DEVO

2022 Devo SOC Performance Report™

SOC Leaders and Staff Are Still Not Aligned

Survey independently conducted by **Wakefield Research**

TABLE OF CONTENTS

PART 1.

PART 2.

PART 3.

PART 1.

INTRODUCTION

Each year, beginning in 2019, Devo has commissioned an independent survey of global professionals who manage and work in security operations centers. The results of the latest survey are featured in the *2022 Devo SOC Performance Report™*. Survey responses show that SOC staff members continue to experience considerable pain while performing their critically important — and highly stressful — work. The results indicate that SOC leaders and their teams continue to wrestle with several ongoing challenges, including:

- Alignment of SOC objectives and business needs
- Barriers to successful SOC operation
- Reasons for SOC ineffectiveness
- The ongoing pain of SOC workers and what's causing it
- SOC workers quitting or seriously considering it — and the difficulty of replacing them

The 2022 report also breaks down the survey results by presenting responses from SOC leaders and staff members side by side. The disparities in some key areas provide clear evidence that the issues facing organizations since the start of the global pandemic in early 2020 continue to affect SOC performance, including challenges in hiring and retaining SOC talent during the ongoing Great Resignation.

Our fourth annual *SOC Performance Report* is based on the results of a comprehensive, independent survey commissioned by Devo and conducted by Wakefield Research (www.wakefieldresearch.com) among 1,100 decision-makers and non-management staff from organizations with 1,000+ employees that operate a security operations center across the U.S., Canada, UK, France, Germany, Italy, and Australia/New Zealand between July 15th and August 2nd, 2022, using an email invitation and an online survey.

PART 2.

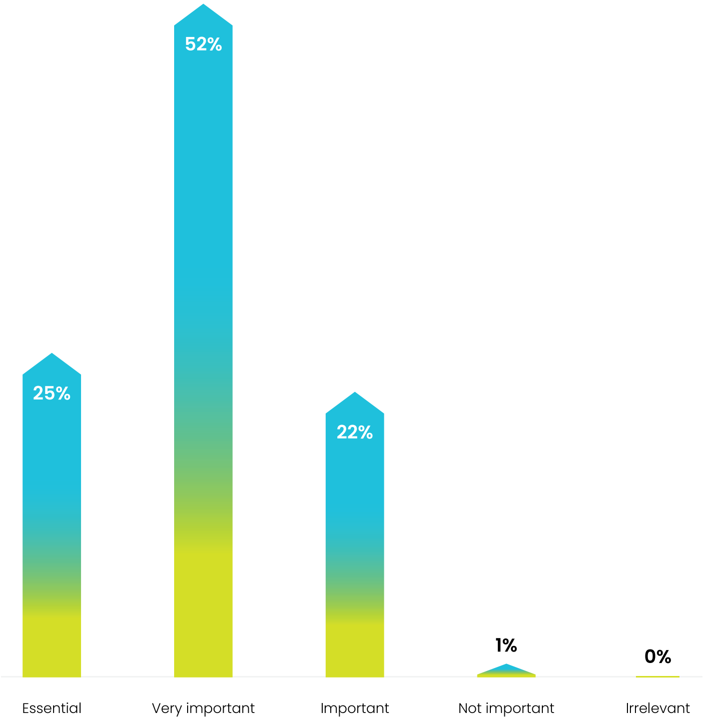
KEY FINDINGS — OVERALL RESULTS

Let’s Begin with the Good News

While this report will delve into a number of challenges and obstacles that are inhibiting success for many SOCs, which potentially compromises organizational security, the vast majority (99%) of respondents agree that the SOC plays a very important role for their organization.

Figure 1.

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



Virtually all professionals surveyed believe the SOC is significant to their organization’s cybersecurity strategy. In fact, 77% of respondents say their SOC is “very important” or “essential” to their organization. While not surprising, it’s reassuring to see, due to both the critical role SOCs play and — as this report will show — how painful many SOC staff members find their work.

The consensus in this year’s survey is that the SOC continues to play a pivotal role in cybersecurity programs. The 77% who rate the importance of their SOC highly represents a slight uptick from the 2021 survey, where 73% of respondents held their SOC in such high regard. This isn’t especially surprising since cybersecurity professionals who devote their careers to SOC work and leadership should be expected to feel that their efforts do make an important contribution.

Respondents believe their SOC is important, but do they also feel that it operates effectively?

Figure 2.

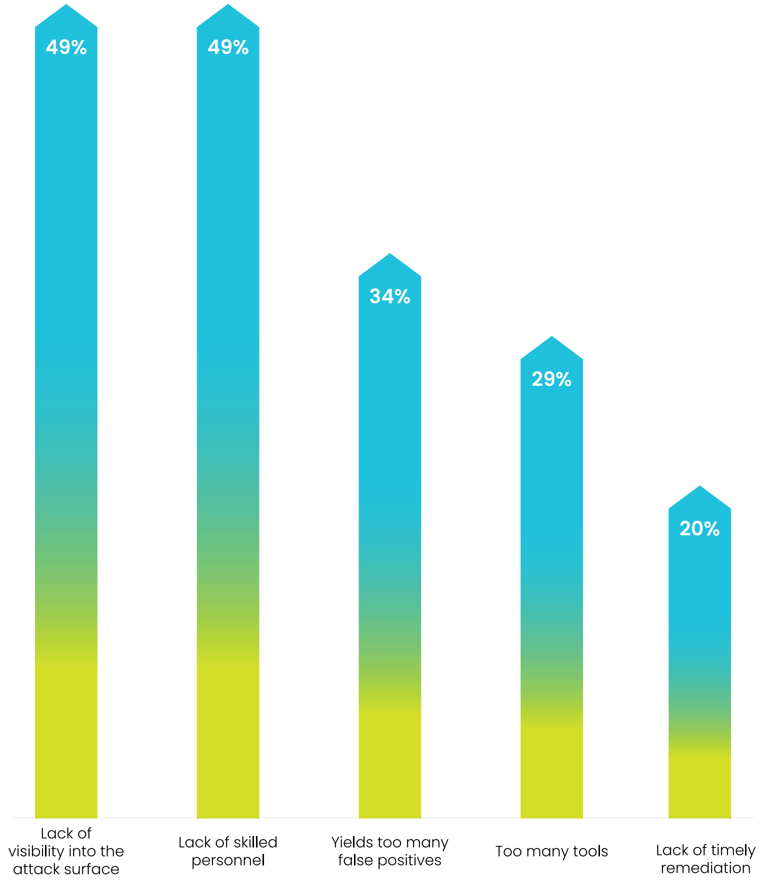
Using the following 10-point scale, please rate the effectiveness of your organization's SOC from 1 = Ineffective to 10 = Very effective.	
1	0%
2	0%
3	1%
4	2%
5	3%
6	5%
7	28%
8	37%
9	17%
10	7%

While a distinct minority of respondents rated their SOC as largely or somewhat ineffective (4 or below on the 10-point scale), it's worthwhile to look at the reasons for those ratings since even the most effective SOCs are not immune to at least occasional bouts with some of these challenges.

What's the Problem?

Figure 3.

What makes your organization's SOC ineffective? (More than one response permitted.)



"Lack of visibility" is cited as SOC challenge, which has been a recurring theme in all of the Devo SOC Performance Reports. And challenges hiring and retaining skilled personnel also is a frequent problem. One of the more interesting responses is "too many tools." We'll see later on how it's not the number of tools that make for an effective SOC but whether the team has the *right* tools for their environment and activities.

As with questions related to overall SOC effectiveness, some issues are prevalent for virtually all SOCs, as shown by the responses provided when respondents were asked how well their SOC performs in gathering evidence, investigating, and finding the source of threats.

Figure 4.

Rate the effectiveness of the ability of the SOC to gather evidence, investigate and find the source of threats.	
1 = Ineffective	0%
2	1%
3	3%
4	5%
5	6%
6	10%
7	20%
8	30%
9	17%
10 = Very effective	9%

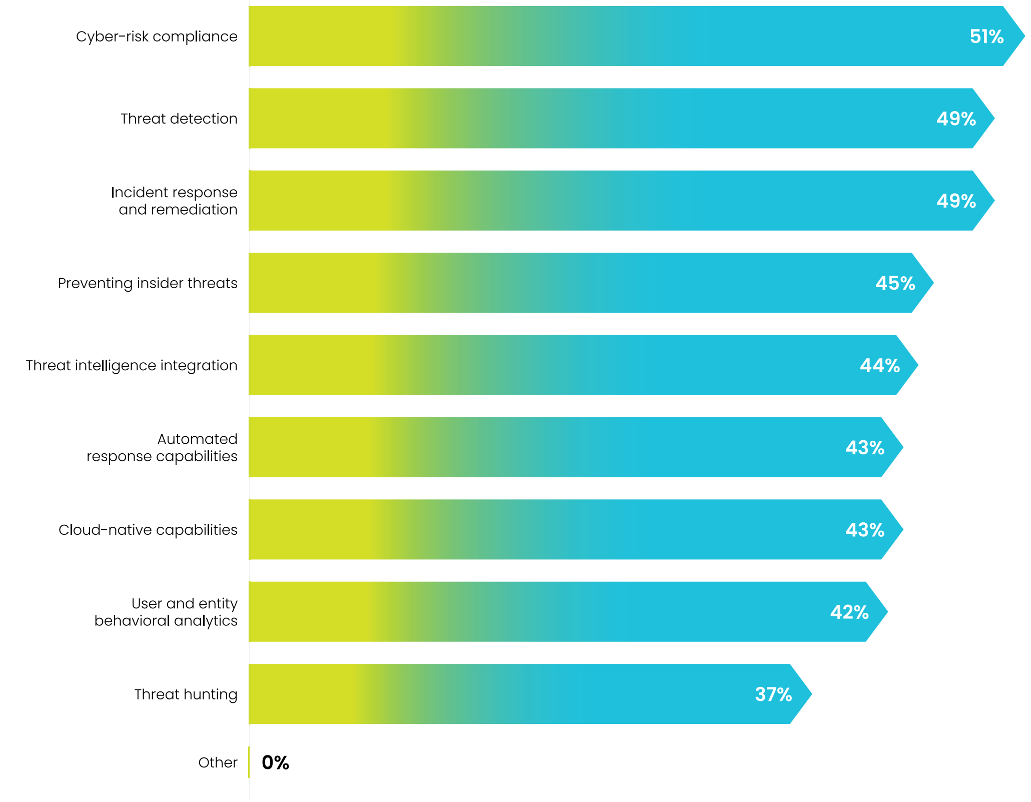
50% of respondents gave their SOC a score between 6 and 8 on a 10-point scale, putting half of all respondents in the "effective" category. 26% gave their SOC a rating of 9 or 10 for a "very effective" grade. But, the number of SOCs that truly excel at key performance metrics remains smaller than organizations and security professionals would prefer.

In section II, which compares and contrasts the responses of SOC leaders and staff on these same questions, you will see which issues hinder SOC success and where leaders and staff sometimes see things very differently.

Before delving into that topic, here are more level-setting questions and overall responses about SOC work.

Figure 5.

Which services within the SOC environment does your organization currently provide?

