SANS | Research Program

2025 SURVEY

SANS SOC Survey 2025

Written by **Christopher Crowley**

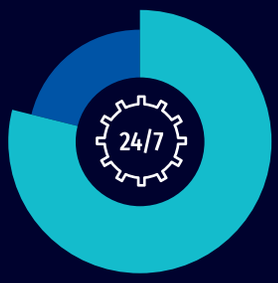
July 2025

infoblox.

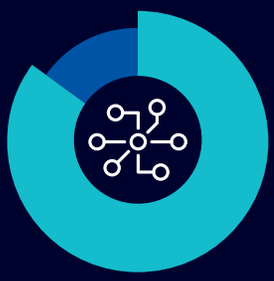
SANS 2025 SOC SURVEY

Key Findings

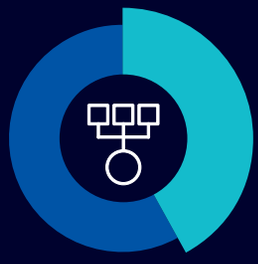
Operations and Technology Use



79% of SOCs are operational **24/7**.

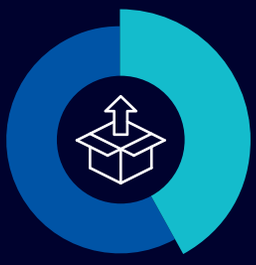


85% of respondents say **endpoint security alerts** are their **primary trigger for response**.



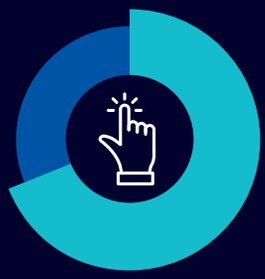
42% of SOCs **dump all incoming data into a SIEM**, often without a retrieval or management plan.

43% of respondents say **SIEM** is the **top tech skill** they seek when hiring—**more than double** the next highest response.



42% of SOCs use **AI/ML tools "out of the box"** with **no customization**.

69% of SOCs use **cyber threat intelligence (CTI)** data primarily for **incident response**.



69% of SOCs still rely on **manual or mostly manual processes** to report metrics.

Staffing and Workforce Dynamics

2–10 people is the most common size for a fully staffed SOC.

3–5 years is the most common tenure for SOC staff.

73% of organizations allow remote work for SOC team members at least some of the time.

62% of SOC professionals say their organization isn't doing enough to retain top talent.

42% of SOC staff don't know the SOC's budget, indicating a disconnect between technical and business teams.

Survey Author

VIEW PROFILE

Christopher Crowley
SANS Senior Instructor

CURRENTLY TEACHING

SEC595: Applied Data Science and AI/Machine Learning for Cybersecurity Professionals™

SEC511: Cybersecurity Engineering: Advanced Threat Detection and Monitoring™

SEC504: Hacker Tools, Techniques, and Incident Handling

FORMERLY TAUGHT

FOR585, SEC401, SEC503, SEC560, SEC575, SEC580 MGT535, MGT517

Christopher Crowley has 25 years of industry experience managing and securing networks. He has authored numerous courses and is considered a leading expert in building an effective SOC. He currently works as an independent consultant in the Washington, DC, area focusing on effective computer network defense. His work experience includes penetration testing, security operations, incident response, and forensic analysis. Chris holds several industry certifications including the GSEC, GCIA, GCIH (gold), GCFA, GPEN, GPYC, GMOB, GMLE, GASF, GREM, GXPN, and CISSP.

Chris was awarded the SANS 2009 Local Mentor of the Year Award. The Mentor of the Year Award is given to SANS Mentors who excel in leading SANS Mentor Training classes in their local communities. He is also a faculty member of the SANS Technology Institute and the NSA Center of Academic Excellence in Cyber Defense as well as a multi-time winner of the National Cyber League Competition. Chris spends his spare time mountain biking, rock climbing, and savoring epicurean treats.

Executive Summary

Over the past nine years, the SANS Institute has conducted an annual industry survey to better understand how security operations centers (SOCs) are built, staffed, and run, and to learn more about SOC analysts' biggest challenges and potential industry improvements. This year's goal was to provide insights into SOC performance against peers, prioritize improvements for the coming year, and gain insight into valued and less-effective technologies across the industry.

This year's report outlines data and insights behind SOC structure comparisons, outsourcing trends, technology considerations, areas for improvement, and ways in which various technologies are being implemented.

Although AI is the latest technological trend, it's notable that over the nine years of conducting this survey, capabilities, staffing levels, outsourced services, and challenges in security operations have remained largely consistent.

Security operations is a long-term, gradually maturing effort that demands both patience and persistence.

Demographics

Most respondents were based in the United States, with participants from 57 different countries. The top industries represented were the usual mix of respondents from banking/finance (16%), cybersecurity (14%), technology (14%), and government (14%) and there was a diverse representation of organization size. Figure 1 shows the survey demographics in detail.

