The CISO Report

From Risk to Resilience in the AI Era

splunk>
a CISCO company

Contents

Executive foreword

CISOs operate in the eye of the storm, at the center of constant transformation. Role responsibilities expand, threats evolve, and AI accelerates everything. It's relentless, but exhilarating.

Over the past 20 years, I've seen CISOs rise to the challenge. None more consequential than pioneering and securing AI initiatives across the enterprise. With AI now a priority for most, if not all organizations, our security stewardship is integral to business strategy.

This expanded mandate brings with it an exceptional level of pressure and personal accountability. We are not just managing technology. We are managing risk, talent, and the very digital resilience that drives critical business outcomes. To move forward, we have to work differently. This is our moment to innovate, adapt, and lead with a clarity that cuts through the noise.

We surveyed 650 global CISOs to learn how they're meeting the moment — from quantifying and communicating ROI to leadership to developing the next generation of cybersecurity talent. We also explore emerging technologies like generative and agentic AI — not as silver bullets, but as necessary enhancements to our human teams both within and outside of security.

The research findings are a testament to the resilience of the CISO. My hope is that you see your own experiences reflected in the data and walk away with the confidence to shape what's next.

For CISOs, the target will never stop moving. We wouldn't have it any other way.

Michael Fanning

CISO, Splunk

The CISO stands resilient

The CISO's role is more demanding *and* dangerous, with very real, personal stakes on the line. Seventy-eight percent of CISOs are now concerned about their own liability for security incidents, a sharp jump from last year, when 56% expressed similar fears.

Yet, in the face of escalating demands, the CISO stands resilient. They are meeting modern needs by investing in solutions like generative and agentic AI to strengthen their organization's security and boost productivity. The CISO's keen eye recognizes that human intelligence and creativity will always be security's most powerful tool. So, they prioritize upskilling their staff and hiring for critical roles like threat hunting, rather than relying solely on technology.

CISOs are also navigating more organizational complexities, working alongside non-technical executives on key security and business initiatives in a greater capacity. But communication and cybersecurity knowledge gaps persist. The solution? Leverage data to transform technical nuances into a clear business imperative that non-technical leaders can get behind.

When the going gets tough, CISOs show true grit. Survey data suggests that despite everything coming at CISOs, they are staying in the fight to not just defend their organizations, but champion true digital resilience.

Chapter 1

The expanding role of the CISO

The CISO's role isn't just evolving — it's *expanding*. They are now architects of trust and resilience for the entire organization, responsible for data privacy, regulatory compliance, third-party cyber risk, and so much more. No wonder 79% report their role has become significantly more complex.

When leadership priorities shift, as they often do, the resilient CISO steps up to transform vision into secure execution. Take AI, for instance. The survey reveals a whopping 96% of CISOs are now responsible for AI governance and risk management, making them the de facto AI policy leaders at their organizations. That's not just an add-on duty: It's a full-blown extension of their already overwhelming mandates. CISOs are also participating in cross-functional governance committees to vet proposed AI usage. These committees explore which models are being used, how they are trained, and whether they can learn and update themselves automatically (in the case of agentic AI).

And who knew CISOs would oversee engineers and software developers? Eighty-five percent report that secure software development (DevSecOps) now falls under their purview. Meanwhile, 67% of CISOs are wrangling the wild world of IoT/OT/ICS security integrations, ensuring security isn't an afterthought, but a foundational ingredient of digital resilience.

71%

say changing leadership priorities create at least a *minimal challenge* for their cybersecurity strategy

> **The CISO's role is no longer just about data privacy or preventing breaches. Now, it includes regulation and compliance, resilience and uptime, and collaboration with departments outside security.**
>
> — Kirsty Paine, Field CTO, Splunk

CISOs rise to the challenge

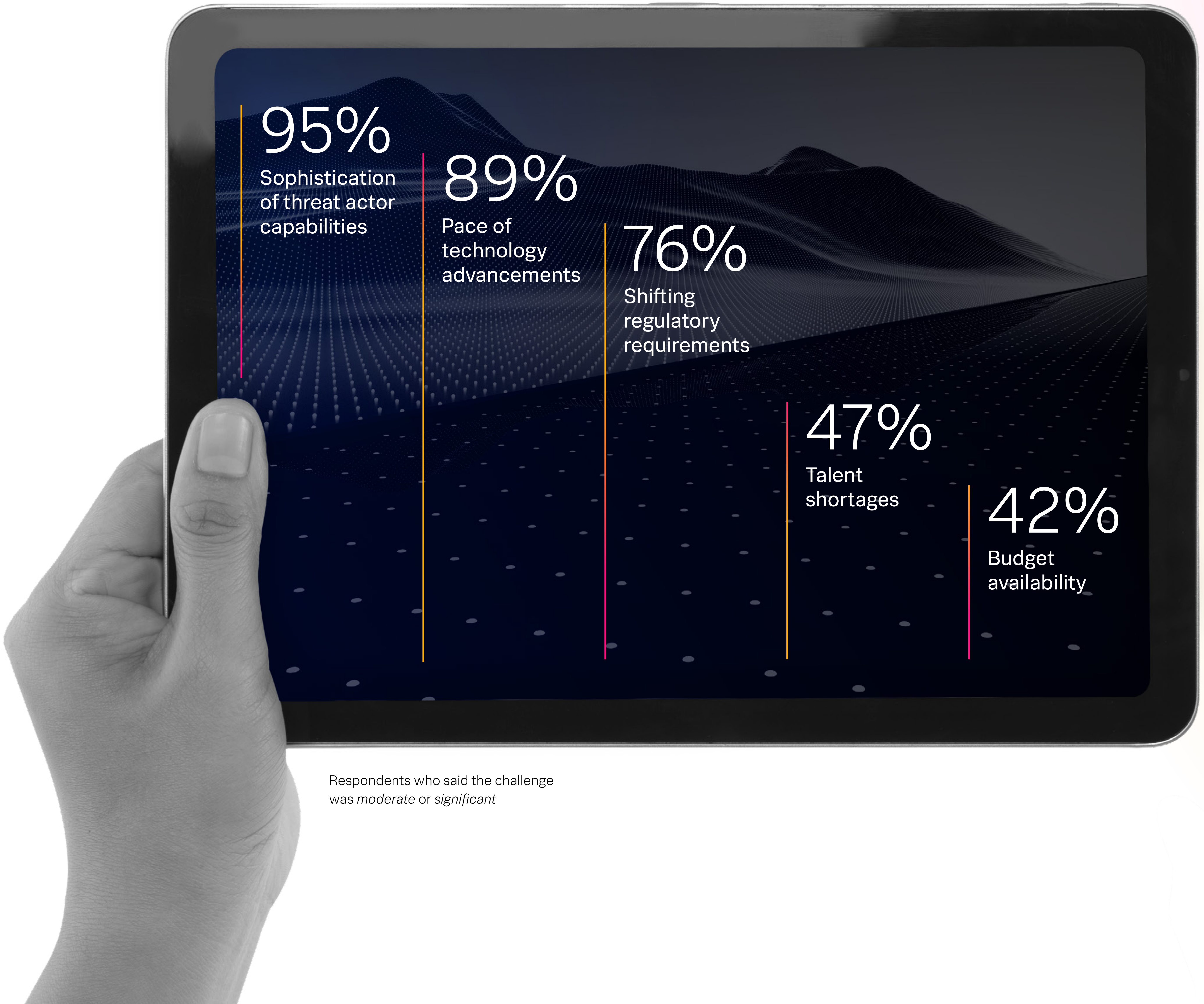
CISOs face a dual challenge: Externally, they confront an increasingly sophisticated threat landscape; internally, they must orchestrate and manage budget, talent, and executive buy-in to mount their defense.

