2021 Devo SOC Performance Report™

SOC Leaders and Staff Not Aligned

Survey independently conducted by Ponemon Institute

2021 Devo SOC Performance Report™
SOC Leaders and Staff Not Aligned

TABLE OF CONTENTS

Part 1.

Part 2.

Part 3.

Part 4.

PART 1.
INTRODUCTION

The *2021 Devo SOC Performance Report™* shows that security operations centers — and those who work in them — continue to have a number of challenges to overcome. Based on an independent survey of global cybersecurity professionals, our third annual report examines current trends for those who lead and work in SOCs. While there are some indicators of slight improvement, it's clear that for too many people, working in the SOC remains painful. The 2020 survey results told a tale of two SOCs — high and low performers. High performers are those with the funding, tools and staff to accomplish most of their cybersecurity goals. Low performers are those SOCs lacking in some or all of the foundational elements required for success, which is why they struggle in the face of myriad challenges. This year's report provides fresh insights about what separates high- and low-performing SOCs.

The 2021 report also presents a new perspective on the challenges facing SOCs and those who work there by focusing on survey responses from SOC leaders and the staff members who work for them. The results from the two groups often diverge widely, which points to the vastly different perspectives of analysts and leaders about how well SOCs are accomplishing their goals. There are more differences than areas of agreement about what makes a SOC successful, especially in its ability to gather evidence, investigate and identify the source of threats.

The report is based on the results of a comprehensive, independent survey Devo commissioned and Ponemon Institute conducted in September 2021 of more than 1,000 global cybersecurity professionals.

The survey generated insightful responses about key challenges affecting SOC operations, including:

- The continuing gap between high-performing and low-performing SOCs
- The ongoing pain driving SOC analysts to consider quitting their jobs
- The disconnect between SOC leaders and staff

In general, the year-over-year findings of SOC performance remain largely consistent. Some areas show slight improvement while others indicate problems have worsened. Overall, the results plateaued in 2021, which shines a spotlight on the challenges for organizations' cybersecurity programs and the job satisfaction and mental well-being of SOC analysts.

First, a Bit of Positive News

2021 has not been a typical year for most organizations worldwide. The ongoing pandemic and its impact on where and how people work has presented numerous challenges. It's reasonable to expect that responses to a survey about security operations centers would reflect those unusual circumstances. As with any survey, this one is a product of its time and reflects the opinions of respondents as they dealt with a range of internal and external issues.

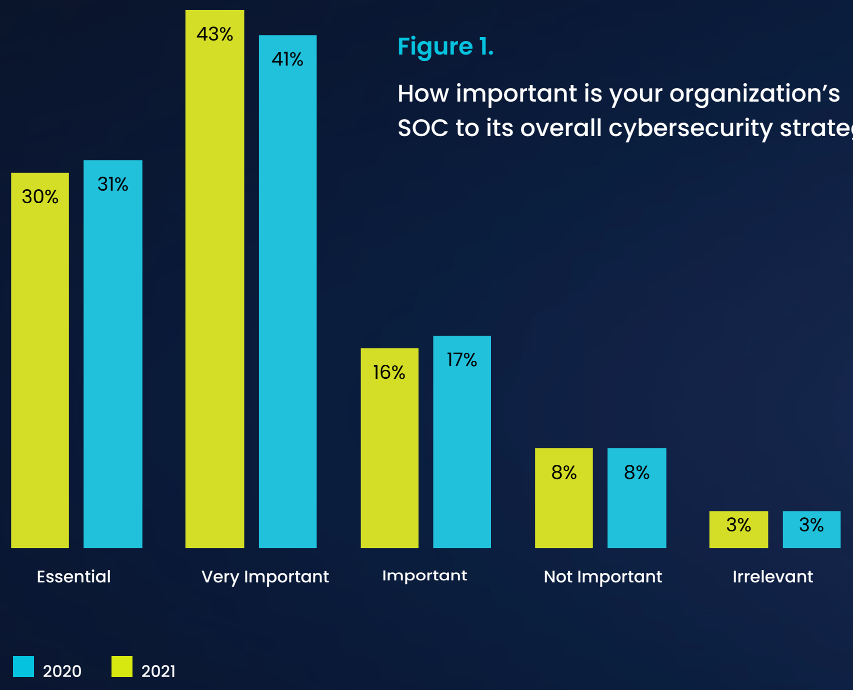


Figure 1.

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

There is not a great deal of positive news about SOC performance and culture in this year's results. But before we look at the problem areas and examine their causes and effects, let's first see what respondents think about the value the SOC provides to their organizations. This year, 73% of respondents said their SOC is a key component of their cybersecurity strategy. That's the slightest of gains from 72% in 2020, but it reflects the continuing strong support respondents have for what their SOC and its team deliver to the organization.

But... The Pain Remains

This year's survey results reflect the significant gap between high- and low-performing SOCs. High-performing SOCs continue to do a good job fulfilling the needs of their organizations because they have the resources — human and technical — to perform their work effectively. Low-performing SOCs, on the other hand, continue to struggle because they lack those same resources, which hinders their ability to effectively secure organizational data and respond to relentless threats. Analysts working in low-performing SOCs generally struggle more with job satisfaction and burnout issues. These issues combine to suppress improvements in SOC performance and analysts' well-being.

It's important to note that even high-performing SOCs and the people who lead and work in them face challenges. That said, we'll take a look at both the differences and similarities between the two groups and the factors that hinder the critical work performed by many SOCS.

So, What's Causing This Pain?

The overall level of perceived pain from working in a SOC declined slightly in 2021 from the prior year, but that's not much cause for cheer. On a 10-point scale, where 10 indicates SOC staff have a "very painful" experience performing their jobs, 72% of respondents rated the pain of SOC analysts at a 7 or above. That's a bit lower than the 2020 number (78%), but it remains clear that working in a SOC continues to be far more painful than staff members and organizations can tolerate. This continuing high level of pain presents a wide range of challenges for SOC leaders, particularly when it comes to recruiting and, more importantly, retaining employees. And having an understaffed SOC or constant turnover of security talent can cripple an organization's security posture.

The dissatisfaction of SOC workers is exacerbated by poor communication from SOC leaders. Almost 60% of respondents gave low grades to leaders for how well they communicate SOC strategy to those "in the trenches." 13% of respondents rated their bosses a 2 or lower on the 10-point scale, while the majority rated this important skill for building and managing teams at no higher than 6. This is unacceptable. Budgets, skills training, tools, etc., require investment, which many organizations may not be able to afford during challenging economic times.

But when leaders who cannot effectively communicate with their teams are a significant cause of SOC analyst pain — which often leads to resignations — it seems reasonable for leaders to invest some time and effort to improve their ability in this important component of people management.

SOC Leaders and Staff Not Aligned

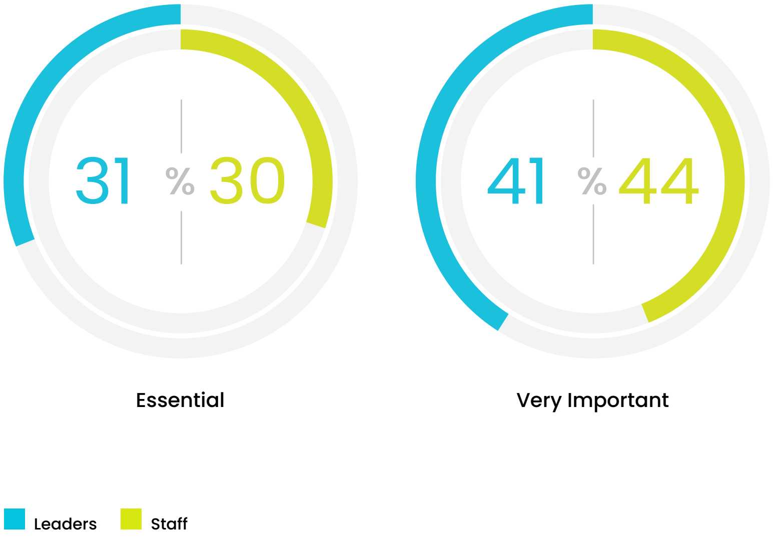
This year's survey, for the first time, compared responses from SOC leaders (senior executives, vice presidents, directors and managers) with those of staff members (supervisors, technicians and contractors). It doesn't spoil the ending to tell you these two groups, which should be working in unison to protect their organizations from nonstop cyberthreats, do not see eye to eye on many key issues.

The survey responses from 535 SOC leaders and 485 staff members show that the two groups are not aligned when it comes to many important practices. Identifying and understanding these differences is a key first step toward closing the gaps to improve SOC performance and organizational security — as well as alleviate analyst pain.

One topic on which leaders and staff strongly agree is that their SOC is a valuable part of the organization's overall cybersecurity strategy.

Figure 2.

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



When it comes to SOC leaders and staff not being in sync, one of the primary places to examine that gap is the groups' responses about SOC effectiveness. When asked how effective their SOC is, leaders scored it a 5 and staff a 3.9 on the 10-point scale. The gap widens in response to the question of how effective their SOC is in its ability to gather evidence, investigate and find the source of threats, which earned a 5.5 from leaders and only a 3.3 from staff.

What's causing these disparate perspectives between SOC leaders and staff? It's reasonable to conclude that leaders may be looking at "big picture" issues, such as has the organization been breached, did it suffer any financial losses or reputational harm due to a cyberattack, malware, etc. Staff, however, tend to focus on how many events come across their screens that require some degree of action to determine which are innocuous and which require investigation and response. But even if that's the case, it shows the two groups are not in sync about what is happening in SOCs on a daily basis and the toll this nonstop work is taking on staff members.

Other Differences Between SOC Leaders and Staff

When it comes to areas of ineffectiveness in their SOCs, leaders and staff members agree that those issues exist — but they disagree on the root cause.

For example, when asked to identify the biggest cause of SOC ineffectiveness, 65% of leaders cited "visibility into the attack surface." 61% of staff, on the other hand, believe the primary factor contributing to SOC ineffectiveness is "having too many tools."

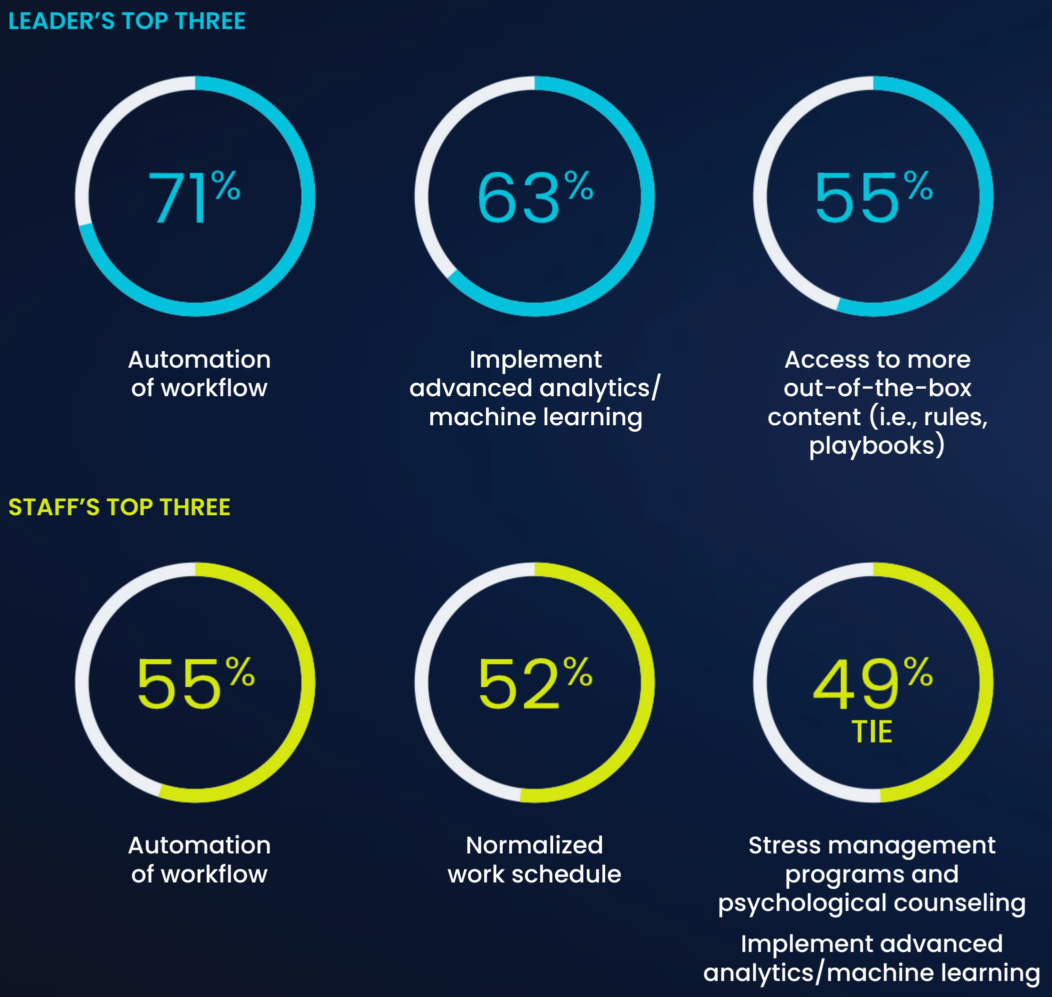
Another subject with some sharp disagreement is the two groups' perceptions about the SOC's effectiveness in mitigating risks after they are identified. 51% of leaders say their SOC does an effective job mitigating risks after they are identified, but only 35% of staff feel the same.