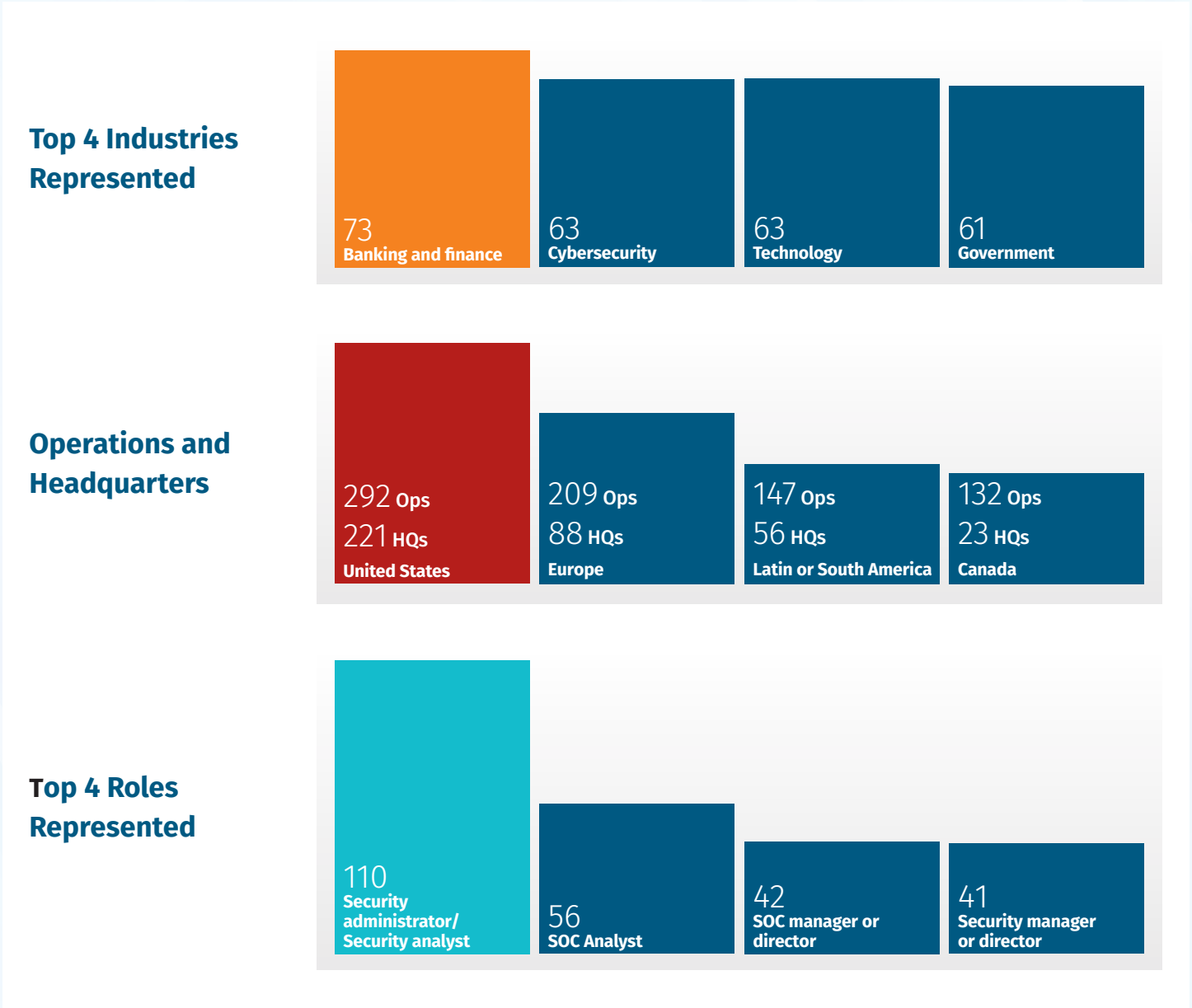


Figure 1. Demographics of Survey Respondents

Security Operations Center (SOC) Defined

The modern SOC in 2025 is built around a few foundational elements that define how it functions, where its strengths lie, and how it adapts to evolving threats. These include its core capabilities, operational model (in-house vs. outsourced), data architecture, and staffing strategy. Based on current survey data, a typical operational SOC reflects the following four characteristics:

- **Capabilities—**The core functions of a SOC and the tasks it handles on a routine basis
- **In-house vs. outsourced functions—**The tasks that are handled internally vs. by third parties
- **Architecture—**The structure for how and where data is collected, stored, and accessed
- **Staffing and hours of operation—**Details on team size, roles, expected skill set, and whether the SOC operates around the clock or during limited hours

In addition, according to the data, a baseline SOC can be defined as:

- **Prioritizes alert triage, threat detection, and incident response as core functions** with threat intelligence, vulnerability management, and hunting as supporting functions.
- **Employs 10 full-time team members** (or full-time equivalent) with the average length of employee tenure of three to five years.
- **Handles most monitoring, detection, and incident response in-house,** while outsourcing pen-testing, digital forensics, some threat intel, and other functions requiring higher levels of expertise or specialization.
- **Operates a centralized architecture,** with cloud adoption growing but still lagging behind the cloud adoption volume of IT.
- **Maintains 24/7 operational coverage in most cases,** with some still relying on rotating coverage or “as-needed” escalation.
- **Reports metrics manually,** even though nearly half say it’s too time-consuming. Automation remains limited.
- **Relies heavily on EDR** as the most trusted and mature tool in use. AI/ML is at the bottom of the satisfaction list.
- **Stores more data than ever before,** often dumping everything into SIEM or syslog without a clear plan in place to manage or analyze it, creating visibility issues.

Capabilities and Outsourcing

The expectations of SOC functions are robust and comprehensive. Survey responses make it clear: Failing to cover core responsibilities, whether in-house or outsourced, results in a SOC that is ineffective at detecting and responding to threats.

Although there is variety in the activities split between internal teams and external vendors, such as MSSPs, the core expectations for what a SOC must be able to do remain largely consistent year-over-year with the top three activities reported as security roadmap and planning (80%), security administration (80%), and security architecture and engineering (78%) (see Figure 2).