According to 95% of CISOs, the growing sophistication of threat actor capabilities poses the greatest threat to their cybersecurity strategies. Gone are the days of obvious phishing emails filled with bad spelling and grammar. Today's attacks are far more bespoke and convincing: A voice memo under the guise of your CEO may urgently request confidential documents. An email purportedly from your company's HR department may ask you to complete an anonymous employee survey.

But that's not all. "New, highly sophisticated malware proof-of-concepts, like BlackMamba, use AI to change their own underlying code, structure, or behavior to evade EDR detection," explains Splunk Field CTO Kirsty Paine. "It's not long before this becomes a widespread attack methodology, and security teams will need equally advanced defenses to counter it."

Meanwhile, the breakneck pace of technology advancements remains a challenge for 89% of CISOs. Couple that with the 76% who report shifting regulatory requirements that prompt organizations to focus more on how consumer data is being used, protected, and impacted in the event of a breach. The CISO's work is never truly finished.

The CISO's biggest obstacles



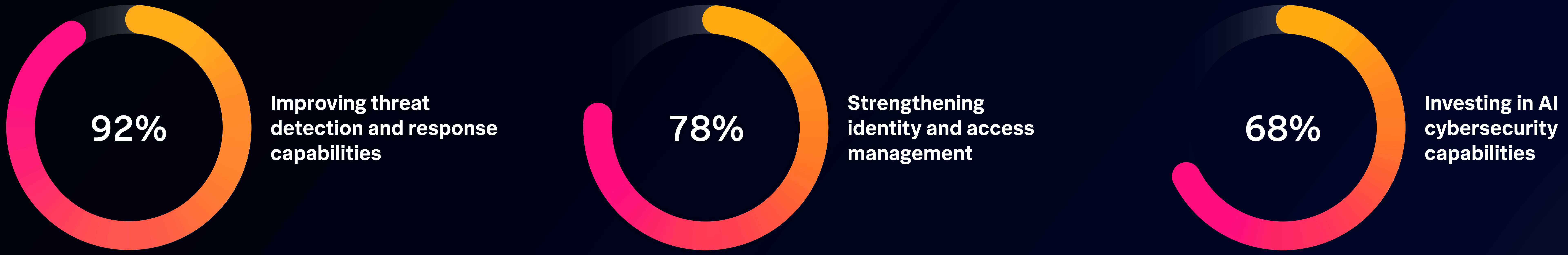
Respondents who said the challenge was *moderate* or *significant*

To bolster their security postures, CISOs are not simply reacting to incidents, they're strategically investing in preventative solutions. Today, boards are mandating AI use across the enterprise (including cybersecurity), so it's unsurprising that CISOs tell us it's a top-three priority.

However, many CISOs are somewhat skeptical about AI's security and effectiveness. In a sense, adoption is both a priority *and* a challenge. CISOs must ensure their investments are safe, purpose-driven, and aimed at achieving tangible outcomes like improving threat detection and response capabilities. AI adoption presents a unique dilemma for CISOs — one we'll examine more closely in later chapters.

> **I'm concerned we're living through a 'boiling frog' moment. We're so inundated with fake messages, links, and voicemails that our sense of what's real is slowly eroding. By the time we notice, the water's already boiling — and the damage is done.**
>
> — Bjoern Watne, Global CISO, Interpol

The CISO's top priorities



Respondents who ranked *very* or *most important*

Chapter 2

Strategies shaped by shared visions

No CISO is an island. Their expanded scope places them shoulder to shoulder with their C-suite counterparts, sharing accountability for critical initiatives. Survey data reveals CISOs are shaping strategies, managing tools, and overseeing resources that extend beyond the traditional security domain.

So, who are CISOs teaming up with most often? Unsurprisingly, technical C-suite roles like the CIO and CTO are the CISO's closest allies, particularly on security-related initiatives. However, when it comes to KPIs, CISOs most commonly work with other executives, such as the CFO and Chief Legal Officer. This could be because CISOs often get their funding from the CFO, while legal often directs cyber-incident response efforts. These roles truly help CISOs get the job done.

According to Splunk Field CTO Peter Sprenger, CISOs should work closely with the *entire* C-suite. "Joint-accountability isn't just about playing nice — it's a business imperative," says Sprenger. When a CISO is partially responsible for business deliverables (and all executives have skin in the cybersecurity game), organizations are better positioned to manage risk and adapt to regulations without sacrificing innovation or business success.

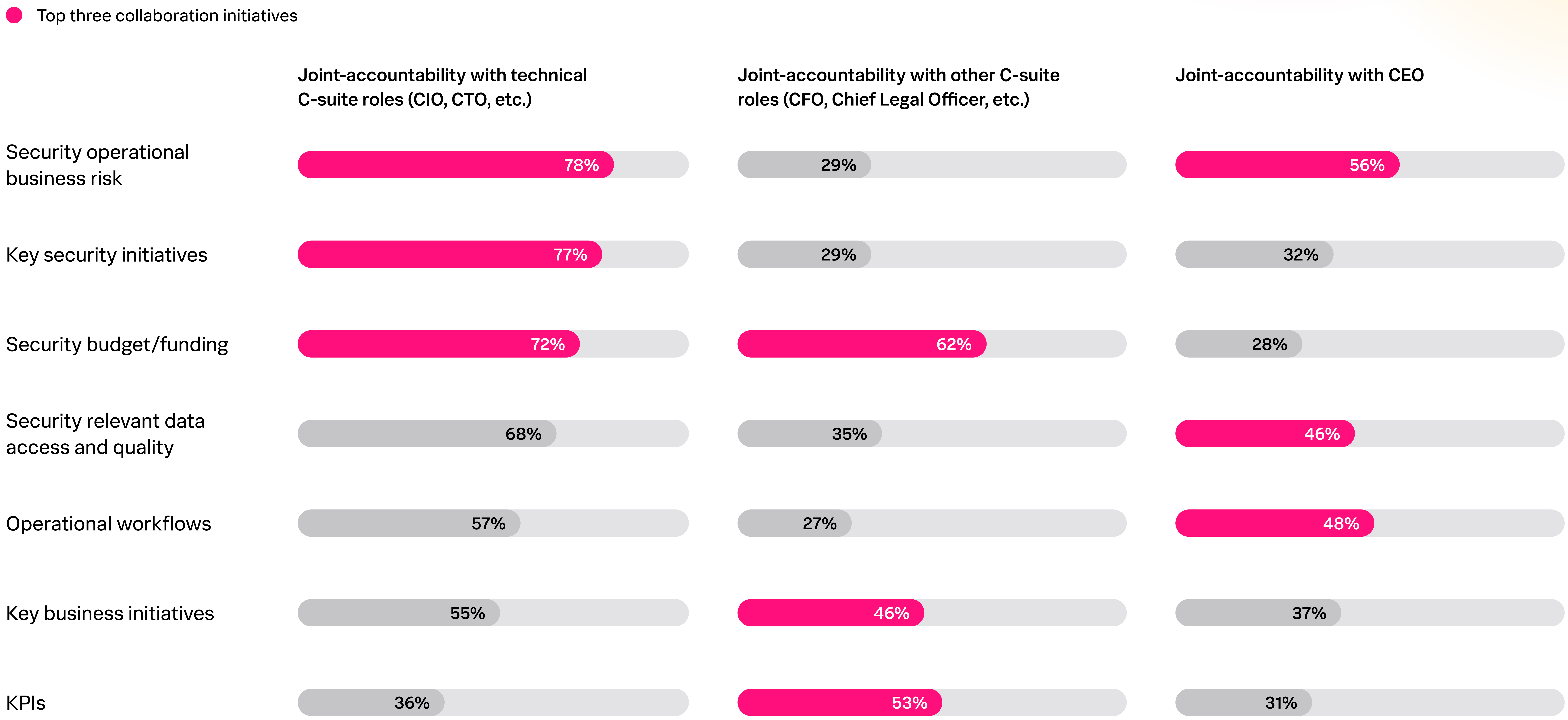
For CISOs, the most critical success factors are organizational. By establishing shared planning cycles, cyber defense becomes proactive and embedded across the entire business.

