The time to transform is now

KPMG Security Operations Center Survey 2024

KPMG. Make the Difference.

kpmg.com

Contents

Foreword

Organizations with a heavy reliance on digital infrastructure are facing a real and immediate threat they can ill afford—the impending growth of cybercrime, which could escalate to a staggering financial cost of nearly $10 trillion annually in 2024. The increasing complexity and sophistication of these cyber threats are straining the resources of corporations across various industries, including healthcare, finance, retail, and technology, as well as government agencies, educational institutions, and nonprofits, clouding their ability to single out genuine threats and placing them in a reactive position. These organizations are being hit from all sides, almost perpetually, by potential attacks, and they're struggling to identify the real ones from the noise. Security Operations Centers (SOCs) are at the epicenter of this dynamic and fluid landscape.

Historically, SOCs focused on security, incident management, and SecOps workflow. In that traditional framework, chief information security officers (CISOs) and their teams receive security log feeds, apply attack signatures to those logs to identify potential patterns, and assign that data to a queuing system that is reviewed by a set of analysts—Tier 1, Tier 2, Tier 3—depending on the type of incident or vulnerability. If Tier 1 is unable to resolve the issue, it is escalated to Tier 2, and if necessary, it goes to Tier 3. That's largely the way most SOCs continue to function today.

It is predicted that in 2024 cybercrime will cost $26 billion/day and $9.5 trillion/year.[1]

In the current environment, however, this approach simply is not sustainable—it is reactive, doesn't stand up to the complexity most organizations require, and largely doesn't take advantage of the latest technology. The rate and complexity of cyber incidents is increasing faster than the SOC's ability to deploy human analysts and there simply isn't enough sophistication in how programs detect and prioritize alerts to quickly pinpoint the legitimate attacks. AI can make real-time predictions, reconcile extremely complex scenarios, and do so faster and on a larger scale than the human brain, but it cannot demonstrate suspicion, curiosity, or intuition. It is for these reasons we believe human analysts and AI will eventually develop a productive symbiosis.

With that in mind, we encourage security leaders, many of whom are confident in their SOCs, to thoroughly revamp their existing operating models. They should aim to construct a more operationally effective, intelligent next-gen SOC that focuses on contextualizing and anticipating threats. Further, it should utilize learning technologies to enhance analysts' capabilities rather than amassing security tools without ensuring proper integration or cohesive deployment.

We believe organizations should focus on creating diverse SOC platforms powered by efficient processes that leverage a technologically and philosophically relevant framework designed to provide the security team with broader and deeper visibility across the network. The goal is to respond to cyber incidents quickly, consistently, accurately, and collaboratively while enhancing the SOC's ability to effectively marshal resources against today's sophisticated threat actors.

[1] Cybersecurity Ventures, 2023 Official Cybercrime Report

About the research

Our online study, fielded in Q2 2024, was based on a survey of 200 CISOs, chief security officers (CSOs), and AI security officers at US companies with at least 500 employees and $1 billion in revenue. Respondents came from 16 separate industries.

Study demographics

Primary function

100% IT, security, or technology

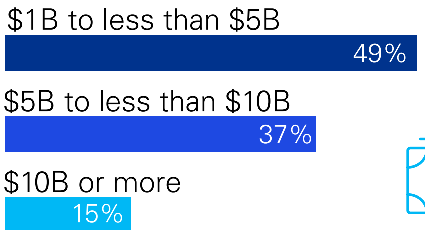
Job title

CISO	66%
CSO	28%
AI security officer	6%

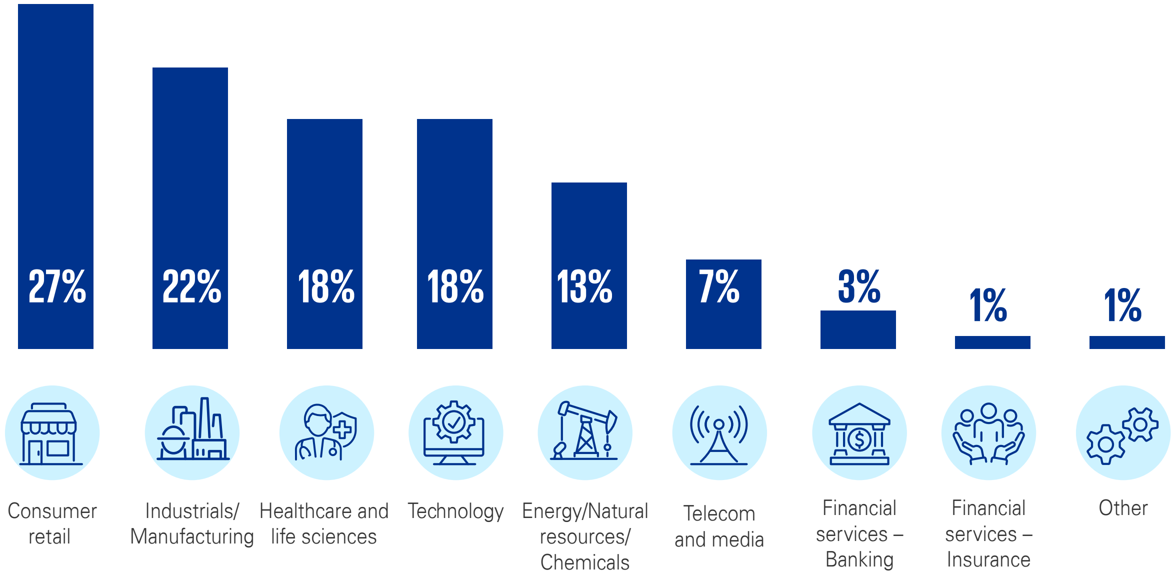
Company size (employees)

500–999	7%	**33%**
1,000–4,999	26%	
5,000–9,999	42%	**67%**
10,000–19,999	15%	
20,000+	10%	

Annual revenue



Industry



*The question regarding industries allowed respondents to select "all that apply." As such, the percentages shown total more than 100 percent.

What we learned

The objective of the survey was to explore SOC leaders' current and future perspectives (two years out) on security practices, cyber threats, the effectiveness of their SecOps, their level of preparedness, and their priorities and challenges. In turn, we believe this information enables our professionals to offer timely threat management guidance and recommendations around identifying real imminent threats, shutting them down, and ensuring ongoing cyber resilience, as well as the allocation of resources, solution usage, and AI adoption—both within the SOC and across the enterprise.

Key findings include:

85% are confident in their SOC's **readiness** to prevent future, sophisticated attacks

76% are concerned about the increasing **sophistication** of new cyber threats and cyberattacks

74% expect to increase SOC **headcount** over the next two years

70% believe **AI will revolutionize** identity and access management, threat detection and response, perimeter monitoring, and predictive analytics

69% of security leaders have a high level of confidence that their SOC has a solid **understanding** of the organization's risk areas and vulnerabilities

68% expect to **increase SOC budgets** over the next two years

40% indicate their SOC has suffered an attack(s) that resulted in a **security breach in the last year**

Cyber leaders are confident, but vigilant

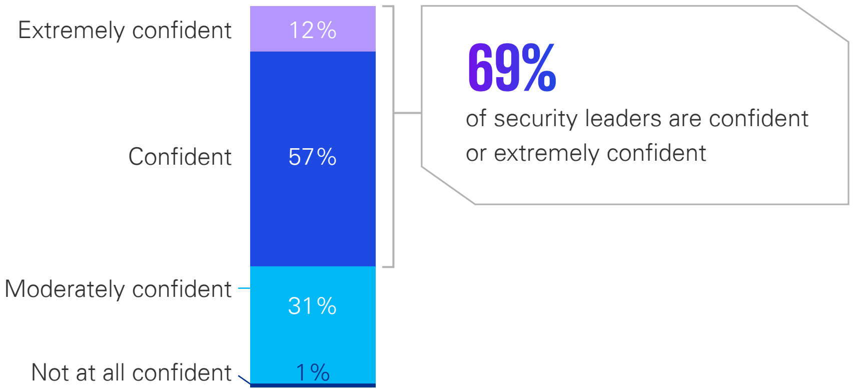
In today's ever-evolving business environment, cyber leaders often feel as though they are constantly reacting to threats after impact while undergoing nonstop technology transformations that make it difficult for analysts to stay even with attackers. Progress often is defined by the classic idiom, "one step forward, two steps back." As a result, cyber teams are perpetually under pressure to act faster just to keep pace with a fluid threat landscape. We believe the most rational mindset for security professionals is to acknowledge they're never going to be able to protect against everything at every moment. In the end, companies must strike a balance between preparation and resilience and control what they can control. If our SOC survey results are an indication, it would appear that security leaders agree.