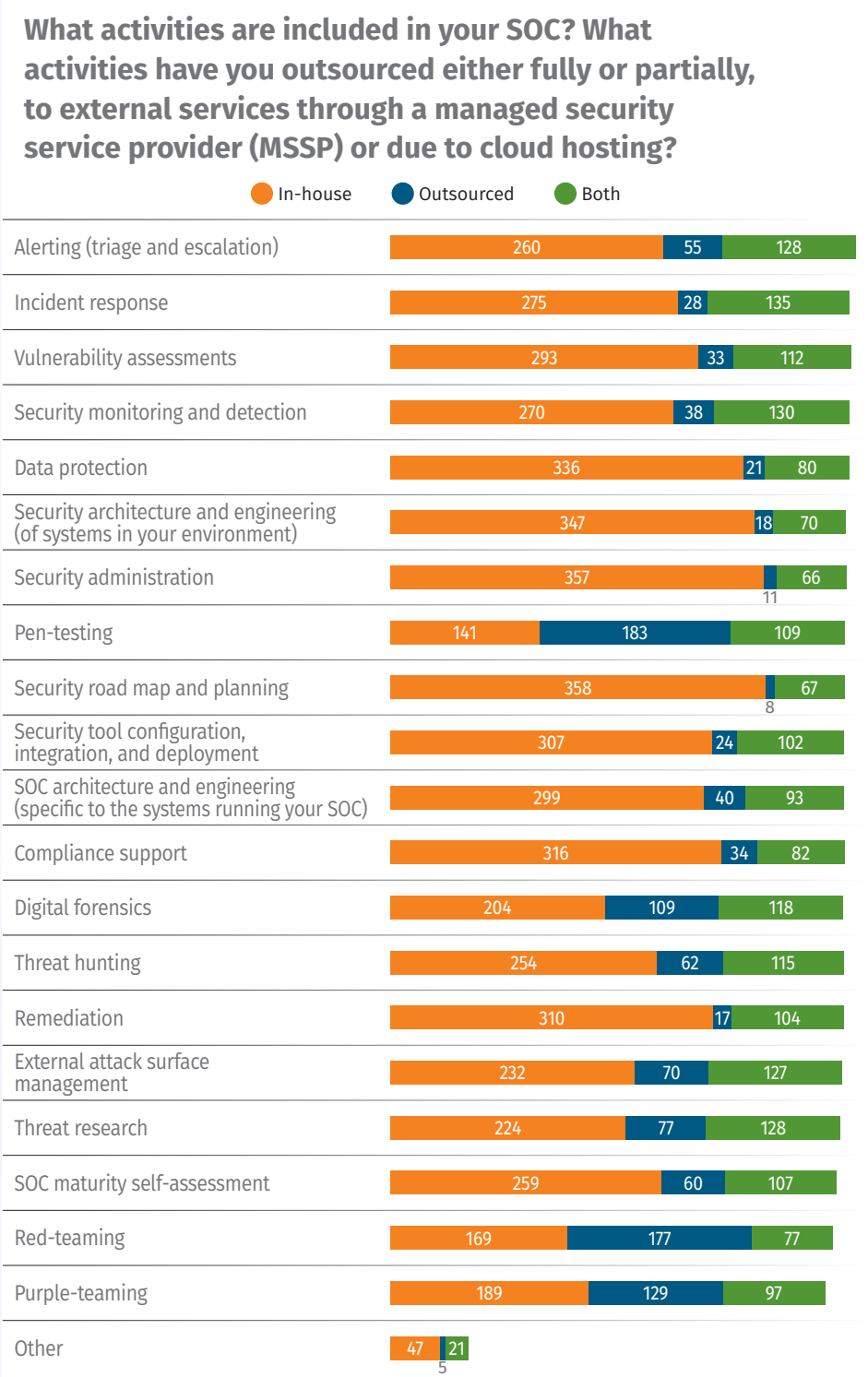


Figure 2. Response Count on SOC Operations Activities Related to Outsourcing

In-House vs. Outsourcing SOC Capabilities

Core SOC functions like architecture, monitoring, and compliance are typically kept in-house. This is likely because these areas demand a deep understanding of internal systems, business priorities, and organizational context. They also involve close coordination with legal and executive stakeholders, making them more effective when owned internally (see Figure 3).

On the other hand, outsourcing makes strategic sense for tasks that are highly specialized, repeatable, and resource intensive. Services like penetration testing and red teaming often fall into this category. These are typically project-based efforts where third-party firms can provide targeted expertise and scalability more efficiently than internal teams.