Given the continuing focus of these annual surveys on the pain experienced by SOC analysts, it's especially enlightening to see where there is a sizable difference of opinion between what SOC leaders feel would help alleviate pain vs. what staff members (the people actually feeling the pain) would like to see. The top response — from 71% of leaders — is automating the SOC workflow, but only 55% of staff agreed. Similarly, 63% of leaders believe that implementing advanced analytics/machine learning would be a boon to reducing pain, an opinion shared by only 49% of staff.

Figure 3.

What steps can be taken to alleviate SOC analysts' pain?

(More than one response permitted)



Where SOC Leaders and Staff More Closely Agree

Both SOC staff (80%) and leaders (76%) agree that providing formal training programs would help retain analysts and reduce the turnover that increases cybersecurity vulnerability and leads to analyst burnout. However, only 48% of all respondents said their organization has such training programs in place.

Regarding what makes working in the SOC painful, leaders (69%) and staff (65%) largely agree that lack of visibility into the attack surface is a big problem. Another area of relatively close agreement between the groups relates to information overload, which 72% of staff and 67% of leaders cite as a significant contributor to analyst pain. The competitive nature of both groups is apparent, as 45% of leaders and 44% of staff say losing to adversaries is a cause of pain.

When it comes to alignment of SOC objectives with the needs of the business, only 21% of SOC leaders and 22% of staff feel their SOC is fully aligned with business needs. 34% of leaders and 40% of staff see at least partial alignment on this important item.

The Gap Between High- and Low-Performing SOCs

Just as the 2020 report showed, a clear and troubling chasm continues to separate SOCs that have the resources — including people — to succeed (high performers) from those that are resource-challenged (low performers). When rating their SOC's effectiveness on a 10-point scale, only 21% rated their organization's SOC as a 9 or 10, i.e., a high performer. The other 79% felt their SOC's performance was deficient, with 55% rating their SOC at 6 or below, including 23% who rated their SOC as no better than a 4 out of 10. These results are marginally better than the 2020 figures, but problems persist.

Figure 4.

How High and Low Performers View SOC Effectiveness

Using the following 10-point scale, please rate the effectiveness of your organization's SOC. On a scale from 1 = ineffective to 9+ = Very effective	**2021**	**2020**
1 or 2	8%	7%
3 or 4	15%	15%
5 or 6	32%	28%
7 or 8	24%	35%
9 or 10	**21%**	**15%**

Consistent with these results, 32% of high performers reported that their SOC's objectives are fully aligned with the organization's business needs. Contrast that with just 19% of low performers who see that same level of alignment.

As you would expect, the perspectives on what barriers are preventing their SOC from operating successfully (or more successfully) diverge between high and low performers. Turf or silo issues between the organization's IT security operations and the SOC are a problem for 66% of respondents from low-performing SOCs. Conversely, only 42% of respondents from high-performing SOCs see the same issue as a barrier to success. 28% of respondents from low-performing SOCs cited compliance with internal policies and contractual requirements as an impediment to success, compared with just 12% of those from high-performing SOCs.

Interestingly, 64% of respondents from high-performing SOCs said the lack of available analyst talent is a problem, while only 49% of respondents from low-performing SOCs saw that as an issue. Given the difficulties most organizations have been experiencing for the past several years to recruit and retain technical talent, which has been compounded by the pandemic-related Great Resignation, this skills shortage is a problem across the board.

PART 2.
KEY FINDINGS

This section dives more deeply into the survey results. The report also compares the 2021 findings to the 2020 responses to identify where attitudes have changed or remained consistent. The complete audited findings are available in the Appendix of the report at https://www.devo.com/wp-content/uploads/sites/1/2021/12/2021-Devo-SOC-Performance-Report-Appendix.pdf.

We have organized the research into the following topics:

1. The overall survey results
2. SOC leaders vs. staff responses
3. High vs. low performers

Examining the Full Survey Results

Let’s begin by presenting the survey results from all respondents to key questions and compare them to the 2020 responses. This will identify whether areas have improved, remained the same, or worsened.

What Respondents Say About SOC Value and Effectiveness

Are SOCs valuable to their organizations? Yes, but no more than they were in 2020, according to respondents. This year, 73% of respondents said their SOC is essential or very important, while 72% said the same last year. In fact, the number of people who feel their SOC is essential declined slightly.

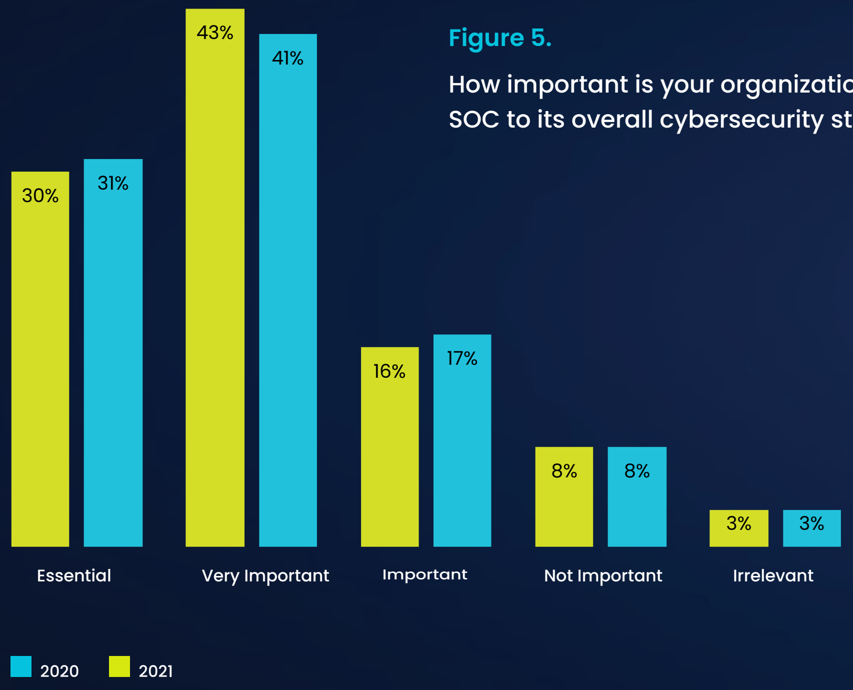


Figure 5.

How important is your organization’s SOC to its overall cybersecurity strategy?

While the perceived value of SOCs remained constant, SOC effectiveness is an area where the year-over-year results reflect some noticeable shifts. Respondents were asked to rate the effectiveness of their organizations' SOC on a scale from 1 = not effective to 10 = highly effective. In 2021, less than 50% of those surveyed believe their SOC is highly effective (responses of 7+) when it comes to gathering evidence and performing other fundamental functions.

Since the primary job of a SOC is to identify, investigate and stop attacks or other suspicious activity that hits the organization, survey responses regarding these critical areas are especially informative about the overall state of SOC performance. This year, less than half (45%) of respondents consider their SOC to be effective (7 or higher out of 10) at these functions, which is a sharp decline from the 55% who said their SOC was effective in 2020.

Figure 6.

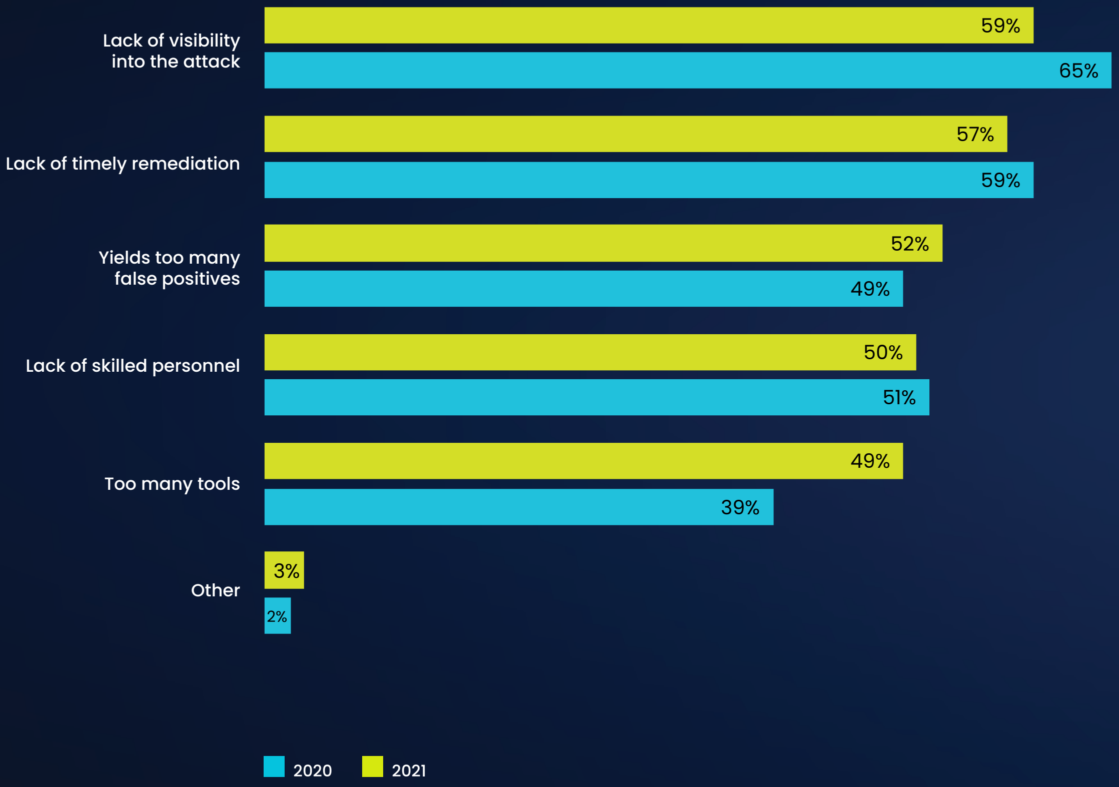
Using the following 10-point scale, please rate the effectiveness of the ability of the SOC to gather evidence, investigate and find the source of threats from 1 = ineffective to 10 = very effective.	**2021**	**2020**
1 or 2	9%	7%
3 or 4	15%	15%
5 or 6	31%	23%
7 or 8	22%	30%
9 or 10	**23%**	**25%**

So, what makes SOCs ineffective? The response with the biggest percentage increase in 2021 is "Too many tools," which is cited by 49% of respondents, up 10 percentage points from the prior year. The other response to tick upward in 2021 is "Yields too many false positives," according to 52% of those surveyed.

Figure 7.

What makes your organization's SOC ineffective (responses 1 to 4 on the scale above)?

(Please select all that apply).

