2025

State of Security

The stronger, smarter SOC of the future

splunk> a CISCO company

Contents

Executive foreword

Building an effective SOC is one of the greatest lessons in adaptability. As a former SOC leader, I've built security operations ranging from the Department of Homeland Security to managed security services for small- and medium-sized businesses. No matter the size or mission, the lesson is always the same: If you're not thinking ahead, you're already behind.

Many of us, myself included, are drawn to cybersecurity because it's so dynamic. Cybersecurity has always been a game of rapid shifts — new threats, new malware, and now, the breakneck pace of AI. But for all the external challenges, the real problem is often internal.

We surveyed 2,058 security leaders — including SOC managers, directors, analysts, and engineers — to understand the biggest barriers to evolving the SOC and the most impactful strategies for the future.

Our data uncovers that SOCs are burning too much effort on the wrong things — babysitting tools, chasing the same false alarms over and over, and wrestling with messy data. Nearly half of them admit they spend more time maintaining their tech stack than actually defending their organization. That's not just frustrating — it's a failure of strategy.

But the survey also reveals that some SOCs are embracing new forward-leaning technologies and processes to help eliminate these inefficiencies. They're leaning on AI to boost productivity, uplevel their existing teams, and become more resilient. They're exploring detection-as-code to stay ahead of attackers. They're rethinking their approach to investigation and response, ditching silos for a unified strategy.

We hope that *State of Security 2025: The smarter, stronger SOC of the future* will help propel your SOC. Because if you're still fighting yesterday's battles, you've already lost.

David Dalling
GVP, Global Cyber Strategist, Splunk

Transforming the SOC from overwhelmed to optimized

Think of the biggest threats to the SOC. Industry stereotypes might lead you to picture a hacker in a hoodie, enveloped in shadows as they type prompts into a command line. Or perhaps a team of highly skilled and credentialed nation-state actors poring over top-secret threat intel in a windowless, undisclosed government office.

Imagining these threat actors can fuel any SOC member's drive to defend. No doubt, these are all very real threats. But what's often overlooked is internal — the threat of inefficiency. Analysts play an endless game of Whac-A-Mole™, missing critical incidents that end up as costly breaches. Teams spend more time maintaining tools than defending the organization. Faulty data leads to faulty detections, weakening cyber defenses. And persistent skills gaps continue to stretch existing teams thin.

Teams will reach a crossroads as toolsets expand, the skills gap widens, and technologies like AI become more central to the SOC. Will security tools pile up, creating even more complexity? Will collaboration across the business become second nature to SOC teams, or will they remain in their comfort zone?

It's time to reimagine the SOC and what it could be. SOC teams of the future will elevate their skills by relying on AI and automation. As a result, analysts will spend their time building stronger defense methods like detection as code (DaC) and perfecting their investigation protocols. They'll take a smarter, unified approach to threat detection and response, leading to tighter collaboration and bringing more context and speed to investigations.

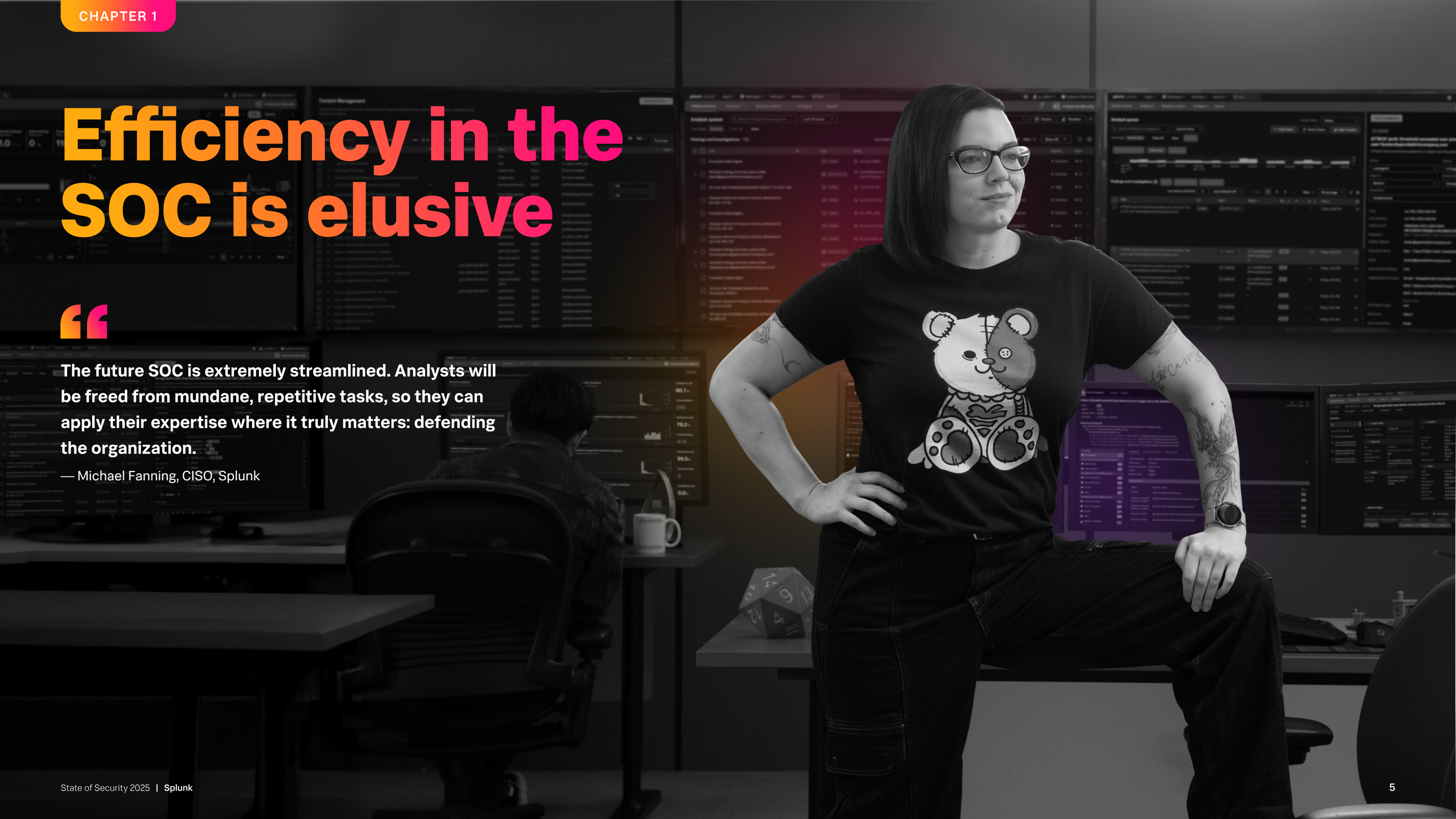
Does this sound like sci-fi? Believe it or not, some teams are already taking steps to build a faster, stronger, and smarter SOC. These SOCs have evolved from overloaded to optimized and resilient.

Launching into the future is an exhilarating adventure, but it's worth the ride.

Efficiency in the SOC is elusive

The future SOC is extremely streamlined. Analysts will be freed from mundane, repetitive tasks, so they can apply their expertise where it truly matters: defending the organization.

— Michael Fanning, CISO, Splunk



If you've spent time in the security weeds, you know the nuisance of troubleshooting with no clear resolution, the hassle of reconfiguring a setting for the tenth time, or the drudgery of managing inventory.

The SOC of the future, on the other hand, will run much more efficiently. Tools are well-orchestrated and generate alerts rich with context. Every team member performs strategic tasks typically reserved for senior analysts, like in-depth analysis and investigations. They also lean on automation and AI to resolve lower-level alerts.

The top sources of inefficiency in the SOC

59%
We spend too much time and/or effort maintaining tools and associated workflows

51%
Our tools do not integrate well with one another

47%
We face alerting issues

32%
Our team does not have the requisite skills

31%
We have inadequate and/or outdated processes

28%
We spend too much time normalizing data

27%
Managing the number of vendors is complex

24%
We lack an established incident response process

Busywork stifles progress and passion

What's holding teams back from achieving a high level of efficiency? Tool maintenance, for one. Nearly half (46%) of respondents say they spend more time doing busywork — like configuring and troubleshooting tools — than addressing critical efforts like threat investigation and mitigation.