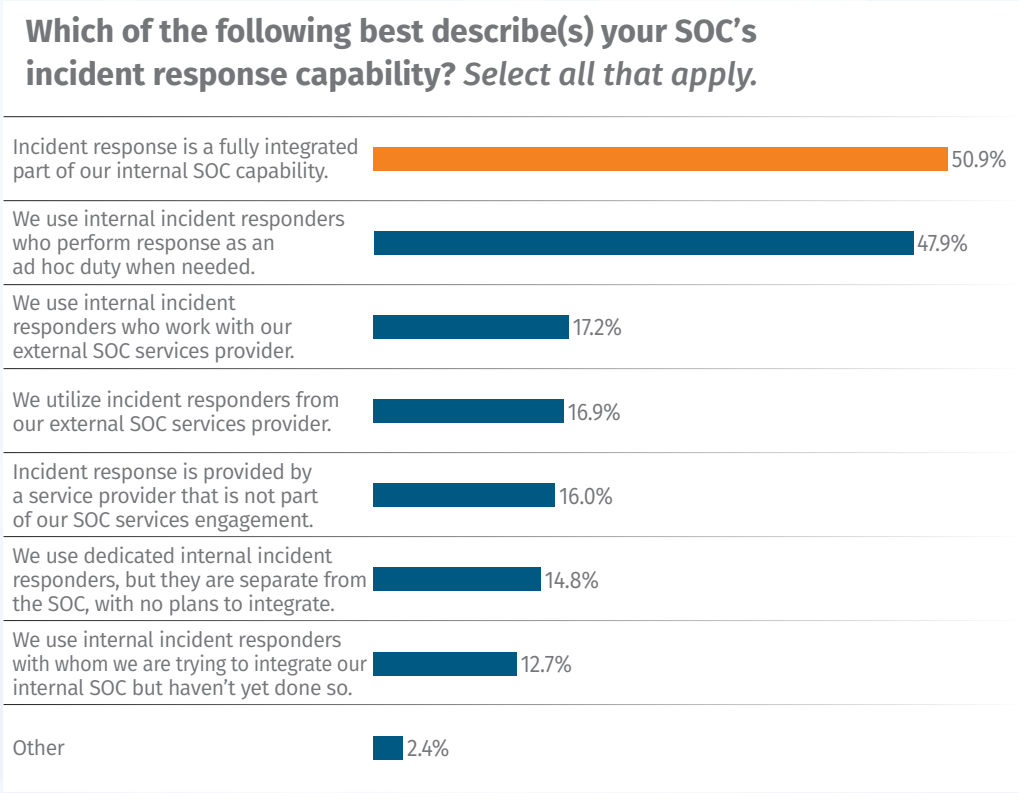


Figure 3. Incident Response Capabilities

Security monitoring and incident response are often hybrid models—partially staffed in-house, with external providers filling in for overflow or specialized coverage. This blended approach allows for flexibility while maintaining core control.

Interestingly, 55% of respondents say SOC use is mandatory across their organizations, and another 30% say there's latitude to use external providers. That indicates SOCs are still viewed as foundational—but organizations are open to flexible deployment models depending on institutional requirements and resources. Incident response remains the most internally managed function. Given its role in real-time crisis management, it makes sense that most organizations keep this capability under their control.

Architecture

Most respondents (38%) report operating a single, centralized SOC, making it the most common architecture today. Cloud-based SOC deployments follow at 24%, but respondent's indicate planned changes will increase that number to 29% over the next 12 months indicating growing interest in cloud-native security operations.

Despite the hype around cloud-based SOCs, centralized, on-prem architectures remain the prevailing model. The gap between stated cloud ambitions and current deployments highlights the reality: Cloud migration, particularly for security operations, is still in transition.

Although single, centralized SOCs continue to lead, year-over-year data doesn't yet point to a decisive architectural shift to the cloud (see Figure 4).

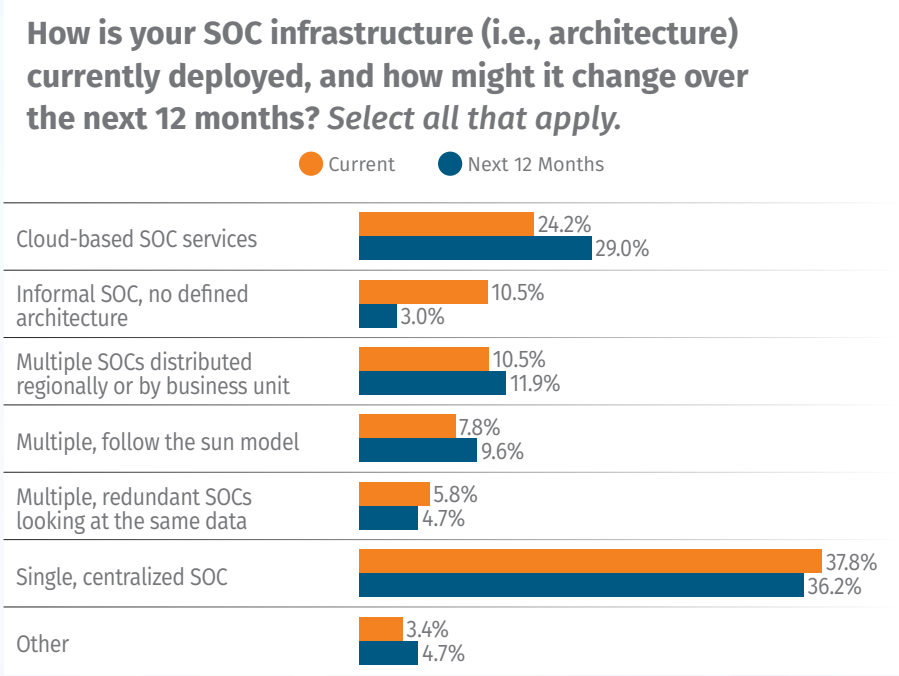


Figure 4. SOC Architecture, Current and Planned

As global political uncertainty intensifies through 2025 and into 2026, SOCs can expect increased scrutiny around international data flows. Geopolitical conflict is driving greater regulatory and organizational focus on how and where data is stored, who can access it, and which entities are monitoring it.

SOCs should be prepared to respond to tough questions around cross-border visibility, third-party monitoring, and data residency. These aren't just technical issues—they're legal and strategic concerns. Security leaders should anticipate deeper engagement from legal, compliance, and business stakeholders as these topics rise on the agenda.

Modern SOC Challenges

Today's SOCs are under pressure to deliver faster, smarter, and more proactive security outcomes—but several critical gaps are holding them back. AI/ML tools are being adopted rapidly, yet without intentional integration and oversight, they often waste budget, increase risk, and fail to provide meaningful support. At the same time, threat intelligence—while abundant—is frequently underutilized due to inconsistent application and a lack of objective analysis, keeping teams stuck in reactive mode. And although not a direct source of intel, TLS interception has emerged as a flashpoint in the visibility debate, raising concerns about privacy, performance, and trust. These issues collectively reflect a deeper need for strategic alignment and smarter operational practices across the SOC.

