer
- General council
- Other

Chart 3 reports the primary industry focus of respondents' organizations. This chart identifies financial services (19% of respondents) as the largest industry focus, which includes banking, investment management, insurance, brokerage, payments, and credit cards. This is followed by public sector (12%), healthcare (11%), and retail sector (9%).

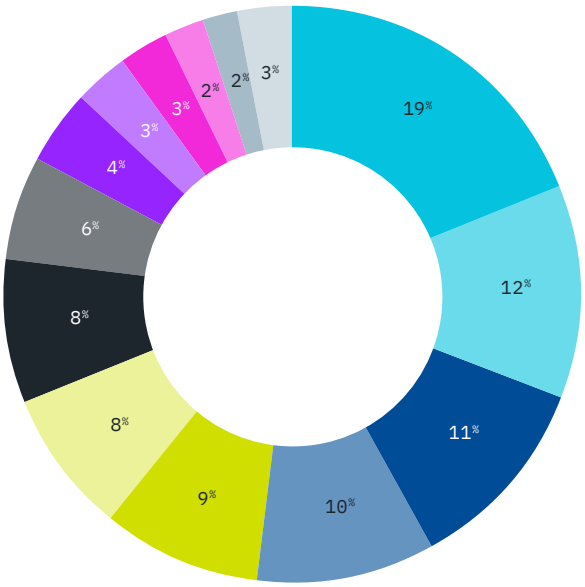


Chart 3.
Primary industry focus

- Financial services
- Public sector
- Healthcare
- Services
- Retailing
- Industrial & manufacturing
- Technology & software
- Energy & utilities
- Transportation
- Education
- Hospitality
- Communications
- Entertainment & media
- Other

As shown in Chart 4, half of the respondents (51%) are from organizations with a global headcount of more than 10,000 employees.

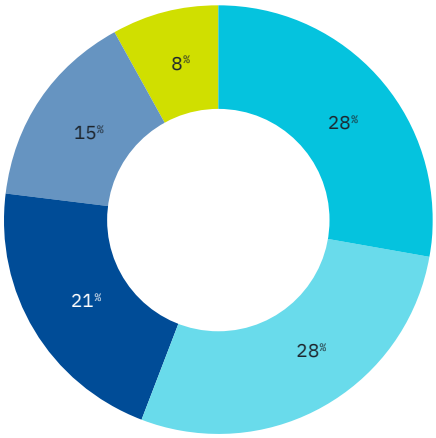


Chart 4.
Worldwide headcount of the organization

- 75,000+
- 25,001 to 75,000
- 10,001 to 25,000
- 5,001 to 10,000
- 1,000 to 5,000

Part 4.

CAVEATS TO THIS STUDY

There are inherent limitations to survey research that need to be carefully considered before drawing inferences from findings. The following items are specific limitations that are germane to most web-based surveys.

NON-RESPONSE BIAS

The current findings are based on a sample of survey returns. Ponemon sent surveys to a representative sample of IT and IT security practitioners, resulting in a large number of usable returned responses. Despite non-response tests, it is always possible that individuals who did not participate are substantially different in terms of underlying beliefs from those who completed the survey.

SAMPLING-FRAME BIAS

The accuracy is based on contact information and the degree to which the list is representative of individuals from organizations that have a SOC. Because Ponemon used a web-based collection method, it is possible that non-web responses by mailed survey or telephone call would result in a different pattern of findings.

SELF-REPORTED RESULTS

The quality of survey research is based on the integrity of confidential responses received from subjects. While certain checks and balances can be incorporated into the survey process, the possibility remains that a subject did not provide accurate responses.

SURVEY CONDUCTED BY PONEMON INSTITUTE

Ponemon Institute is dedicated to independent research and education that advances responsible information and privacy management practices within business and government. Our mission is to conduct high quality, empirical studies on critical issues affecting the management and security of sensitive information about people and organizations.

ABOUT DEVO

Devo unlocks the full value of machine data for the world's most instrumented enterprises, putting more data to work—now. Only the Devo Data Analytics Platform addresses both the explosion in volume of machine data and the new, crushing demands of algorithms and automation. This enables IT operations and security teams to realize the full transformational promise of machine data to move businesses forward. Devo is headquartered in Cambridge, Mass.

Learn more at **www.devo.com**.

 | June 2020