Collaborating with C-suite counterparts makes a difference in security outcomes. According to CISOs, joint accountability drives the most value for key security initiatives (62%), security budget and funding (55%), and access to security-relevant data (49%). CISOs typically share these high-value efforts with their technical C-suite counterparts.

A key evolution in my role has been establishing a dotted-line relationship with the CEO and CFO. Through regular discussions, we connect business strategy with cyber risk and its measurable impact on the bottom line.

— Stephen Davis, CISO, Hubbell Inc.

CISOs collaborate across the C-suite



Respondents could select all that apply

Bridging the cyber knowledge gap

The data reveals that low cybersecurity fluency among other C-suite leaders is the most significant hurdle to collaboration (85%). While CISOs recognize value in these partnerships, cyber knowledge gaps create tension.

So, how do CISOs bridge these knowledge gaps and ensure everyone in the C-suite — from the CEO to CFO — speaks the same language of risk, security, and business impact? The answer is data. It's a common tongue that can soundly express the nuances of digital resilience, illuminate shared risks, and drive unified decisions. When departments across an organization share data and context, teams can work from a mutual base of understanding, and the conversations shift from "why" to "what next?"

However, the CISO stands in a gray area. Their conservative (and entirely justifiable) outlook on privacy means they aren't always willing to dole out every byte of data. An overwhelming 91% of CISOs cite data privacy concerns as the top challenge to improving cross-departmental data sharing. Other blockers include the high costs of storing data (76%) and a lack of shared data views or operating layers (70%), creating silos that hinder holistic visibility.

Rather than introducing unnecessary risk by generating and moving duplicate data or working in silos, organizations can adopt a data fabric architecture. This shared data layer provides a unified and secure way to manage data, acting as a connective tissue by connecting disparate data sources. Capabilities like federated search allow teams to access and analyze data without costly movement or duplication.

With a data fabric architecture, CISOs can better enforce granular privacy and governance policies at the data layer itself, ensuring security teams have the context they need for improved alerting, detection, and response — all without risking the exposure of sensitive information.

C-suite collaboration obstacles

85%

Low cybersecurity fluency among non-technical executives

71%

Risk appetite misalignment

66%

Lack of shared understanding of security's role in business success

31%

Lack of integrated workflows with other teams

28%

High data volumes and related costs

Chapter 3

The AI imperative

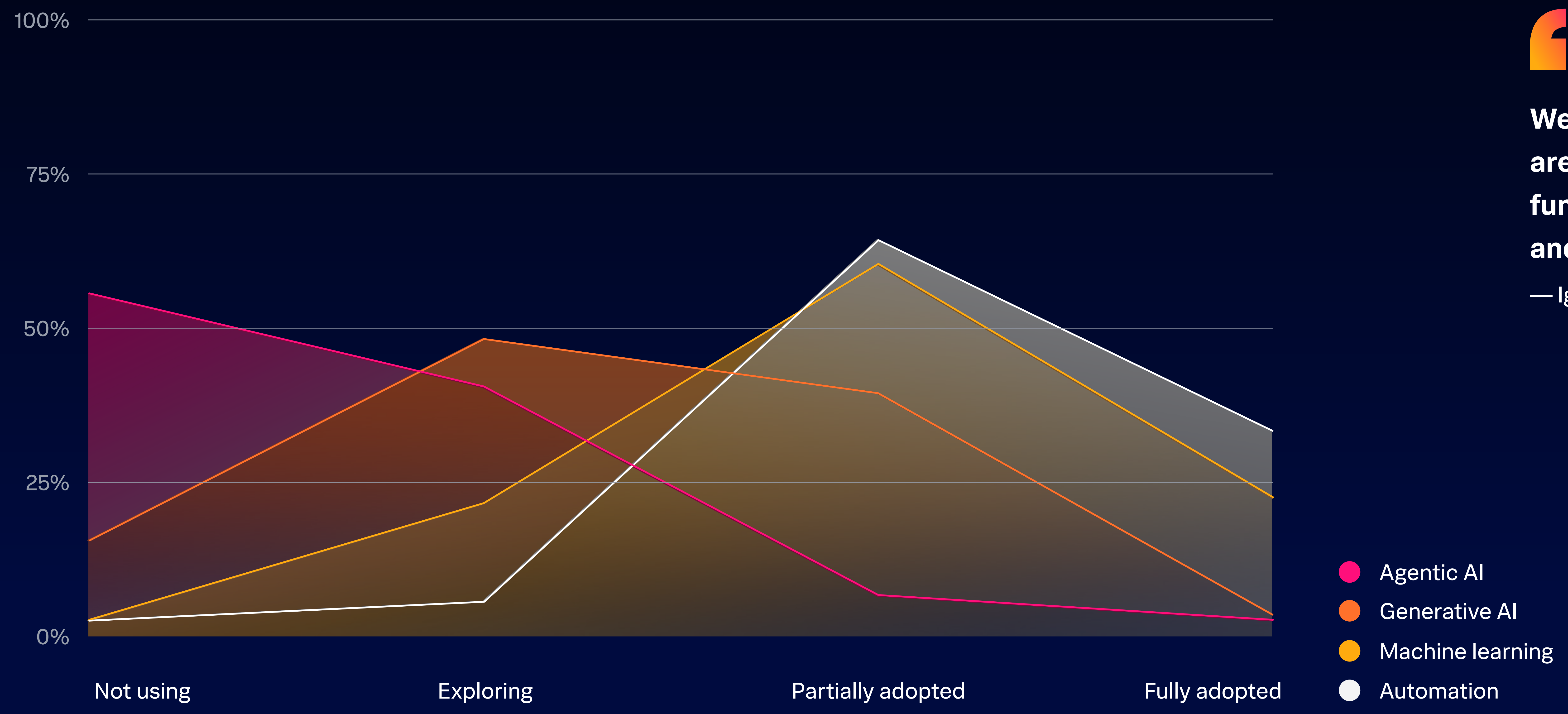
AI adoption is no longer a question of “if,” but “how much,” and “what kind?” As boards mandate AI use across the business, CISOs must proactively manage risk to safeguard their organizations. This means establishing a robust governance framework that enables safe AI, ensuring the pursuit of new capabilities doesn’t introduce critical vulnerabilities.

From automation to agentic AI, survey data reveals a clear adoption curve linked to the maturity and perceived risk of each technology. CISOs are actively experimenting with generative AI, but less than half (40%) currently use it in their security functions.