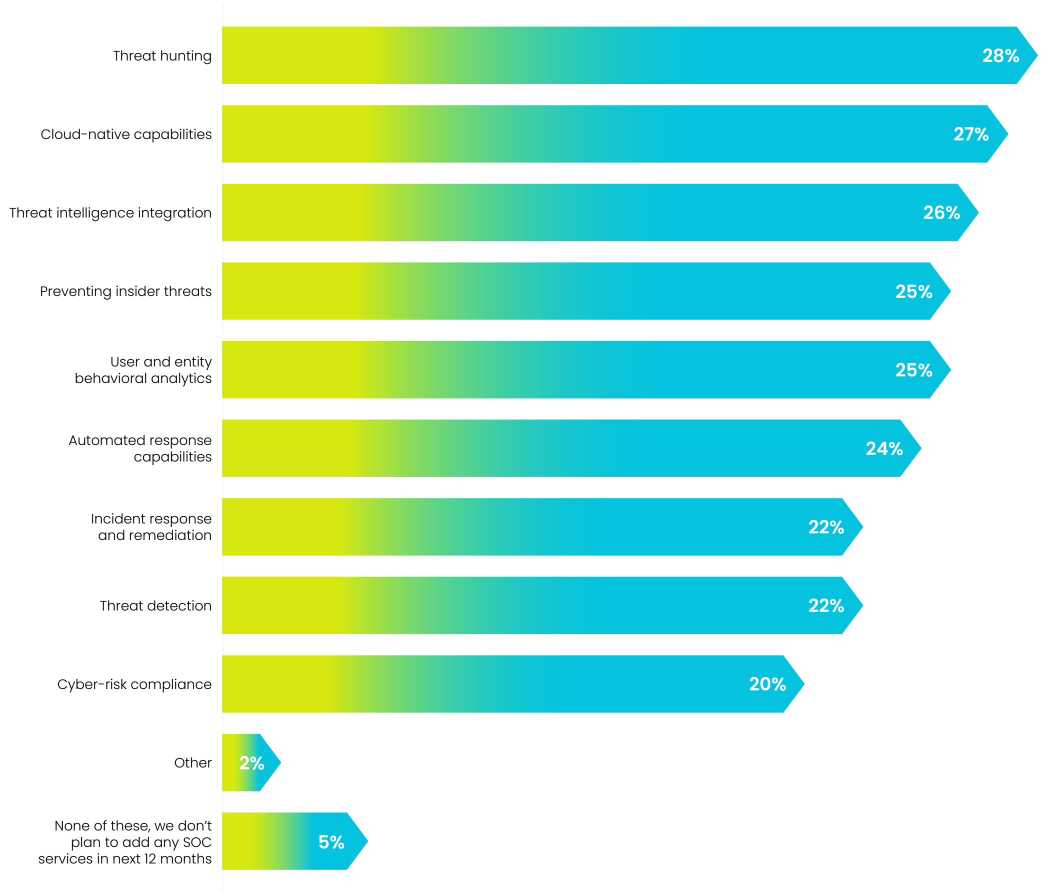


SOCs provide a variety of services, from cyber-risk compliance to threat hunting. The specific services a SOC provides reflect the various industries in which the respondents work and the needs of those organizations. But approximately half of the SOCs that survey respondents manage or work in provide most of the typical security services listed in the table above.

Because the cybersecurity threat landscape is always evolving, usually quite rapidly, the services SOCs perform also change often. The next question looks at the services respondents' SOCs do *not* perform today but are expected to add to their portfolios within the next year.

Figure 6.

Which SOC services, if any, does your organization plan to add in the next 12 months? (More than one response permitted.)

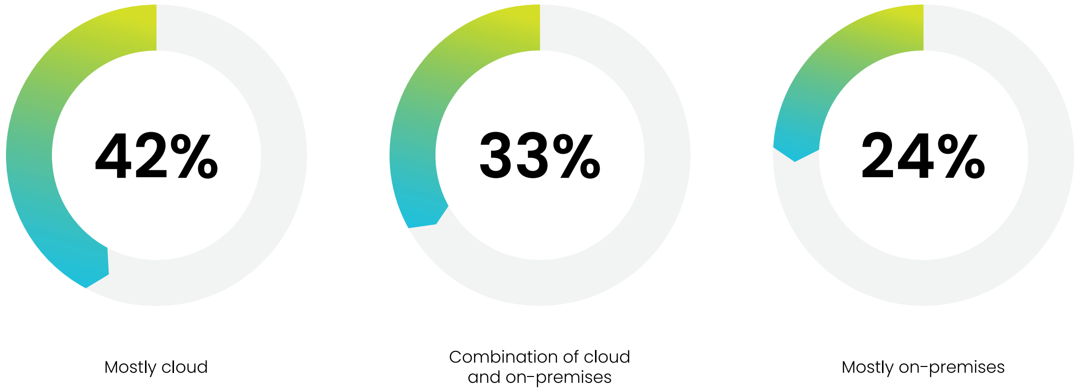


Only a small minority of respondents say their SOC doesn't plan to add any new services in the near future. This reinforces the perception that SOCs are dynamic environments — out of necessity. Due to the relentless nature of threat actors who are constantly trying to find and exploit vulnerabilities so they can access data for nefarious purposes, SOCs and their teams must always be ready to implement and become expert users of new services. Consistent with that approach, 95% of respondents expect their SOC will implement one or more new services within the next year. Services ranging from threat hunting (28%) to cyber-risk compliance (20%) all received a similar number of responses.

As SOCs continue to evolve, the IT infrastructure in which they operate also is changing. This year's survey shows that a growing majority of organizations use the cloud for some or all of their SOC work.

Figure 7.

What best defines the IT infrastructure that houses your SOC?



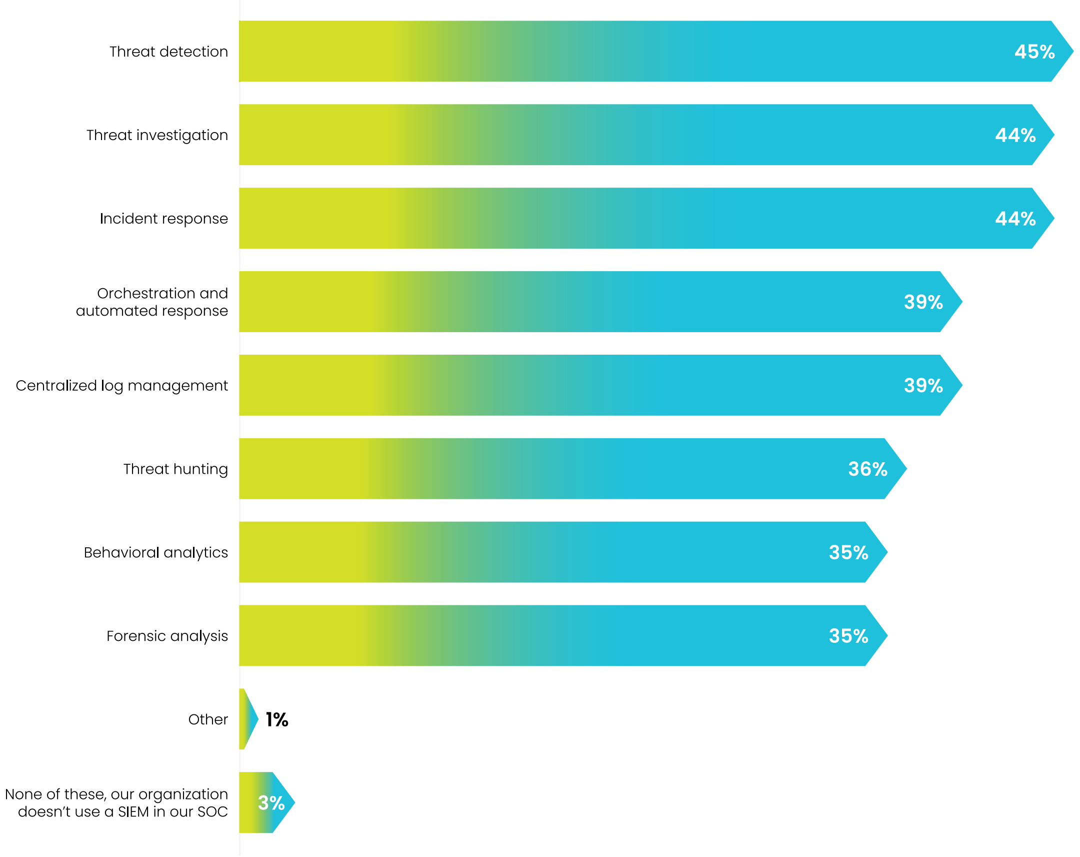
By comparison, the 2020 report showed only 60% of respondents said their SOC operated fully or partly in the cloud. This year, more than two full years after the start of the pandemic, which changed so much about how organizations operate, that figure has jumped to 75%. During that same period, the number of organizations identified as "mostly cloud" has risen to 42% from 34%. This is consistent with the continued migration of more IT and business operations technologies to the cloud to take advantage of its scalability and cost benefits.

The Role of the SIEM

For the vast majority (97%) of organizations represented in this survey, their SOC is driven by a security information and event management (SIEM) solution. The following questions deliver insights into the role of the SIEM at those organizations.

Figure 8.

What key functions, if any, does your organization's SIEM provide? (More than one response permitted.)



Detecting and investigating threats and responding to incidents are the top three SIEM functions used by more than 40% of respondents' organizations. Security orchestration and response (SOAR) is performed by nearly 40% of SIEMs, which shows the increasing synergy and convergence of SIEM and SOAR solutions throughout the industry.

Figure 9.

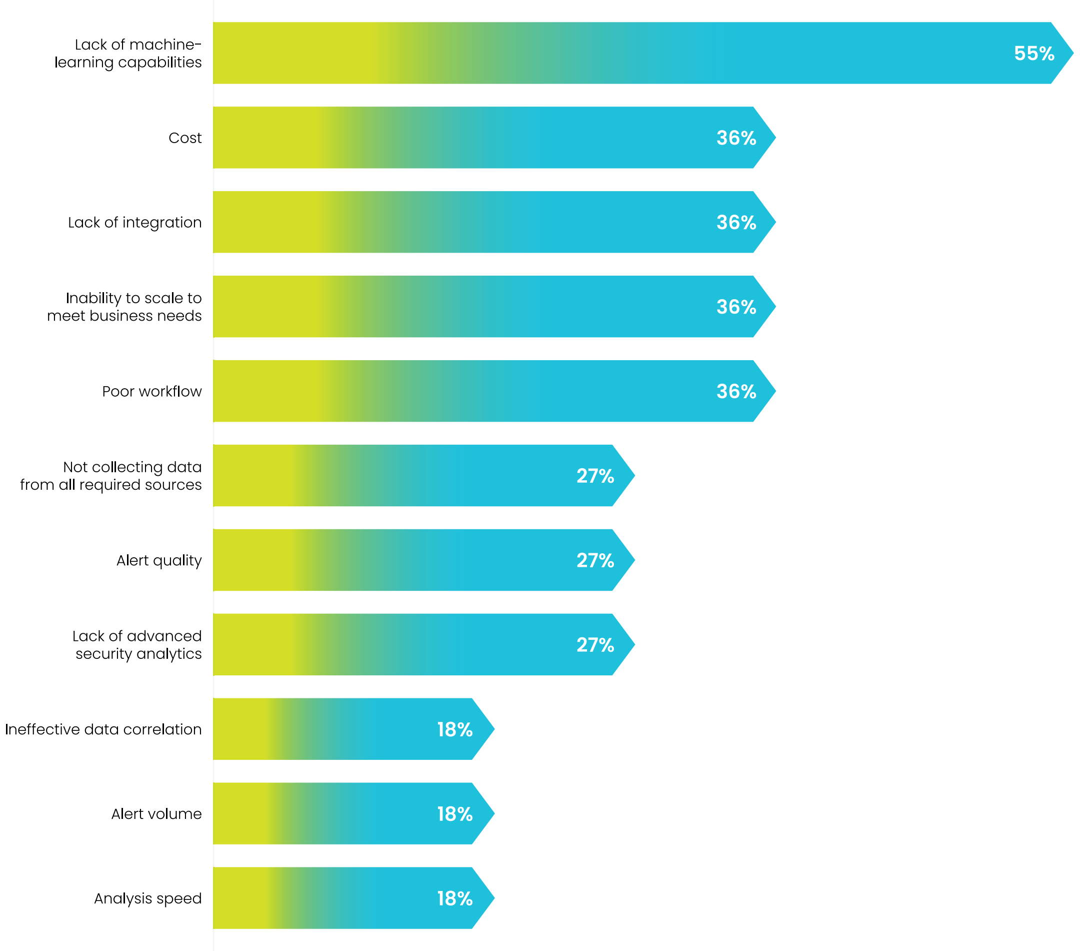
Rate the effectiveness of your organization's SIEM in providing the SOC with the data, alerts, context and evidence it requires.	
1 = Not effective	0%
2	0%
3	0%
4	1%
5	4%
6	6%
7	26%
8	38%
9	18%
10 = Very effective	7%

Nearly 90% of respondents rate their SIEM as "effective" to "very effective" with 25% rating it a 9 or 10 on the 10-point scale. These results, including the fact that just 3% of survey respondents work for organizations that have not deployed a SIEM, point to the significant and pivotal role this technology provides to the vast majority of SOCs.