SOC employees are making abundant use of AI/ML tools without intentional integration and oversight. AI/ML tools provide value, but potentially waste budget, add risk, and fail to deliver meaningful support to SOC operations—technology satisfaction is low, but reported use is nonetheless high.

Artificial Intelligence (AI) and Machine Learning (ML)

With the substantial influence of AI and ML tools on the SOC in recent years, learning more about the influence of both will continue to be important. **Interestingly, data shows that the majority (40%) use the tools, but they are not part of the defined operations** (see Figure 5).

A SOC likely has two internal tasks to address:

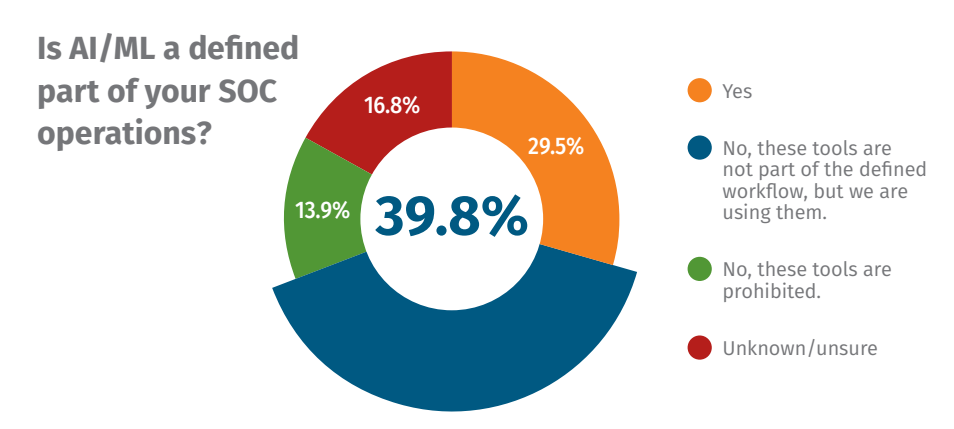


Figure 5. AI/ML Within SOC Operations

1. **Internal SOC priority—**Shift from uncoordinated, individual use of AI/ML tools to a team-approved, standardized implementation—one that maximizes their strengths while minimizing risk.
2. **External SOC priority—**Maintain oversight of data flowing from the organization to AI/ML platforms and unsanctioned shadow IT deployments. Although much of this data may seem low-risk, it's essential to have host-based data loss prevention (DLP) tools in place as part of your standard deployment to ensure visibility and control.

Expert Corner

The 2025 SOC Survey highlights a worrisome juxtaposition; SOCs struggle to hire and retain skilled analysts, while AI/ML and automation are the most commonly planned expansions, despite ranking lowest in value delivered. AI should augment analysts, not replace them. My concern is that leadership may see AI as a shortcut to fill staffing gaps, instead of investing in the talent and thoughtful integration of AI needed for substantive SOC improvement.

VIEW PROFILE

Seth Misner
SANS Faculty Fellow and author of two SANS courses: **LDR414: SANS Training Program for CISSP® Certification, SEC511: Cybersecurity Engineering: Advanced Threat Detection and Monitoring,** and **SEC411: AI Security Principles and Practices: GenAI and LLM Defense**.

Cybersecurity teams may not own the risk of AI hallucinations or inaccurate outputs, but the SOC can play a key role in mitigating their business impact. Governance, risk, and compliance (GRC) teams need technical support to monitor how AI tools are used and what systems or data they interact with.

Threat Intelligence

Threat intelligence activities are a significant part of SOC operations (73%) with the primary usage as incident response (69%). Figure 6 outlines the various ways in which CTI data and information are being used. CTI information is typically disseminated through email or documents (56%) and/or reports (55%).

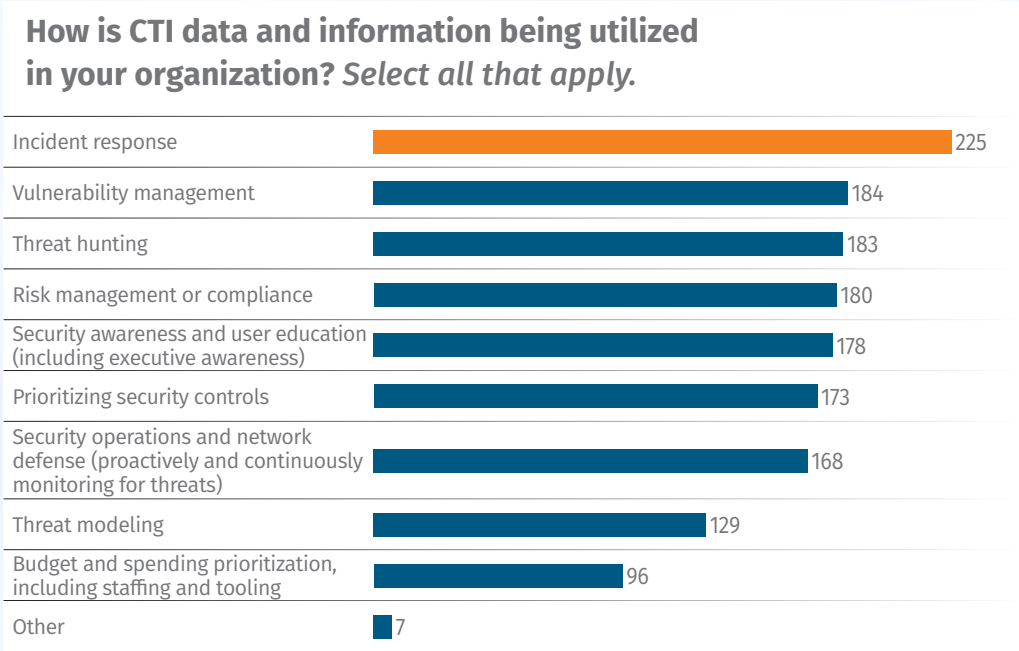


Figure 6. Count of Responses on CTI Data usage Within the Organization

Because threat intelligence is largely analysis-driven, respondents were asked about the analysis methods they most use. The most common answer (72%) was that analysts use their experience and intuition. Although expertise is essential, there's a strong case for incorporating more structured analytical approaches, such as conceptual or inductive methods, to improve consistency and reduce bias.