At a time when more than three-quarters (76 percent) of respondents said they are concerned about the increasing sophistication of new cyber threats and attacks, 69 percent said they are confident their SOC understands the organization's risk areas and vulnerabilities while 91 percent said their SOC has full visibility across these potential susceptibilities.

That optimism is not just a snapshot; it is forward looking, with 85 percent telling us they are confident in their SOC's readiness to prevent future sophisticated attacks, a view that was particularly common among some of the bigger companies at the higher end of the revenue scale.

This level of confidence is undiminished by the fact that, according to the survey, 40 percent of security leaders indicated their SOC has suffered at least one attack in the last year that resulted in a security breach. This suggests they feel battle tested and, while they don’t want to see an attack on their network, the experience is considered valuable.

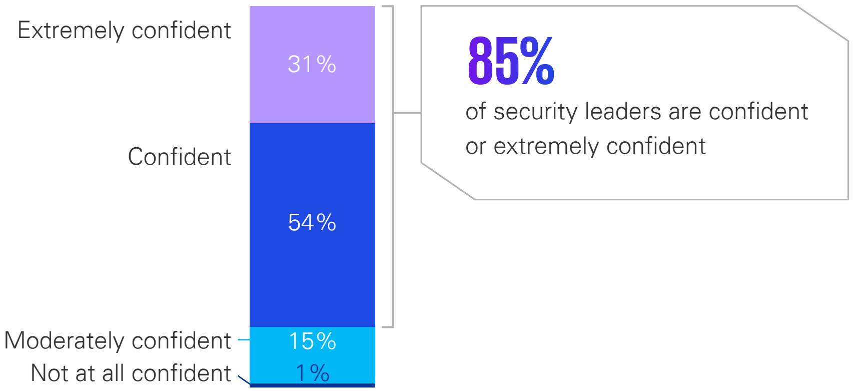
Confidence that SOCs have a solid understanding of the organization’s risk areas and vulnerabilities



69%
of security leaders are confident or extremely confident

Base: Total security leaders, n = 200

SOC preparedness to prevent increasingly sophisticated cyberattacks



85%
of security leaders are confident or extremely confident

Base: Total security leaders, n = 200

As for execution, we asked security leaders about the amount of time it takes their SOC to respond to and remediate a vulnerability. While the percentage was not as high as the question pertaining to the perception of readiness, about two-thirds (64 percent)—a solid majority—said they are satisfied. Similarly, we also asked them to estimate the number of days it takes their SOC to respond to and remediate a vulnerability and gave them some ranges. While the vast majority (92 percent) said it's under 75 days, the average is about 15 days. Interestingly, respondents who are extremely satisfied with the time it takes their SOC to act said they're able to resolve vulnerabilities in less than 10 days, whereas for those who are only somewhat satisfied it takes around 25 days on average. Clearly, satisfaction is a function of the SOC's ability to resolve incidents expeditiously.

> **On average security leaders say it takes about 15 days for their SOC to remediate a vulnerability and most are satisfied with this timing**

14.7 days

average number of days for the organization's SOC to respond to and remediate a vulnerability

9.2 days Among those satisfied with remediation time

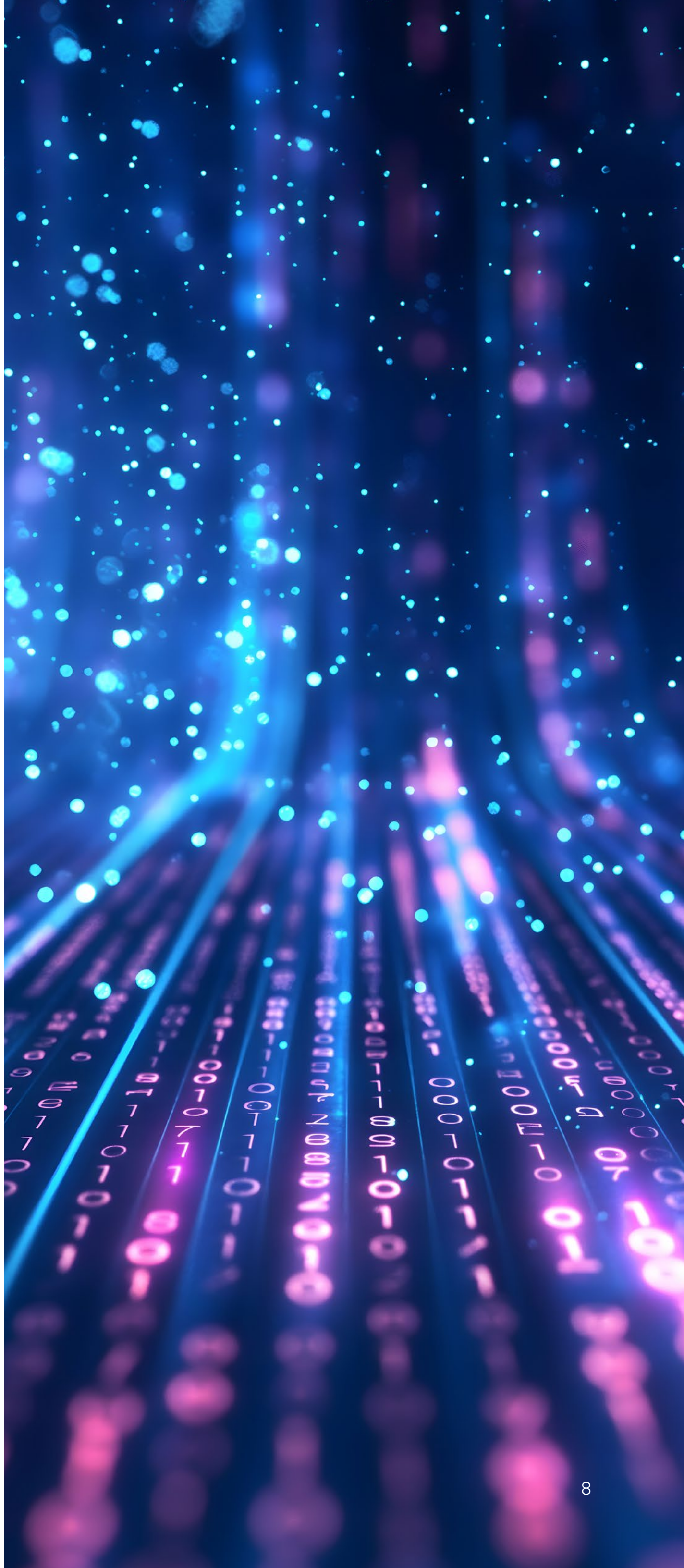
vs

24.5 days Among those not satisfied with remediation time

Specific responses

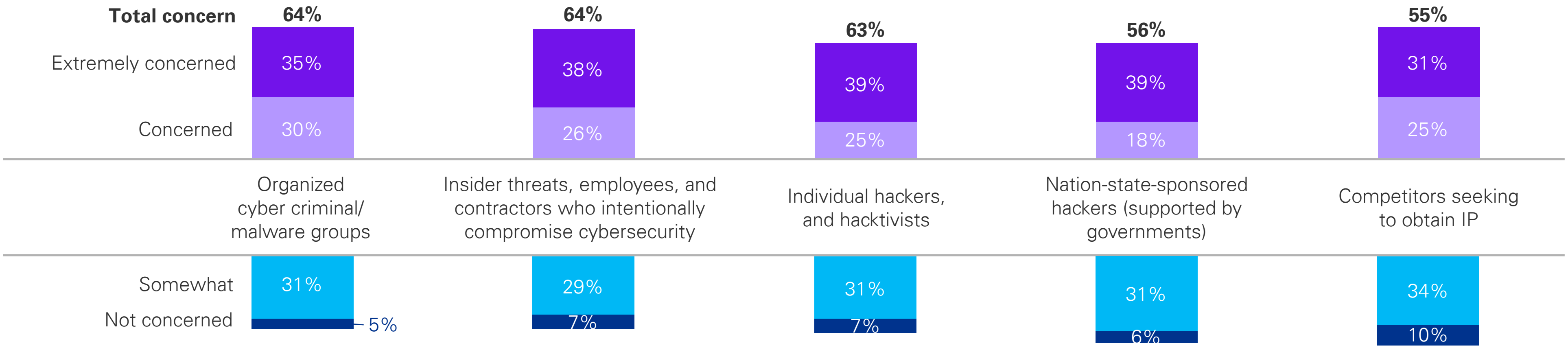
92%	<75 days
4%	75 days–<150 days
5%	150 days–<250 days
1%	>250 days

Base: Total security leaders, n = 200



We noted previously that nearly 80 percent of security leaders cited concerns about the increasing sophistication of threats. To add specificity to that data point, we asked about the types of attackers they are most concerned about. Nearly two-thirds said organized cyber criminal malware groups (this aligns with Q14, which revealed that malware attacks are the most common incident), insiders (employees or contractors/suppliers), and individual hackers and "hacktivists."