Don't get us wrong; tool maintenance has its place in the SOC. It can optimize workflows and improve accuracy. But respondents point to the imbalance as a growing problem, with 59% saying that it's the main source of inefficiency for their teams, followed closely by tools not integrating well together (51%).

"Maintenance is more complicated than it used to be," says Marcus LaFerrera, director of SURGe at Splunk. "Tools are more feature-rich with more frequent updates. And while vendors have introduced support to cut down on the guesswork, there's far more network complexity that makes the job harder."

Passion and purpose motivate security professionals in their mission to keep organizations safe. But no one gets jazzed about tool maintenance. A team that spends the majority of its time defending is a team that maximizes the passions of its analysts. These SOCs enable the business by being strategic, innovative, and proactive.

46%

spend more time maintaining tools than defending threats

Analysts who can flex their critical thinking muscles rather than say, endlessly adjusting alert thresholds, aren't simply more satisfied — they're doing more valuable work and contributing to the organization's bottom line.

— Kirsty Paine, Field CTO and Strategic Advisor, EMEA, Splunk

Alert overload slows down SOCs

Every second counts in the SOC, especially during a major investigation. Inefficiencies aren't minor headaches. Even a small bottleneck — like a missed alert that results in a data breach — can cause significant reputational, legal, or financial consequences. Downtime is just one example, and it can cost organizations $540,000 per *hour*, according to The Hidden Costs of Downtime report.

Alerts are another "can't live with them, can't live without them" part of the job for analysts, with 47% pointing to alerting issues as the most common source of inefficiency in the SOC. Respondents said most troublesome issues were having too many alerts (59%), dealing with too many false positives (55%), and deciphering alerts that lack context (46%). Each of these issues waste analysts' precious time as they question alert validity or ignore them altogether. And who can blame them? After investigating a string of alerts that turn out to be false positives, what's the motivation for investigating the next one?

59%

have too many alerts

Data deficits derail investigations

Wasted time extends beyond just tool management and alert overload. Data problems also play a significant role. In fact, 57% of respondents report losing valuable time during investigations due to gaps in their data management strategies.

Whether those gaps are attributed to accessibility concerns (39%) or data silos (35%) — both common data challenges flagged by respondents — not being able to access the right data in the right place makes it even harder for SOC teams to act quickly and decisively when facing threats.

"You want to bring your analytics to your data, not the other way around," says Paine. "SOC teams that recognize this and have strategies involving data federation are already a step ahead."

57%

have lost valuable investigation time due to data management gaps

You want to bring your analytics to your data, not the other way around. SOC teams that recognize this and have strategies involving data federation are already a step ahead.

— Kirsty Paine, Field CTO and Strategic Advisor, EMEA, Splunk

AI leads SOCs into the future

In the future, AI will become an integral part of the security analyst experience. AI can enable self-healing systems to detect and mitigate malicious behavior in real time. Imagine what that technology could do once it's embedded in the SOC.

— Tamara Chacon, Security Strategist, Splunk SURGe

Peanut butter and jelly. Thunder and lightning. AI and the future. Some pairings simply make sense.

AI is already a powerful tool for both adversaries and defenders. In the SOC of the future, analysts will learn to wield AI to their advantage, applying it to the right tasks at the right time. No magic AI pixie dust needed.

AI isn't a cure-all, but it's certainly an appealing remedy for teams seeking more efficiency. Let AI search through endless rows of logs for a specific IP address? We'd be hard-pressed to find any SOC team not on board with that. Applying AI to security workflows was this year's highest cybersecurity priority, with 56% listing it as one of their top three initiatives. Productivity gains are real for those who've jumped in; 59% say they've *moderately* or *significantly* boosted their efficiency with AI.

Building trust in AI

Security pros are notoriously skeptical. It's sort of their job. But trust comes in different shades — from blind faith to complete cynicism and everything in between. Successfully adopting AI is all about balance — trusting it enough to reap the benefits while staying cautious enough to put the right checks and safeguards in place.

Only about 11% of respondents say they trust AI *completely* to perform mission-critical activities within the SOC. But it's unlikely that this group is blindly trusting AI; rather, they may be running their own models and are more easily able to trust a system they've built themselves.

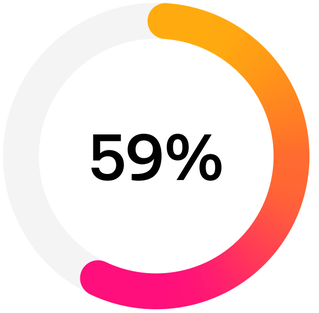
"Trust will grow as organizations mature in their AI implementations," says Petra Jenner, senior vice president and general manager for EMEA at Splunk. "Teams with the resources to build, train, and test their own models will naturally have a higher level of trust in that system."

However, the majority of respondents (61%) say they *somewhat* trust AI for mission-critical operations. Security teams need some trust to successfully adopt AI in the SOC, but taking a human-in-the-loop approach is paramount — especially when it comes to generative AI.

"Generative AI is like that overconfident colleague who will never say they don't know, and will assuredly tell you about something they read about once," says Paine. "Expert checking and proper tests will make sure you're getting the right outputs."

Trust will grow as organizations mature in their AI implementations. Teams with the resources to build, train, and test their own models will naturally have a higher level of trust in that system.

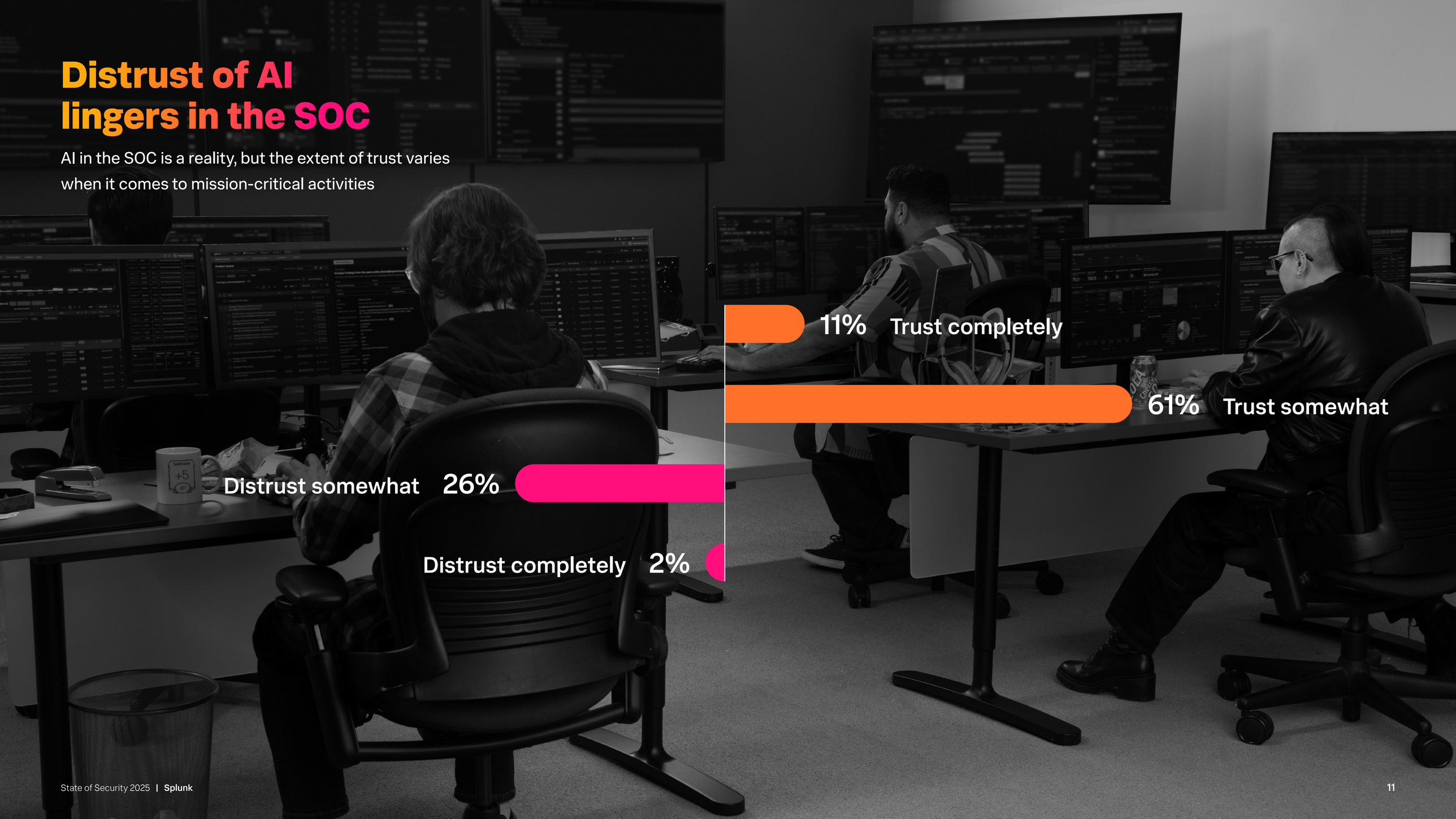
— Petra Jenner, Senior Vice President and General Manager, EMEA, Splunk