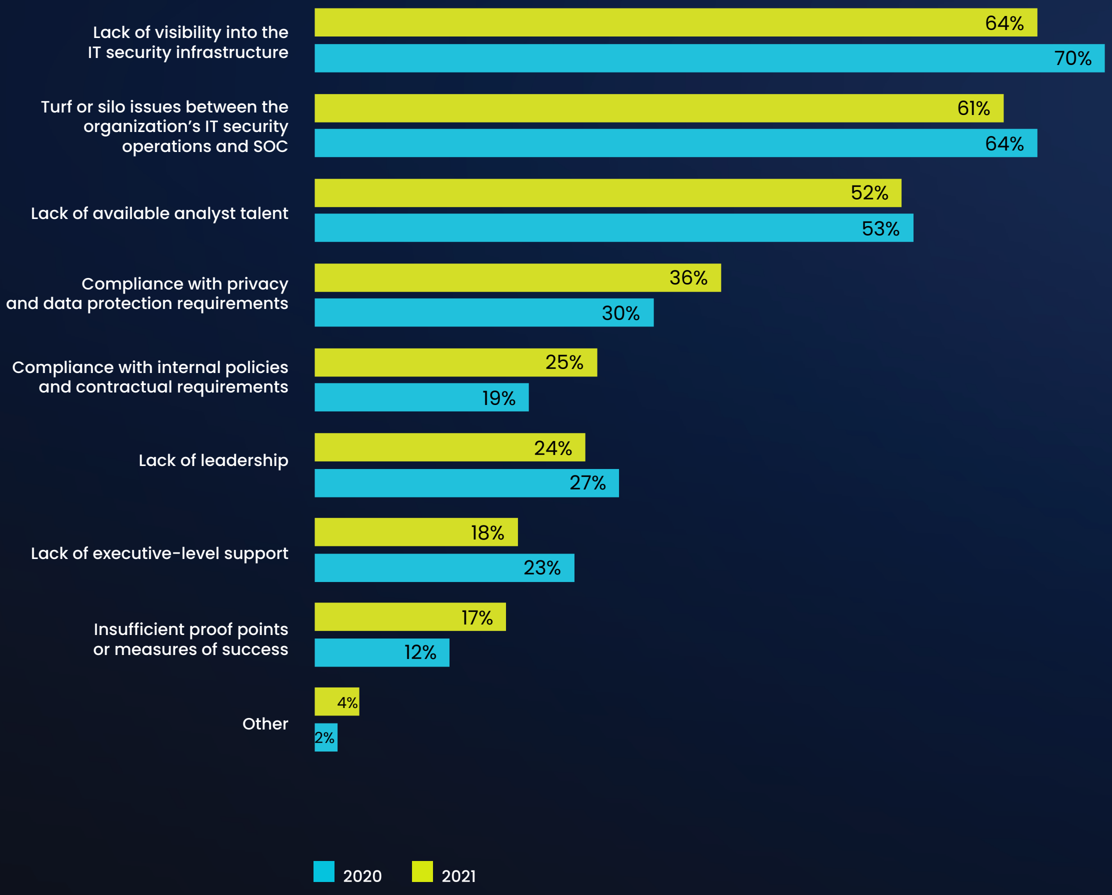


When it comes to what prevents SOCs from operating successfully, this year's responses are largely consistent with those from 2020. But what's interesting are the areas respondents identify as barriers to success. In particular, the top two responses, once again, are "Lack of visibility into the IT security infrastructure" (64%) and "Turf or silo issues between the organization's IT security operations and SOC." These related topics point to internal friction that persists and continues to hinder SOC performance. While the need for more people, tools or other areas generally require additional funding (or at least budget reallocation), organizational control issues can be addressed with better communication and cooperation between groups. After all, both security operations and the SOC have the same goal: keeping the organization safe from cybersecurity issues.

Figure 8.

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

(More than one response permitted)



The good news is there was a bit of improvement on these two issues in 2021, with fewer respondents feeling that turf/silo issues and lack of visibility into IT infrastructure are the top problems facing their organization. But that said, as the only two responses cited by more than 60% of those surveyed, these issues still require much more work. And let's not forget that more than half of respondents once again said the lack of available analyst talent continues to be a major challenge.

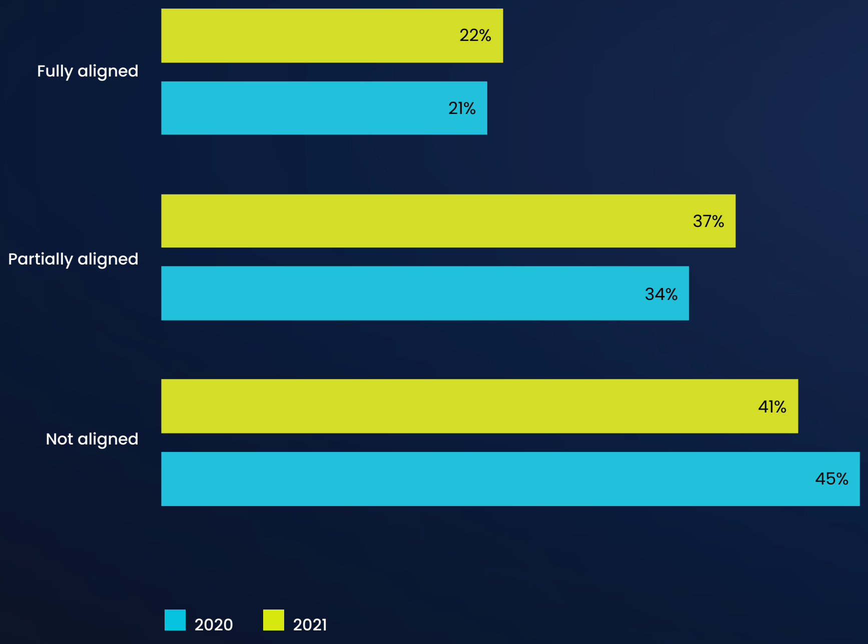
Alignment with Business Needs

So far, we've seen that respondents feel that their SOC is essential to the organization. And we've also seen there are a number of barriers that prevent SOCs from operating effectively. Another area that points to why there are problems with SOC performance and effectiveness is how SOCs align (or don't) with the needs of the business.

Only 22% of respondents say their SOC is fully aligned with business needs, compared to 21% last year.

Figure 9.

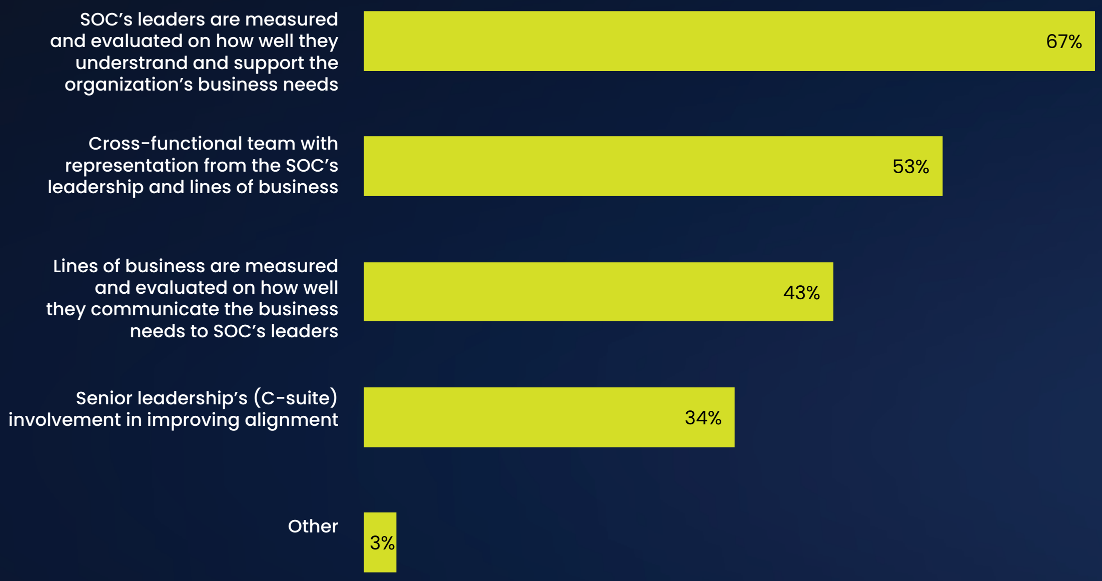
Within your organization, are SOC objectives aligned with business needs?



One of the more interesting findings of the survey is the top response to what can be done to improve alignment. This is a new question added to the 2021 research.

Figure 10.

If alignment between the SOC's objectives and your organization's business needs is only partially or not aligned, what would improve alignment? Please select your top two choices.



Measuring job performance of SOC leaders based on how well they are able to grasp and support the business needs of the organization seems to be not only a good idea, but a fairly common practice in various departments of many organizations. If this particular discipline is not widely applied to those who lead SOCs, then it's high time it is.

“There are no gains without pains.”

That quote is from the autobiography of Benjamin Franklin. If Ben’s words are true, then SOC analysts must be doing a lot of gaining these days because according to this year’s survey, working in a SOC remains a very painful occupation.

Figure 11.

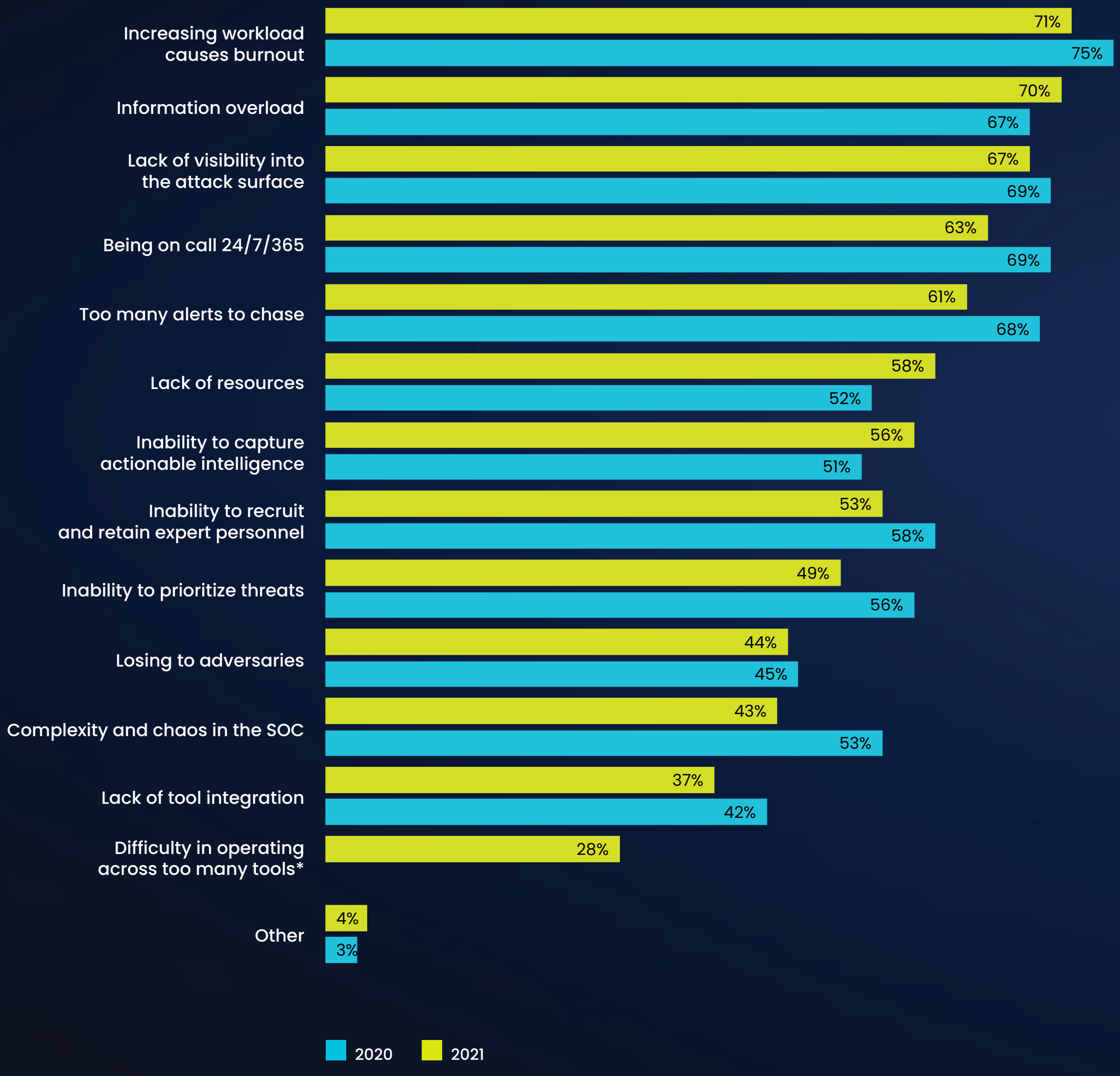
Using the following 10-point scale, please rate the “pain” your organization’s SOC security personnel experience in meeting their daily job requirements. From 1 = low pain to 10 = very painful	2021	2020
1 or 2	6%	5%
3 or 4	6%	4%
5 or 6	16%	13%
7 or 8	32%	28%
9 or 10	**40%**	**50%**

When asked, “What makes working in the SOC painful?” respondents said information overload, lack of resources, and inability to capture actionable intelligence were worse in 2021 than 2020.

Figure 12.

What makes working in the SOC painful (7+ responses on the scale above)?

(More than one response permitted)



* New question in 2021 survey.

Job-related pain affects workers in most occupations at one time or another. But if the pain persists at a high level for a long time, it's much more likely to result in workers taking action they believe will improve their mental and physical health. That's the case in SOCs where almost two-thirds of survey respondents said on-the-job pain has caused them to consider changing careers or leaving their jobs.