Leaders are concerned about organized cybercrime groups, insider threats, and individual hackers



Base: Total security leaders, n = 200

AI expected to be a SOC “game changer”

The collective conversation at virtually every organization and across every industry has been dominated by generative AI, but other aspects of AI, such as machine learning, natural language processing, and robotics, are transforming business as well and exacerbating cybersecurity planning. It’s challenging for cyber professionals to standardize the risks of adopting these technologies. As such, they look to devise frameworks and approaches that build confidence and trust from both security and privacy perspectives.

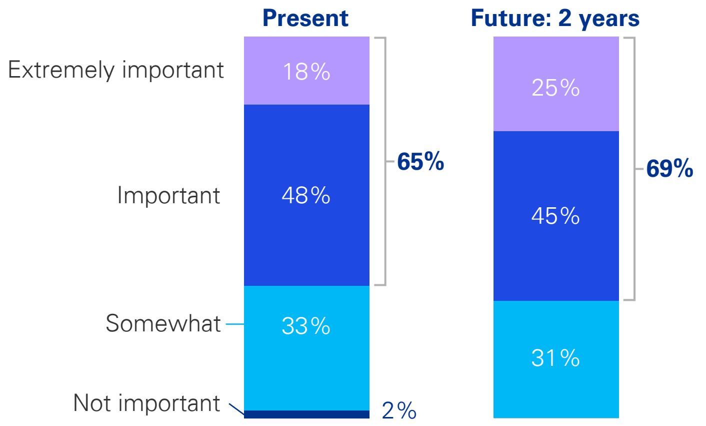
Regulation in this space is also ramping up as are ethical debates and the continuing shift left of controls and their inevitable automation. This all manifests in continuous controls monitoring, SecDevOps, and the application of AI as a decision augmentation tool for SOC staff or in a first-line query and advisory capacity. The skills mix within the SOC will continue to evolve as automation replaces/displaces more labor-intensive roles.

Given the focus on AI in the broad marketplace, the SOC survey specifically explored how security leaders are using or planning to use AI and their overall perceptions of AI as a key tool. The not-so-surprising takeaway is that a plurality of respondents consider AI-based automation not only to be critical now and going forward but they also view it as a game changer.

Two-thirds (66 percent) of respondents said AI-driven automation is important or extremely important—right now. Looking out two years, the conviction deepens, with 69 percent seeing AI as a key tool. Interestingly, one-third said AI-delivered automation is only somewhat important—we suspect these are organizations that have not yet fully embraced AI philosophically or operationally.

This view dovetails with the survey’s initial question, which asked security leaders to describe their SOC in terms of how it views innovation and evolving its approach. Nearly three-quarters (72 percent) describe their SOC as an “innovator.” They perceive the SOC as a “first adopter” of new solutions approaches, even without having existing use cases. AI is likely providing support for much of that posture.

Two-thirds of security leaders believe AI-based automation in the SOC is important now and will remain so over the next two years

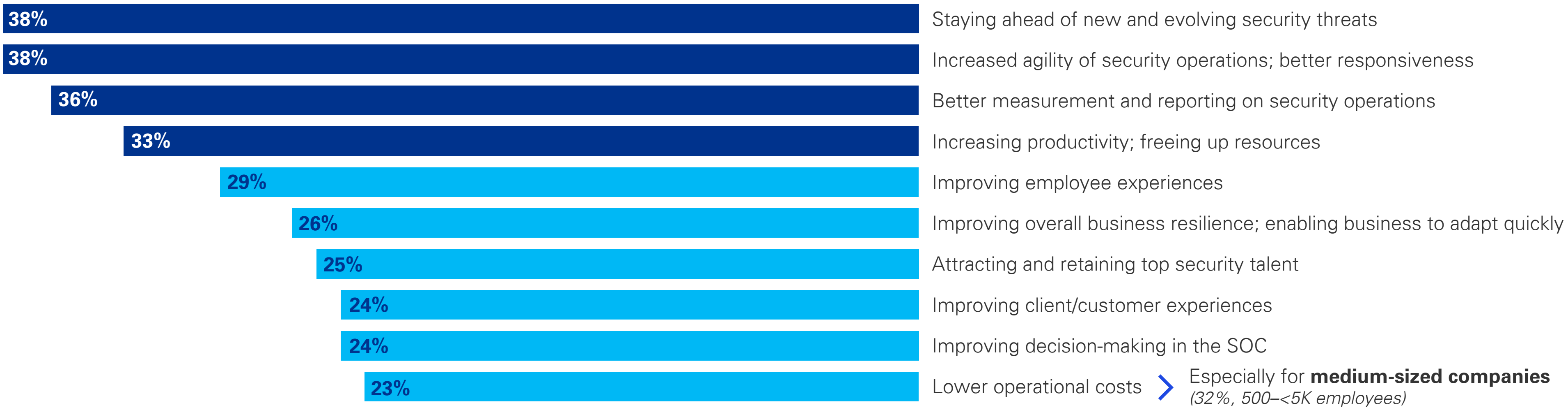


Base: Total security leaders, n = 200

Turning from the theoretical to the practical, the survey asked respondents what benefits security leaders are looking to derive from AI-driven automation. The top responses reveal that security leaders see AI as a means of staying ahead of new and evolving threats, a tool for improving agility in the SOC, and as a way to measure SOC performance and increase productivity. These responses also seem to align with the perception of the SOC as a center of organizational innovation.

AI-based automation is viewed as a critical capability to increase SOC agility and response