have *moderately* or *significantly* boosted their efficiency with AI

Distrust of AI lingers in the SOC

AI in the SOC is a reality, but the extent of trust varies when it comes to mission-critical activities



Tapping into the power of generative AI

Reaping the benefits of generative AI involves leaning on its biggest superpower: filling in the blanks. For example, it can create search query strings and suggest investigative steps based on what it's seen before. Nearly a third (31%) currently use generative AI to query security tasks in the SOC, and another 48% say they will do so in the near future.

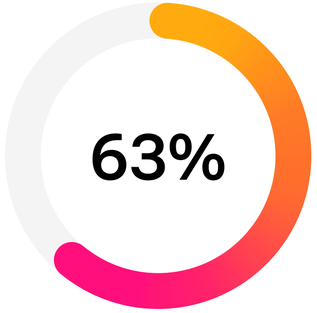
Other security tasks require a bit more finesse. Respondents were more likely to be wary of generative AI developing security content, such as scripts and signatures, with 29% saying that it *should* never or *will* never perform these duties.

Domain-specific generative AI tools can help build trust with embedded intelligence about cybersecurity use cases, surfacing the right information at the right time with context. This is the future of generative AI, and respondents are enthusiastic about its role in cybersecurity. Nearly two thirds (63%) agree that it *extremely* or *significantly* enhances security operations compared to publicly available tools.

General AI tools like ChatGPT or Google Gemini are trained on broad datasets, so they have some knowledge on just about everything — from obscure dog breeds to the military history of ancient Rome. But using these tools for threat detection and response is like trying to build a house with a Swiss Army knife — a highly technical field demands a specialized approach.

Domain-specific generative AI, on the other hand, is trained on datasets that focus on a particular subject, like cybersecurity. With this deep knowledge it can make more expert recommendations. It also reduces the risk of data leakage by keeping the workflows in-house. Keeping data from unauthorized access is a top priority for security pros, as nearly half (46%) cite data loss prevention as one of their top three priorities they'll focus on over the next year.

"Domain-specific AI will simply have better outputs because it's dialed into a specific function," says Hao Yang, VP of AI at Splunk. "It's the next chapter of AI."



say domain-specific AI *significantly* or *extremely* enhances security operations compared to publicly available tools

> **Domain-specific AI will simply have better outputs because it's dialed into a specific function. It's the next chapter of AI.**
>
> — Hao Yang, VP of AI, Splunk

Skills to power the future SOC

Cybersecurity is far from stagnant. The SOC teams that thrive will be the ones that quickly adapt and harness emerging skills and technology.

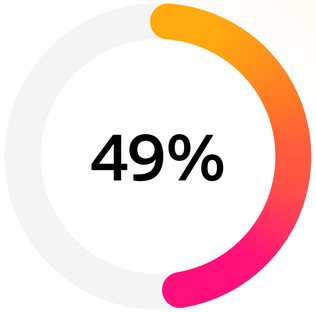
— David Dalling, GVP, Global Cyber Strategy, Splunk

Tomorrow's SOC may be a well-oiled machine, but that doesn't mean it relies only on technology. It's home to some pretty major decisions. Kick off your breach communications immediately after an incident, or wait to understand the full scope? Protect customer-facing services first, or internal infrastructure that supports the core business?

None of these are simple choices, and they'll only become more nuanced. Regulations deepen. Attackers hone their techniques. New technologies emerge. That's why people (and their skillsets) will always be at the cornerstone of the SOC — to be decisive and analytical as they navigate these situations.

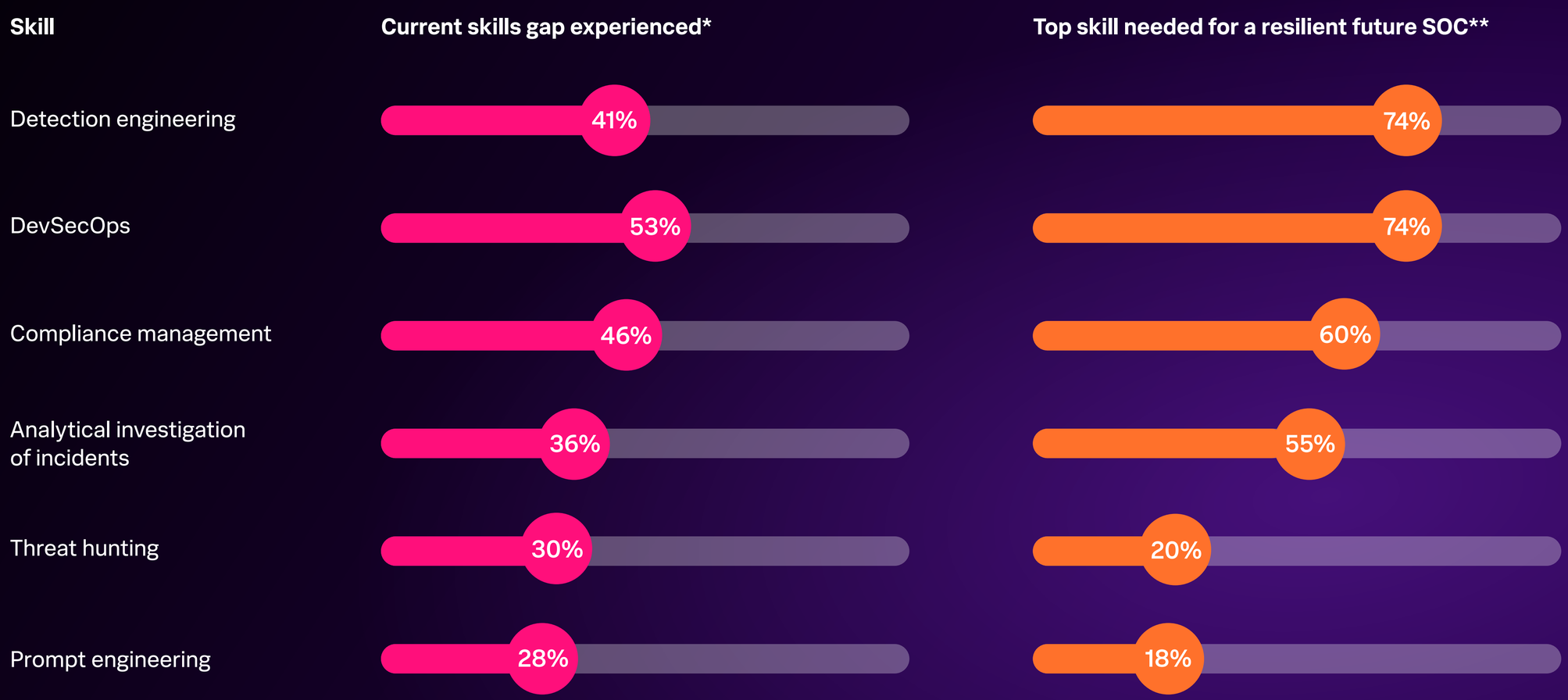
Skills that drive resilience are biggest shortcomings

Being understaffed and underskilled are serious dilemmas for security teams. Nearly half (49%) call this the biggest cybersecurity challenge in their organization. What's more, when we asked respondents to rank the most vital skills for building a resilient SOC and then about proficiency of those skills, we found glaring gaps. Respondents say detection engineering, DevSecOps, and compliance management are simultaneously the most crucial for the future and their weakest capabilities.



say being understaffed and underskilled is the biggest cybersecurity challenge in their organization

Today’s biggest skills gaps are also the most important for the future



* Respondents could select all that apply

** Top 3 rankings combined

These three in-demand skills paint a picture of what the future SOC will look like.