Before leaving this topic, let's look at some of the concerns expressed by the 11% of respondents who rated their SIEM a 6 or lower.

Figure 10.

Why is your SIEM not effective? (More than one response permitted.)



Since respondents to this question are describing the SIEM their organization uses, as opposed to expressing their opinions about SIEMs in general, it's reasonable to say that many of the perceived shortcomings are specific to their SIEM. However, the frustrations these respondents are experiencing with their SIEMs significantly impede the smooth and effective operation of the SOC.

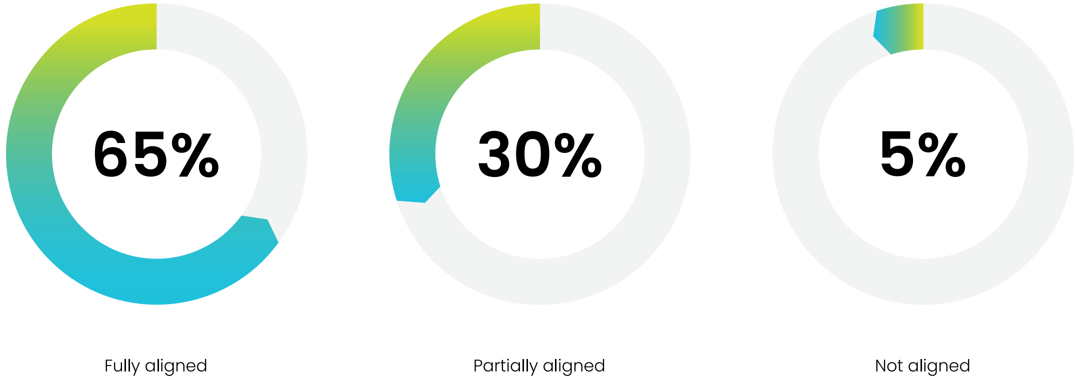
Machine learning is quickly becoming a standard feature of modern SIEMs. The same is true of the ability to scale, integrate with other SOC solutions, and, in particular, the ability to collect data from all required sources. In fact, a SIEM that cannot collect all the data the SOC team needs to protect is a liability. Finally, SIEMs that lack advanced security analytics, cited as an issue by 27% of respondents, are truly behind the curve of what a truly modern and effective SIEM can provide to SOCs.

The Question of SOC Alignment

Later, this report will delve into issues related to areas where SOC leaders and staff are not aligned. But first, let's look at that issue based on the overall survey results.

Figure 11.

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

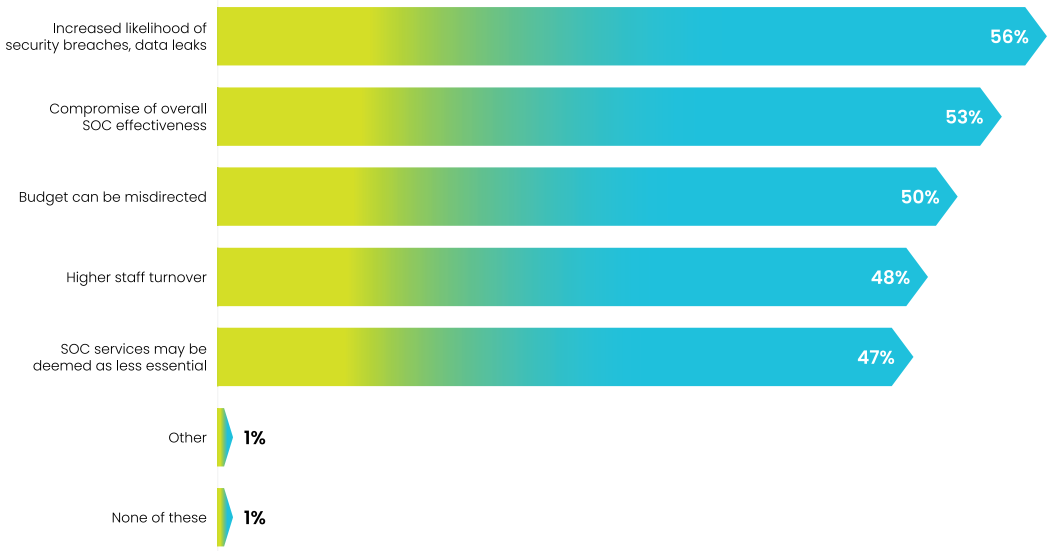


This important metric is a very positive sign for SOCs. It shows that organizations have been taking action to improve how well the SOC is aligned with business needs. Unfortunately, progress toward greater alignment of the SOC with the organization continues to be a major challenge for low-performing SOCs, which we'll see when we examine the gaps between high- and low-performing SOCs.

What are the consequences when SOCs fail to align with business goals? Respondents identify problems they believe could likely develop in their organizations if the SOC and business goals are misaligned.

Figure 12.

Which of the following consequences, if any, would your organization likely face if SOC objectives were not fully aligned with its business needs? (More than one response permitted.)

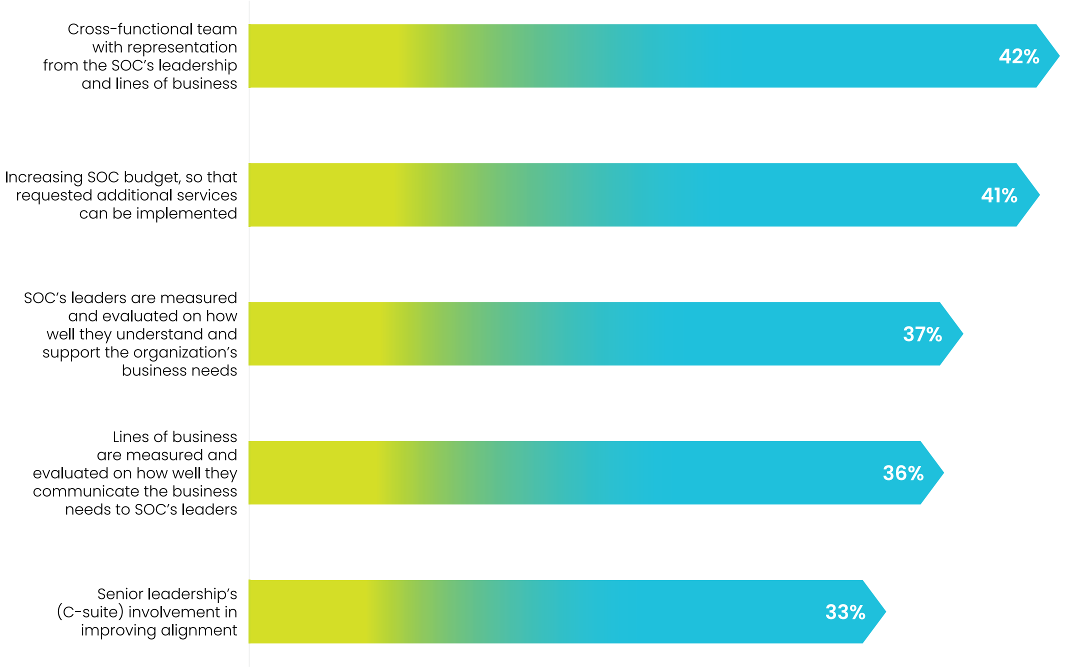


While this year's survey results show a very positive response to questions of SOC alignment with business goals, such agreement is often tenuous and can never be taken for granted. Achieving and then keeping the SOC in alignment with the organization's business goals requires ongoing effort and commitment.

To show that survey respondents are aware of the often-fragile nature of this key alignment, we asked them about efforts that could be undertaken to make this partnership even stronger.

Figure 13.

What do you think would improve alignment of your SOC objectives and business needs? (Up to two responses permitted.)

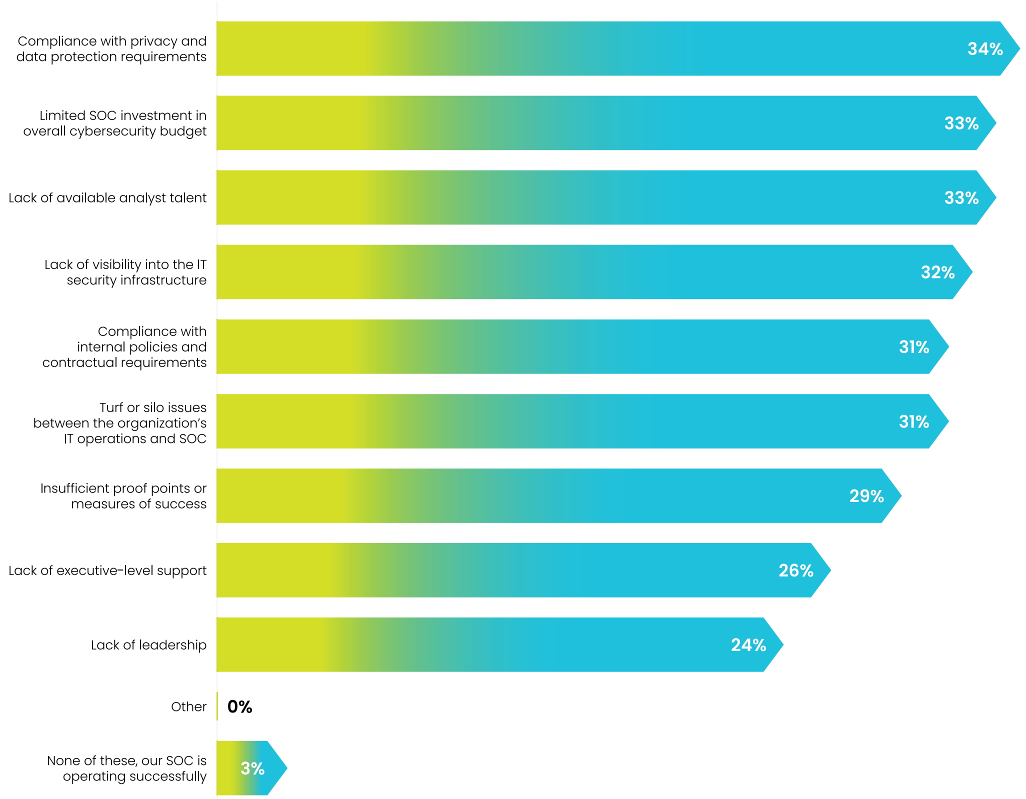


The responses were spread relatively evenly among the possible responses. The top response, not surprisingly, involved establishing a closer working relationship between management from the SOC and lines of business. And right behind it, also not surprisingly, was a call for a larger SOC budget to pay for the implementation of additional services.

Now let's delve a bit deeper into what hampers SOC teams from being successful.

Figure 14.

What do you see as the main barriers to successfully operating the SOC? (Up to three responses permitted.)



Starting at the bottom, only 3% of respondents believe their SOC has no barriers preventing it from doing its job as intended. That sounds about right, given the many challenges we have consistently seen in the surveys for prior editions of this report.

Insufficient budgets. Challenges in complying with privacy requirements and with internal and contractual requirements. Lack of leadership and insufficient executive support. All of these are serious challenges that can undermine the efforts of most SOCs. But let's home in on a few of these challenges that are particularly difficult to overcome.