Additionally, most information comes from external sources, indicating there's a growing need to generate threat intelligence from internal data sources and not just rely on external feeds. Leveraging internal data can enhance risk assessment, threat hunting, and response capabilities. The most effective way to build internal threat intelligence is through collaboration and information sharing. However, SOC-based threat intelligence teams may lack organizational support for this. In such cases, informal peer collaboration can serve as a practical and acceptable alternative.

Incident Response Is Reactive, Not Proactive

The SOC's incident response capability is primarily described as either fully integrated as part of the internal SOC (51%) or provided through internal incident responders who perform ad hoc as needed (48%). The data also showed that incident response starts are primarily triggered by internal security alerts (85%). When asked about satisfaction levels for incident response capabilities, respondents are most satisfied with EDR and adversary containment and are least satisfied with deception technologies, a consistent trend since 2022. Only AI/ML tools have ranked worse in recent years.

When asked about threat hunting, the picture was similar. Most teams described partially automated hunting using vendor-provided tools (48%). Although technically a form of hunting, this often amounts to retroactive analysis rather than true, technique-driven hunts. The distinction matters because effective hunting requires skilled analysts, who remain in short supply. A lack of skilled staff remains the top-cited barrier for why teams aren't taking the time to do more sophisticated hunting (16%). More details on this in the next section.

Running Windows Defender with updated signatures and scanning the file system is not threat hunting. It's basic detection. Although historical search capabilities are improving due to advancements in vendor tools, SOCs need to stop calling this "hunting." There's still real value in doing it the hard way. True threat hunting relies on proven methodologies, hypothesis-driven analysis, and deep familiarity with attacker behavior. Alerts are designed to catch known threats, but sophisticated adversaries don't always trigger them. They operate quietly, below the detection threshold—and if you're not actively hunting, you're not going to find them.

Running Windows Defender scans isn't threat hunting, it's basic detection. True threat hunting involves hypothesis-driven analysis and deep knowledge of attacker behavior to uncover stealthy threats that evade alerts.

SOC Staff and Retention

Despite a growing "return to office" (RTO) trend in the United States, 73% of respondents indicated that SOC staff *can* work from home. However, responses show that if they are permitted, it depends on the specific role and skill set. In short, although most SOCs support remote work in principle, not every team member is granted that flexibility—even when the necessary technology is in place.

SOC teams are perennially short on highly skilled staff. It's a continuous struggle, and SOC leaders say their organizations aren't doing enough to keep the best people they have. Retention isn't just an HR issue. It's a signal of leadership's priorities. And it's hard to keep a SOC operating at its highest efficiency and effectiveness if the turnover rate is too high. If you want your team to stay, show them you're serious about understanding the factors that lead to job satisfaction.

One of the most common questions SOC leaders face is: *How many people does it take to run a SOC?* The most common answer is 10 (expressed as fulltime equivalents) and it's a good place to start your planning. This allows for adequate coverage across key functions like monitoring, incident response, threat intelligence, and engineering. Of course, in large, multinational enterprises, SOC teams can easily scale into the hundreds. But for most organizations aiming to maintain a solid internal capability, 10 is the number to plan around.

While the lack of skilled staff continues to be cited as the top challenge facing SOCs, 62% of respondents express a clear lack of confidence in their organization's ability or willingness to address it through meaningful retention efforts (see Figure 7). This disconnect highlights a deeper issue: Retention strategies may exist, but they aren't visible or credible to the people they're meant to support. Improving transparency around retention programs and demonstrating real follow-through—not just marketing platitudes—can go a long way toward rebuilding trust and keeping talent in place. Interestingly, even with this lack of confidence, respondents tend to stay employed three to five years in a SOC environment (31%) with very few staying 10-plus years (4%).

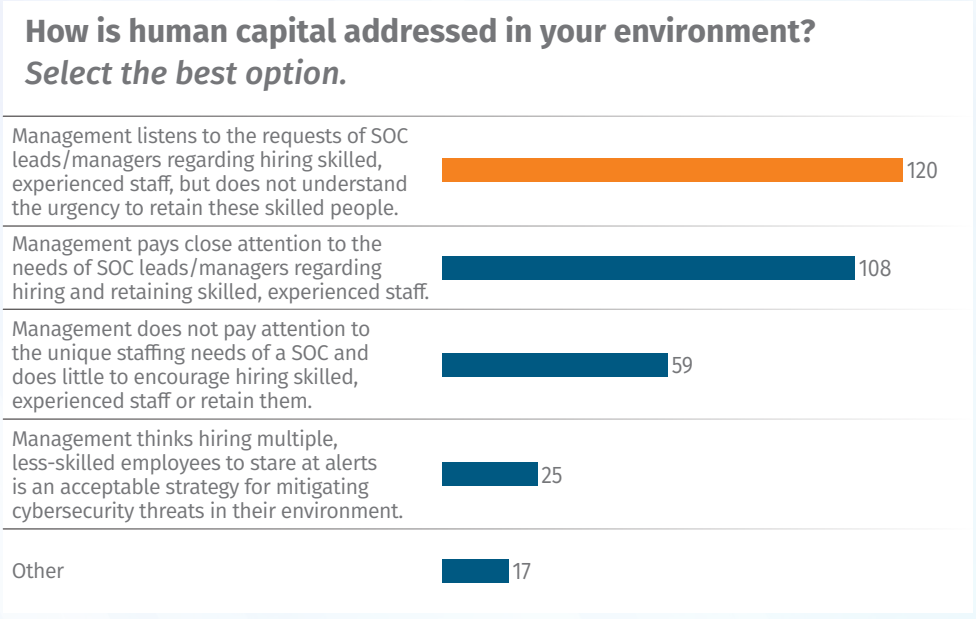


Figure 7. Count of Responses on Retention Efforts

Year-over-year comparisons show that compensation and engaging work are increasingly seen as effective retention strategies. Although career progression opportunities dipped in importance in 2024, they appear to be making a strong comeback in 2025 (see Figure 8).