1. Detection engineering

Respondents rated detection engineering as the most important skill for building the future SOC, with nearly three-quarters (74%) ranking it in the top three. Forty-one percent report a proficiency gap in this area.

Detection engineers set the bar for the quality and accuracy of an organization's detections. They design, build, and fine-tune detections so their organizations can better identify sophisticated threats. They're also responsible for adopting detection as code (we'll get to that later) to update this content quickly based on real-time performance indicators.

Fast and accurate detections will be even more vital in the future as threat actors continue to advance their tactics. Nailing down a detection strategy will also address some other pressing concerns for SOC teams, like reducing false positives, minimizing time on tweaking thresholds, and easing maintenance as the SOC scales.

2. DevSecOps

DevSecOps closely followed detection engineering as a high-priority capability. Yet over half (53%) report their teams aren't up to speed in this area.

An evolution of DevOps methodology, DevSecOps involves baking security into the software development lifecycle (SDLC) early and often. It's a practice that arguably should be the standard as every business becomes even more tied to software — and organizations that embrace a DevSecOps culture will be more apt to uphold that standard.

"The future of the SOC comes down to streamlining and making it less onerous to perform maintenance and deployment," says LaFerrera. "DevSecOps is a part of that evolution."

3. Compliance management

Sixty percent of respondents rate compliance management as a top three skill, yet 46% say they fall short here. That's no surprise — the speed at which regulatory requirements change and assets multiply challenge security teams to keep pace. In fact, over half (52%) of respondents failed compliance mandates because they couldn't see data about their assets. The implementation side of compliance management — the 'box checking' tasks like patching — also requires heavy maintenance, an area in which security teams are already drowning.

The demand for these three skills suggest that critical thinking, collaboration, and creativity — qualities that are unique to people rather than tech — will never go out of style. DevSecOps and compliance management require tight collaboration with other departments, from IT and engineering to legal. Detection engineering leans on creativity to get in the mindset of an attacker, and to build custom detections to the organization's specific environment.

"You can't tool your way out of detection engineering. It requires a very specific skillset that isn't easily cultivated," says Tamara Chacon, security strategist at Splunk's SURGe security team research.

> **The future of the SOC comes down to streamlining and making it less onerous to perform maintenance and deployment. DevSecOps is a part of that evolution.**
>
> — Marcus LaFerrera, Director of SURGe, Splunk

Automating the mundane to find reprieve

By their nature, high-pressure roles in the SOC are stressful, but there are more factors that test security pros' mental health. For one, the skills gaps that SOC teams have been battling for years are taking a toll. Over half (52%) say their team is overworked and 42% say they're understaffed. So it's no surprise that 52% say stress on the job has prompted them to think about leaving the cybersecurity industry altogether.

Job-related stress is a historical trend that's likely to continue, but there are more solutions ahead. Some organizations will take traditional paths, such as hiring and upskilling current employees (44% plan to fill gaps this way) or enlisting third-party partners (19%). But a considerable number are focusing forward — about a third (33%) plan to resolve these deficiencies with AI and automation.

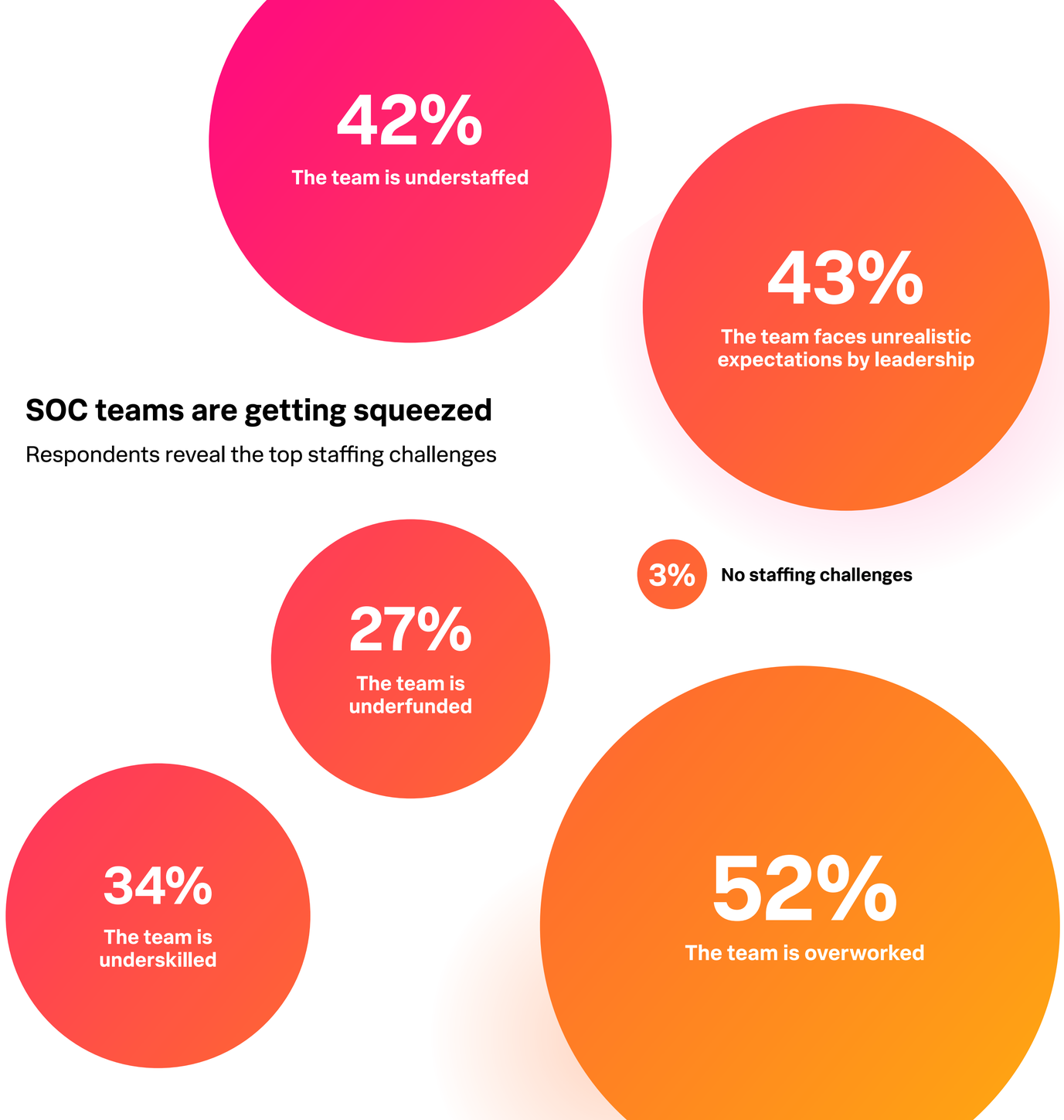
Don't panic — this doesn't necessarily mean jobs in the SOC will be automated away (or at least the parts of the job your teams actually enjoy). Addressing skills shortages could take the form of an automated response to non-critical alerts (forget the days of chasing down "malicious IPs" only to find a user torrenting *The Sopranos*).

Threat analysis is an area that's ripe with opportunity here, with 38% of respondents saying it's their top priority for future automation implementations.