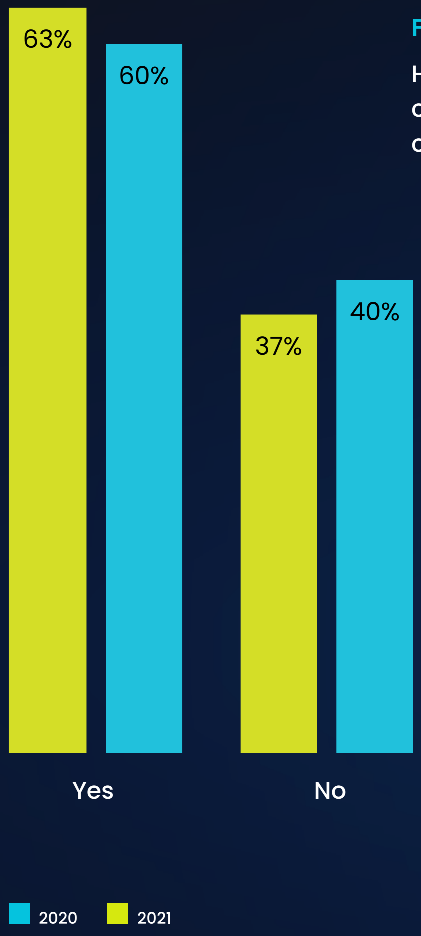


Figure 13.

Have any of the above pain factors caused you to consider changing careers or leaving your job?

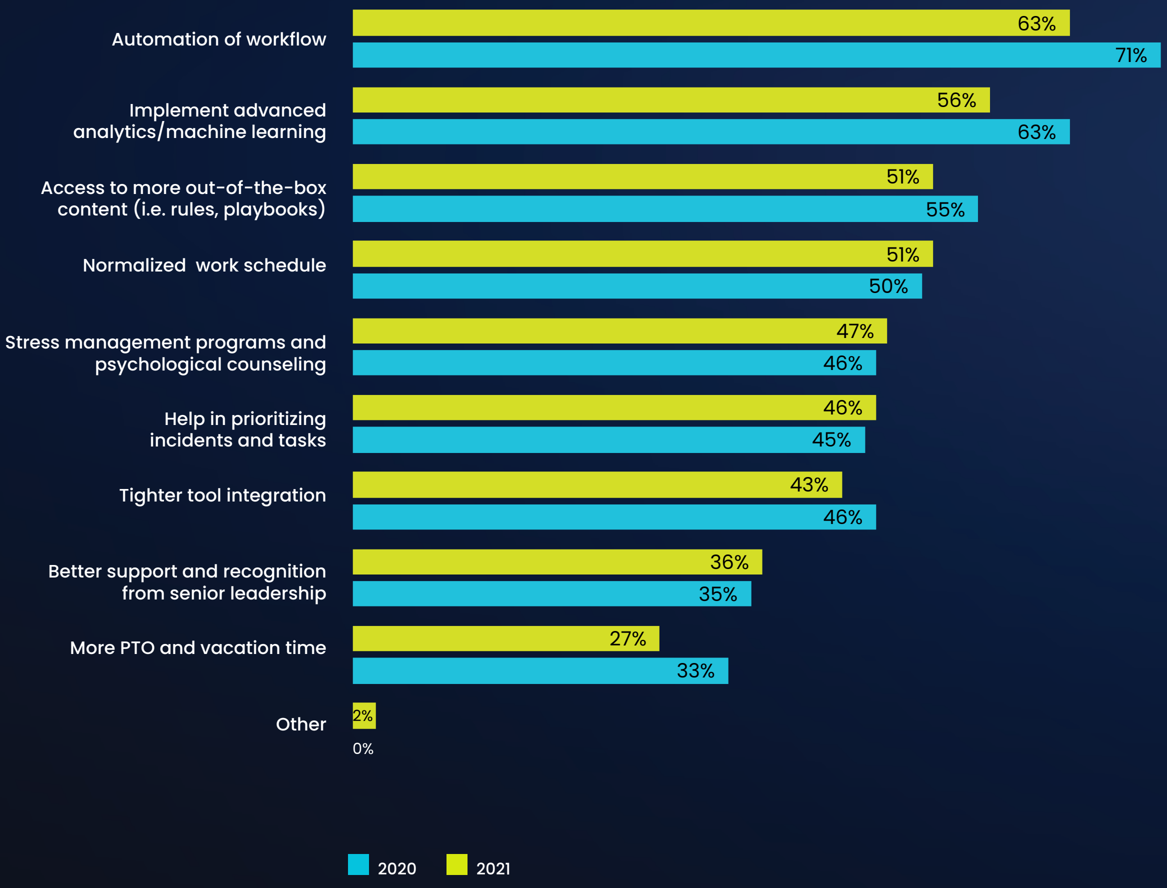
What Can Be Done to Rein in the Pain?

With such high numbers of SOC workers identifying job pain as possibly driving them to quit their jobs or choose a new career, there is no shortage of ideas for what organizations can do to try and at least minimize the pain afflicting analysts. Once again, workflow automation was the top choice for how to alleviate the pain of SOC work, although fewer respondents chose it this year than in 2020. Another technological approach — implementing advanced analytics/machine learning — was the second most popular response.

Figure 14.

What steps can be taken to alleviate SOC analysts' pain?

(More than one response permitted)



Are SOC Leaders and Staff on the Same Page (or Even Reading the Same Book)?

For the first time in the three years Devo has published this report, we are providing a look at the survey results based on whether the respondent is a SOC leader (executive/VP, director or manager) or a staff member (supervisor, technician or contractor). The results show significant differences of opinion between the two groups about what makes a SOC successful.

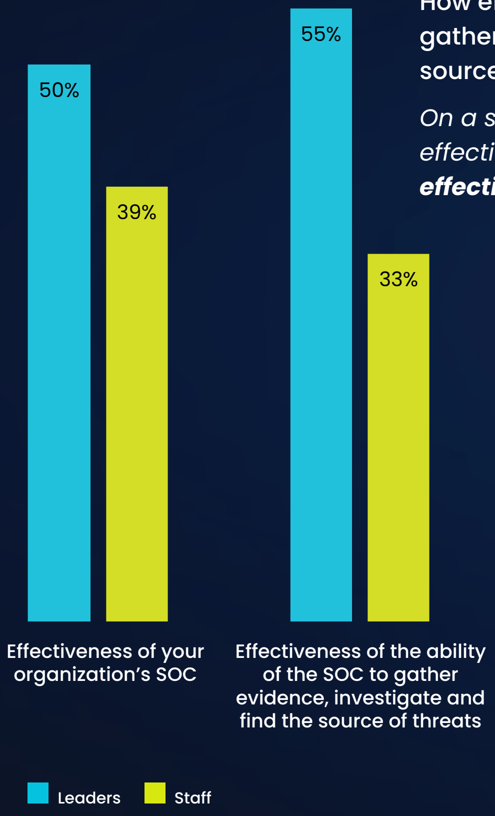
SOC leaders and staff are not in sync concerning important SOC practices. The survey results can serve as a guide for steps organizations can take to address these gaps with the goal of improving the alignment of the SOC's objectives with the goals and needs of the business.

To begin, let's look at how each group feels about the effectiveness of their SOC.

Figure 15.

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

On a scale of 1 = not effective to 10 = highly effective. ***Responses are from those who rated effectiveness at 7 or above.***



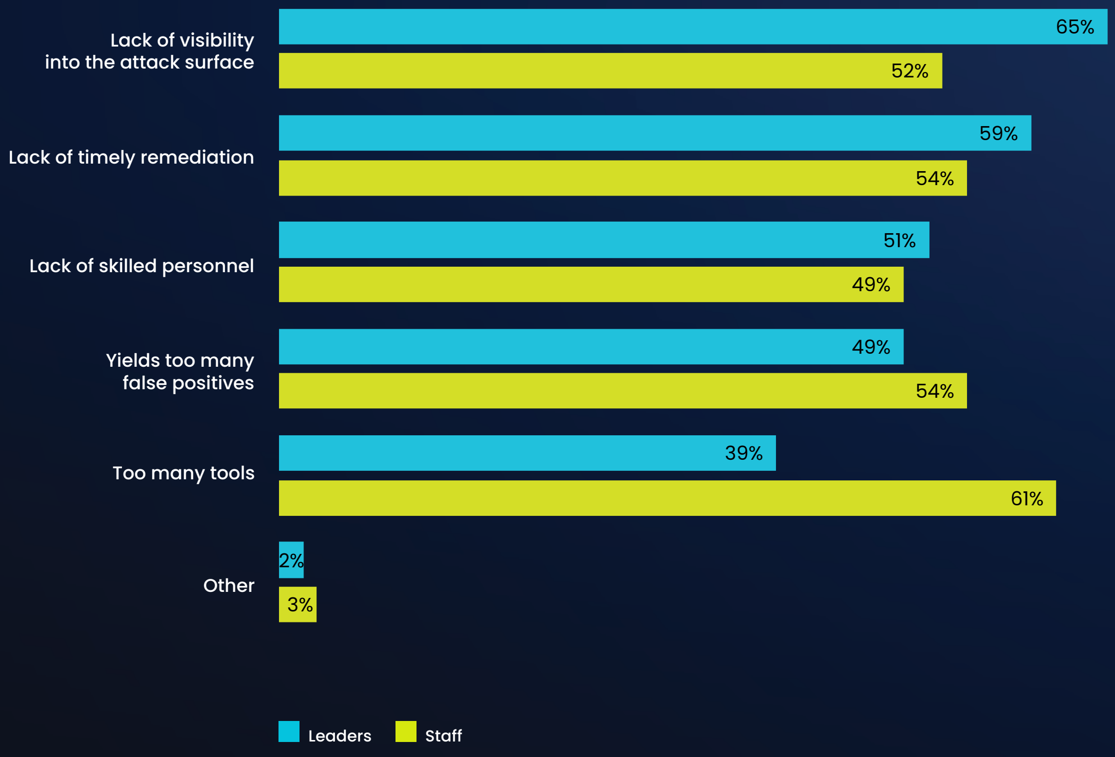
There are sizable gaps between how leaders rate SOC effectiveness compared to staff. Some of that is likely due to the nature of their work and how well the SOC hits performance goals (assuming the organization has implemented them and tracks results). But overall, these responses show the two groups do not see the complete picture of what the SOC needs to accomplish and how well it performs. Clearly, better communications and sharing of perspectives and goals would at least help improve each group's ability to understand how the other views their shared world.

Another gap between leaders and staff comes to light when comparing responses to the question of what makes their organization's SOC ineffective. Leaders blame ineffectiveness on the lack of visibility into the attack surface and the lack of timely remediation. Conversely, staff members cite the complexity caused by too many tools and too many false-positive alerts.

Figure 16.

What makes your organization's SOC ineffective (responses 1 to 4 on the 10-point scale)?

(More than one response permitted)

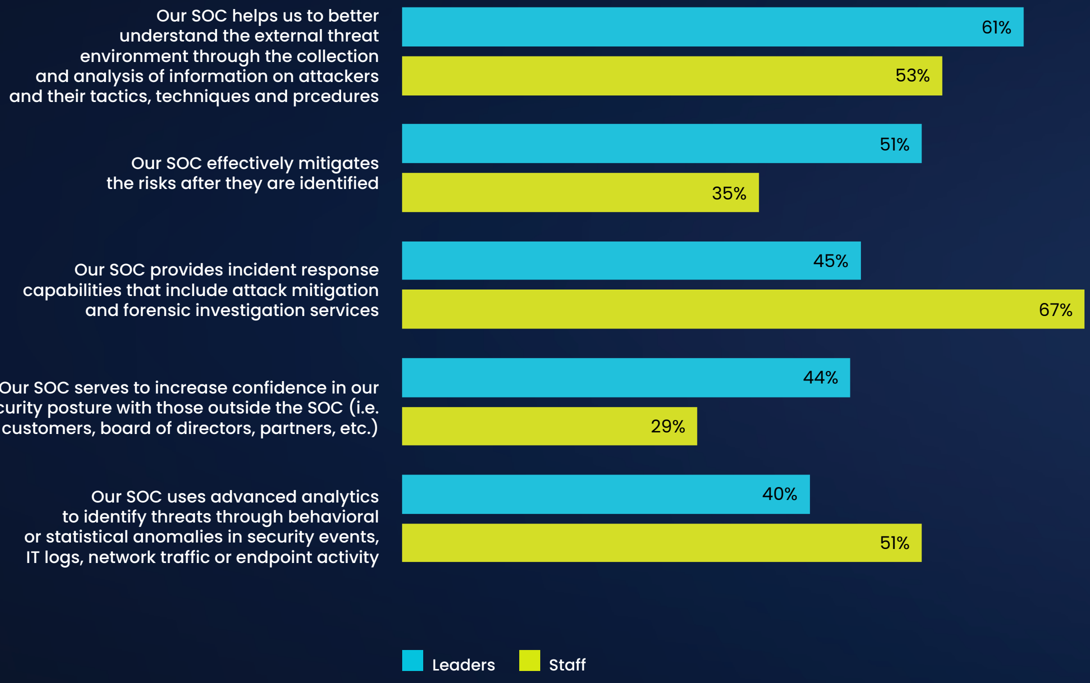


Another area of misalignment comes from each group's perception of the SOC's security posture. The disparities seemingly point to a lack of awareness by leaders about the capabilities and skills of their teams. The greatest area of disagreement is about the effectiveness of mitigating risks after they have been identified and the SOC team's ability to provide incident response capabilities, including attack mitigation and forensic investigation services.