Percentage selected as one of up to three benefits

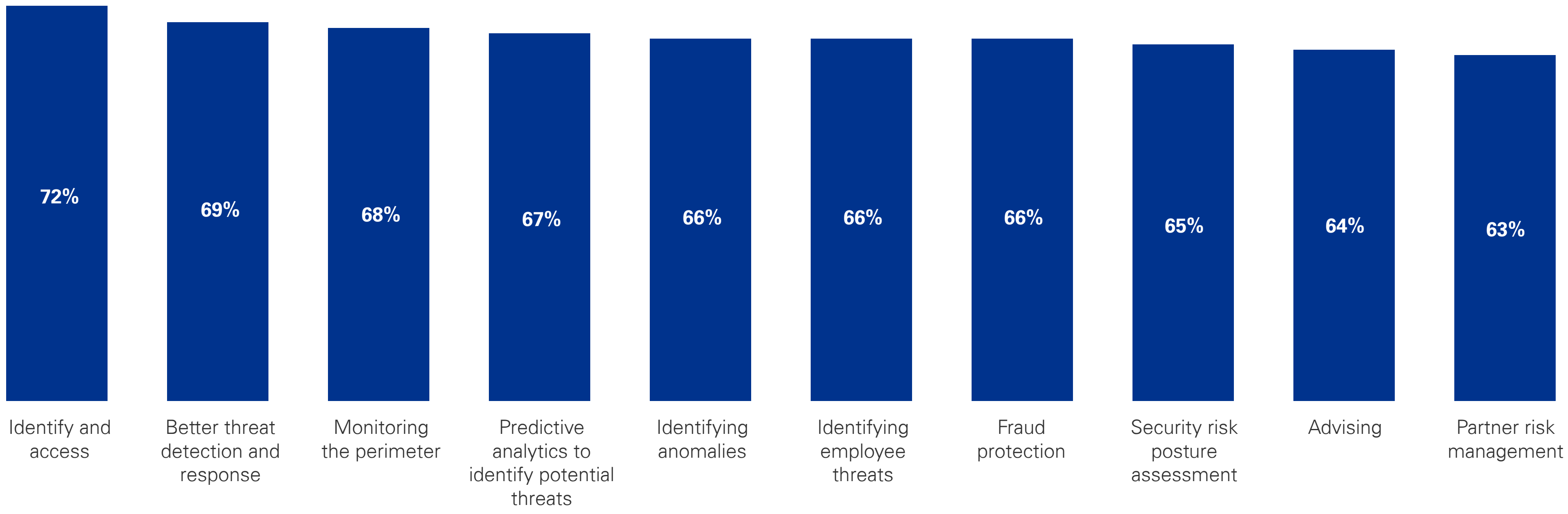


Especially for **medium-sized companies** *(32%, 500–<5K employees)*

Base: Select up to three answers, n = 200

On the issue of how AI will be revolutionary as a foundational SOC tool, the survey asked security leaders to consider a broad array of functions and rate AI as a tool for identifying and remediating threats and vulnerabilities. At least two-thirds expect AI to be a "game changer" across all security functions. Respondents see AI as crucial to essentially every aspect of their teams' work, with the greatest focus on identity and access management (71 percent) followed by threat detection and response (69 percent) monitoring the perimeter (68 percent).

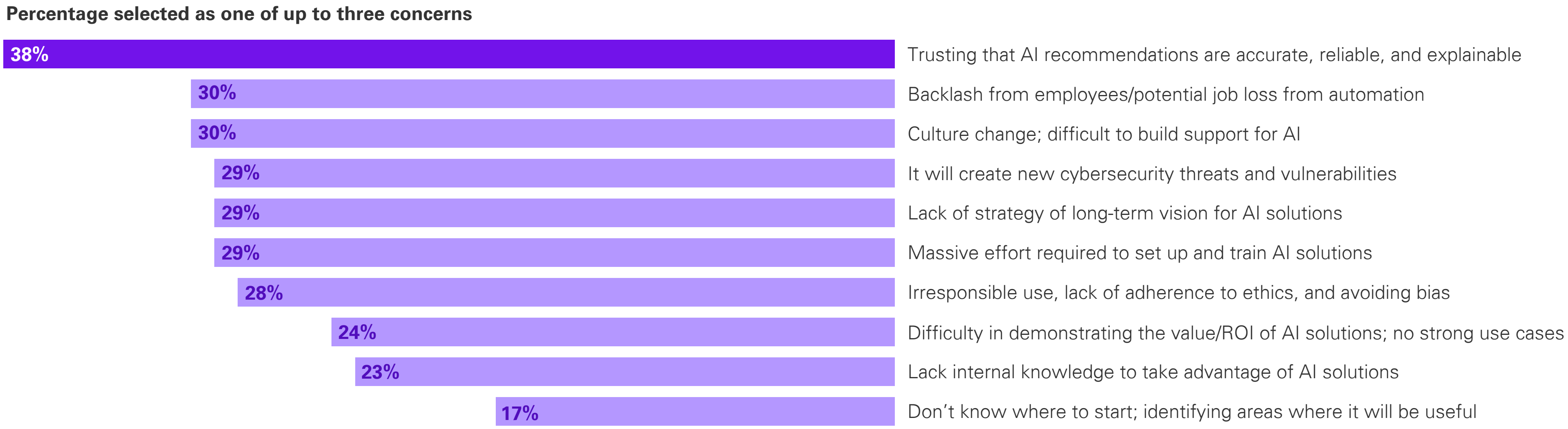
The majority of security leaders believe AI will be a "game changer" for identifying and remediating threats/vulnerabilities



Base: Total security leaders, n = 200

With AI is being embedded more and more into business processes and technology, AI security has become a major organizational priority. With that imperative in mind, the survey also asked security leaders about their concerns in regard to adopting AI in their SOCs. For nearly 4 in 10 respondents (38 percent), the top concern, not surprisingly, is trusting that AI recommendations are accurate, reliable, and explainable. To that end, the KPMG AI security framework provides security teams with a tailored playbook to proactively assess their organization's AI systems in development and production environments. The framework helps to secure those systems against a variety of threats and respond effectively in the event of an attack.

While security leaders see numerous AI-based benefits, there are concerns, particularly the reliability of AI recommendations



Base: Total security leaders, n = 200

On a second tier, nearly one-third of security leaders are concerned about factors such as potential backlash from employees over job loss uncertainties, potential new cybersecurity threats and vulnerabilities, the lack of a long-term AI strategy, and the effort required to set up and train AI solutions.

A year ago, the AI narrative around fear of job losses was huge, but those concerns seem to have waned. Today, organizations are more concerned about determining how to effectively infuse it into their workflows and gain confidence that the output will be accurate and reliable.

Clearly, many repetitive tasks are being impacted by AI, particularly generative AI, but there has not been significant job losses to date. AI is being eased into the mainstream now, and workforces appear to be flexible enough to adapt.

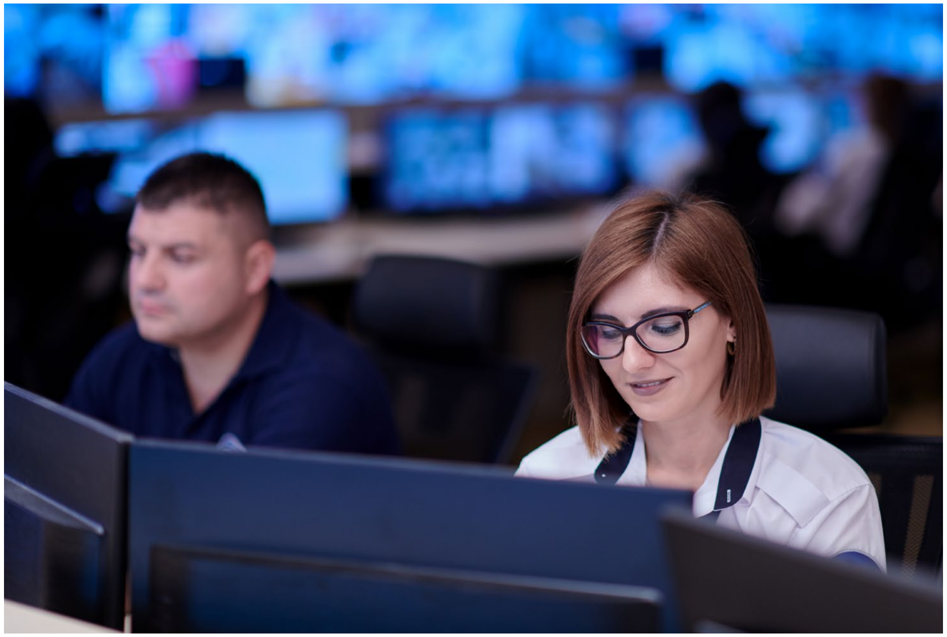
AI is not merely a tool. It's a transformative force that is reshaping the future of work. Rather than being a wholesale job replacer, we believe AI will shift some employees to new or modified roles, while all employees will ultimately work side by side with AI-powered systems and processes.

Getting it “right” demands human and financial resources

Many senior executives outside the SOC may not have an appreciation for what goes into security by design. Everyone agrees with architecting the digital environment securely, but often there’s an unstated bias in the business toward fast and cheap. However, the cost of doing it right—while initially more expensive and time-consuming—can be considerably less than doing it wrong. And that cost often takes the form of a breach, which can lead to a loss of customers, investors, and reputation.