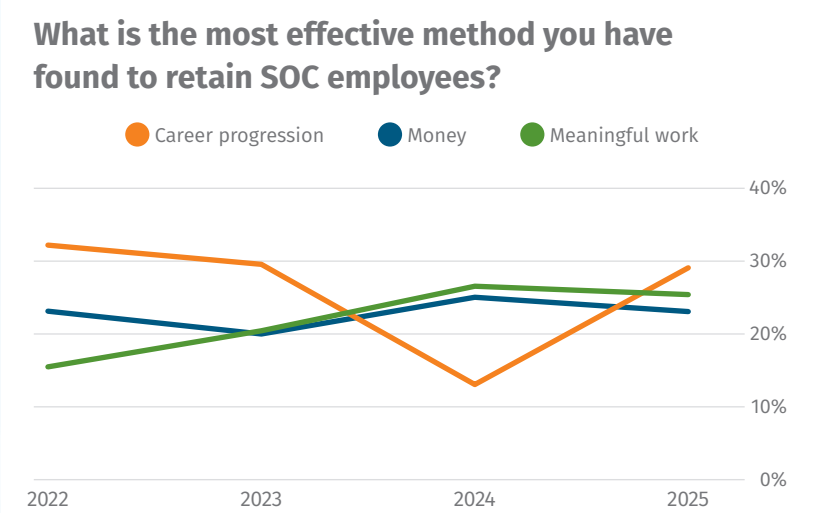


Figure 8. Effective Methods for Employee Retention

What SOC Leaders Want in an Employee

When asked about the most important technical skill deficit when hiring staff for technical roles (i.e., which skill is most lacking), respondents identified information systems and network security (14%) and digital forensics (12%) as the highest, followed by a broad range of other competencies outlined in Figure 9. For nontechnical skills, risk management topped the list at 14%.