"Automated security tools can take phishing emails, run them against threat feeds, use these results to create a score, and use that score to either quarantine, block, or report the email," says Paine. "They can work faster than any human."

SOC teams are getting squeezed

Respondents reveal the top staffing challenges



The new era of threat detection

Detection as code represents a new era of threat detection. It's a smarter, faster, and more automated way to outpace the next generation of adversaries.

— Jose Hernandez, Director, Splunk Threat Research Team

A live phone call that sounds exactly like your CEO. An automated script that scrapes GitHub repositories for security keys. A malicious website that appears in the top spot of a Google search, or masks as a legitimate ad.

Five years ago, these attack techniques were considered obscure and sophisticated. In 2025, they're relatively commonplace. In another five years, these antics will give way to even more creative threats. But while the toolsets of threat actors have expanded significantly, so will the solutions for defending against them.

Data complexity creates new detection dilemmas

Detections are one of the most important tools in a defender's arsenal. Like every powerful tool, detections aren't one-size-fits-all. Many teams lean heavily on vendor detections but also rely on internal analysts to fine-tune them — this is the most common detection method for respondents, with nearly half (46%) reporting they take this approach *frequently* or *always*. Some depend on their in-house engineering teams to manually author and manage detections. A few are adopting the emerging approach, detection as code (DaC), to enable their SOC or engineering teams to create detections quickly and at scale.

Still, teams want to up their detection game. Looking ahead, while over three quarters (77%) say their standing is good, they still plan to increase the quality of their SOC's detections. Only 8% rate their detection quality as *excellent*. Most respondents blame a few factors; 62% point to poor data quality, whether it's due to lack of the *right* data, or lack of data overall. Over half (53%) report that their SOC doesn't have the skills or expertise to create effective detections.

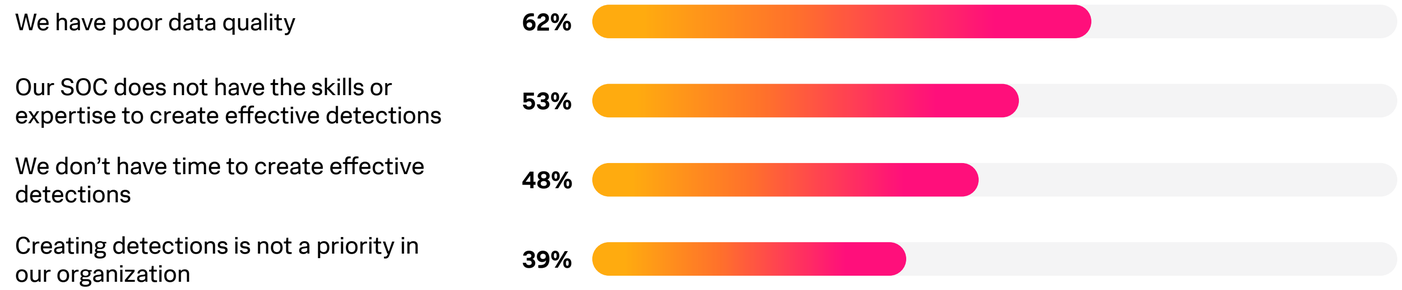
Detections are only as strong as the data they rely on. An explosion of ephemeral data such as service accounts, APIs, token keys, and other data not attached to a person — also called non-human identities — makes it difficult for analysts to effectively capture the data they need for robust detections.

"Every non-human identity represents a potential entry point for attackers," says Shannon Davis, principal security strategist at SURGe. "They proliferate quickly, and it's easy for organizations to lose track of them. Forgotten APIs, orphaned service accounts, and leaked tokens create hidden risks — especially as SOCs struggle to sift through massive amounts of ephemeral data to detect real threats."

According to LaFerrera, it's a challenge for teams to get data in the right spot and in the right format.

"Security teams aren't just dealing with raw syslogs anymore, but massive blobs of data in a multitude of formats that need to be parsed, ingested, and analyzed properly," he says. "It's an incredibly complex endeavor."

The leading causes of poor detection quality



Detection as code unlocks a flexible future

In the SOC, speed and efficiency reign supreme. As attacks become faster and more unpredictable, detections must be even more nimble, standardized, and high quality to keep up. Detection as code is a detection strategy that helps defenders pivot in an instant and adapt.

Detection as code ushers in a new era of detection engineering that's agile, dynamic, and automated. Those who have adopted this practice report considerable benefits. Sixty-two percent say it enables test-driven development practices, such as roll back and auditing — a key element of flexibility. Others say it's allowed them to automate workflows (52%) and standardize deployment (45%), functions that often translate to time savings and efficiency.

Detection as code will be front and center in the SOC of the future. Currently, about a third of respondents (35%) frequently or always use detection as code, but 63% say they would like to frequently or always adopt this method in the future. This signals a desire from SOC teams to take more control of detection speed, precision, and power and rely less on vendor content.

"Out-of-the-box detections will only take you so far," says Hernandez. "Every environment is unique. At the end of the day, there will always be a specific threat that your vendor isn't aware of."

To realize the value of detection as code, SOCs first must bridge the divide between aspiration and adoption. Teams might be wary of the upfront setup involved — especially since 41% say they don't have sufficient detection engineering skills.

A maturing market has produced more solutions to ease detection as code adoption for SOC teams by helping to train analysts and validate detections on their behalf. When SOC teams clear initial hurdles like setting KPIs and piloting noisier detections, the benefits will unfold exponentially.

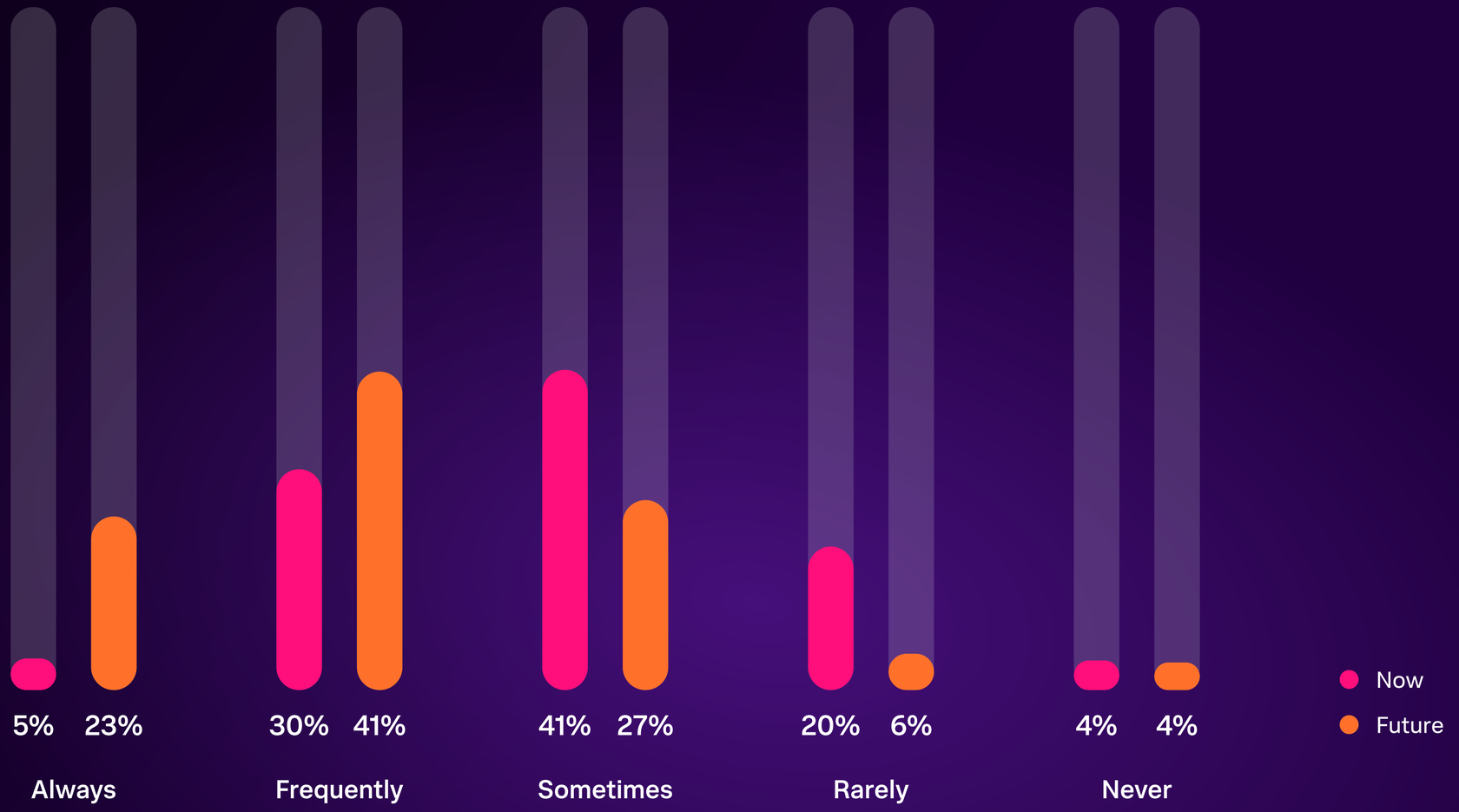
"When you have good detections in place, it becomes a virtuous cycle," says Paine. "Analysts have fewer false positives and more time to refine existing processes, detections become more efficient, and those capabilities keep expanding."