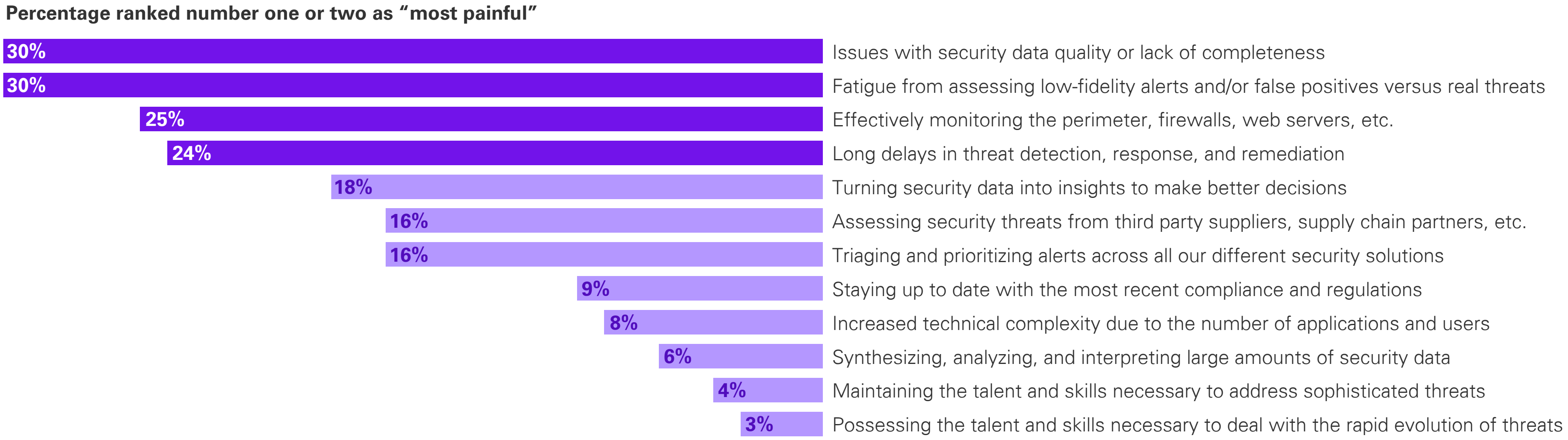
To level set, security leaders were asked to identify their top three SOC priorities for the next two years. The number one objective according to nearly half of respondents (49 percent) is increasing digital trust through better privacy, proactive identification, and threat remediation. This data point dovetails precisely with the top AI concern in regard to adopting AI in the SOC—trusting that AI output is accurate, reliable, and explainable. The second-highest response was identifying and mitigating cybersecurity threats (43 percent), followed by helping the business innovate and create new products and services faster (38 percent).

There are a number of other SOC priorities that are complementary to the business—supporting business agility (33 percent) and providing the business with a competitive edge (31 percent), for example—but the top three are fundamental enterprise goals: trust, safety, and innovation.



Exploring the issues that are keeping CISOs and CIOs up at night, the survey asked respondents to list their top three pain points. The top two, at 30 percent, are data issues and alert fatigue. Clearly, there's a need to refine and optimize data strategies and the efficiency killer of excessive "noise."

Top pain points for security leaders include navigating security data quality and the prioritization of various levels of threats

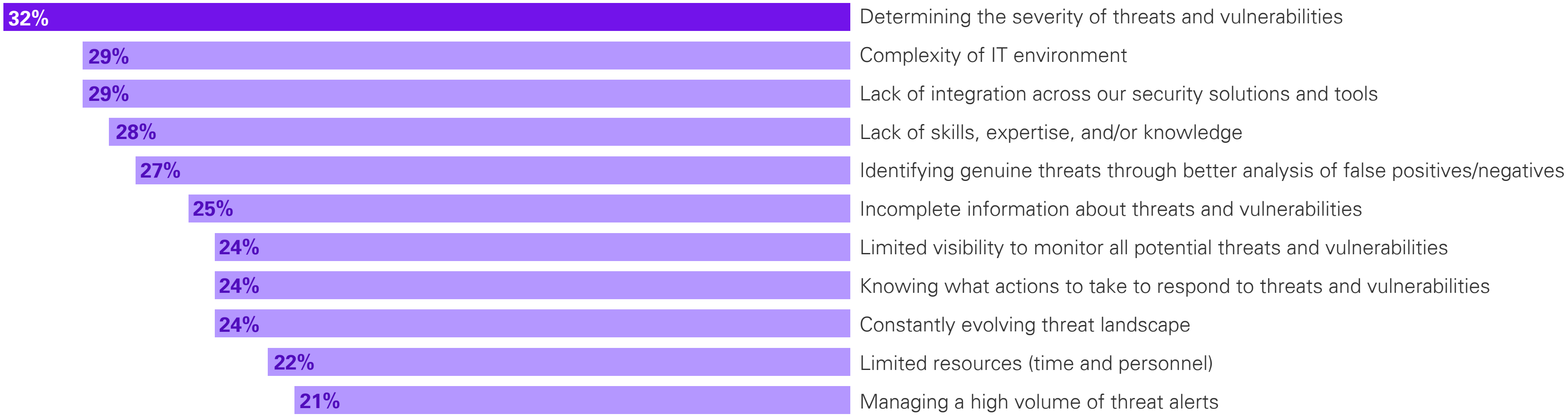


Base: Total security leaders, rank top 3, n = 200

Moving from pain points and actual barriers to identifying and remediating threats and vulnerabilities, nearly one-third (32 percent) of respondents said their biggest barrier is determining the severity of threats and vulnerabilities, which aligns with the preponderance of low-fidelity alerts and false positives as a top pain point. Limited resources and managing the high threat volume are surprisingly low at 22 percent and 21 percent, respectively.

Nearly a third of security leaders indicate their SOC has difficulty determining the severity of cyber threats and vulnerabilities

Percentage selected as one of up to three biggest barriers



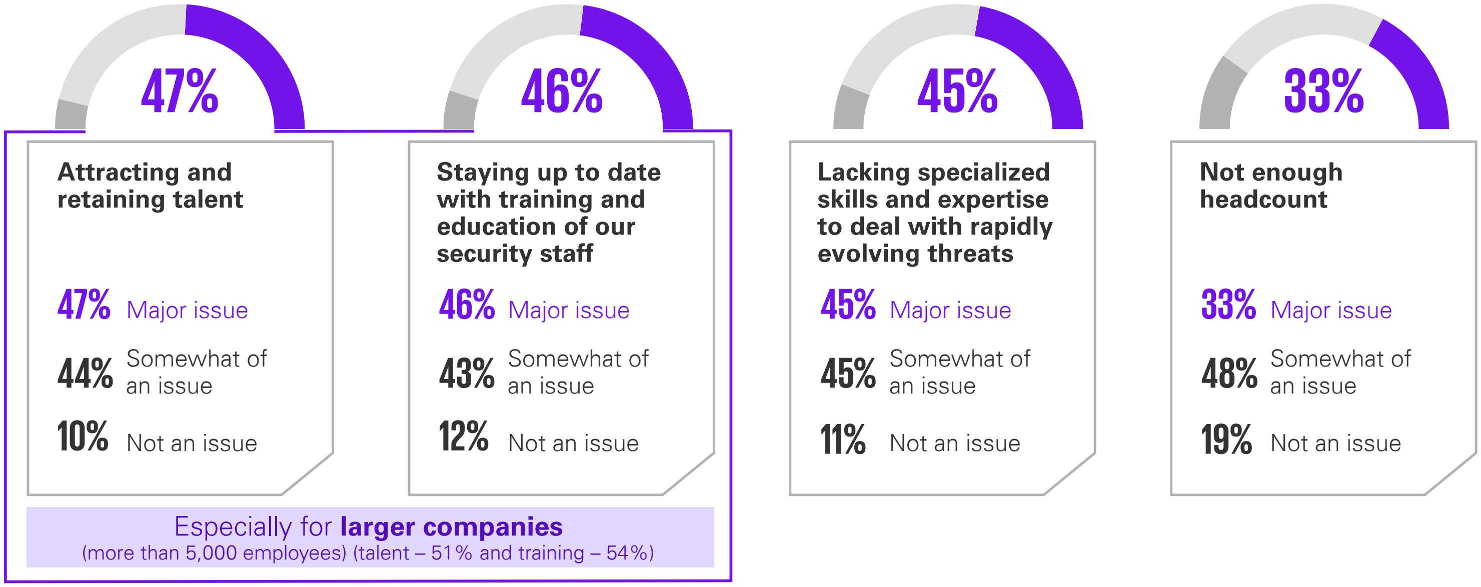
Base: Select up to three answers, n = 200

We view these responses as more of a commentary on actual SOC performance than on underlying capabilities. SOCs uncover new vulnerabilities regularly, but it's difficult to determine whether it's in connection with a critical asset powered by sensitive data, whether there's an active attack in the environment, whether the network was already susceptible that to that type of threat actor, and/or whether the staff is focused on the right mitigating factors. Reconciling these factors is challenging for SOCs using legacy approaches and represents a clear opportunity for improvement.