As the newest and most complex technology, agentic AI carries the highest perceived risk. While only 6% of CISOs are using it, 39% are beginning to explore its potential. The promise of initial capabilities like detection and triage agents, where security assistants rapidly provide more relevant information to an investigation, are too good to pass up. No doubt, adoption will continue to grow, alongside a heavy dose of cautious optimism.

Adoption rates for automation, machine learning, generative AI, and agentic AI correlate to a CISO's confidence with them. Eighty percent of CISOs are at least *very confident* in their team's ability to identify appropriate security use cases for machine learning, while only 37% feel the same for generative AI. This suggests that, as generative and agentic AI become more established, CISO confidence and usage will increase as well.

CISOs explore and embrace new technologies



Percentages may not add up to 100% due to rounding

> **We're in the exploration phase for agentic AI. But we are mindful that every new capability is additional funding, additional investments, additional people, and additional training.**
>
> — Igor Spektor, CISO, Tracfone

Measuring AI’s impact on security

More established technologies are living up to their hype. For example, among CISOs using it, automation is the investment most likely to *exceed expectations* (83%). Meanwhile, CISOs are still figuring out generative AI’s place in the security sandbox: Only 14% of users say it *exceeds expectations*. Its full value proposition and risk profile are still a work in progress. Ironically, 22% of CISOs say agentic AI *exceeds expectations*. At the same time, 25% claim it *misses expectations*. Some CISOs who say agentic AI misses the mark may simply operate in highly-regulated industries, so their efforts are under more scrutiny by leadership and regulators. Another explanation could be overhyped ambitions. Regardless, the technology holds significant promise, but because it’s so new, the mileage will vary widely. Over time, we expect the pendulum to definitively swing one way or the other.

So, what’s the immediate payoff? Right now, AI is largely seen as a productivity powerhouse. Considering that alert volume is becoming unmanageable, CISOs are right to use it to help sift through the noise, identify critical threats, and efficiently manage information.

While productivity gains are critical, when it comes to quantifying AI’s value, CISOs cite metrics such as mean time to detect (MTTD) and mean time to respond (MTTR) as their North Star.

However, a mature AI strategy requires CISOs to look beyond historical metrics such as MTTD and MTTR. With the help of AI, CISOs now have a greater ability to measure detection quality, risk scores, and compliance posture. Looking ahead, these metrics will not only better assess the impacts of AI but will also become essential for evaluating the overall effectiveness of the entire security function.

AI enables productivity gains

92%
Allows more security events to be reviewed

89%
Improves ability to correlate data from multiple sources

65%
Increases reporting speed

51%
Accelerates execution of basic repetitive tasks

Respondents who *somewhat* or *strongly agree*

What worries CISOs most about AI

With newfound capabilities comes a fresh set of anxieties for CISOs. Although some form of AI adoption is now commonplace across security workflows, the risks can outweigh the benefits.

An immense 78% of CISOs rank data leaks as their top concern, which can put an organization and the CISO in hot water with regulators and the public. Hefty fines, revenue and stock price hits, and even termination are all possible outcomes (not to mention the CISO's personal liability). Shadow AI presents a direct challenge to governance, control, and the integrity of security operations — in other words, everything the CISO strives to protect. And if your AI generates plausible but incorrect information, it could lead to misinformed decisions at scale that undermine both critical security choices and the business as a whole.

"To safeguard sensitive data, CISOs are deploying AI tools in private environments that use dedicated clusters and strict training guardrails," says Splunk Global Field CTO Cory Minton. This approach, combined with firewall monitoring and tool instrumentation, also helps combat shadow AI. To manage output quality and minimize hallucinations, Minton suggests that security teams continuously assess responses through internal user feedback systems. This can be done with simple thumbs up/thumbs down buttons, which measure output quality objectively through trend analysis and aggregation. This process both informs model retraining and acts as an alerting system, flagging outputs that violate established guardrails.

Incidentally, the survey reveals that CISOs in organizations with greater AI maturity fear these risks even more. Eighty-five percent of generative AI users cite data leakage as the largest risk, versus 71% of non-users. Meanwhile, 90% of generative AI users rank shadow AI as a top-three concern, versus only 79% of non-users. Clearly, CISOs who are further along in their generative AI journey are starting to notice some trade-offs.

It's now up to the CISO to make sense of it all; strategically embracing AI while building robust guardrails around its use. The path forward requires vigilance and adaptability. It's the CISO's role to ensure that innovation serves security, not compromises it — toeing the line between progress and protection.

1 **Data leakage**

2 **Shadow AI**

3 **Hallucination impacts**

Chapter 4

The promise of agentic AI

Picture a supercharged SOC where autonomous agents tirelessly detect, investigate, and remediate security threats in record time. Today, that vision is closer to reality than ever. But while the buzz around agentic AI is undeniable, the data confirms that CISOs have not deployed it to a meaningful extent — yet.

Around one in five CISOs use AI agents in specific, high-value areas like third-party breach analysis, remediation, and containment tasks. However, for the majority of CISOs, agentic AI is still more of an aspiration than a reality. Many indicate they are either in the exploration phase or plan to adopt it within the next 12 months to help close critical skills gaps like threat hunting. Despite initial hesitancy, CISOs are preparing to make AI agents a core security component.

Regardless of where they land on the adoption curve, CISOs believe agentic AI will fundamentally strengthen their security postures and amplify the impact of their teams. The data paints a picture of autonomous agents sifting through endless alerts and logs, freeing up human analysts to focus on critical thinking and strategic analysis. This positive outlook extends to business and operational benefits like improving security ROI and offsetting security-related talent gaps.