Figure 17.

Perceptions about the security posture: areas of disagreement

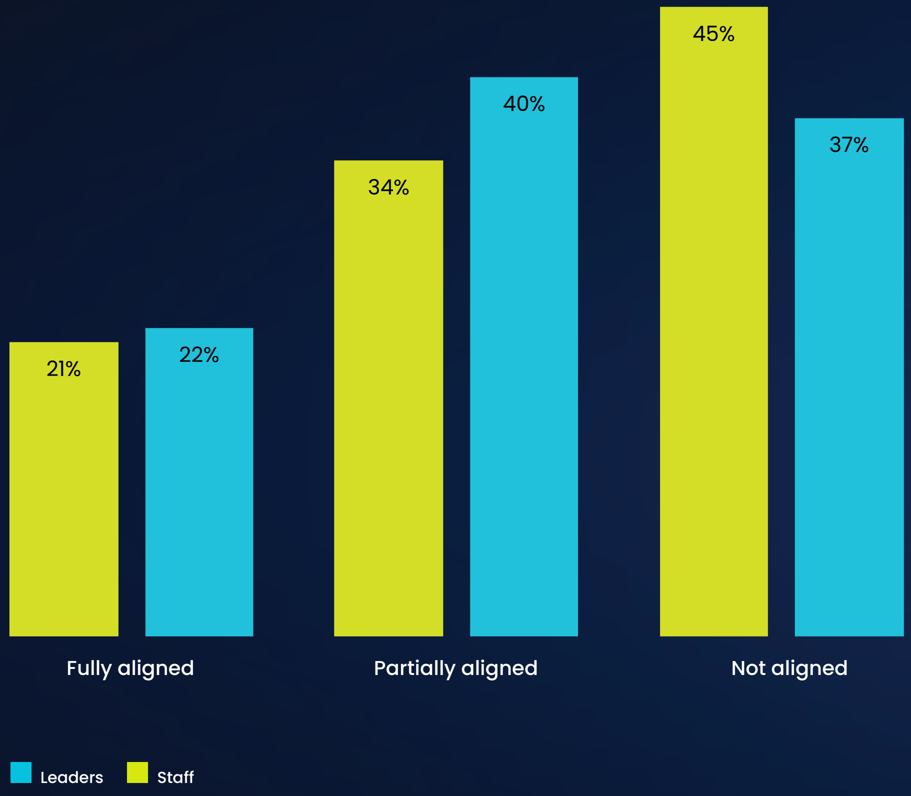
(Strongly Agree and Agree responses combined)



Lack of alignment between the SOC and the overall business can be detrimental to SOC effectiveness. The allocation of resources for the SOC requires support from leadership. However, 79% of SOC leaders and 77% of staff agree that their SOC is only partially or not at all aligned with their organizations' business needs. This lack of alignment presents a likely barrier to obtaining the budget and support required for success.

Figure 18.

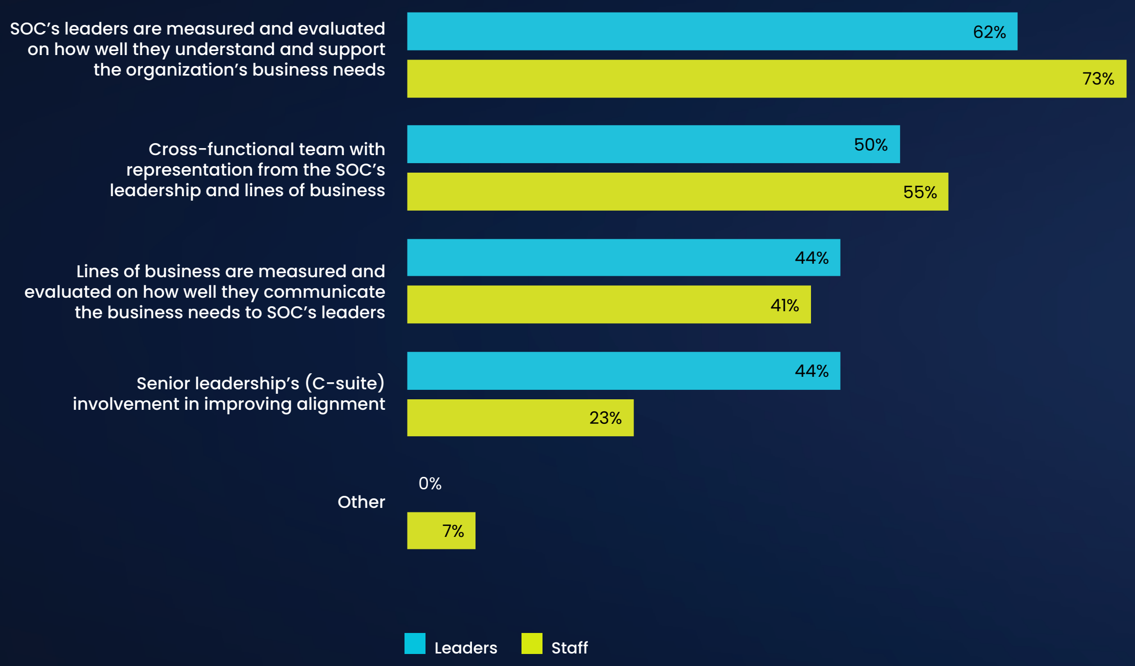
Within your organization, are SOC objectives aligned with business needs?



To improve this alignment, both leaders and staff agree on the importance of measuring SOC leaders by how well they support the organization's business needs. Of the majority of leaders and staff who say business needs and SOC objectives are only partially or not at all aligned, the top response for how to change the situation is to measure and evaluate SOC leaders on how well they understand and support the organizations' business needs.

Figure 19.

How can alignment of your business goals and SOC objectives be improved? *(Two responses permitted)*

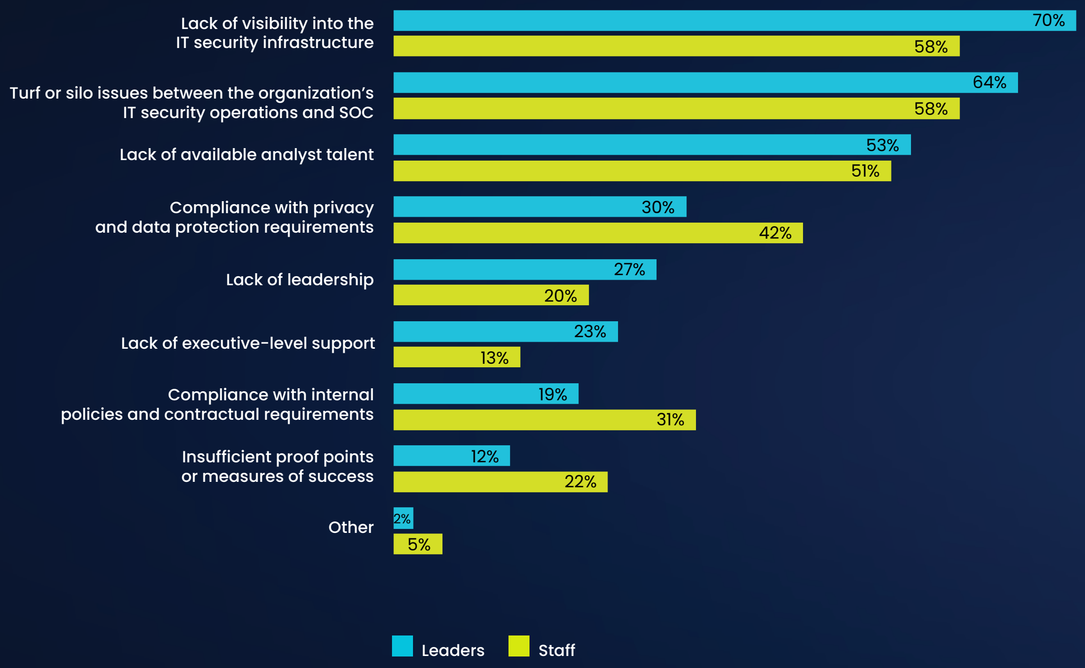


When it comes to identifying what's preventing successful SOC operation, leaders and staff agree that the lack of available analyst talent is a significant barrier. Opinions are split about other roadblocks, including lack of visibility into the IT infrastructure as well as interdepartmental turf and silo issues.

Figure 20.

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

(Three responses permitted)



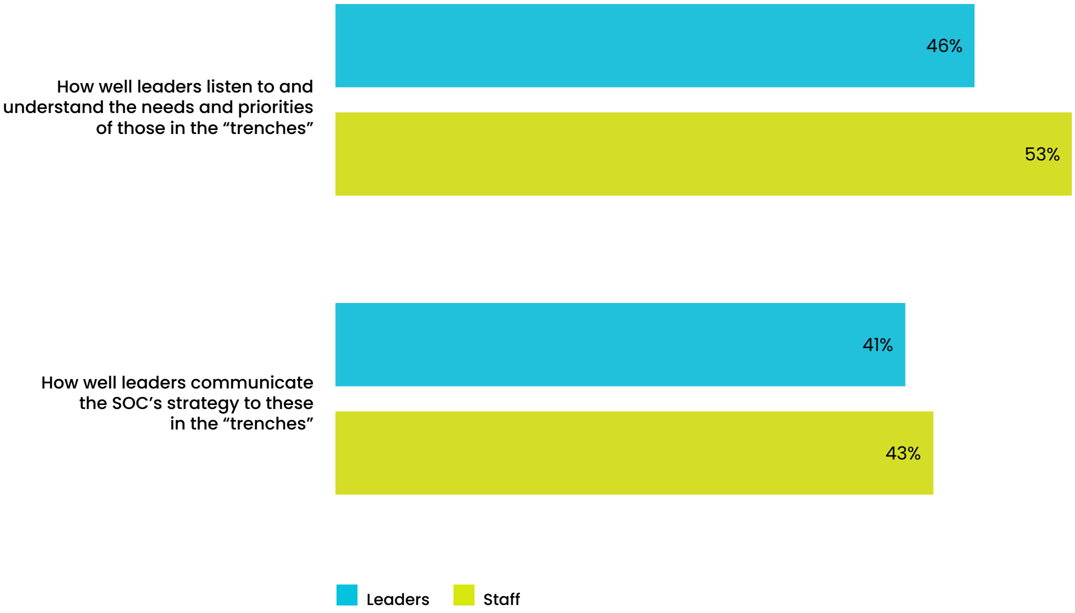
The Path to SOC Effectiveness

With more disagreement than concurrence about challenges facing the SOC, alignment issues, and SOC effectiveness, it's no surprise that both leaders and staff see room for improvement when it comes to how well those who run the SOC communicate with their teams. What is surprising is staff respondents give leaders higher grades for both listening and communicating than the leaders give themselves.

Figure 21.

Effectiveness in how these leaders communicate with those in the trenches.

On a scale from 1 = not well at all to 10 = exceptionally well, 7+ responses presented

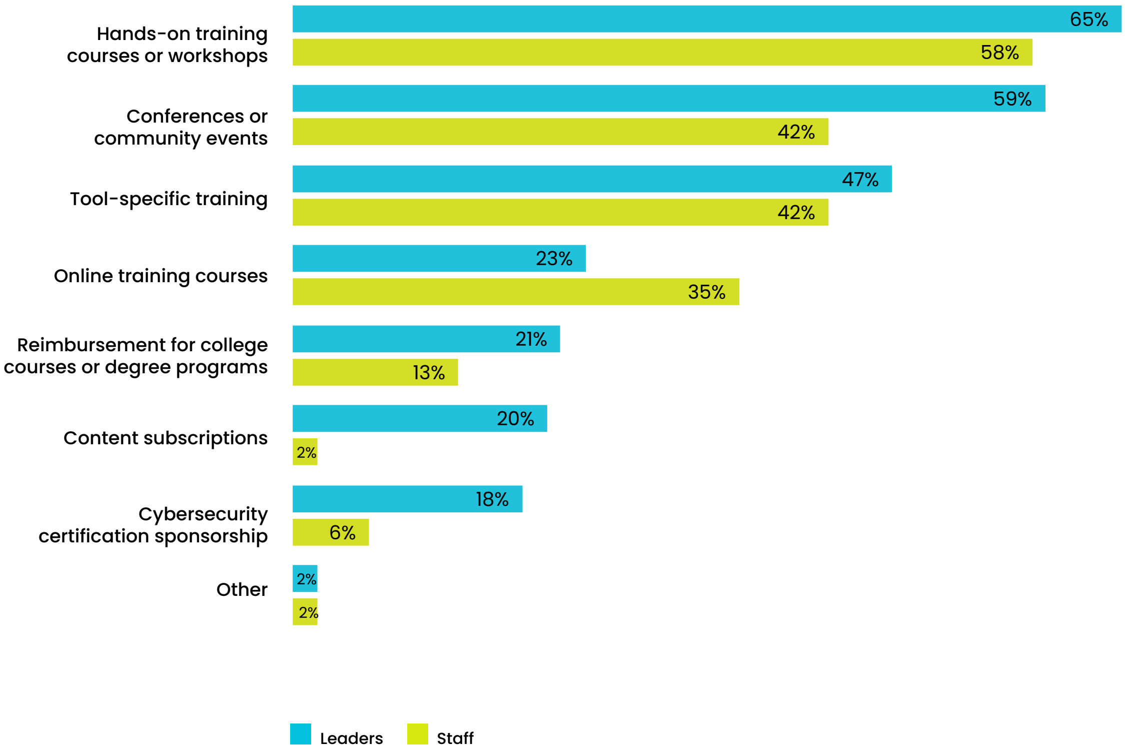


In the fast-paced, high-stress environment of the SOC, highly trained analysts are critical to ensuring effective SOC performance and continuity. Given that, you would think organized analyst training activities would be common. However, less than half of SOC leaders (47%) and staff (49%) say their organizations have a defined program for training and retaining analysts. For respondents who say training and retention of analysts are important, there is no clear consensus about what types of training or tools organizations should provide.