Overall, talent has been a major challenge for cybersecurity leaders for years. The survey asked about the extent to which security leaders are facing a variety of talent-related issues in their SOCs. Nearly half said grappling with attracting and retaining talent, keeping staff educated, and a lack of specialized skills, highlighting the ongoing need for skill development amid the rapidly evolving cybersecurity landscape. These perceptions are especially prevalent among larger companies (more than 5,000 employees). Indeed, 51 percent of respondents from larger companies cited attracting and retaining talent as an issue, while 54 percent reported training and education as a major concern. This suggests that, even with greater resources and budgets, larger companies still need to work on developing effective strategies for recruitment, retention, and training of employees.

The talent gap sentiment feels like it is becoming less acute, but at nearly 50 percent, these responses suggest there's still a fairly long road to go to make it a nonissue. Nonetheless, the fact that less than half of security leaders cite these factors as major issues is a positive sign and suggests progress is being made.

A little under half of security leaders cited challenges retaining talent and keeping up with training and maintaining the necessary expertise to deal with sophisticated threats

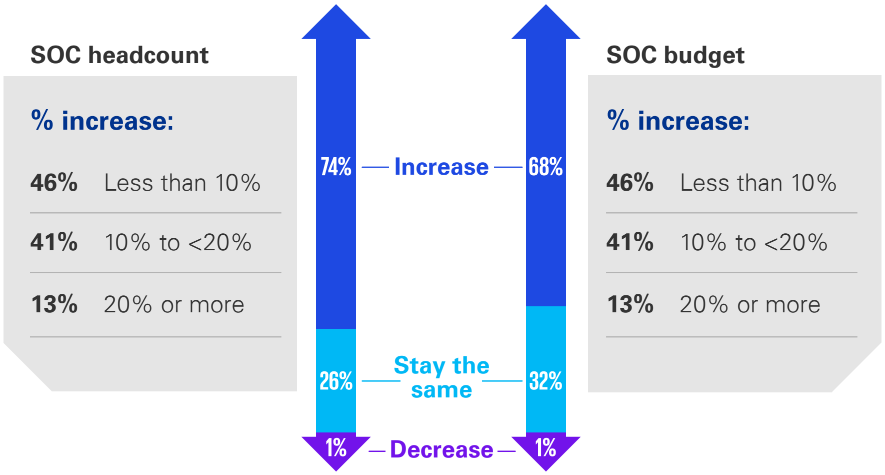


Base: Total security leaders, n = 200

Despite the fluidity of the current talent dynamic, a significant number of respondents (74 percent) expect an increase in their SOC headcount over the next two years while 26 percent anticipate no change. Among those expecting headcount increases, 46 percent believe the increase will be less than 10 percent and 41 percent believe it will be between 10 percent and 20 percent. A small minority, 13 percent, foresees a headcount increase of more than 20 percent. These potential increases are likely a reaction to the growing volume and complexity of threats, which highlights the need for adequate staffing levels to effectively manage cybersecurity going forward.

A similar number of respondents (68 percent) see SOC budgets rising as well. Interestingly, according to a recent survey conducted by Infosecurity Europe, nearly 70 percent of security leaders expect to increase their cybersecurity budgets, with approximately 50 percent allocated toward cloud security and incident response—solutions that are pertinent to day-to-day SOC responsibilities.[2]

Faced with a broad array of priorities and challenges, security leaders expect to increase SOC headcount and budget over the next two years



SOC headcount

% increase:

46%	Less than 10%
41%	10% to <20%
13%	20% or more

SOC budget

% increase:

46%	Less than 10%
41%	10% to <20%
13%	20% or more

Base: Expecting headcount to change, n = 200; percentage headcount expected to change, n = 147; expecting budget to change, n = 200; percentage budget expected to change, n = 135

[2] Infosecurity Europe Survey, 2024

Considering respondents expect both SOC headcount and, importantly, budgets to increase, where are budgets at the moment? According to survey respondents, the average annual SOC budget is about $15 million. In terms of how those dollars are allocated, the distribution is broad, which makes sense, with 19 percent going to prevention, 18 percent to detection, 17 percent to infrastructure, 16 percent to response and remediation, 15 percent each to AI/ML and log management and reporting.

Annual overall SOC budgets average nearly $15 million with nearly 40 percent going to prevention and detection

$14.6 million

Average annual SOC budget

Annual budget breakout

22%	Less than $2 million
38%	$2 million to less than $10 million
39%	$10 million or more

Average distribution of SOC budget across expenses

19%	**Prevention** (vulnerability, and threat intelligence)
18%	**Detection** (intrusion, endpoints, and network traffic)
17%	**Maintaining infrastructure** (i.e., hardware, cloud, storage, and network)
16%	**Response and remediation**
15%	**AI and machine learning**
15%	**Log management and reporting**

Base: Total security leaders, n = 200

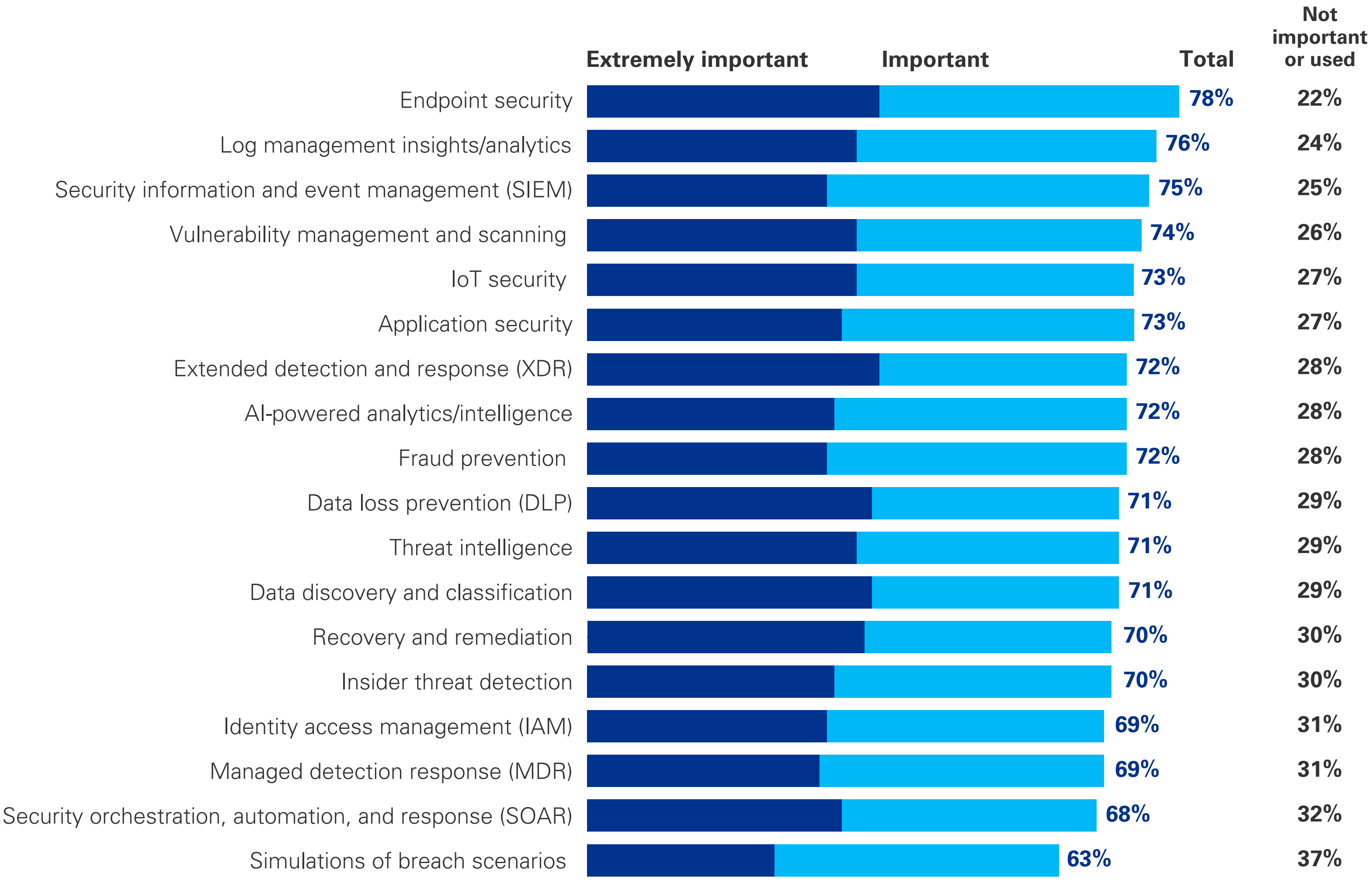
In general, the aggregate cost of security may be going up, but the cost of effective security is getting more and more efficient and optimized. Senior management expects to see justification for increased security investment and more confidence in where that investment is being spent. This aligns with cyber risk quantification as a supporting methodology for today's SOC.