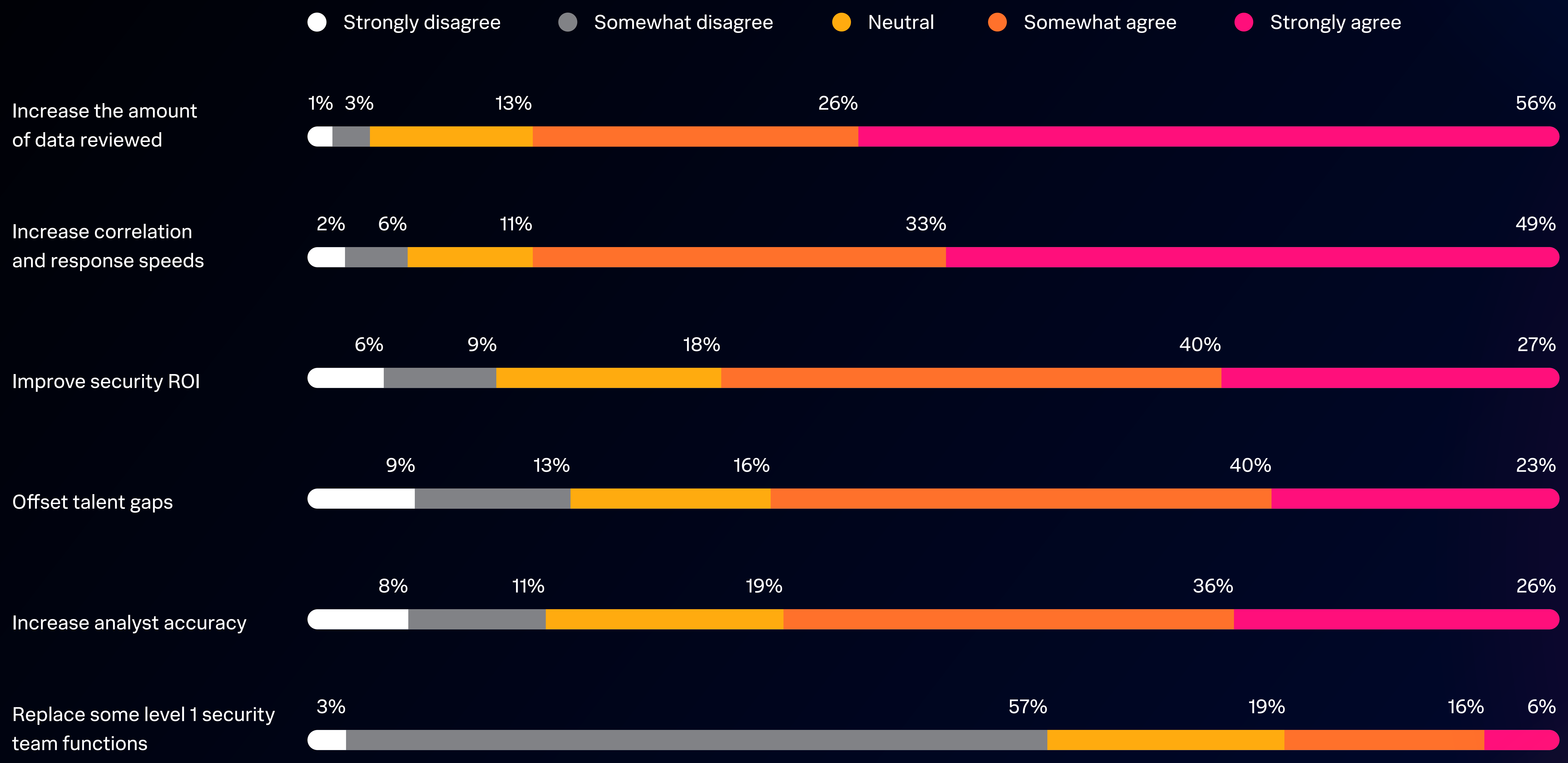
Crucially, CISOs expect AI agents to boost their security teams' efficiency and accuracy, *not* replace analysts outright. In fact, a resounding 60% of CISOs disagree with the statement "agentic AI will replace some level 1 security team functions." The objective here is augmentation and collaboration (more on this in the next chapter).

CISOs are right to feel optimistic. Survey data reveals that those who have implemented agentic AI are already seeing improved operations. Among CISOs who have partially or fully adopted the technology, 39% *strongly agree* it has increased their team's reporting speed by more than double the rate of those who are still exploring (18%). In addition, CISOs who have partially or fully adopted agentic AI reduce time spent on repetitive tasks: They're over twice as likely to *strongly agree* on this point (28% partially and fully adopted versus 13% of those in the exploration stage). For these early adopters, agentic AI is quickly becoming a competitive advantage.

39%

strongly agree **agentic AI has increased their team's reporting speed**

CISOs are bullish on agentic AI's potential



Percentages may not add up to 100% due to rounding

Autonomous, but at what cost?

Despite agentic AI's potential, CISOs are not blind to the inherent risks. Their enthusiasm is paired with skepticism, rooted in very real concerns about the technology's autonomous nature.

CISOs overwhelmingly rank hallucination impacts, like missed alerts or false positives, as their number one concern (83%). Another significant worry is the uncharted waters of ethical and legal responsibility for actions taken by autonomous agents. Who is accountable when an agent makes a mistake with real-world consequences?

Naturally, the prospect of making critical decisions without sufficient human oversight or understanding is also a top concern. CISOs may not share this same apprehension for other, more traditional forms of AI because they don't act autonomously.

Unpredictable behavior and lack of transparency round out the list. According to Splunk Field CTO Peter Sprenger, this makes sense: "CISOs must show a repeatable chain of evidence to ensure the integrity and admissibility of data in investigations, legal proceedings, and compliance audits. How they can provide that to their board or regulators — when autonomous agents make decisions and carry out tasks themselves — remains a challenge."

CISOs are already taking steps to mitigate the shortcomings of agentic AI, building robust governance frameworks and establishing proper human oversight to ensure the technology is used safely and responsibly.

78%

create dedicated security teams for AI agents

CISOs have valid concerns about agentic AI

1. **Hallucination impacts**
2. **Lack of human oversight**
3. **Ethical or legal liability**
4. **Unpredictable behavior**
5. **Lack of transparency**

AI levels up adversaries

While CISOs are busy shoring up their internal defenses, they also believe AI will enhance external threats. But because AI lacks creativity, they aren't stressed that the technology (both agentic and non-agentic) will create novel attacks. Rather, their primary concern is a surge in sophistication, speed, and volume.

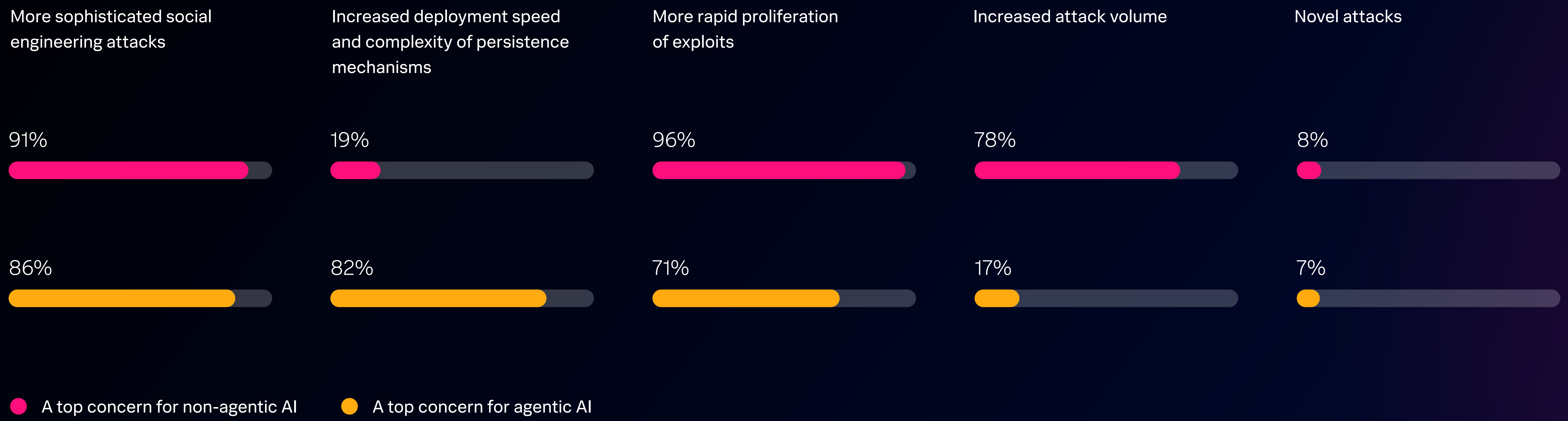
A staggering amount fear that agentic and non-agentic AI will increase the realism and effectiveness of social engineering attacks (86% and 91% respectively), making them more difficult to detect and defend against. CISOs can best prepare for these threats by diligently training *human intelligence* to identify and recognize patterns among subtle anomalies.

Similarly, 82% worry agentic AI will increase deployment speed and complexity of persistence mechanisms, making it significantly harder to dislodge them from compromised systems. This contrasts sharply with only 19% of CISOs who hold the same concern for non-agentic AI, highlighting the perceived leap in damage potential.