First, during this era of "quiet quitting" amidst a continuing wave of resignations that began early in the pandemic, leadership is more valuable than ever before in terms of motivating, coaching and supporting teams. That's especially true in the pressure-packed environment of a SOC.

From a technical perspective, nearly one-third of respondents cited lack of visibility into the IT security infrastructure as a potential barrier to success. Visibility is the most crucial basic ingredient of cybersecurity success. If SOC analysts can't see all the data and infrastructure they are responsible for protecting, the likelihood of them successfully achieving their goals is slim. Other areas, such as turf and silo issues, insufficient budgets, and compliance with data privacy and contractual obligations are common issues for most SOCs. But it all starts with having the right people — and enough of them — and giving them the tools they need to do their jobs.

The next two questions delve into the effectiveness of SOC leaders. When we look at survey responses from leaders and staff, it will shed even more light on that topic.

Figure 15.

Rate how well SOC leaders in your organization communicate the SOC's strategy to staff members.	
1 = Not well at all	0%
2	1%
3	2%
4	5%
5	6%
6	11%
7	21%
8	26%
9	18%
10 = Exceptionally well	9%

The vast majority of respondents — 74% — said their organization's SOC leaders communicate strategy very well to exceptionally well. That's a positive sign both in terms of understanding the job of protecting the organization's data, and operating an efficient SOC where staff members feel informed about the strategy they are expected to follow. The organizations where leaders' ability to communicate the SOC's strategy was rated six or below have their work cut out for them.

On the flip side of leaders' ability to communicate is how well they listen to the people who work for them, who make or break a SOC's performance.

Figure 16.

Rate how well SOC leaders listen to and understand the needs and priorities of SOC staff.	
1 = Not well at all	0%
2	1%
3	2%
4	5%
5	6%
6	9%
7	22%
8	30%
9	16%
10 = Exceptionally well	9%

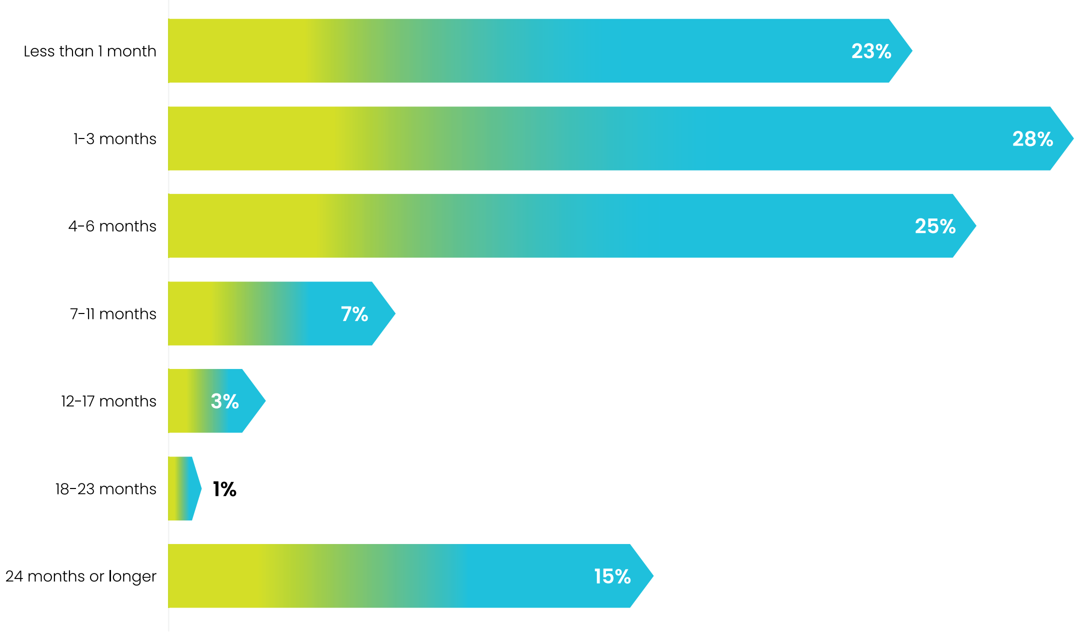
As with the previous question, most respondents — 77% — believe their SOC leaders are good listeners and comprehend what SOC staff need. The 23% of respondents who rate their leaders a five or below on the 10-point scale in this important skill are likely to face more challenges than most SOCs. When we look at the responses to these same questions according to the separate perspectives of leaders and staff, we will see what degree of agreement there is (or isn't) when leaders are evaluating their own performance and staff are giving their thoughts about their bosses.

Good Help Is Hard to Find (and Important to Keep)

In several of the previous questions and responses, the issues related to hiring and retaining employees have been a factor to some extent. Given the significant changes in how people work since the start of the pandemic in 2020 — working from home, changing jobs due to burnout or other areas of dissatisfaction, etc. — it should come as no surprise that it can take time to fill vacant positions with well-qualified hires who fit into an organization's payroll structure. But as you will see, in some cases it's very surprising just how much of an issue this can be for SOCs. This survey question was posed only to SOC leaders.

Figure 17.

How long is the typical hiring process for SOC staff, from the initial job posting to the first day of work?

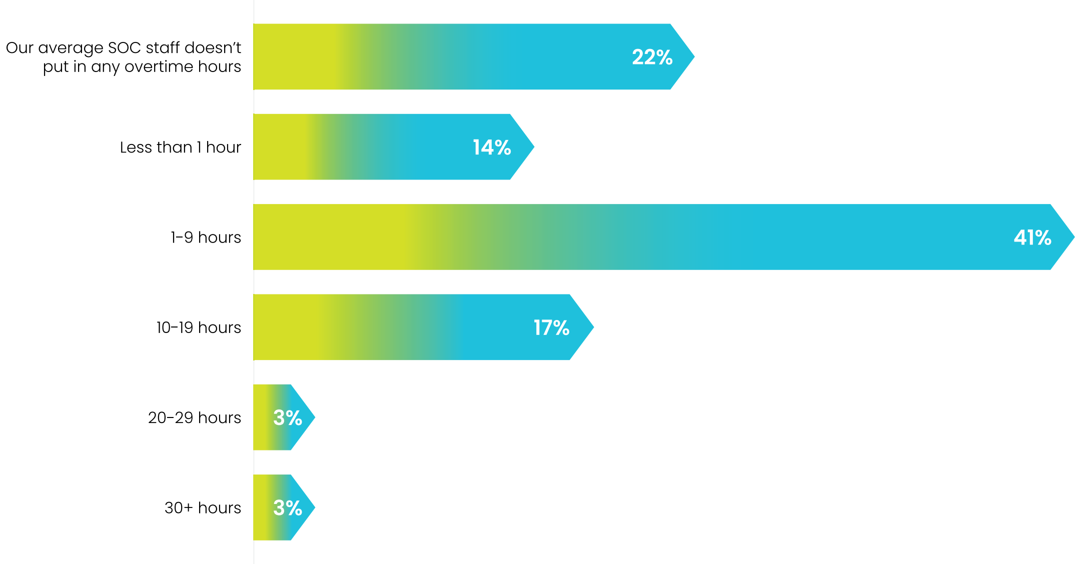


Less than one-quarter of respondents say they can typically fill a SOC vacancy in less than a month. Things generally go downhill from there. The average time respondents said it takes to fill a position is *seven months*, with 15% percent of SOC leaders saying it takes two years or longer to fill a SOC role!

If it takes months to fill a SOC staff position, guess what effect that has on the people who already work there? More work than they can usually handle. This leads right into our next question for SOC leaders.

Figure 18.

What is the number of hours your average SOC staff member spends in a typical week working overtime (beyond standard 40 hours)?

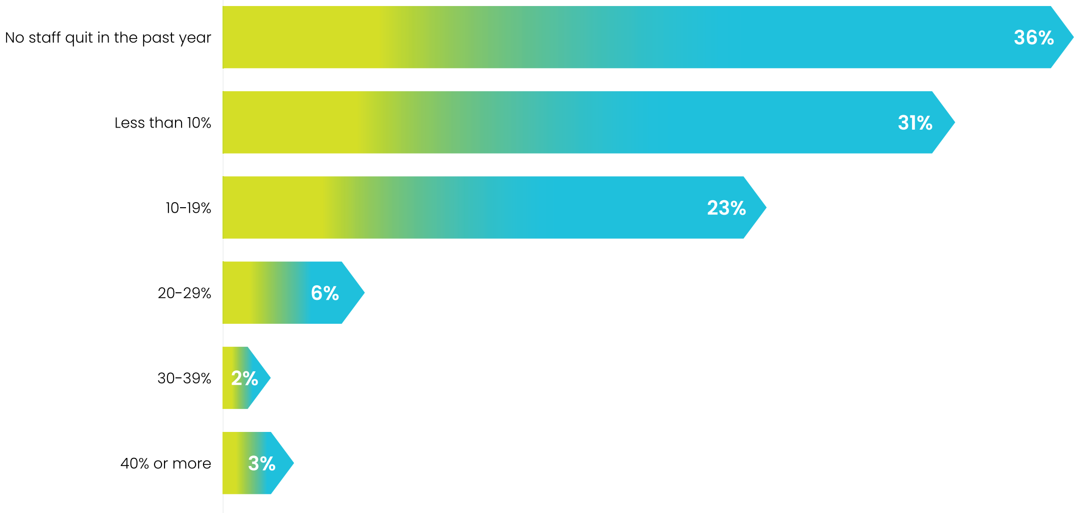


First, a bit of good news: 22% of SOC leaders say their teams do not typically work any overtime. But what about the rest of them? That's where the news becomes significantly "not good." While 14% of leaders say their teams average less than an hour of OT per week, a whopping 41% say their teams work up to nine hours of overtime per week. That's essentially an extra day of work for each typical five-day work week! At the extreme end, 3% of respondents say their teams average between 20 and 29 overtime hours per week, which is another half-week or more. And, worst of all, 3% say their staffs work 30 or more overtime hours each week. That puts the issues of the Great Resignation, quiet quitting and other hiring and retention issues under a harsh light. It's no wonder SOC workers are feeling the pain, as we'll see.

Speaking of resignations, the next question gets to the heart of that issue for SOC leaders.

Figure 19.

In the past year, what percentage of your SOC staff have quit?



Again, beginning with the positive news, 36% of SOC leaders say no one on their staff resigned in the past year. This is great news and seems to indicate those are organizations where the SOC and its people are treated well and managed with care. But what about the other 64% of leaders and their SOCs that have lost people?

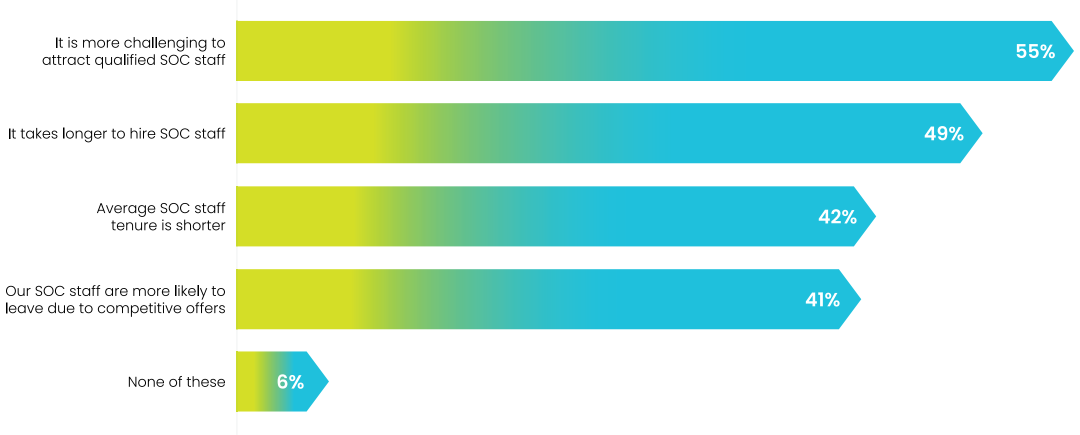
The average number of staffers lost by SOCs that reported some number of resignations is 12. In a very large SOC, that might not be a big percentage. But for most organizations, losing 12 SOC professionals in a year could be devastating to the organization's cybersecurity and the physical and mental well-being of the remaining staff and leaders.