Respondents made it clear that they view every major SOC service and solution as vital, with a range of two-thirds to nearly 8 in 10 classifying them as "extremely important" or "important." Of note, when asked how important these factors will be over the next two years, they all trended downward substantially—some by as much as 10 percentage points. This suggests that security leaders are in the process of consolidating the solutions they're looking to prioritize going forward.

No one expects CISOs to completely walk away from any of these tools—they are not going to declare, "We no longer need application security," for example. However, a rationalization of capabilities is happening. This is a major underlying theme. Security teams are moving from perhaps dozens of solutions in SOC to 8 or 10 because they're evolving to a platform approach or a suite of tools. This aligns with the question about barriers to identifying and remediating threats and vulnerabilities, to which the second most prominent answer was "complexity in the IT environment."

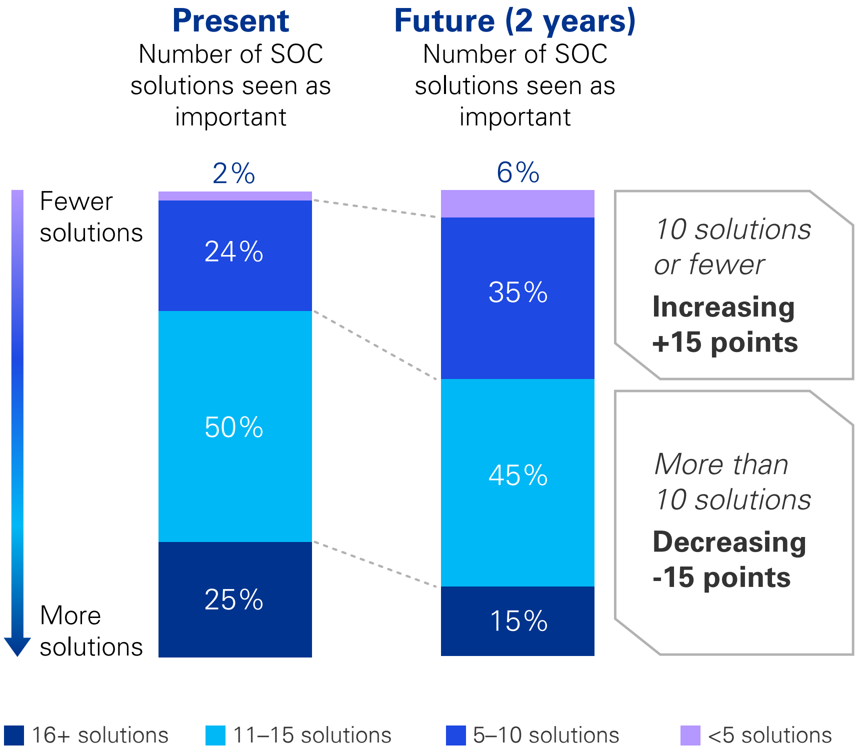
A number of the solutions respondents consider important—endpoint security, log management insights, XDR, and MDR, for example—are typically consolidated into companies' SIEM and SOC platforms, providing a centralized single pane of glass. Other tools—IoT security, fraud prevention, DLP, and IAM—are managed by individual teams on distinct and separate platforms. It's the source of much complexity, and where the single platform approach becomes very intriguing.

Security leaders point to myriad important current solutions currently in use in their SOC



Base: Total security leaders, n = 200

Looking ahead two years, security leaders say fewer services and solutions will be as important



Base: Total security leaders, n = 200

This suggests more prioritization and consolidation of solutions in the future. It also reflects the challenges experienced with complex security environments and lack of integration that security leaders cite as top challenges.

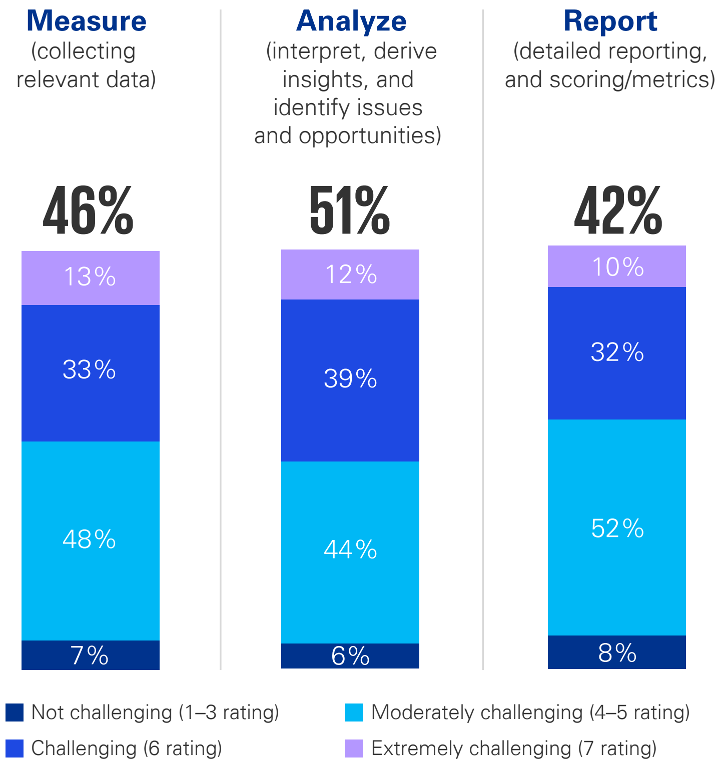
The consolidation of solutions is a binary decision for security teams. Many are weighing the choice of going all in on a platform-based approach versus deploying individual best-of-breed tools and trying to integrate solutions more effectively. The trend seems to be toward a spectrum of approaches. Some clients can't utilize a best-of-breed tool for every security need but can subscribe to one of the leading platforms. However, once they commit to a platform, the provider has negotiating power on pricing, which can get contentious. Instead of a broad expanse of best-of-breed technologies, we're starting to see islands of consolidation. In our view, it is more of a journey toward a platform orientation, with many organizations open to using a few stand-alone products. At minimum, consolidation is something security leaders are seriously exploring.