When it comes to increasing attack volume, CISOs believe agentic AI is a lesser threat than other forms of the technology. Only 17% consider it a core concern for agentic AI, versus 78% who attribute this potential to non-agentic AI. This suggests CISOs view AI agents as an amplifier of quality and impact rather than a generator of more attacks. For the time being, generative AI is the larger threat, mainly because it unlocks more sophisticated attack vectors like deepfakes.

> **If your security function isn't using AI, it's like taking a knife to a gun fight. For CISOs, that can be a tough pill to swallow.**
>
> — Mike Salem, CISO, IHS Towers

CISOs sound the alarm on AI-driven threats



Respondents could select their top three for both categories

Chapter 5

CISOs choose talent over tech

From the boardroom to the SOC, CISOs are expected to be strategic visionaries, operational maestros, and educators all at once. But security is a team sport, requiring the expertise of many highly specialized roles.

According to CISOs surveyed, the skill sets most lacking in their security programs are threat hunting, engineering support (for vendor tooling, detection engineering, or maintenance), software development, and network and cloud architecture. These gaps are especially painful to CISOs as they undermine the ability to address their top challenge, the growing sophistication of threat actor capabilities, and their top priority, improving threat detection and response.

Although CISOs are examining ways AI agents can help increase detection speed, they make it abundantly clear that technology won't replace any security analyst jobs. Instead, they are investing in human capital, recognizing that the nuanced, adaptive intelligence of a skilled workforce is irreplaceable.

In fact, when asked which methods they're using to close skills gaps on their team, addressing them with technology like AI and automation ranked dead last. CISOs know they can't solve the problem with technology alone; security relies on highly creative, seeker-mindset analysts and threat hunters to keep pace with equally creative attackers.

While AI is a productivity lifesaver, it lacks the nuanced judgement needed to recognize subtle anomalies. And automation will merely respond to things it knows. To successfully defend against the growing sophistication of threat actor capabilities, CISOs will continue to rely on human intelligence. Plus, even if a CISO adopts AI to supercharge their security program, they'll always require oversight and control. For the ever-vigilant CISO, ensuring a human is in the loop is not only pragmatic — it's paramount.

1%

view technology investments as a primary means of addressing skills gaps

> **Because of AI, CISOs will need to constantly reskill, upskill, and bring in new talent required to achieve the ROI leadership wants. In this sense, AI will be creating jobs, not eliminating them.**
>
> — Ryan Fetterman, Senior Manager, SURGe by Cisco Foundation AI

Of CISOs who rank threat hunting as their team's biggest skills gap, 71% tell us upskilling their current workforce is a top means for addressing shortages.

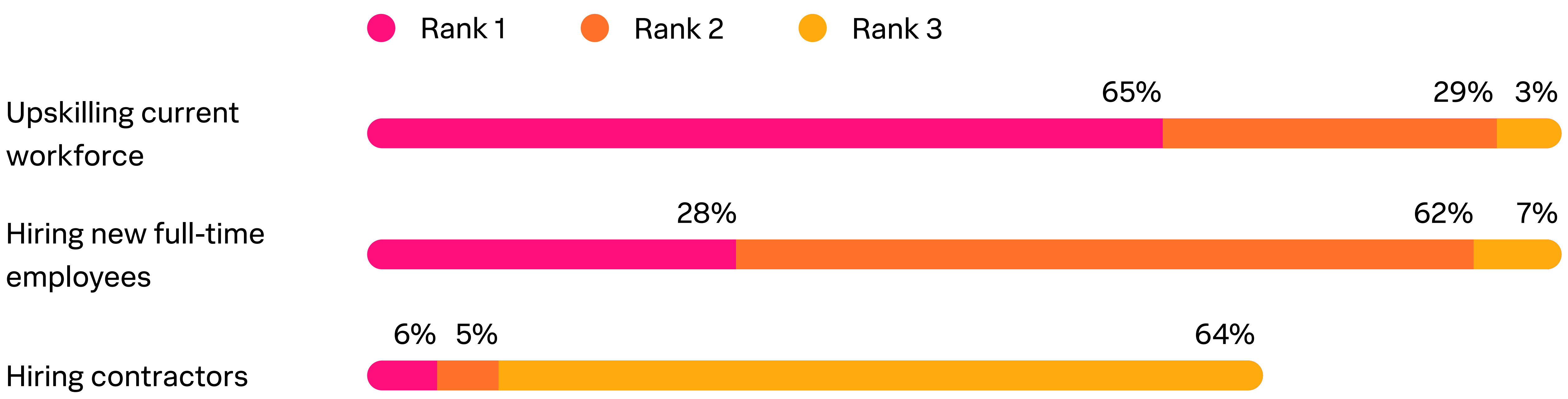
CISOs with bigger engineering gaps tend to focus on hiring new full-time employees. Among the 9% who identify engineering support as their team's most pressing need, nearly half (46%) say hiring is their number one solution, compared to the survey average (28%).

And for CISOs whose biggest gap is software development, hiring contractors to augment their staff stands out as a popular choice: Over a third (35%) of these CISOs rank it as their number one approach to address shortages, nearly 6 times the survey average (6%). "There's generally a limited engineering focus within the CISO's organization," explains Ryan Fetterman, senior manager, SURGe by Cisco Foundation AI. "So there isn't a large need for long-term continuous software development. These contractors would support one-off problems or integrations that wouldn't require permanent headcount."

However, CISOs aren't wholly optimistic about filling these roles any time soon — or at all. A mere 16% expect to fill all their gaps, while a sobering 79% expect *some* or *most* to remain unfilled.

"Investing in your teams, in part, means rethinking your hiring strategy," says Splunk CISO Michael Fanning. "I challenge conventional wisdom that demands a cybersecurity degree or a decade of experience. In a field where technical knowledge becomes obsolete quickly, a candidate's foundational understanding of computing, systems, and networks — as well as curiosity, adaptability, and problem-solving skills — are far more valuable. Cyber knowledge can be taught, where needed, on top of that foundation." By hiring for potential, security functions can build future-proof teams that evolve with the threat landscape. Otherwise, they may buckle under immense pressure and fatigue.

CISOs are taking a people-first approach to closing skills gaps



Respondents ranked their top three choices

The burnout epidemic

Closing skills gaps is only half the battle; there's also retaining your workforce. Unlike AI, humans get tired, stretched thin, and overworked. To prevent a costly churn of security talent, CISOs must actively work to mitigate burnout. Forty-five percent of CISOs sense *moderate burnout* among their employees, while another 20% would characterize it as *significant*. That's nearly two-thirds of security teams feeling the strain.

What's driving the majority of SOC stress? The culprits are clear: alert floods and tool fatigue.

While CISOs navigate their rapidly expanding role at the executive level, their teams are withstanding an onslaught of alerts. This isn't just a nuisance; it's a crisis of context, where critical insights and real threats get buried under a mountain of noise.