Figure 22.

If analyst training/retention is very important to your organization, what training or tools do you provide?

(More than one response permitted)

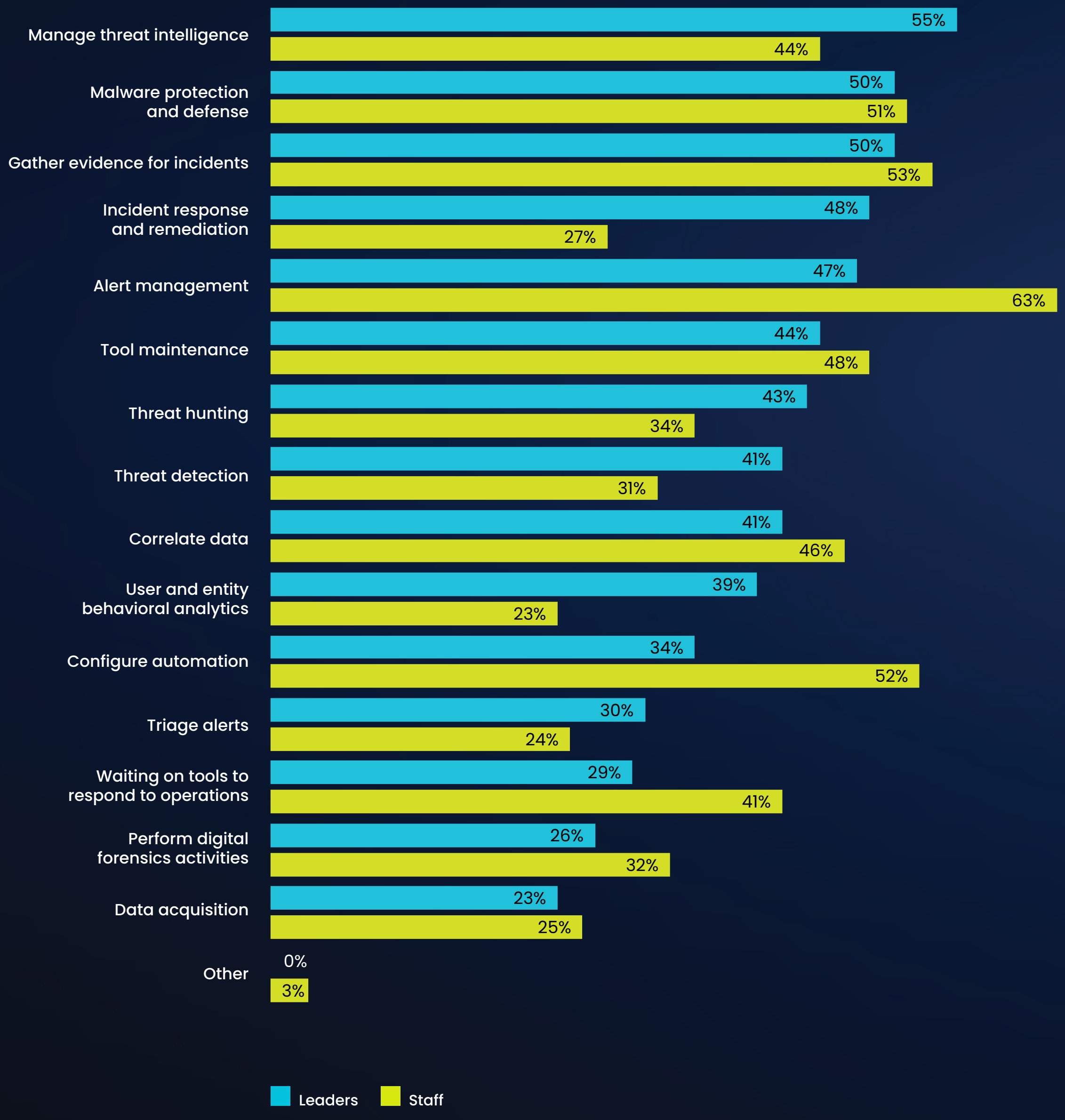


Efforts to improve SOC efficiency, which directly contribute to effectiveness, can take many forms. Leaders and staff have widely varying opinions of what tasks SOC analysts could perform more efficiently if they had the necessary support and tools.

Figure 23.

What tasks for your organization's security analysts would become more efficient and less time-consuming if support and tools were made available?

(Six responses permitted)

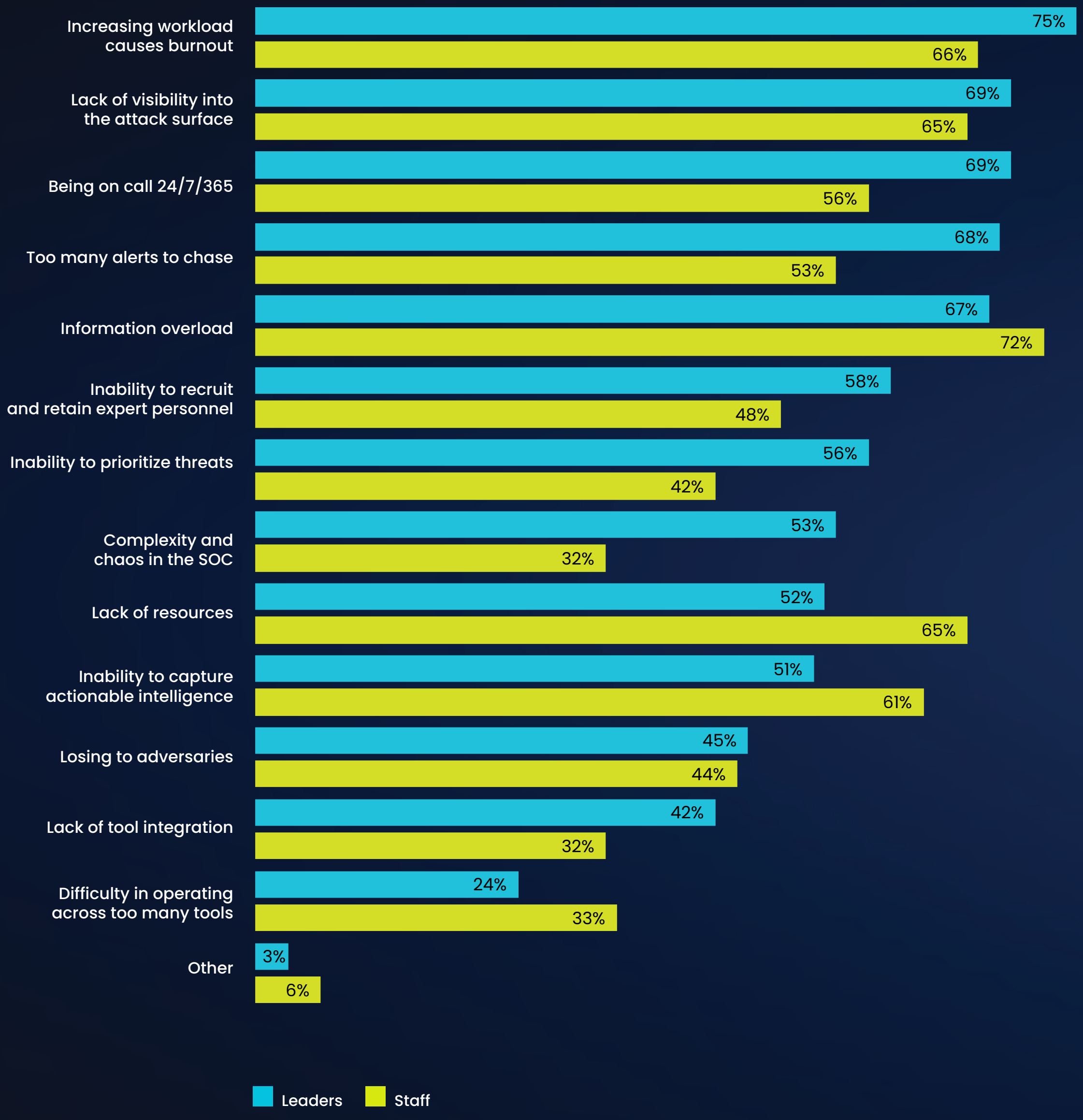


72% of all survey respondents say that working in a SOC is painful. Surprisingly, 78% of SOC leaders say SOC work is painful, but only 66% of staff share that sentiment, despite the fact that they're the ones who would be most adversely affected by painful working conditions. Even with that unexpected disparity in the opinions of the two groups, it is informative to examine which aspects of SOC work leaders and staff believe cause the greatest pain.

Figure 24.

What makes working in the SOC painful?

(More than one response permitted)

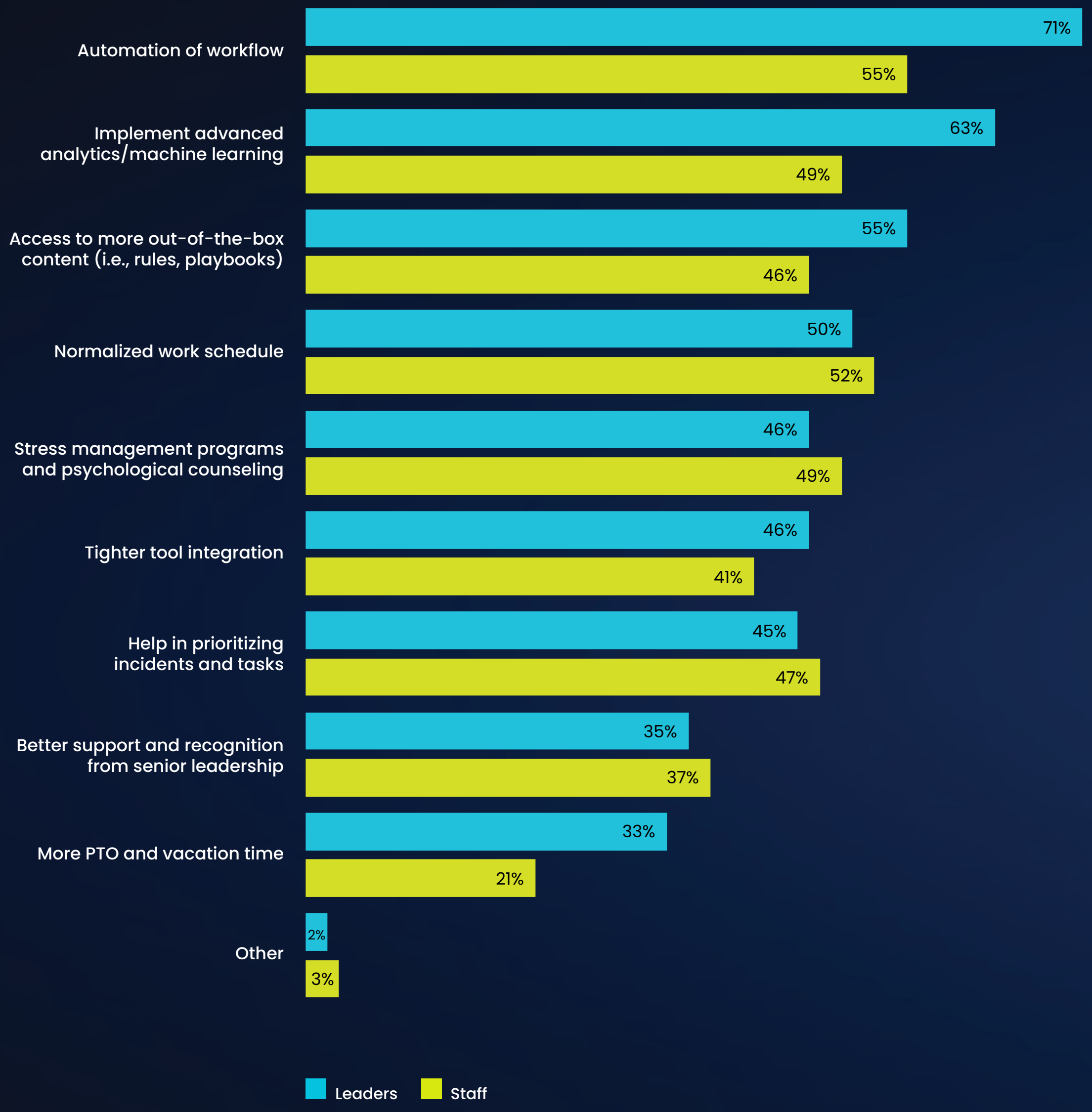


With more leaders than staff expressing the opinion that working in the SOC is painful, there also is disparity in the responses from the two groups about possible solutions to the problem, particularly when it comes to deploying technologies.