Performance:

A struggle, but leaders see the value

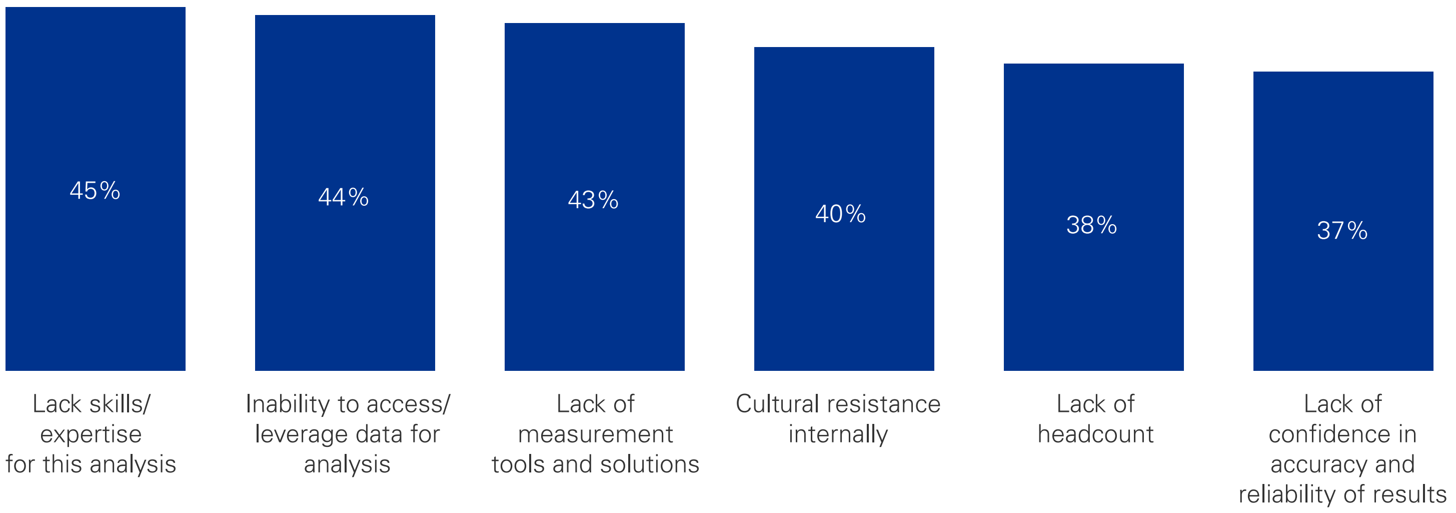
This survey reveals a deep well of optimism among security leaders, with nearly 7 in 10 reporting a high level of confidence in their SOC's understanding of the organization's risks and vulnerabilities, and nearly 9 in 10 saying they are confident in the SOC's readiness to prevent future attacks. At the same time, CISOs also acknowledge that they are not doing well when it comes to measuring and reporting on SOC performance. They talk about cost per incident, MTTD, MTTR, and false positive rates, among others, but only use an average of about three metrics regularly. That is worrisome. However, "better measurement and reporting" is one of the top answers when security leaders were asked about the potential benefits of AI-driven automation. They're struggling in this area, yet they are looking for ways to do better. That is encouraging.

At least 4 in 10 security leaders struggle with assessing their SOC's performance, with analyzing relevant data most prevalent



Base: Total security leaders, n = 200

When it comes to SOC performance, many organizations lack analytical expertise, are unable to access the necessary data, and/or don't have the proper measurement tools



Base: Total security leaders, select all answers that apply, n = 200

Why isn't the utilization of performance metrics higher? Clearly, there are challenges. These respondents are struggling to measure, analyze, and report on SOC performance, it appears, because they don't have the skills, the data, the tools, or the people.

Could it be that companies simply aren't prioritizing performance measurement, which would be a problem—and an opportunity? The fact that nearly 4 in 10 (37 percent) cite a lack of confidence in the accuracy and reliability of the results makes the low-priority hypothesis seem reasonable. A sizable number of respondents (45 percent) say a lack of skills or expertise impacts their ability to derive insights about their SOC performance. This highlights another embedded talent gap, suggesting that, although technology is an essential aspect of SOC solutions, there is still a need for skilled cybersecurity professionals.

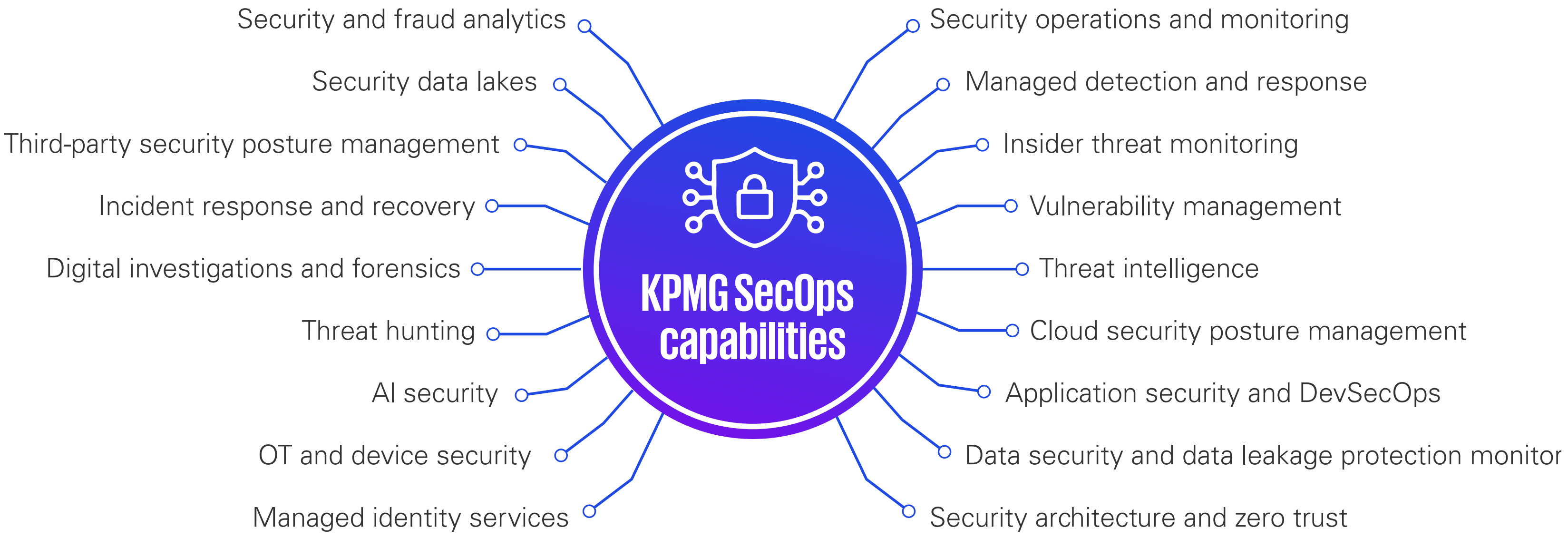
Conclusion:

Build the SOC of the future—today

Amid the chaos and noise from the huge volume of alerts, inevitable blind spots, increasing complexity, and growing costs, organizations big and small, public and private are operating against an ever-evolving cyber threat landscape and increasingly perilous and sophisticated cybersecurity attacks. An effective, intelligent SOC can help you manage and mitigate your cybersecurity risk. But building that capability requires collaboration, coordination, and communication.

Explore how our SOC support is different

KPMG can help you rethink and recalibrate your SOC strategy. From cyber managed services to more targeted tools, KPMG cybersecurity professionals are prepared to help address issues such as data quality, performance measurement and reporting, attracting and retaining talent, solution consolidation, and the impact of AI.

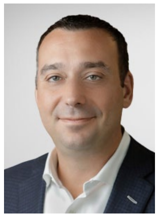

KPMG SecOps capabilities
Security and fraud analytics
Security data lakes
Third-party security posture management
Incident response and recovery
Digital investigations and forensics
Threat hunting
AI security
OT and device security
Managed identity services
Security operations and monitoring
Managed detection and response
Insider threat monitoring
Vulnerability management
Threat intelligence
Cloud security posture management
Application security and DevSecOps
Data security and data leakage protection monitor
Security architecture and zero trust

KPMG RANKED 1ST FOR QUALITY in AI advice and implementation in the US 2024

KPMG has been recognized as the top provider for quality in AI advice and implementation services in Source's annual US survey of senior buyers of consulting services. The study, titled "Perceptions of Consulting in the US in 2024," gathered insights from 700 senior executives, directors, and senior managers in the US. Source, a research-led consultancy specializing in the professional services sector, conducted the survey to understand how clients perceive consulting firms at different stages of engagement.

KPMG. Make the Difference.

For more information, contact us:



Charles Jacco
Principal, Cyber Security Services
KPMG LLP
212-954-1949
cjacco@kpmg.com

Ryan Budnik
Director, Cyber Security Services
KPMG LLP
512-320-5200
rbudnik@kpmg.com

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

Please visit us: in | **kpmg.com** | **Subscribe**

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act upon such information without appropriate professional advice after a thorough examination of the particular situation.