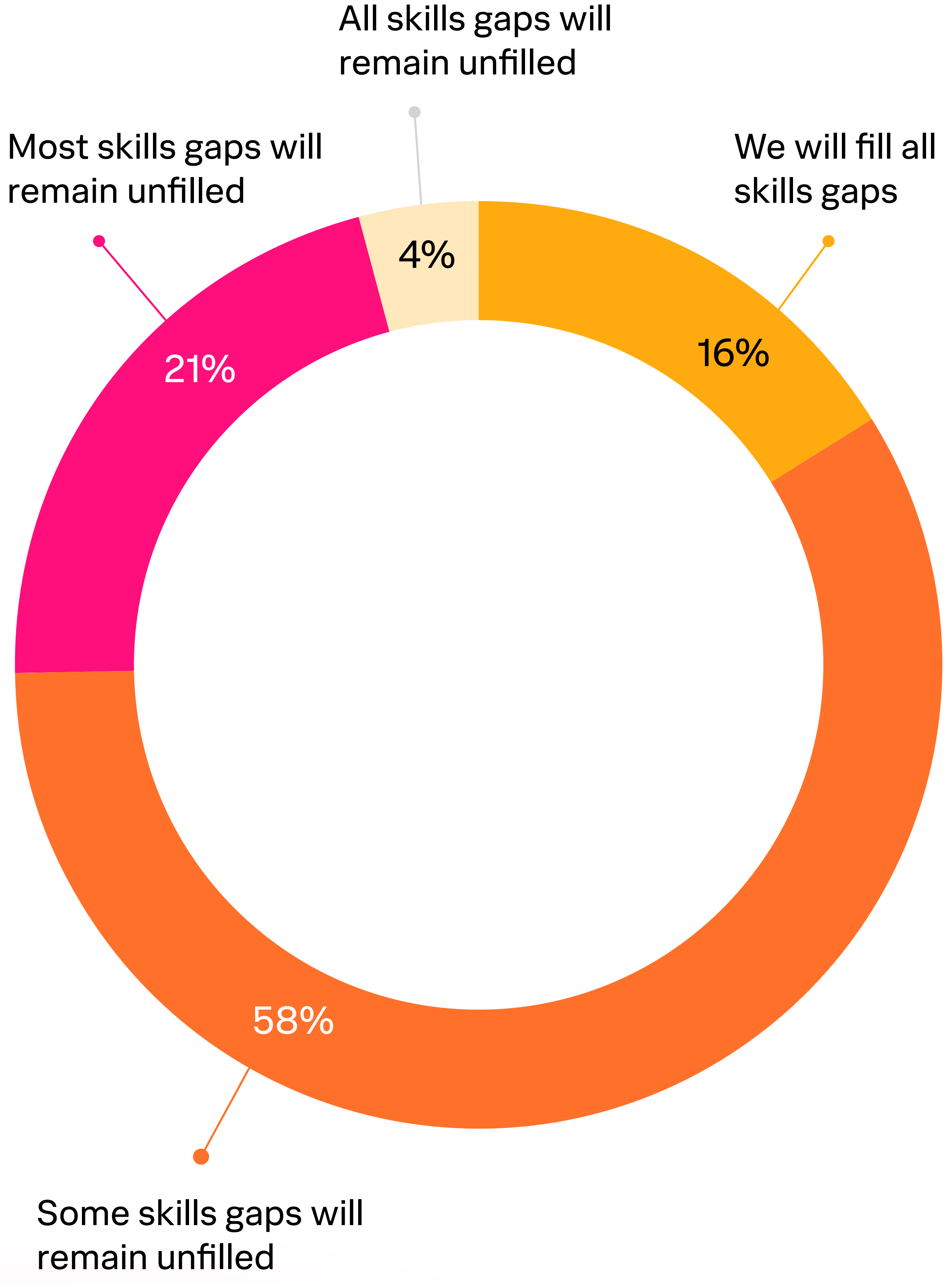
It's difficult to prioritize alerts when everything feels urgent. "Fine-tuning detections and leveraging automation will reduce the overall number of alerts, while creating context-enriched tickets will reduce manual effort," says Splunk Field CTO Kirsty Paine. "This will not only streamline investigations, but help to mitigate alert fatigue and burnout."

Data sharing can also provide context and clarity, but only 54% of CISOs admit they have consolidated security data into a single view. A shared data layer, like an intelligent data fabric, addresses the root causes of burnout head on by automating the entire data collection process across security tools. Connecting and contextualizing data from multiple sources provides analysts with context-enriched alerts, which filters out noise and eliminates fatigue.

We have so many tools that it's difficult to make them work together effectively. Our focus now is to provide analysts with higher quality alerts.

— CISO at an international insurance group

Talent gaps will continue



Percentages may not add up to 100% due to rounding

Alert floods and tool fatigue drive SOC stress

98%	High alert volume
94%	High false alert volume
79%	Number of tools (“swivel chair syndrome”)
63%	Understaffed team
20%	Rapidly changing technology landscape

Chapter 6

Measuring security success

On top of their core security functions, CISOs must also translate the complex and often chaotic world of cybersecurity into clear-cut business value. They're asked to prove worth, justify investments, and demonstrate progress to a board and C-suite that require clarity, but don't always understand technical nuance.

Historically seen as a cost center, CISOs are beginning to reframe security as a business enabler. According to Splunk CISO Michael Fanning, “CISOs shouldn’t expect leadership to inherently understand security’s value. We have to showcase it — proactively.” By quantifying ROI on cybersecurity spend, CISOs can build a more compelling business case. However, being able to do so is somewhat of a mixed bag.

Forty-one percent of CISOs admit they cannot correlate ROI directly to risk mitigation and remediation activities. This may be linked to how well CISOs collaborate with their peers. “In my experience, CISOs who have trouble correlating ROI to risk mitigation still think of it like insurance,” says Splunk Field CTO Anthony Pierce. “But CISOs who open up that black hole of data and work directly with their CFOs and other business units are able to put a number on these measures.”

To this end, survey data shows that CISOs who share joint-accountability for their security budget with non-technical C-suite peers are more likely to say they can directly correlate ROI to risk mitigation and remediation activities (35% versus 25%). The same goes for those who work directly with their technical peers on security budgeting efforts (35% versus 20%).

Beyond reporting metrics, successful CISOs craft compelling data-driven narratives that reframe security spending not as a cost to be justified, but as a strategic investment essential for secure innovation. That’s why they’re reframing the conversation to something more holistic — incident reduction.

For the C-suite and board, fewer incidents mean the company has successfully avoided revenue loss, reputational damage, and other costly consequences of a major breach. Considering downtime costs Global 2000 companies $400 billion a year*, preventing incidents that cause it is a logical way to prove the worth of a security program.

If you’re doing security for the sake of security, you’re failing as a CISO. You’re becoming a business barrier instead of being a business enabler.