On the more positive end of the curve (relatively speaking), 31% say they lost less than 10% of their staff in the last year. As for the rest, things just get worse as the resignations pile up. 23% of leaders say they lost up to 19% of their staff all the way to 3% who lost 40% or more of their SOC teams! In a year!!

And while losing staff is obviously an obstacle to running a successful SOC, it's not the only one.

Figure 20.

Over the past 2 years, what SOC staff challenges has your organization encountered?



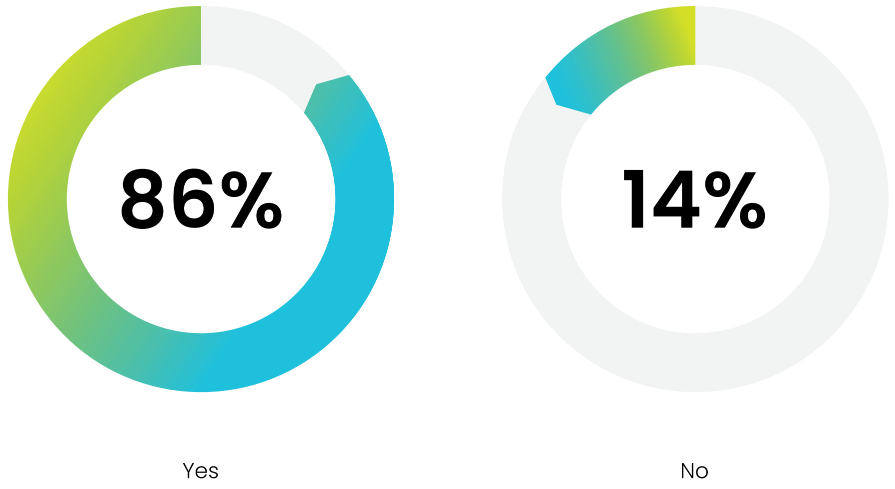
Only 6% of leaders say their SOC hasn't experienced any of the listed challenges. As for the other 94%? The news is not quite as good.

A whopping 55% say they have had difficulty over the past couple of years hiring qualified people. And even when they hire them, 42% say the average tenure of their staffers is shrinking compared to the past. And in a time of more jobs than qualified people to fill them, 41% of leaders say they are likely to lose SOC staffers to better compensation from competitors.

One way to retain skilled SOC analysts is to make it an organizational priority to train and keep them.

Figure 21.

Does your organization have a defined program to train/retain SOC staff?



Clearly SOC leaders and their organizations realize the value of providing proper training to their analysts and implementing programs to retain them. With work as sensitive and important as cybersecurity, it's unfathomable that 14% of respondents say their organization doesn't have any sort of training or retention program for analysts.

Now let's see exactly how survey respondents rate the importance of programs designed to prepare SOC analysts for their jobs and make them want to stay with the organization.

Figure 22.

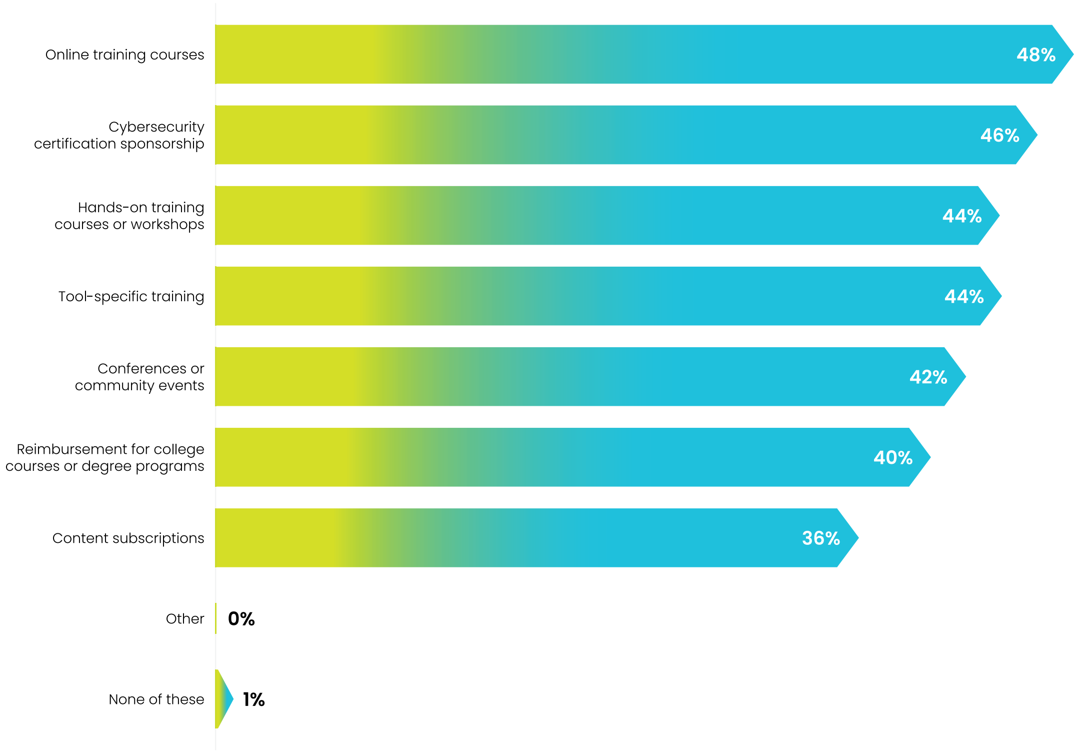
Rate the importance of staff training/retention for your organization.

1 = Not important	0%
2	0%
3	0%
4	1%
5	1%
6	4%
7	21%
8	36%
9	21%
10 = Extremely important	15%

It's good to see that no SOC leaders said training and retaining staff is of minimal or no importance to their organization. Most of the respondents (93%) rated these programs as a 7 or above on a 10-point scale, which reflects their belief that these efforts are very to extremely important to operating a successful SOC. Next, we'll take a look at how they do it.

Figure 23.

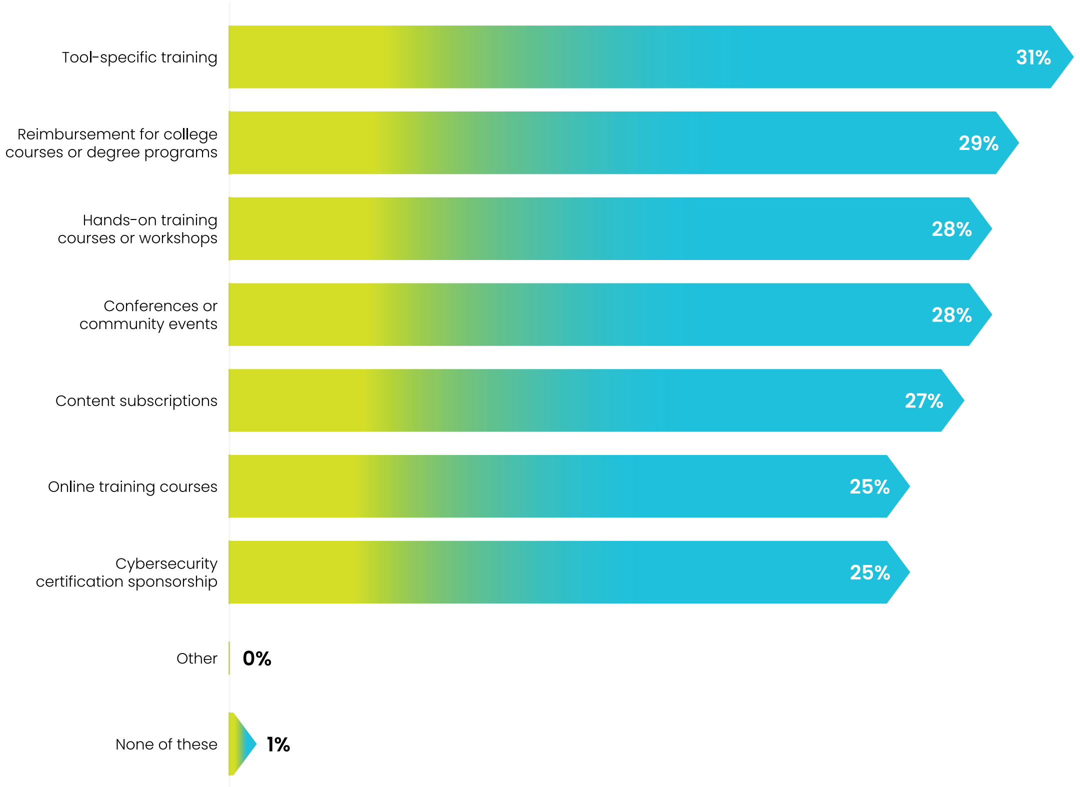
What training or tools does your organization currently provide?



Just 1% of respondents offer no training or tools or any type. That may be inexplicable, but 99% of SOCs do provide such essential offerings.

Figure 24.

What training or tools would you like your organization to offer?



The responses to this question are tightly clustered between 25% and 31%. At the top of the list may be the most obvious of all education options: tool-specific training. After all, if an organization makes a significant investment in software or other tools intended to improve the performance of their SOC, why wouldn't they also provide appropriate training, so SOC analysts are able to get the most out of those tools as they work to protect the organization?

In addition to directly work-related offerings, nearly 30% of respondents say their organization provides reimbursement for higher education. This is a valuable benefit for employees while also helping to create a pipeline of well-educated individuals who are already familiar with the organization who will be better prepared to step into a SOC leadership role or a management position in another department. Organizations invest in their own success by investing in their people.

Pain Remains a Sore Spot for Most SOCs

Based on the survey questions and responses we've looked at thus far, a few factors are in play. First, many SOCs appear to be trying to address the challenges that typically afflict SOCs and the people who work there. It's difficult work. There is almost constant pressure. Failing to succeed can have catastrophic consequences on the organization. But despite progress and some positive responses throughout the report, there is no question that SOC work is painful, and it takes a toll on those who perform it. The next group of questions specifically addresses this issue.

Figure 25.

Rate the "pain" your organization's SOC personnel experience in meeting their daily job requirement.	
1 = Low pain	2%
2	2%
3	8%
4	7%
5	9%
6	11%
7	23%
8	30%
9	7%
10 = Very painful	2%

These responses present themselves in a classic bell curve. Only 4% of respondents rate the pain of their SOC team at a very low 1 or 2 on the 10-point scale. On the other end, just 9% believe that working in their SOC is very painful.