Out-of-the-box detections will only take you so far. Every environment is unique. At the end of the day, there will always be a specific threat that your vendor isn't aware of.

— Jose Hernandez, Director, Splunk Threat Research Team

The future of detections

How frequently respondents use detection as code now, versus how often they want to use it in the future



Popular threats pack a punch

SOC teams can easily justify polishing their detection strategies, given the current threat landscape. In 2025, cybersecurity threats are hitting organizations where it hurts. Respondents report the most commonly experienced type of incident, data breaches, is also the most impactful.

Two-thirds (66%) of respondents fell victim to a data breach over the past year, making it the most commonly experienced incident for the third year in a row, according to previous *State of Security* research.

"Data breaches won't slow down until organizations have incentives, like comprehensive data privacy laws, to prevent them from happening," says Mick Baccio, global security strategist at Splunk SURGe.

Additionally, nearly half (49%) of respondents admit to violating security regulations over the past year. A significant portion of respondents also report being victims of ransomware (41%) and insider risk (38%).

The impact of a cybersecurity incident isn't always immediate; it reverberates through an organization much like a power outage. The initial blackout is sudden and frightening, but the aftereffects can be the most damaging.

Most common cybersecurity incidents

66%
Data breach

49%
Regulatory compliance violation

41%
Ransomware

38%
Insider risk

The pain of a cyberattack extends way past an initial ransom payout or data loss, or even just the long and intensive recovery. Hefty fines, negative reputations, and eroded customer trust create organization-wide damage that's far more long-lasting.

— Kirsty Paine, Field CTO and Strategic Advisor, EMEA, Splunk

CHAPTER 5

Unifying and connecting the SOC

Security teams have been vying for a single platform for a long time. In the future, we'll finally see that come to fruition.

— Kamal Hathi, SVP, Products & Technology, Splunk

The SOC is a busy place. But busy does not (or should not) equal chaos. And although busy people often need to work heads down, operating on an island is not the way — and in fact, can result in chaos when a critical incident occurs. Teams within the SOC, from threat intelligence to incident response, should communicate efficiently and often. And while communication with external teams like HR, legal, and IT happens less frequently, it should be seamless — not frantically searching for the right contact to get a response in the knick of time.

The SOC of the future is more coordinated — harmonious, even. Teams will have information at their fingertips to quickly and smoothly investigate alerts, spot anomalies, and respond to incidents. A well-orchestrated environment means fewer fires, fumbles or flubs, and a more resilient security posture.

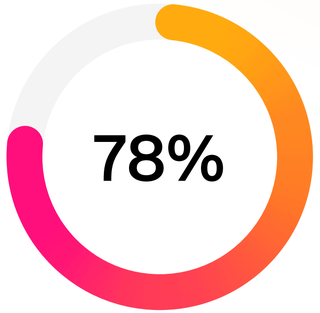
The alphabet soup of security tools like XDR, SOAR, and SIEM will never go away (nor should it), but the disjointed nature of how they interoperate will. A platform that ties together these technologies enables security analysts to work collaboratively and quickly across the threat detection and response lifecycle. That's the future.

Everything in its right place

Tools can provide the necessary context during incidents and keep a SOC humming along smoothly — but they can cause confusion and gaps in coverage if not properly integrated. When tools become a collection of disjointed elements, maintaining them all becomes a full-time job.

Over three-quarters of respondents (78%) say their security tools are dispersed and disconnected. This isn't just a minor inconvenience, either; 69% say this disconnect creates *moderate* to *significant* challenges for their team. These challenges can take many forms, from overwhelming alerts, illogical workflows, visibility gaps, and more. That all translates to a weaker security posture.

"During an incident, an analyst might have to leave their SIEM to check their case management system for the right data, then their knowledge base, and so on — all spending critical time just searching," says Baccio. "That's where the power of the platform comes into play. Everything they're looking for is right there."



say their security tools are dispersed and disconnected

Respondents believe a unified platform would ease these frustrations. And those who take this approach confirm: the benefits are real. Adopting a unified security platform has led to faster incident response (59%), less time maintaining tools (53%), and better threat coverage (49%), according to respondents.

Less tool upkeep is appealing for a large portion of teams that spend more time in maintenance mode than defending the organization. Better threat coverage is also a major win, as half of respondents say they have low visibility over critical areas like network infrastructure they don't own and operate, third-party assets, and configuration management.

A unified approach unlocks major benefits

Respondents report the benefits they've experienced since adopting a unified platform approach for threat detection and response.

Data sharing accelerates operations

Less tool maintenance is just the starting point for benefits of a unified security platform. Collaboration becomes much easier too.

The SOC is increasingly a single strand in an interconnected web. It relies on other departments, like HR, legal, IT, and others, to either take an action or deliver information during a critical security incident.

Twenty-one percent of respondents agree that SOCs aren't standalone functions today. But perceptions are changing; that percentage doubles to 40% when asked if that will be true in the near future.

The future is ultra-collaborative. No one knows that better than a SOC analyst who resolved an incident in record time — and saved their organization's you-know-what — by bringing in their organization's IT and engineering data. Sharing data helps teams get a swift understanding of what's happening in the environment and why.

Sharing information across security and observability isn't fully embraced yet. More often, this process happens gradually or on an as-needed basis, with 37% of respondents reporting that they reuse data *sometimes*. Only 9% say they *always* practice this.

"Security teams often hesitate to involve engineering personnel during incident investigations, primarily to control the spread of sensitive information," says Craig Robin, field CTO, Americas at Splunk. "They prefer to keep critical incidents under wraps, leading them to either investigate in isolation or conduct their own searches based on available indicators. This approach, however, can significantly prolong the investigation process and mitigation time."

Those who have made the leap, however, report noteworthy advantages. Respondents agree that speed — either in the form of faster incident detection or remediation — is where information sharing delivers, with 78% and 66% reporting *moderate* to *transformative* benefits, respectively.

That's just the tip of the iceberg. When SOCs work with other teams, data sharing is just one of many benefits for those involved. Unifying, and then automating, workflows between IT, engineering, identity management, HR teams, and others will unlock even more efficiency.

"Integrating with other teams' ticketing software or processes opens up a lot of automation opportunities," says Dalling. "If a user is sending suspected sensitive data externally, for example, the platform can then automatically notify the security team of potential exfiltration, retain or turn on packet capture for all data being sent to that destination, disable the user's access to other sensitive data, and open up a case with HR or your insider threat team. Each of these teams might have their own ticketing system, but by using a threat detection and response approach, all the teams would use their standard interface and still have immediate feedback and collaboration."

A more collaborative SOC is coming

Respondents that agree SOCs are not standalone functions *today* and in *the near future*.

Words to the wise

There’s no magic button for building the SOC of the future. It’s an intentional, iterative process that requires collaboration and buy-in across the entire business.