— Bjoern Watne, Global CISO, Interpol

* *The Hidden Costs of Downtime* (Splunk, 2024)

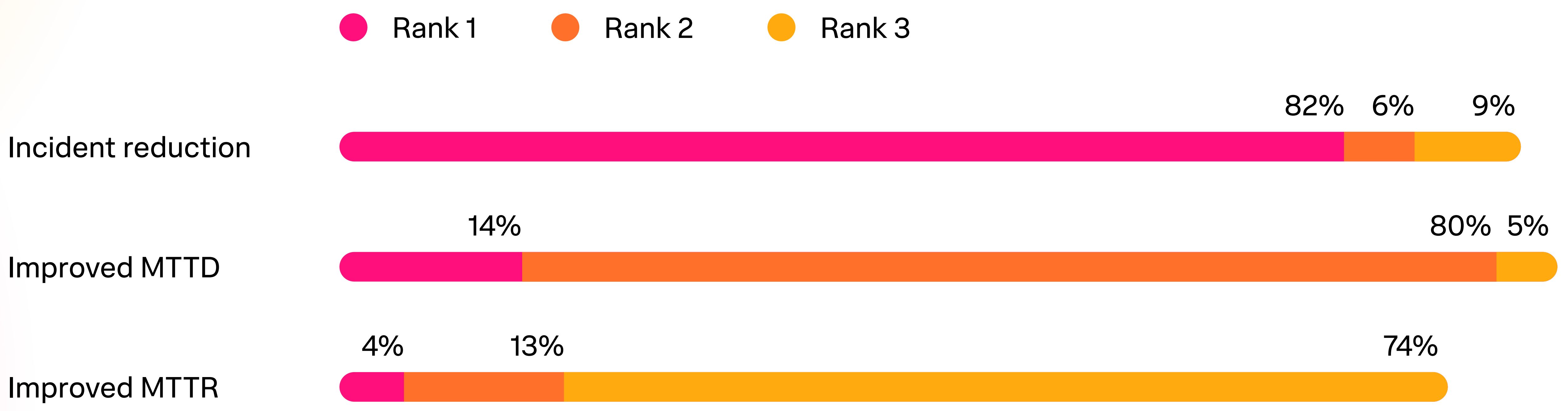
Bridging the expectation divide

Poorly communicating security's value can create a fundamental misunderstanding of achievable goals. In fact, the survey finds that CISOs and leadership are often misaligned. An astonishing 73% claim their leadership sets unrealistic expectations for vulnerability remediation speed. Similarly, 72% report unrealistic objectives when it comes to the revenue impact of an attack.

This misalignment can cause frustration, erode trust, and create friction during budgeting cycles. To help their leadership set more realistic goals, Splunk Field CTO Anthony Pierce suggests CISOs leverage a list of targeted common vulnerabilities and exposures (CVEs) based on business criticality. By prioritizing and addressing known weaknesses that would cause the most damage if exploited, CISOs can more effectively mitigate clear and present dangers that matter most to the business.

Not only are CISOs defenders of their organizations, they're also educators and realists in the boardroom.

How CISOs communicate security ROI across the business



Respondents ranked their top three choices

The CISO steps forward

The CISO stands at a critical moment where expanding responsibilities meet escalating threats and accelerating AI. The pressure is immense, but so are the opportunities. If anyone can meet the moment, it's the resilient CISO.

But resilience isn't about enduring — it's about advancing. The road ahead is paved with data-driven strategies, human-centric leadership, and an embrace of innovation. As CISOs step into their next chapter, we're offering five key strategies to help them champion true digital resilience and empower their organizations to *thrive*.

> **Escalating threats, expanding duties, and AI acceleration aren't meant to break us. It's forging us into the business leaders of tomorrow.**
>
> — Michael Fanning, CISO, Splunk

1 Bridge the C-suite knowledge gap with skillful storytelling.

The most significant challenge for a CISO isn't necessarily stopping threats; it's translating the value of their work into a language the rest of the business understands. To better communicate how security protects revenue and enables growth, transform the technical into the strategic by marrying data with context and business language.

Raw metrics like "CPU utilization" are meaningless to a CFO. Instead, create a compelling narrative that directly maps security initiatives to business outcomes like risk, cost, and revenue. To enhance your storytelling, invite colleagues to observe table-top exercises. This will provide a firsthand look at the complex decision-making and processes required to manage a major incident. Remember: Data tells you what happened. A narrative tells you *why it matters*.

2 Refocus security initiatives around quality, not quantity.

It's no secret that security teams are overworked and exhausted. To combat burnout and reclaim your team's strategic focus, shift their mandate from alert quantity to investigation quality. As a leader, empower your security team to concentrate on high-impact investigations, and enable this focus by leveraging automation to filter out noise.

Focusing on more impactful metrics like detection quality improves analyst investigations and provides a more accurate assessment of security posture. SOC stressors like alert storms and tool fatigue are also symptoms of a fragmented data landscape. A shared source of truth (where data from across the organization is connected) enables unified workflows where analysts gain immediate context and clarity.

3 Unlock security success through collaboration with C-suite peers.

Organizations with more collaborative leadership are better positioned to manage risk and regulations without sacrificing innovation. To elevate partnerships with other executives, focus on driving two organizational shifts. First, establish a shared planning cycle to embed security into business strategy, making it proactive by design.

Second, build joint-accountability on key security initiatives and KPIs to transform security from a siloed function into a shared responsibility. CISOs that expand their influence beyond traditional domains to shape strategy, manage technology, and oversee resources across the enterprise will establish security as a core driver of business success.

4 Empower humans with AI to strategize and think creatively.

Contrary to speculation, AI will not replace human roles, but rather serve as a co-pilot for more strategic and creative security work. By automating routine detection and response tasks, AI frees analysts to focus on higher-order activities such as threat hunting and designing original defenses.

The real opportunity lies in pairing machine precision and scale with human intuition and creativity. This means using AI to surface insights while security teams craft the “why” and “what next?” CISOs must build an environment where AI augments human expertise, amplifies curiosity, and empowers security professionals. Analyst intelligence is irreplaceable in situations that require context, creativity, and accountability.

5 You can’t opt out of the AI era, so ensure you own it.

For security leaders, the greatest risk from AI isn’t its adoption — it’s being left on the sidelines. The business will implement AI, with or without your direct involvement, so CISOs need to help shape its rollout or face the consequences of ungoverned usage. Championing a clear governance, privacy, and accountability strategy is not a barrier to progress. It ensures AI is trusted, transparent, and secure.

Start with building comprehensive guardrails for everything from private data use in training models to ensuring meaningful human-in-the-loop protocols for critical decisions. And once implemented, continuously monitor model behavior for bias, drift, and data leakage while maintaining audit trails. By embracing and shaping AI strategy now, you transform inevitable, high-risk experiments into secure, trusted capabilities with real business impact.

“

AI automates the routine, unlocking human capital to focus on the complex and strategic challenges that require true ingenuity.

— Cory Minton, Global Field CTO, Splunk

Become a resilience leader with Splunk

2025

State of Security

The stronger, smarter SOC of the future

splunk> a cisco company

State of Security 2025:
The Stronger, Smarter SOC of the Future

Looking to break free from inefficiencies in the SOC? Learn how to eliminate busywork, overcome alert overload, and close critical data gaps — transforming the SOC from overwhelmed to optimized.

Download the report

Perspectives by Splunk — by leaders, for leaders

Looking for more thought leadership and insights from CISOs? Learn how security leaders address today’s most pressing challenges, including regulatory compliance, AI, and the evolving threat landscape.

Get executive insights

Methodology

Oxford Economics researchers surveyed 650 Chief Information Security Officers (CISOs) in July and August of 2025. Respondents resided in Australia, France, Germany, India, Japan, New Zealand, Singapore, the United Kingdom, and the United States. They represented nine industry groups: manufacturing, telecommunications, media, and communications, financial services, public sector, energy and utilities, transportation and logistics, retail and consumer goods, healthcare and life sciences, and information services and technology.

About Splunk

Splunk, a Cisco company, helps make organizations more digitally resilient. Leading organizations use our unified security and observability platform to keep their digital systems secure and reliable. Organizations trust Splunk to prevent infrastructure, application, and security incidents from becoming major issues, recover faster from shocks to digital systems, and adapt quickly to new opportunities.

Keep the conversation going with Splunk.

splunk>
a CISCO company

25_CMP_report_The-CISO-report-2026_v18