Figure 25.

What steps can be taken to alleviate SOC analysts' pain?

(More than one response permitted)



A Fresh Look at High- and Low-Performing SOCs

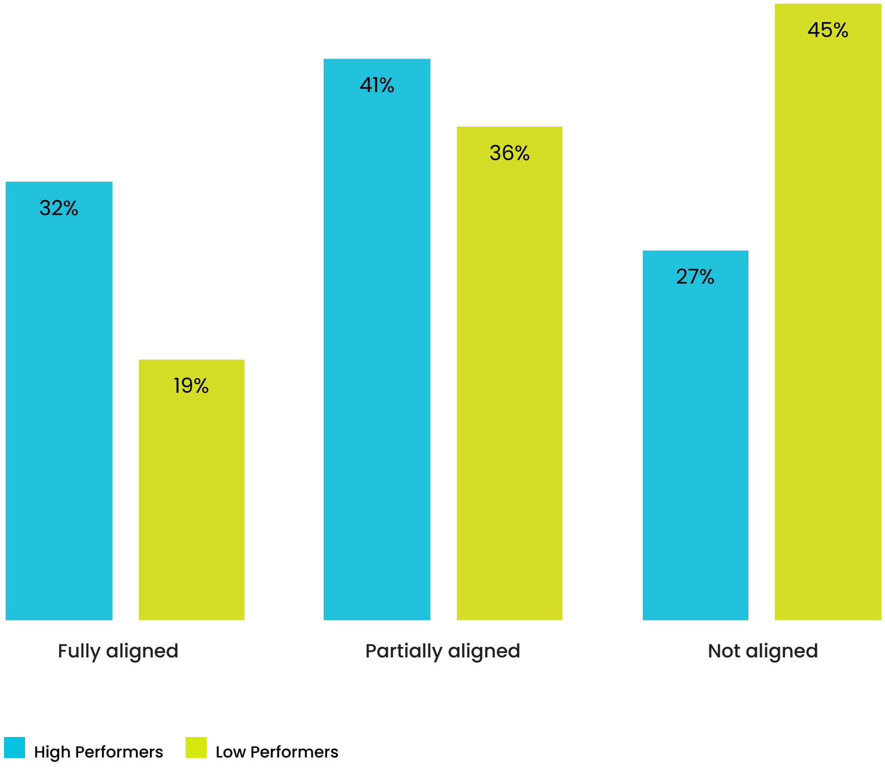
Finally, we will compare and contrast the survey results from respondents at high- and low-performing SOCs. This was the primary focus of the 2020 survey, and now we have the opportunity to once again look at several key questions and see how members of each group responded.

High-performing SOCs are those rated by survey respondents as a 9 or above on a 10-point scale measuring SOC effectiveness. In the 2021 survey, 21% of SOCs were classified as high performers. While defined by their effectiveness, even highly effective SOCs are not immune to the challenges faced by most SOCs, including lack of available talent, and turf or silo issues within their organizations. What separates high performers from their less fortunate counterparts is the degree to which these challenges affect them.

In Figure 26 you can see how respondents from high- and low-performing SOCs deviate from the overall survey results when it comes to their SOC's alignment with the needs of the business.

Figure 26.

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

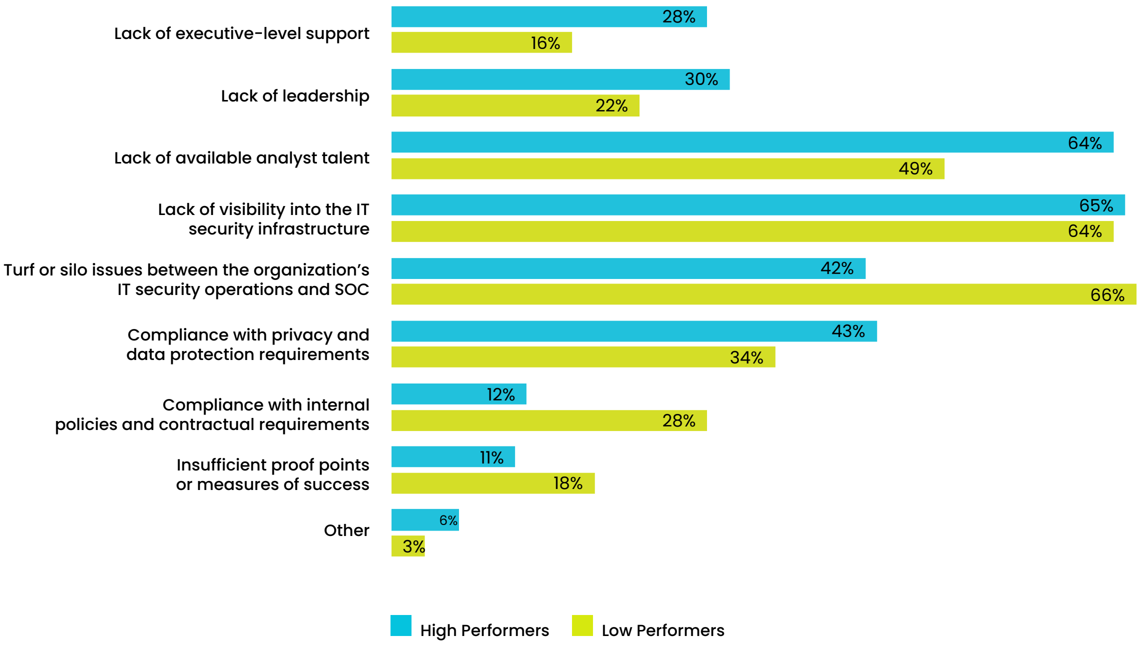


It's particularly interesting to note the areas where more respondents from high-performing SOCs say they face greater challenges than their counterparts. In particular, the lack of executive support and leadership are perceived to be more significant problems for high performers. Of course, those responses are all relative, since respondents from low-performing SOCs say they face more fundamental challenges, including turf or silo issues with IT security operations, compliance with policies and contract requirements, and lack of proof of success.

Figure 27.

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

(Three responses permitted)

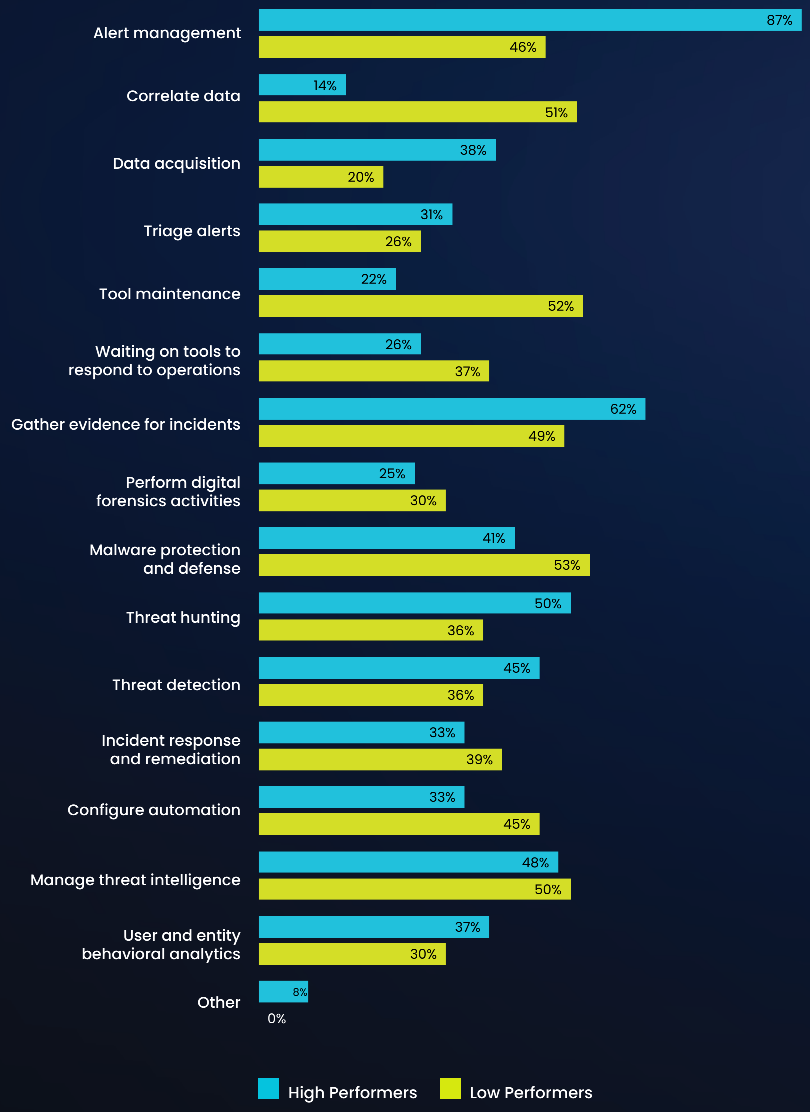


There are wide swings in the responses from members from each SOC type regarding which support and tools would increase efficiency and make work less time-consuming. 87% of respondents from high-performing SOCs, for example, cited alert management as their top priority, that's more than 30 percentage points above the overall survey results and almost twice the response from those in the low-performing group. The biggest gap in the other direction shows 51% of respondents from low-performing SOCs who say correlating data would be a major boon to performance, while only 14% from high-performing SOCs shared that perspective, indicating they already have the capability to do this.

Figure 28.

What tasks for your organization's security analysts would become more efficient and less time-consuming if support and tools were made available?

(Six responses permitted)



In one of the least surprising gaps between the two classes of SOCs, 54% of those from high-performing SOCs say it is very likely their organization will add new technologies or change what they currently use in an effort to improve SOC operations. Conversely, only 31% of respondents from low performers believe such innovation is very likely. Although the numbers are significantly closer when it comes to the somewhat likely and unlikely responses.