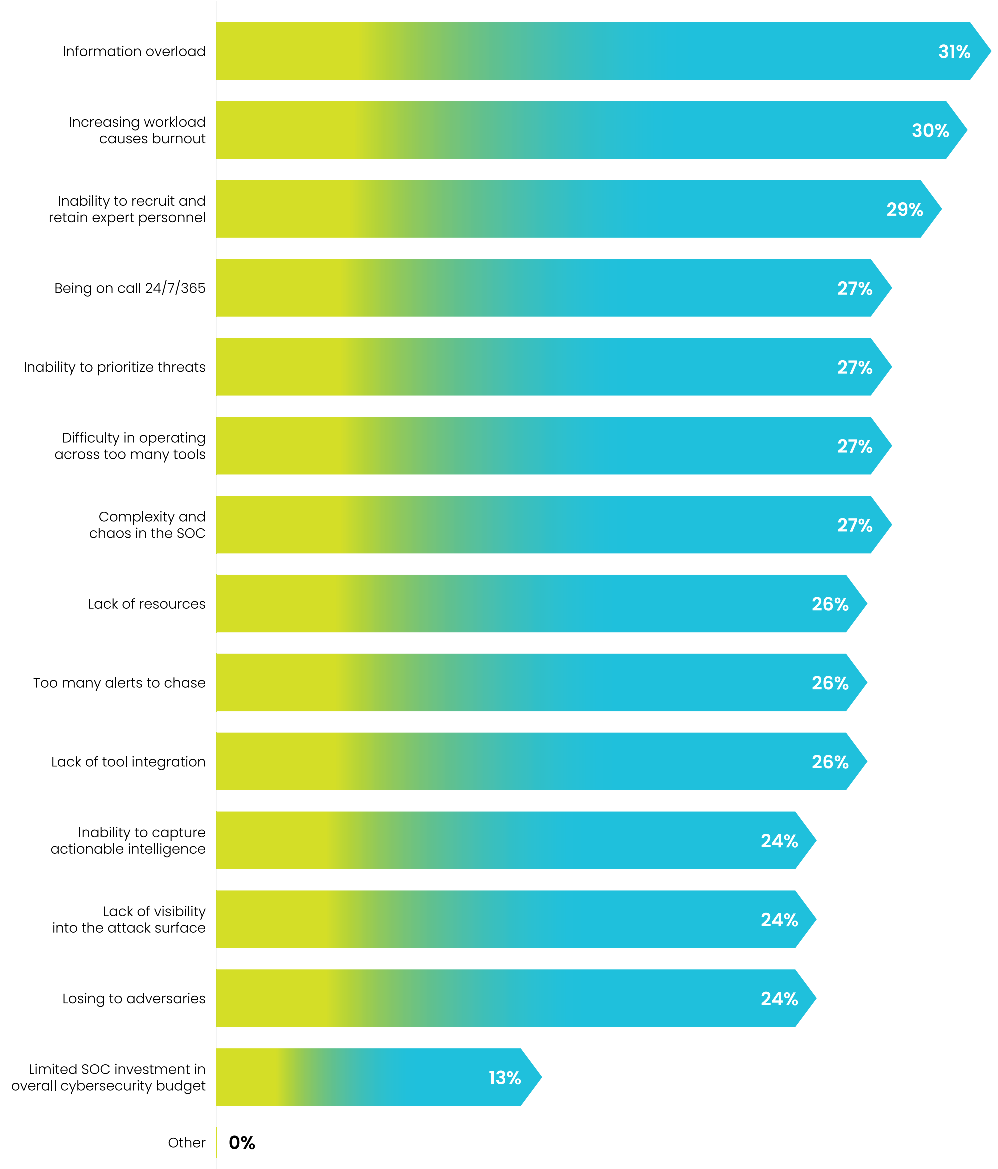
The real story is in the 71% of respondents who rate the pain of SOC staffers at 6 through 9 out of 10. That shows a very high level of discomfort among workers in those SOCs. While that's certainly not unexpected, given the results shown by previous surveys, it confirms that most SOCs need to make significant adjustments in how they operate and manage their people to make SOC work less painful while also improving their organizations' overall security posture.

Tell Us Where It Hurts

Now that we see the perception of how painful working in the SOC remains, let's examine why that pain persists.

Figure 26.

What, if anything, makes working in the SOC painful? (More than one response permitted.)



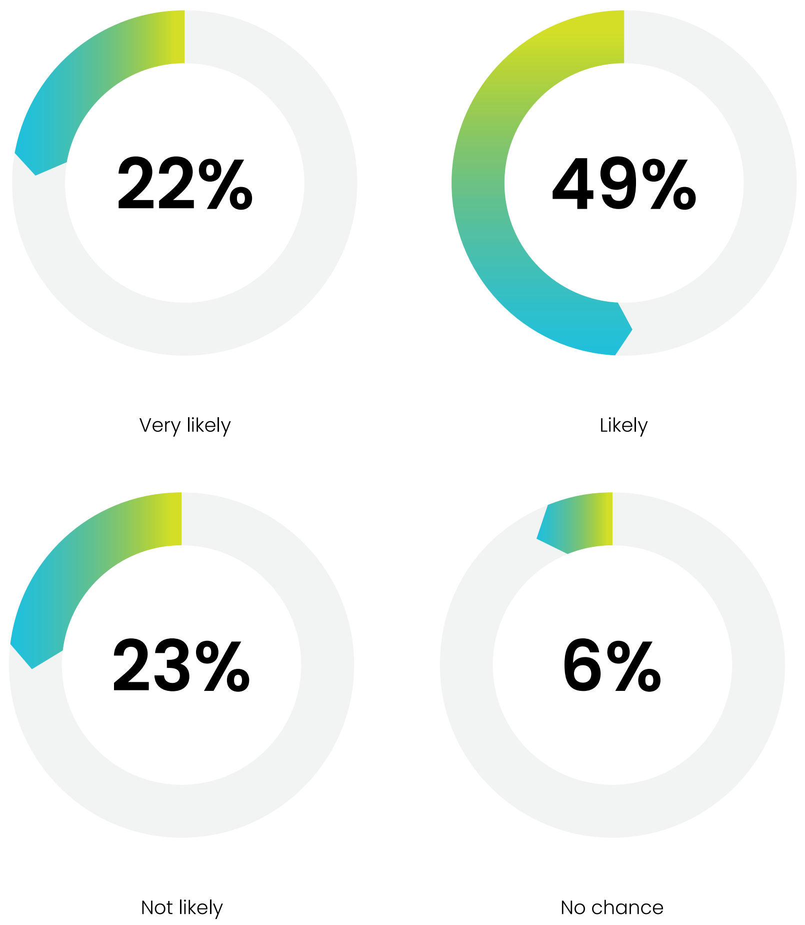
Topping the list of causes of SOC pain are the usual suspects: too much information, more work than analysts can handle, difficulty finding and keeping SOC experts, insufficient downtime, too many tools (and lack of tool integration), and too many alerts to chase. Respondents also cited a few of the key challenges that are inherent to any cybersecurity program: inability to capture actionable intelligence and prioritize threats, and lack of visibility into the attack surface.

In other words, there are many reasons for the pervasive pain experienced by too many SOC analysts. And it's reasonable to assume, the pain of SOC work is also affecting leaders. The pressure on those who manage SOCs and those who do the hunting, investigating and resolving of threats may be different, but both groups are under intense pressure — some of it likely due to professional integrity and the desire to protect their organization's assets — and if this level of pain isn't addressed, it will become even more difficult to attract and retain skilled SOC workers. This would be devastating for organizational security, and a boon for cyberthreat actors around the world. Which leads to the next question.

Those in Pain Are Less Likely to Remain

Figure 27.

What is the likelihood that these pain factors would cause any experienced security staff to quit your organization's SOC?

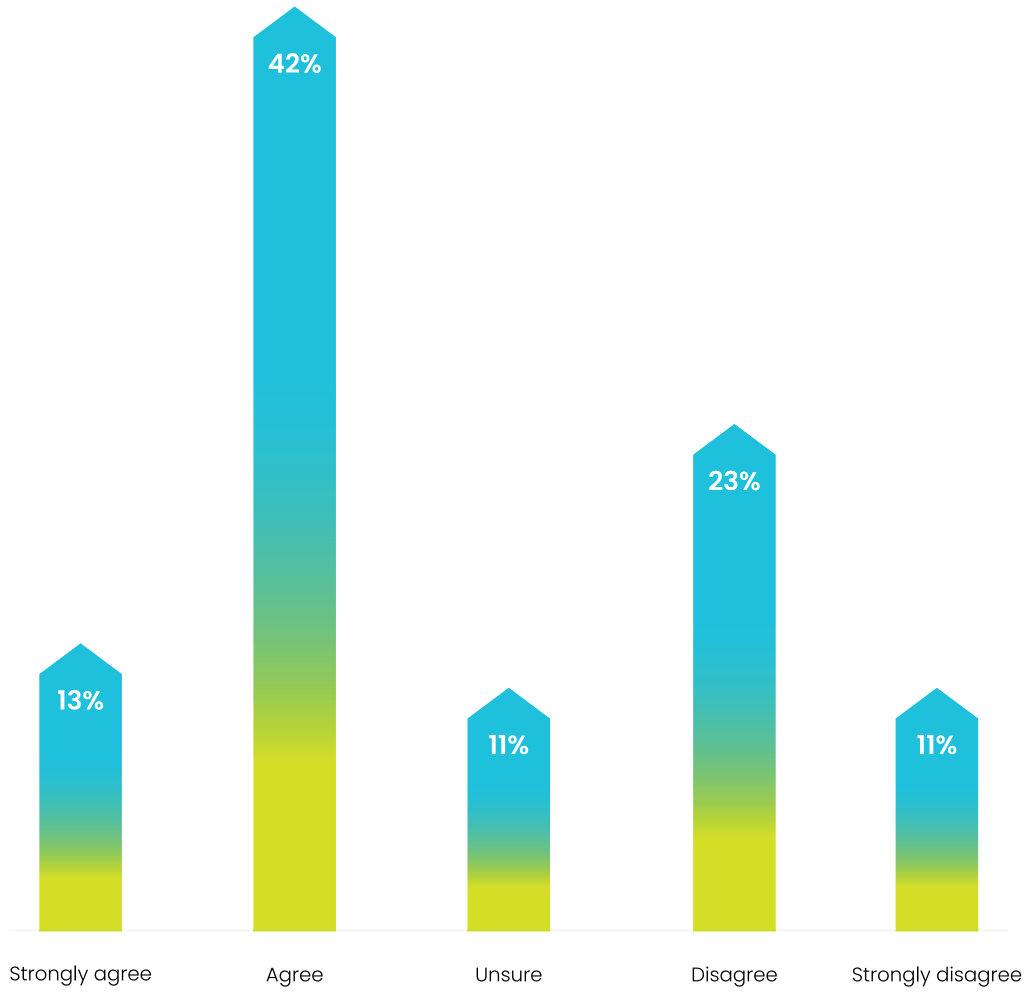


The bottom line is 71% of experienced SOC staff are likely to quit their jobs due to the combination of challenges identified in the previous questions. If organizations don't take meaningful action to improve the conditions in their SOCs, how will they be able to identify and stop the threats that matter most to their business?

Let's see what SOC workers themselves say about how likely they are to quit their jobs due to working conditions.

Figure 28.

How strongly do you agree or disagree with the following statement? "I have considered leaving my current role due to pain factors associated with working in the SOC."



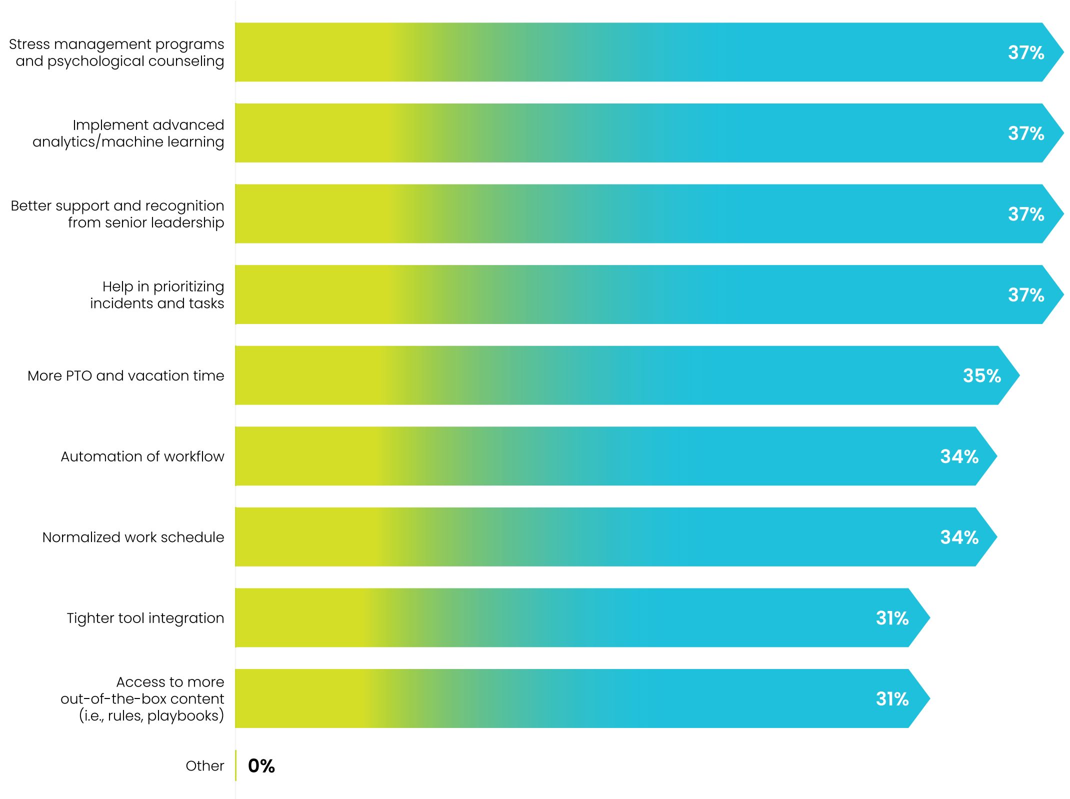
Overall, 55% of respondents say they have considered walking away from their jobs due to the pressure they feel.