— Mike Horn, SVP and GM, Splunk Security Products, Cisco

How to propel your SOC into the future

1

Spring clean your toolset

SOC teams are drowning in tool upkeep, with 46% of respondents saying they spend more time maintaining their tools than defending the organization. To help teams get out of the weeds, take a good, hard look at your current toolset to identify what might be contributing to the burden:

- **Figure out your footprint and assess.** As you audit, consider not just security tools and software, but sensors and cloud infrastructure, too. Then, set clear KPIs, like criticality scores, false positive rates, and time-to-incident resolution, to evaluate tool effectiveness and understand which tools are actually adding value.
- **Decide to cut, consolidate, or upgrade.** For tools you've marked as underused, dig into why. Is your team not properly trained? Are they integrated with other tools? Determine if it's worth the effort to fill these gaps. If you take the decommission route, consider if you're getting the capability from other existing tools, or if you simply don't need the utility anymore.

2

Adapt your team's skillsets for the future

Skills that respondents rated as most vital for building a resilient SOC — detection engineering, DevSecOps, and compliance management, respectively — were also the areas most afflicted with gaps. Here's how you can close them:

- **Equip the team with resources to learn.** Teams should have adequate resources to learn the things they're curious about. Individuals who want to learn detection engineering, for example, should have access to GitHub. Encourage team members to attend local meetups and conferences to expand their skillsets.
- **Emphasize curiosity while hiring.** Curiosity and a willingness to learn can rarely be taught, which is why leaders should evaluate these qualities during the hiring process. Ask prospective hires about passion projects and other topics that will get their gears going.

3

Lighten the load of alerts

Alerting is still a source of frustration and inefficiency for SOC teams; 59% of respondents grapple with too many alerts and 55% deal with too many false positives. Here's how to tame the fire hose:

- **Adopt an iterative review process.** Develop a repeatable process to understand what's causing alerts. Continuous improvement can help identify where the data gap exists, and how your team can close it.
- **Lean on AI for less critical alerts.** AI can correlate similar alerts or auto-close duplicated false positives to tamp down the noise and give analysts a clearer picture of potentially malicious behavior. With the right context, AI tools can automatically respond to alerts that would otherwise be flagged, like a user downloading batches of files when they start a new project.
- **Consider risk-based alerting.** Risk-based alerting (RBA) focuses on complex behavior over various time periods rather than point-in-time alerting. Adopting this practice is an iterative process — but once fully implemented, it cuts down on false positives and overall alert volume. It also ensures analysts first focus on the highest priority and risky alerts.

4

Opt for domain-specific generative AI

The future SOC demands a more purpose-built approach to generative AI, and 63% agree that domain-specific generative AI tools will *significantly* or *extremely* enhance security operations compared to publicly available platforms. Here's how to take advantage:

- **Do your research.** AI software is a crowded market, so it's important to ask the right questions when evaluating a domain-specific generative AI tool. For example, what is the privacy policy? What data is the model trained on? Does the vendor adhere to any AI principles? Ideally, you'll want to validate the LLM before purchasing to ensure it addresses the problem your team is looking to solve.
- **Partner with vendors.** Once you've identified an innovative AI vendor partner, build domain-specific AI into your tools, or as part of their foundation. For the best outcomes, tightly embed AI into your team's everyday workflows.
- **Keep humans in the loop.** Domain-specific doesn't mean completely free of hallucinations or misunderstandings. A seasoned analyst should always validate the output of AI tools to maintain accuracy.

5

Set the groundwork for collaboration

Respondents say that adopting a unified platform approach speeds up incident response (59%) and cuts down on tool maintenance (53%). Truly embracing this approach, however, involves some cultural shifts:

- **Develop clear processes for incidents.** Document clear processes for who to contact during an incident and how to take a detection to its conclusion. Building these processes across teams — and practicing them with tabletop exercises — will help teams understand exactly how to collaborate. This process also helps security teams establish relationships with your organization's ITOps and engineering teams, which will smooth the process when you need results fast.
- **Embed the unified platform as part of everyone's jobs.** A unified platform approach should be a collaborative effort, with all involved teams fully embracing and working in that same platform rather than treating it like an afterthought. When SOCs can integrate their platform with other teams' ticketing software, for example, they can more easily collaborate within a standard interface.

6

Make detection as code a team sport

Detection as code offers powerful efficiency benefits, including the abilities to automate workflows and standardize detection deployments. But while 63% say they would *frequently* or *always* like to use this method in the future, only 35% say they've reached this level of adoption.

- **Get buy-in across the organization.** Everyone — from executives to the team members carrying out the work — should be on board with adopting detection as code. Position detection as code as a strategic advantage. Showcase the benefits, such as versioning and quality assurance, keeping in mind each team's priorities and desires.
- **Hone detection as code skills as a team.** Assign detection as code responsibilities as 10% of every analyst's role and encourage knowledge-sharing so everyone upskills together. This enables the entire team to have a shared understanding of when, why, and how detections are working during the validation process. A democratized approach also prevents backfill emergencies.

Step into the SOC of the future with Splunk

The CISO Report

Explore how CISOs and their boards can bridge divides on top priorities, budgeting, compliance approaches, and success metrics.

Get on the path to greater resilience

Perspectives
by Splunk

Perspectives by Splunk — by leaders, for leaders

Looking for more insights on cybersecurity trends? Learn how leaders are preparing for the challenges ahead — including AI, emerging threats, and the talent gap.

Get executive insights

Industry highlights

We identified key insights across four select industries worldwide.

Communications and media

Organizations in the communications and media industry tend to have more advanced security capabilities than their counterparts. Forty-five percent currently use detection as code, and many of them have benefited from the ability to automate workflows (51%) and deploy test-driven detection development (67%). AI enthusiasm also runs high in communications and media, as 19% completely trust AI to perform mission-critical SOC activities — almost double the average across all industries. They're particularly optimistic about the potential of domain-specific generative AI, with 77% saying that it would *significantly* or *extremely* enhance security operations compared to publicly available tools like ChatGPT.

The communications and media sector benefits from reusing data across IT, engineering, and security. Forty-four percent say they *frequently* or *always* do so, with data reuse accelerating incident remediation (48%) and improving processes (57%) to a *significant* or *transformative* extent. The industry is more likely to understand the value of data sharing and collaboration, which may explain why they're realizing the advantages of a unified platform approach more often than their peers; 55% spend less time maintaining tools and 59% accelerate incident response.

Financial services

An impressive 26% of financial services institutions say keeping up with cybersecurity requirements has gotten easier this past year — more than double the cross-industry average. The industry shines when it comes to data management strategy. Eighty-nine percent of financial services respondents regularly use data federation, compared to 72% across all industries. Forty-one percent of respondents in this sector *frequently* or *always* share data across IT, engineering, and security — and they're reaping rewards such as accelerated incident detection (50%).

Seventy percent say an understaffed or underskilled team is their biggest cybersecurity challenge, which is substantially higher than the cross-industry average of 49%. Fifty-seven percent of respondents have a compliance management skills gap, which is concerning for the highly regulated industry. For 50% of respondents in financial services, regulatory compliance violations were one of the most common incidents over the past year, ahead of supply chain attacks (15%) and ransomware (24%) combined.

As a whole, the industry is optimistic about AI's function within the SOC. For 43% of respondents in financial services, applying AI to security workflows is the top cybersecurity initiative for the next year.

Public sector

The public sector is making strides in its cybersecurity maturity journey, as 63% have seen a *moderate* or *significant* decrease in successful cyberattacks this past year. However, it still lags behind its peers in a few key areas. Low visibility is a foundational challenge, especially over users and data (41% say it *needs improvement*) and network infrastructure they own or operate (51% say it's *somewhat* or *very low*).

SOC teams also struggle with disconnected tools. Public sector respondents are twice as likely as the industry-wide average to say their dispersed tools create *significant* challenges (48% versus 24% across all industries). Some have adopted a unified security platform approach, which could help address tool dispersion. Of those who've taken the leap, 48% of respondents from the public sector now spend less time maintaining tools.