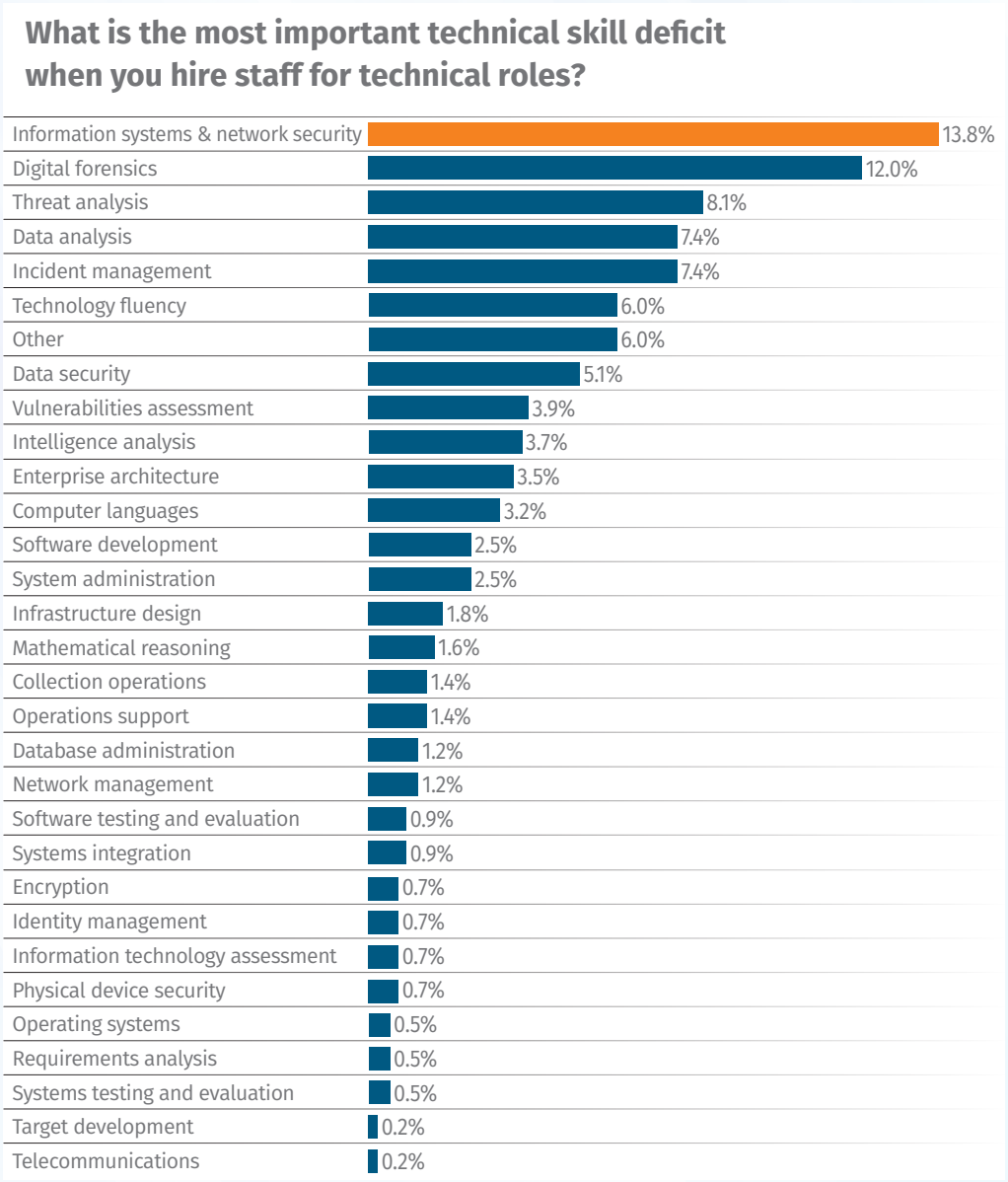


Figure 9. Skill Deficits

Expert Corner

Survey indicates that 62% of SOC professionals say their organization isn't doing enough to retain top staff. A great SOC isn't created by tooling, it's created with culture that recognizes and rewards the analysts who do amazing work. When analysts feel connected to the company mission and understand their contributions are an important part of that mission, they bring the energy, resourcefulness, and creativity needed to be successful. Managers need to recognize the talented analysts who set the model for success at all levels of technical ability and empower them to be leaders for others to follow.

Joshua Wright
SANS Faculty Fellow and Author of **SEC504: Hacker Tools, Techniques, and Incident Handling**.

VIEW PROFILE

What's Hot, What's Not in SOC Technology

If company leadership isn't prepared to fully commit the resources to make a tool effective, it would be better not to deploy it at all. A shiny new technology that seems like a great solution requires budget, training, time, and integration into workflow.

Endpoint or extended detection and response (EDR/XDR) once again tops the list for satisfaction, and it's the only technology this year to earn a score above a 3 out of 4 (when comparing technologies used and level of satisfaction). It's the most fully deployed, most trusted tool in the stack. EDR/XDR earns high satisfaction ratings because it's fully deployed, effective for initiating incident response workflows, and backed by proper training and support.

AI/ML tools continue to underperform. Of the three AI/ML technologies measured, two ranked at the very bottom, including generative language tools, which scored just a 2 out of 4. AI/ML tools underperform because they're new, often introduced without clear ownership or authorization, adequate deployment budget, or plans for integration into day-to-day operations.

Overall, established tools continue to earn the highest marks. EDR remains the top-rated technology, because it's trusted for its reliability and maturity. These are the workhorses of the SOC: well understood, widely deployed, and proven over time.

In contrast, newer technologies like AI/ML and deception are still struggling to meet expectations. Satisfaction remains low, suggesting that although interest is high, real-world performance and integration haven't caught up yet. This is very likely to change over time, and vendors of AI/ML technology shouldn't despair. Back in 2017, "asset discovery and inventory" held the bottom spot and now it's solidly mid-pack. Progress for AI is likely.

Conclusion: Encouraging Trends, but There's Still Work to Do

The 2025 SOC Survey confirms that the SOC is continuing to evolve encouragingly in the direction of established trends, but very slowly in some areas. Core capabilities are strong, but the balance still tilts toward reactive work. AI/ML remains underwhelming. Threat hunting is limited by staffing. And tool satisfaction, as always, depends on full deployment and thoughtful integration.

The 2025 SOC Survey paints a familiar picture: solid capability, some hopeful trends, but limited forward motion and ongoing staff dissatisfaction.

What's clear is that progress takes intention—in hiring, training, architecture, and tool use. Collecting data is easy. Using it wisely is the hard part.

SOC teams know what they need—tools that work, staff who stay, and time to do more than respond to alerts. But budget, turnover, and shifting priorities continue to get in the way. Metrics are tracked, but still manually. Cloud adoption ebbs and flows. AI/ML tools remain overhyped and under-delivering.

Meanwhile, a growing number of organizations are defaulting to "just store everything in the SIEM," a trend that's easy to justify today and hard to pay for tomorrow. It's a visibility strategy that risks collapsing under its own weight.

Tools don't solve these problems on their own. People do. And while progress is happening, it's uneven and often held back by the same structural issues year after year. The bottom line is that SOCs aren't stuck—but they're not moving fast either. Real gains will come from clarity, coordination, and the decision to stop calling retroactive workflows "hunting."

Five Reasons to Be Optimistic About the Future of the SOC

Widespread 24/7 coverage
79% of SOCs now operate around the clock, signaling SOC maturity and commitment to continuous monitoring and support from business stakeholders who recognize the seriousness of global cyber threats.

Increased cloud use
Although centralized SOCs are the most common architecture, migration to cloud resources is reportedly planned for the SOC systems.

Growing reporting of proactive detection
Even if it's still a minority, more teams report using SIEM searches and threat hunting, not just alerts.

More clarity on AI/ML use
Organizations are very slowly starting to intentionally integrate AI/ML tools into workflows, which proves it can be done when there's a plan.

Career progression tops retention factors
People want to stay where they are, but only if they see a future. That's a call to action for leadership.

Sponsor

SANS would like to thank this survey's sponsor:

SANS | Research Program

About the SANS Research Program

The SANS Research Program is a key initiative by the SANS Institute and a premier global provider of cybersecurity research and information. SANS Research Program is designed to provide cybersecurity practitioners and leaders with data-driven insights, thought leadership and solutions that help them better understand and respond to evolving security challenges. All content is authored by SANS instructor experts from around the world who apply their years of experience from hands-on practitioner work in the field, advisory roles and the classroom to provide education, guidance, and actionable insights that help make the cyber world a safer place.

To learn about Sponsorship opportunities for research and content, in-person, or virtual events, email us at **Sponsorships@sans.org** or go to **www.sans.org/sponsorship**.