Treating the Sources of Pain

The survey results show the level of pain for SOC workers remains unacceptably high. And they show the causes of the pain. So, the next obvious question is what can be done about it?

Figure 29.

What steps do you think your organization should take to alleviate the pain experienced by SOC staff? (More than one response permitted.)



The responses to this question fall into a couple of primary categories. The first category involves traditional stress management techniques, including focusing on tactics and techniques to alleviate stress, providing better support for workers, and giving them more time away from work to rest and recharge. The second category of ways to alleviate SOC analyst pain approaches the problem from a technology perspective.

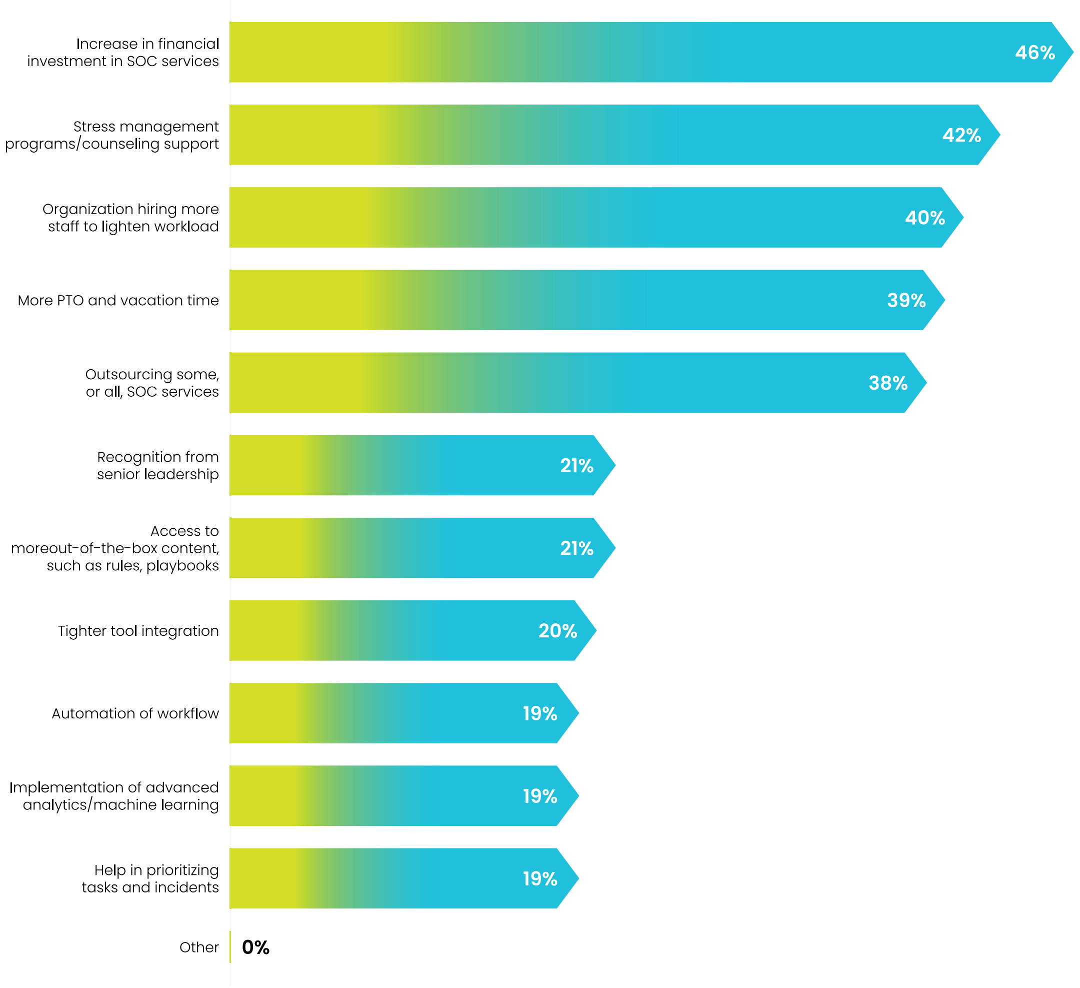
Introducing advanced analytics and machine learning, and automating workflows, are two of the modern approaches to SOC work that are gaining traction. Ultimately, the industry is headed toward the era of the autonomous SOC. That doesn't mean machines and artificial intelligence are going to put human SOC analysts out of jobs. Rather, it means advanced technologies are rapidly becoming available that will be able to take on some of the more tedious, exhausting areas of SOC work, including sorting through alerts to determine which are significant enough to require a response from SOC staff.

Given the talent shortage, difficulty in hiring SOC talent, and burnout issues that are already too prevalent in the industry, technological solutions to the many challenges overwhelming today's SOCs may be the only effective way to stem the tide of resignations, inability to fill open positions, and growing vulnerability of organizations to relentless attackers.

SOC workers who indicated in previous responses that they are experiencing pain from their work also provided their opinions on possible remedies.

Figure 30.

What type of support, if any, would help to alleviate any pain associated with working in the SOC? (More than one response permitted.)



By this point in reading the survey results, it is reasonable to expect that several of the most popular responses to this question pertain to ways of alleviating stress, crushing workloads, and not enough time off to recharge, which are three of the top four responses. And, although they are near the bottom of the responses, once again technological solutions, including better tool integration and implementation of workflow automation and advanced analytics/machine learning each were cited by 19% of respondents.

Next, let's look at the survey results again, but this time with responses from leaders side by side with those from SOC staff.

PART 3.

RESPONSES FROM SOC LEADERS AND STAFF — A COMPARISON

SOC Leaders and Staff Still Not Aligned

Like a car that's difficult to steer straight, many SOCs are badly in need of alignment. That lack of alignment manifests itself in terms of often significantly different perspectives on issues between SOC leaders and staff.

As we did for the first time in the 2021 report, we once again compared responses from SOC leaders (senior executives, vice presidents, directors and managers) and staff members (supervisors, technicians and contractors) to determine where they agree on key issues and, more importantly, where they differ.

As with any manager/staff member relationship, there are going to be differences of opinion on how to do things, what's important, etc. The two groups' (553 leaders and 547 staff members) survey responses demonstrate where those differences arise, how big the gaps may be, and perhaps enable SOC professionals to gain greater perspective about these critical relationships for the success of every SOC.

Figure 31.

How important is your organization's SOC to its overall cybersecurity strategy?	LEADERS	STAFF
Essential	31%	18%
Very important	51%	52%
Important	16%	28%
Not important	1%	1%
Irrelevant	0%	0%

For starters, neither group feels their SOC is "irrelevant" and only 1% feel it is "not important." So that's a good start. Now, at the other end of the range, leaders feel the SOC is more "essential" by 13 percentage points. But when you look at those who recognize their SOC is "very important," the responses are almost identical. Interestingly, the gap in the "essential" rating is reversed in the "important" results, where staff gave a higher rating.

At this very basic level, there is really no misalignment between SOC leaders and staff when it comes to the importance of the SOC. Will the same hold true when they're asked how effective their SOC is?

Let's look next at how respondents feel about their SOC's alignment with the needs of the business.

Figure 32.

Within your organization, are SOC objectives aligned with business needs?	LEADERS	STAFF
Fully aligned	66%	63%
Partially aligned	31%	30%
Not aligned	3%	7%

Once again, as they say at the scene of an accident to keep people moving, "There's nothing to see here, folks." Leaders and staff both agree on how well their SOC is aligned with business needs. The next question provides an opportunity to see if the alignment we're seeing thus far will continue.

Figure 33.

Which of the following consequences, if any, would your organization likely face if SOC objectives were not fully aligned with its business needs? (More than one response permitted.)	LEADERS	STAFF
Increased likelihood of security breaches, data leaks	61%	52%
Compromise of overall SOC effectiveness	56%	50%
Budget can be misdirected	46%	54%
Higher staff turnover	46%	49%
SOC services may be deemed as less essential	48%	46%
Other	1%	1%
None of these	1%	1%

Once again, there are no truly significant gaps in the responses from leaders and staff. Leaders do see a greater likelihood of breaches and data leaks than staffers do. The same goes for possible compromise of SOC effectiveness. Interestingly, more staff members than leaders feel the lack of SOC and business alignment could result in misdirection of budget.

Figure 34.

What do you think would improve alignment of your SOC objectives and business needs? (Up to two responses permitted.)	LEADERS	STAFF
Cross-functional team with representation from the SOC's leadership and lines of business	43%	42%
Increasing SOC budget, so that requested additional services can be implemented	41%	41%
SOC's leaders are measured and evaluated on how well they understand and support the organization's business needs	37%	37%
Lines of business are measured and evaluated on how well they communicate the business needs to SOC's leaders	33%	40%
Senior leadership's (C-suite) involvement in improving alignment	33%	33%

The only response with any noticeable difference between leaders and staff pertains to how well business leaders communicate the organization's needs to the SOC. That 7-percentage-point difference isn't surprising, given that SOC staff can easily feel excluded from such issues. But it's worth noting that it's the only area where an effort could be made to get that response more in line with what SOC leaders think.

Figure 35.

Using the following 10-point scale, please rate the effectiveness of your organization's SOC from 1 = Ineffective to 10 = Very effective.	LEADERS	STAFF
1	0%	0%
2	0%	0%
3	0%	3%
4	1%	3%
5	1%	4%
6	5%	5%
7	25%	30%
8	36%	39%
9	21%	14%
10	10%	3%

Finally, there's a larger gap between the perceptions of leaders and staff regarding the effectiveness of their SOC. While more staff (69%) rate their SOC higher than leaders (61%) in the "effective" range (7 or 8 on the 10-point scale), the results flip in the "very effective" range (9 or 10) with 31% of leaders having a higher opinion of their SOC's effectiveness than staff (17%). Let's see what is behind that difference in ratings.

Figure 36.

What makes your organization's SOC ineffective? (More than one response permitted.)	LEADERS	STAFF
Lack of visibility into the attack surface	60%	45%
Lack of skilled personnel	50%	48%
Yields too many false positives	30%	35%
Too many tools	30%	29%
Lack of timely remediation	30%	16%

The response to the next question, about how well their SOC performs key activities, yielded similar results from leaders and staff.

Figure 37.

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.	LEADERS	STAFF
1 = Ineffective	0%	0%
2	0%	2%
3	1%	4%
4	2%	7%
5	4%	8%
6	8%	11%
7	21%	20%
8	33%	27%
9	18%	15%
10 = Very effective	12%	6%

Few respondents from either group believe their SOC performs poorly in these areas. Toward the high end of the range (7 and above out of 10), leaders had a slightly more positive outlook on the effectiveness of their SOC when it comes to these key activities, but even then, the largest difference was just 6 percentage points.

Talking the Talk

The next two questions shine a light on how well leaders believe they convey the SOC's strategy to their teams and what staff think of their bosses' skill in this area.