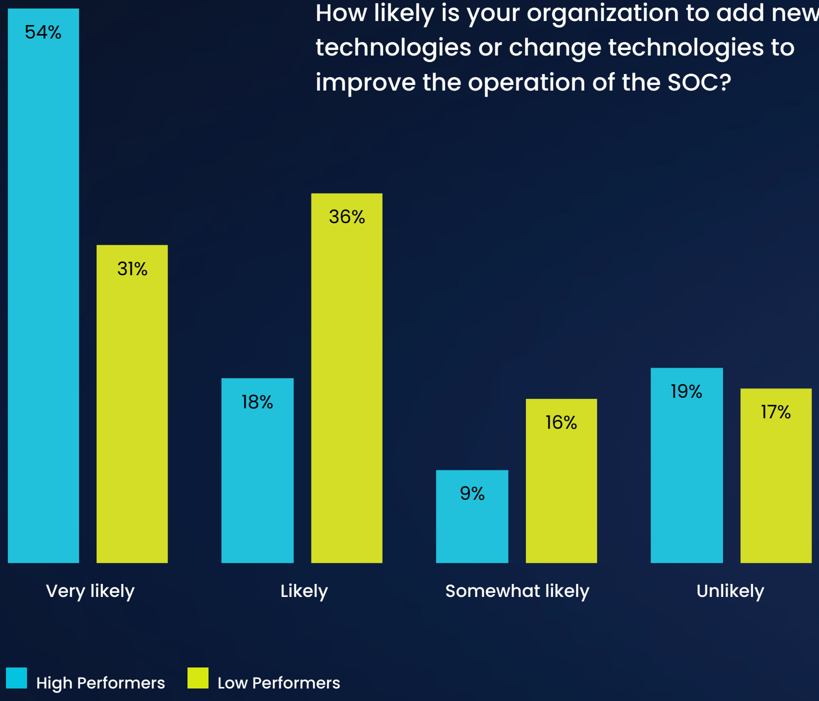


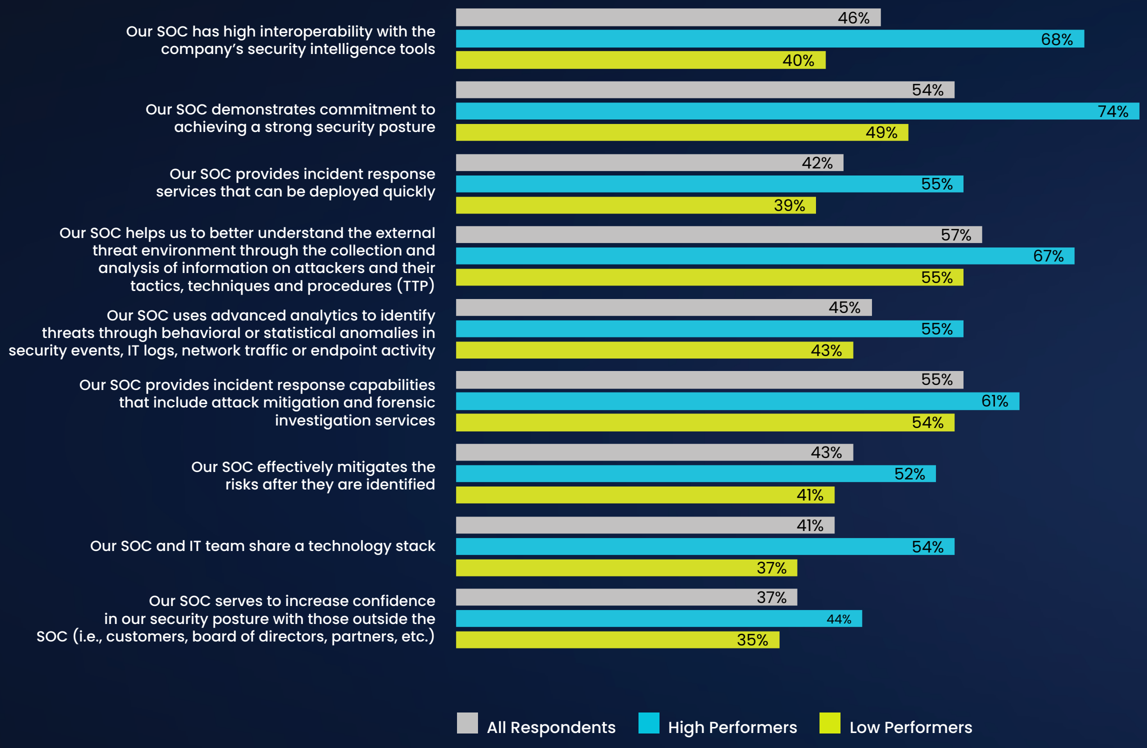
Figure 29.

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

Our final chart homes in on responses from those at high- and low-performing SOCs on a variety of SOC attributes, with those answers alongside the overall survey results to the same questions. The responses epitomize what separates high- and low-performing SOCs, with the high responders consistently showing much more positive perceptions about how well they execute in a number of key areas. The high performers also exceed the responses of the overall survey right across the board.

Figure 30.

Comparing results from respondents at high- and low-performing SOCs with those from all respondents to key questions about overall SOC performance (strongly agree and agree responses are combined).



PART 3.

SURVEY METHODS

The sampling frame is composed of 29,791 cybersecurity practitioners in organizations that have a SOC. As shown in Table 1, 1,150 respondents completed the survey. Screening removed 130 surveys. The final sample was 1,020 surveys resulting in a 3.4% response rate. The leader respondent final sample was 535 (3.5% response rate) and the staff final sample was 485 (3.4% response rate).

The leader respondent has approximately 9.7 years of employment experience of which 8.6 years have been in cybersecurity. The leader respondent has 4.6 years in their current position. The staff respondent has approximately 8.9 years of employment experience of which 8.3 years have been in cybersecurity. The staff respondent has 4.2 years in their current position.

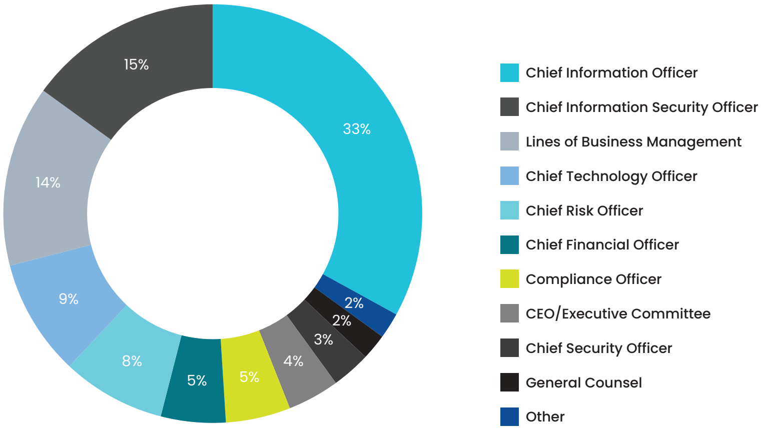
Table 1.

SAMPLE RESPONSE	LEADERS	STAFF
Total sampling frame	15,422	14,369
Total returns	602	548
Rejected or screened surveys	67	63
Final sample	535	485
Response rate	3.5%	3.4%

As shown in Pie Chart 1, 33% of leader respondents report to the chief information officer, 15% report to the chief information security officer, 14% report to the lines of business management and 9% of respondents indicated they report to the chief technology officer.

Pie Chart 1.

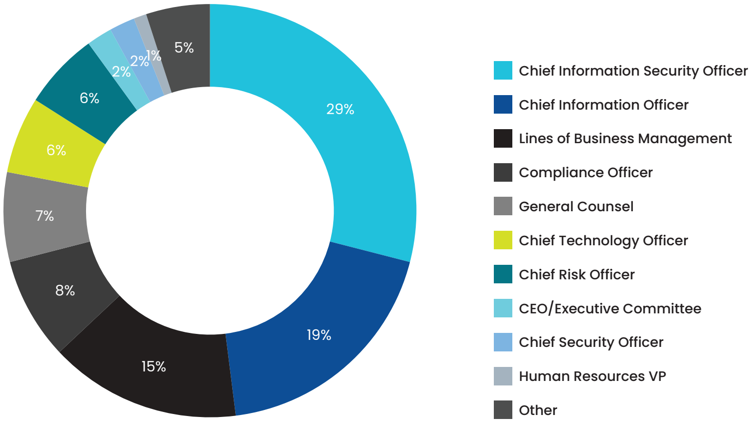
Primary person SOC leader or their superior reports to



As shown in Pie Chart 2, 29% of staff respondents report to the chief information security officer, 19% report to the chief information officer, 15% report to the lines of business management and 8% of respondents indicated they report to the compliance officer.

Pie Chart 2.

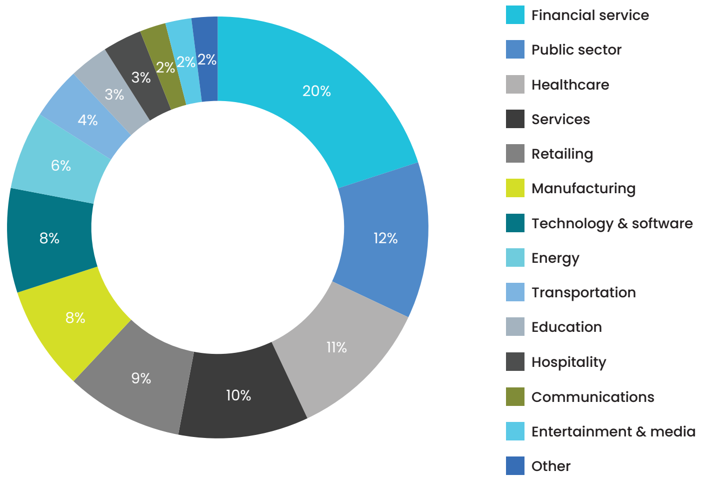
Primary person staff or staff's leader reports to



Pie Chart 3 reports the primary industry focus of leader respondents' organizations. This chart identifies financial services (20% 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% of respondents), healthcare (11% of respondents), and services (10% of respondents).

Pie Chart 3.

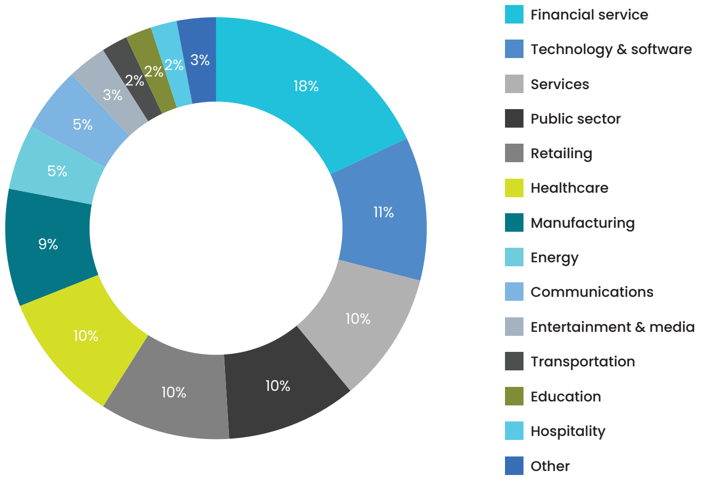
Primary industry focus of SOC leader respondent



Pie Chart 4 reports the primary industry focus of SOC staff respondents' organizations. This chart identifies financial services (18% of respondents) as the largest industry focus, which includes banking, investment management, insurance, brokerage, payments and credit cards. This is followed by technology and software (11%), services, public sector, retailing and healthcare (each at 10% of respondents).

Pie Chart 4.

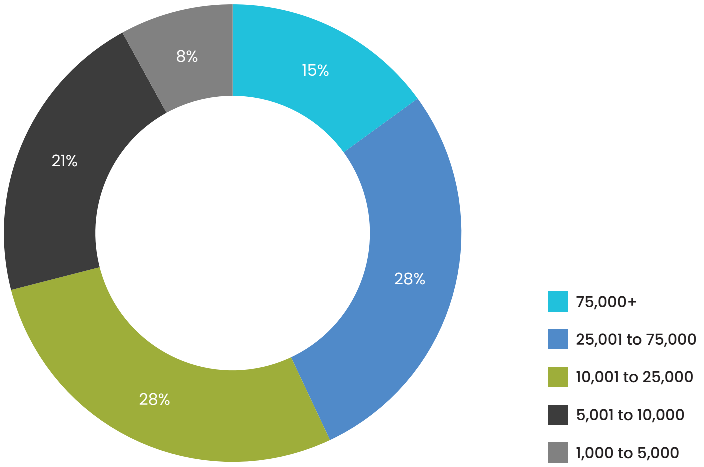
Primary industry focus of the staff respondent



According to Pie Chart 5, half of the leader respondents (51%) are from organizations with a global headcount of more than 10,000 employees.

Pie Chart 5.

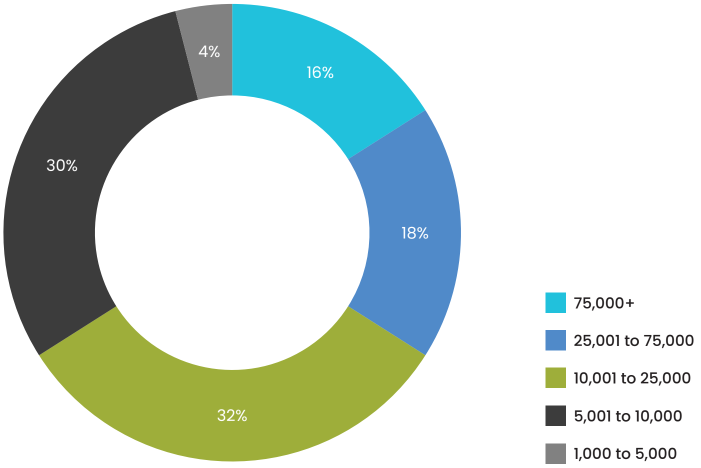
Worldwide headcount of the leader respondents' organization



According to Pie Chart 6, 70% of staff respondents are from organizations with a global headcount of more than 5,000 employees.

Pie Chart 6.

Worldwide headcount of the staff respondents' organization



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 Institute sent surveys to a representative sample of cybersecurity 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 is the only cloud-native logging and security analytics platform that releases the full potential of your data to empower bold, confident action. With unrivaled scale to collect all of your data without compromise, speed to give you immediate access and answers, and clarity to focus on the signals that matter most, Devo is your ally in protecting your organization today and tomorrow. Devo is headquartered in Cambridge, Mass.

Learn more at www.devo.com.