A common skills gap in the industry is DevSecOps, cited by 49%. DevSecOps is a foundational skill for detection as code, and although 46% currently have detection as code capabilities, just a subset have achieved outcomes like standardizing the deployment of detections (27% versus 45% in the aggregate) and increasing SOC productivity (25% versus 41% in the aggregate).

Manufacturing

A third (33%) of manufacturing respondents saw an uptick in successful attacks this past year. Data breaches were the most common attack type, cited by 77%. Security teams struggle to spend enough time on strategic defense, as 76% expend more time on tool maintenance than on threat investigation and mitigation (compared to 46% across all industries). Additionally, the vast majority believe their tools are too dispersed (95% versus 78% for all industries). Some SOCs have adopted a unified security platform approach, and of these, 58% say they now spend less time maintaining tools.

Manufacturing organizations also struggle with alerting; 57% say they have alerts without context, while 44% report their alerts are not properly prioritized. These alerting challenges could be related to the industry's low visibility. When asked to rate their visibility across different areas, 59% say it's *somewhat* or *very low* for their on-premises infrastructure (compared with 31% of their industry counterparts).

The industry has been slow to adopt AI for its SOC functions, but is planning to expand its use cases soon. Although just 10% currently use generative AI for threat hunting, another 71% say they will in the near future. Seventeen percent are using generative AI to enhance threat detection right now, and another 43% plan to follow suit.

Country highlights

Snapshots from nine countries across the globe.

Australia and New Zealand

SOCs in Australia and New Zealand are understaffed and underskilled, which 59% cite as one of their biggest cybersecurity challenges. As a result, 60% say their team members have been asked to lead projects without experience, while 66% experienced delays to a critical security initiative.

To close these gaps, 71% of organizations in this region are investing more in AI and machine learning technologies. Twenty percent of respondents from Australia and New Zealand currently use generative AI to create documentation, while another 57% say this will be the case soon.

Some security teams in the region adopted a unified security platform approach, and are reporting benefits such as faster incident response (65%). Thirty-three percent of respondents in Australia and New Zealand have detection as code capabilities, and another 51% plan to use detection as code in the near future.

France

Data management is a significant challenge for teams in this region, as 62% have lost valuable time in investigations due to gaps in their strategy. When asked about the toughest aspects of data management, 58% cite the high cost of data storage and movement.

Security teams in France tend to have a more connected SOC. Fifteen percent *always* use the same data across IT, engineering, and security, more than respondents from every other country surveyed. Many in the region use a unified security platform, which reduced the amount of time needed for tool maintenance (54%).

SOCs in France are also ahead in their adoption of detection as code. More than half (56%) have this capability, compared to 41% across all countries, and they've experienced wins like deploying test-driven detection development (65%), automating workflows (44%), and increased SOC productivity (40%).

Germany

Many security teams in Germany have dispersed tools and high alert volumes. Eighty-one percent say their tools are disconnected; of these, 68% say this has introduced *moderate* to *significant* challenges. As for alerting, 61% of organizations in Germany say their analysts receive too many alerts, while 54% receive too many false positives.

SOCs in this region with a unified security platform approach spend less time maintaining tools (55%) and respond faster to incidents (62%). The future of the SOC is incredibly collaborative, and security teams in Germany demonstrate some of that behavior currently. Twenty-seven percent say their SOC is not a standalone function. Meanwhile, 67% use the same data across IT, engineering, and security *sometimes* or *frequently*, while 5% do so *always*.

In Germany, SOCs are entrusting AI with more responsibilities. Generative AI is already performing tasks like threat detection and prioritization (29%) and threat hunting (15%), and more say this will happen soon (50% and 53%, respectively).

India

Two-thirds (68%) of SOCs in India have dispersed and disconnected tools. Some have found a solution in using a unified security platform approach, as 55% of them now spend less time maintaining tools.

Data management is a challenge for SOCs in India, as 58% struggle with the high cost of data storage and movement. They're also less likely to use best practices like data tiering (46%) and filtering (39%). Due to gaps in their data management strategies, security teams have violated compliance and regulatory mandates (46%) and lost precious time during investigations (56%).

The adoption rate of detection as code is also low among security teams in India; 35% have such capabilities, which is below the worldwide average. DevSecOps is a foundational skill for using detection as code, and 59% of respondents from India say they have a skills gap in this area. That said, adopters of detection as code are seeing payoffs, including the ability to deploy test-driven detection development (65%) and automate workflows (49%).

Japan

Many organizations in Japan face data management challenges, with 51% finding it hard to maintain data accessibility. As a result of such gaps, security teams have lost valuable time during investigations (57%) and increased their overall risk and number of blindspots (52%). Forty-three percent also say they have too many data silos. SOCs in Japan can benefit from best practices like data federation; however, the country has the lowest adoption rate compared to other nations (65%).

Security teams in this country are embracing AI and seeing greater efficiency as a result. Japan has the highest percentage of respondents who said securing AI workloads is their top cybersecurity initiative for the year (18%). Sixty-two percent say using AI has boosted the productivity and efficiency of their SOC either *moderately* or *significantly*, and many have plans to use generative AI soon for use cases like threat detection (53%) and security data summaries (48%).

Singapore

Cybersecurity programs in Singapore tend to be more mature, given their success with advanced technologies like detection as code and generative AI. Fifty-seven percent of SOCs here have detection as code capabilities already, ahead of 41% of respondents worldwide. As a result, they can deploy test-driven detection development (61%) and improve SOC productivity (52%).

Respondents from Singapore are enthusiastic about AI's future within the SOC. Twenty percent say they completely trust the technology to perform mission-critical tasks, almost double the 11% worldwide average. When asked about the benefits, 61% say AI has increased productivity *moderately* or *significantly*.

SOCs in Singapore that have embraced a unified security platform approach see benefits like faster incident response (62%). They are also less likely to experience *significant* challenges from dispersed tools (11%, compared to 24% in the aggregate).

U.K.

Many SOCs in the U.K. say their top source of inefficiency comes from their tools not integrating well, cited by 58%. Some security teams found a solution in using a unified security platform, which decreased the amount of time they spent on tool maintenance (52%). Many also found that it accelerated incident response (58%) and improved threat coverage (54%).

Gaps in data management strategies also cause inefficiencies within SOCs in the U.K., such as decreases in team productivity (43%). When asked about their main difficulties with data management, respondents most frequently mentioned the high cost of data storage/movement (57%) and data ingestion (41%).

More foundationally, security teams in the country have less visibility across different parts of their infrastructure compared to their counterparts. They say visibility is *somewhat* or *very low* for their on-premises infrastructure (33%), software vulnerabilities (44%), and third-party assets (49%).

U.S.

Fifty-nine percent of respondents in the U.S. experienced a decrease in successful cyberattacks this past year, despite staffing shortages. Many are reporting that their team is overworked (52%), understaffed (46%), and underskilled (36%). Meanwhile, 65% say they receive too many alerts.

These staffing problems extend to areas such as detection as code. American security teams have high enthusiasm for this capability, as 29% say they want to use it all the time. However, almost half (46%) have a detection as code skills gap. And 58% say their SOC simply doesn't have the skills or expertise to create effective detections.

AI could alleviate some staffing and bandwidth issues, and SOCs in the U.S. have started tapping into the technology. Eleven percent trust AI completely to perform mission-critical SOC activities, with another 60% saying they trust it *somewhat*. About a quarter, on average, of security teams in the country already use generative AI for cybersecurity tasks like threat detection (24%), development (23%), and querying security data (30%).

Methodology

Oxford Economics researchers surveyed 2,058 security leaders (including directors of security, vice presidents of cybersecurity, directors of security operations, and security analysts) October 2024 through December 2024. Respondents were in Australia, France, Germany, India, Japan, New Zealand, Singapore, United Kingdom, and United States. They also represented 16 industries: business services, construction and engineering, consumer packaged goods, education, financial services, government (federal/national, state and local), healthcare, life sciences, manufacturing, technology, media, oil/gas, retail/wholesale, telecom, transportation/logistics, and utilities.

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_state-of-security-2025_v15