Figure 38.

Using the following 10-point scale, please rate how well SOC leaders in your organization communicate the SOC's strategy to staff members from 1 = Not well at all to 10 = Exceptionally well.	LEADERS	STAFF
1 = Not well at all	0%	0%
2	1%	2%
3	1%	3%
4	2%	9%
5	4%	8%
6	10%	12%
7	19%	23%
8	30%	22%
9	21%	16%
10 = Exceptionally well	12%	6%

It's human nature for people to perceive they are performing a given task more effectively than others do. That's certainly to be expected when leaders are asked how well they communicate. The relatively close results in each of the categories show that SOCs can function very effectively as teams when everyone is working toward the same goals.

Now, for the flip side of this equation, let's take a look at what respondents think about SOC leaders' listening skills.

Figure 39.

Using the following 10-point scale, rate how well SOC leaders listen to and understand the needs and priorities of SOC staff from 1 = Not well at all to 10 = Exceptionally well.	LEADERS	STAFF
1 = Not well at all	0%	0%
2	0%	1%
3	1%	3%
4	2%	7%
5	4%	9%
6	7%	11%
7	23%	22%
8	30%	29%
9	20%	12%
10 = Exceptionally well	14%	5%

No matter how much pressure and pain they experience, SOC teams are known for working together as a unit to get the job done of protecting their organization's data. When you pose a question about how well you or the people you report to listen and understand staff priorities, it's a highly subjective question. The responses to this question are generally positive and leaders and staff are not too far apart. The most positive aspect is few respondents gave themselves or their leaders poor ratings for listening and understanding. Most of the responses are clustered at 7 and above out of 10. That indicates that the general level of communication is relatively high in most SOCs, showing no significant misalignment between SOC leaders and staff — at least in this area. Let's see how they align on the subject of training and staff retention.

Figure 40.

Using the following 10-point scale, please rate the importance of staff training/retention for your organization from 1 = Not important to 10 = Extremely important.	LEADERS	STAFF
1 = Not important	0%	0%
2	0%	0%
3	0%	0%
4	0%	1%
5	1%	1%
6	3%	5%
7	19%	22%
8	31%	41%
9	25%	18%
10 = Extremely important	20%	11%

Another good sign for the alignment of SOC leaders and their staffs is whether or not they share the same perspective on the value of training and retaining staff to benefit SOC performance. As with the past few questions about communication, most of the responses from leaders and staff are clustered toward the top of the 10-point scale. For leaders, 95% rated this issue a 7 or higher, while SOC staff were just behind with a 7-and-above rating of 92%. Score another victory for SOC alignment.

Figure 41.

What training or tools would you like your organization to offer? Select all that apply.	LEADERS	STAFF
Tool-specific training	32%	29%
Reimbursement for college courses or degree programs	31%	28%
Hands-on training courses or workshops	28%	29%
Conferences or community events	25%	31%
Content subscriptions	24%	29%
Online training courses	24%	26%
Cybersecurity certification sponsorship	25%	26%
Other	1%	0%
None of these	2%	1%

The trend of SOC leaders and staff being more aligned than not in their responses continues with this question. Of all of these training methods and tools, the only choice that has more than a 5-percentage-point gap between the two groups is "conferences or community events."

The Pain Remains (and It's Chronic)

In our previous SOC Performance Reports, the most significant issue has been the level of pain experienced by those who work as SOC analysts. That's not much of a surprise for such a pressure-packed, high-stakes job. But what do SOC managers and analysts have to say about it this year? With a question such as this, one group is primarily responding based on what they see and hear from the people who report to them, while the other group consists of the people who are more likely to be experiencing a painful workplace themselves. What did this year's survey respondents have to say about the pain of SOC work?

Figure 42.

Using the following 10-point scale, please rate the "pain" your organization's SOC personnel experience in meeting their daily job requirement from 1 = low pain to 10 = very painful.	LEADERS	STAFF
1 = Low pain	3%	0%
2	2%	1%
3	9%	7%
4	5%	9%
5	9%	9%
6	13%	10%
7	19%	27%
8	26%	33%
9	10%	4%
10 = Very painful	4%	0%

There's a lot to unpack here. SOC leaders and staff agree that working in the SOC is painful. As in previous surveys, the key question is "how painful is it?" Well, leaders and staff agree that the pain experienced by SOC analysts is very high.

The good news, if you can call it that, is no staff respondents rated their on-the-job pain at a 10 on the 10-point scale. Interestingly, 4% of leaders rated SOC workers' pain level at a 10.

Overall, the majority of leader and staff respondents put the level of pain between 6 and 10. Specifically, 68% of leaders and 74% of staff rated the pain level of SOC work at that level. For each group, the pain level cited by the largest segment of respondents is 8 on the 10-point scale, with 26% of leaders and 33% of staff estimating workers' pain level is that high. To state the obvious, this is not good — or sustainable.

What's Causing the Pain?

The next question asks leaders and staff to identify what is causing pain in their SOC. Let's look at the responses and how aligned or not leaders and staff are when it comes to identifying what's painful in their work environments.

Figure 43.

What, if anything, makes working in the SOC painful? (More than one response permitted.)	LEADERS	STAFF
Information overload	31%	31%
Increasing workload causes burnout	25%	34%
Inability to recruit and retain expert personnel	27%	30%
Being on call 24/7/365	27%	27%
Inability to prioritize threats	23%	31%
Difficulty in operating across too many tools	22%	31%
Complexity and chaos in the SOC	22%	31%
Lack of resources	26%	27%
Too many alerts to chase	22%	31%
Lack of tool integration	25%	26%
Inability to capture actionable intelligence	22%	27%
Lack of visibility into the attack surface	20%	28%
Losing to adversaries	16%	32%
Limited SOC investment in overall cybersecurity budget	25%	0%
Other	0%	0%

Survey respondents could choose from up to 14 possible causes of SOC pain covering a wide spectrum. 31% of both leaders and staff cited information overload as a significant factor in SOC workers' pain. That was the reason cited most often by leaders and was the third highest choice of staff respondents. For 24% of staff, the top cause of pain was burnout caused by a growing workload. Only 25% of leaders agreed.

The largest gap in responses from the two groups was not enough money spent on the SOC as part of their organization's overall cybersecurity budget. 25% of leaders said that is an issue but no staff members chose it.

Another interesting gap was "losing to adversaries," which was cited by 32% of staff but only 16% of leaders. And interesting, but for a different reason, is "being on call 24/7/365," which would seem to be a textbook reason for work-related burnout but was chosen by just 27% of both groups.

Effects of Ongoing SOC Pain

Whenever significant job-related pain exists it's reasonable to expect affected employees to "vote with their feet" and find another job, either the same work with another organization or by pivoting to a different occupation. SOC analysts are highly trained and dedicated cybersecurity experts. They study, train and move up the ranks of their chosen profession because it's what they want to do for a living. Certainly, it is no different from other dangerous, pressure-packed, and exhausting occupations in which many people spend entire careers. But is there a breaking point for SOC workers? Is there a level of pain from their work that is more than they can take? Let's look at the responses to the next question.

Figure 44.

What is the likelihood that these pain factors would cause any experienced security staff to quit your organization's SOC?	LEADERS	STAFF
Very likely	21%	22%
Likely	48%	50%
Not likely	26%	20%
No chance	5%	7%

The responses from leaders and staff are largely consistent across the board. Fewer than one-quarter of respondents from both groups believe job-related pain is “very likely” to cause experienced SOC analysts to quit their current jobs. However, 48% of leaders and 50% of staff say ongoing job-related pain is “likely” to result in staff quitting. When you factor in all of the work-related changes that have occurred since the start of the pandemic along with persistent pain experienced by SOC workers the picture is grim. And, as we’ve seen earlier in this report, it’s already very difficult to hire qualified SOC analysts. Nothing in these survey results indicates the situation is likely to improve in the near term.

What Can Be Done?

It’s naive to think there’s a way to completely eliminate the pain of working in the SOC. And with an ongoing problem such as SOC analyst pain, there are many possible remedies that might reduce the problem, at least to some extent. SOC leaders and staff weigh in on several possible solutions.

Figure 45.

What steps do you think your organization should take to alleviate the pain experienced by SOC staff? (More than one response permitted.)	LEADERS	STAFF
Stress management programs and psychological counseling	34%	41%
Implement advanced analytics/machine learning	39%	35%
Better support and recognition from senior leadership	38%	35%
Help in prioritizing incidents and tasks	36%	37%
More PTO and vacation time	35%	35%
Automation of workflow	31%	37%
Normalized work schedule	33%	35%
Tighter tool integration	30%	33%
Access to more out-of-the-box content (i.e., rules, playbooks)	31%	31%
Other	0%	0%

SOC staffers favor a physical and mental well-being approach to addressing pain with 41% selecting “stress management” and “psychological counseling,” making it the top prospective remedy. Just 34% of leaders favor that solution.

SOC leaders took a different tack. Their top choice was a technological one, with 39% recommending the implementation of “advanced analytics/machine learning.” That choice was favored by 35% of SOC staff.

Overall, there was significant agreement between the two groups with just a few percentage points separating most of the leaders’ and staffers’ preferences.

Figure 46.

How strongly do you agree or disagree with the following statement? "I have considered leaving my current role due to pain factors associated with working in the SOC."	LEADERS	STAFF
Strongly agree	12%	14%
Agree	36%	48%
Unsure	13%	9%
Disagree	25%	20%
Strongly disagree	13%	9%

The possibility of SOC leaders and staffers quitting their jobs due to the pain they experience is real. 48% of leaders said they “agree” or “strongly agree” that they have at least considered making such a move. For SOC staff, the number is even higher, with 62% saying they have considered it. Only 13% of leaders and 9% of staff said they were unsure of whether they would stay or leave.

Figure 47.

What type of support, if any, would help to alleviate any pain associated with working in the SOC? (More than one response permitted.)	LEADERS	STAFF
Increase in financial investment in SOC services	54%	39%
Stress management programs/counseling support	49%	37%
Organization hiring more staff to lighten workload	49%	33%
More PTO and vacation time	46%	34%
Outsourcing some, or all, SOC services	45%	32%
Recognition from senior leadership	0%	38%
Access to more out-of-the-box content, such as rules, playbooks	0%	37%
Tighter tool integration	0%	36%
Automation of workflow	0%	35%
Implementation of advanced analytics/machine learning	0%	34%
Help in prioritizing tasks and incidents	0%	33%
Other	1%	0%

What actions can organizations take to improve the situation for SOC workers? Spending more money on SOC services was seen as the top method of support by 54% of leaders and 39% of staff. There also were a number of interesting responses that highlight the different perspectives of those who manage SOCs and those who work there. For example, 38% of staffers said “recognition from senior leadership” would help alleviate pain. But that didn’t register with SOC leaders, as none chose that as a possible remedy.

CONCLUSION

SOC workers’ pain is real. They are frustrated in their work, and even if not ready to do so, many are thinking of quitting. For jobs that play such a critical role in protecting organizations against relentless cyberthreats, that’s the kind of doomsday scenario that is likely keeping SOC leaders, and other executives, up at night.

METHODOLOGICAL NOTES:

The Devo Survey was conducted by Wakefield Research (www.wakefieldresearch.com) among 1,100 decision-makers and non-management staff at organizations with a security operations center (SOC) and 1,000+ employees located in the U.S., Canada, UK, France, Germany, Italy, and Australia/New Zealand. The responses were collected between July 15 and August 2, 2022, using an email invitation and an online survey.

Results of any sample are subject to sampling variation. The magnitude of the variation is measurable and is affected by the number of interviews and the level of the percentages expressing the results. For the interviews conducted in this particular study, the chances are 95 in 100 that a survey result does not vary, plus or minus, by more than 3.0 percentage points for the overall sample and 8.7 percentage points in the U.S. Public Sector subsample, from the result that would be obtained if interviews had been conducted with all persons in the universe represented by the sample.