SANS | Research Program

SURVEY

2026 SANS SOC Survey Insights: A Decade of Evolution in Cyber Defense

Written by **Christopher Crowley**

June 2026

HORIZON3.ai

Foreword

Security operations is one of the few disciplines where the pace of external change and the pace of internal change have almost nothing to do with each other. Threats evolve daily. Adversaries adapt in hours. The SOC adapts in years. That is not a failure of ambition or resources. It is the nature of a function built on accumulated expertise, institutional knowledge, and hard-won operational maturity. Deliberate change, in this field, is often the right kind.

This 10th annual SANS SOC Survey captures that reality with unusual clarity. The data shows a profession that has absorbed a decade of pressure from cloud migration, the proliferation of tooling, and the persistent gap between what management believes it provides and what practitioners experience. Now, it is facing something qualitatively different. Artificial intelligence is not arriving the way SIEM arrived or SOAR or EDR. It is arriving faster, with less organizational preparation and with implications for staffing, governance, and operational accountability that most SOCs have not yet worked through. The gap between AI adoption and AI integration, documented here for the first time at this scale, is the signal that deserves the most attention.

What makes this year's report different from prior editions is not the discovery of new problems. Every tension in this data—the staffing misalignment, the intent-action gap in technology strategy, the distance between executive perception and practitioner experience—has appeared in earlier surveys. What is different is the context in which those tensions now exist. AI will not wait for organizations to resolve them at their customary pace. The defenders who will navigate the next several years most effectively are the ones who understand where their organizations actually stand today, not where they intend to be. That is what this report is for.

—Christopher Crowley

Christopher Crowley
SANS Senior Instructor

CURRENTLY TEACHING

SEC504:
Hacker Tools, Techniques, and Incident Handling

SEC511:
Cybersecurity Engineering: Advanced Threat Detection and Monitoring

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

VIEW PROFILE

Cyber Leaders

SANS | Research Program

For the first time, the 2026 SANS SOC Survey includes a dedicated cyber leaders' module, capturing responses primarily from CISOs and VP-level leaders. Their responses do not validate the primary survey, but instead complicate it. Executives and practitioners describe the same organization and reach fundamentally different conclusions about how well it functions. **That divergence is not a measurement artifact; it is the finding.**

The through-line across every subsection below is the same: Executives are governing a function they cannot fully see, with beliefs they do not fully fund, from a position that practitioners do not recognize as engaged. Each data point below is a different expression of that single problem.

Key Highlights

1. **Visibility is the executive-level bottleneck.** 24% of cyber leaders identify lack of enterprise-wide visibility as the single biggest barrier to leveraging SOC capabilities, ranking it higher than staffing or automation gaps. Frontline practitioners name the same problem in different words: too many uncorrelated alerts, too many unintegrated tools, not enough context.
2. **Leaders believe they are more aligned than their teams do.** 59% of cyber leaders say management pays close attention to SOC hiring and retention needs. Only 32% of practitioners agree. That 27-point gap is not a data discrepancy; it is a relationship problem that compounds every staffing decision.
3. **CTI is being used. Budget is not following.** 74% of cyber leaders apply CTI to security operations and threat hunting. Only 26% use it to inform budget and spending prioritization. Intelligence that drives tactics but not investment is only doing half its job.
4. **Human capital is the binding constraint.** When asked what most limits their ability to fund cybersecurity priorities, cyber leaders cite human capital above all else (i.e., headcount limits, hiring freezes, and competition for experienced practitioners). Technology budgets move faster than headcount approvals, and that asymmetry shapes every resourcing decision downstream.

Cyber Leaders

SANS | Research Program

The Perception Gap

59% of cyber leaders say management pays close attention to SOC hiring and retention needs and 32% of practitioners agree. That 27-point gap has persisted across every year this question has been asked. Executives describe an intent. Practitioners describe an outcome. Both are accurate accounts of different parts of the same decision process, and the distance between them is where retention problems are born.

22% of cyber leaders acknowledge that management listens to retention requests but does not understand the urgency. 14% describe organizations where management does not engage with SOC staffing needs at all. That is 36% of security executives describing a management relationship with SOC talent that ranges from insufficient to absent, in a field where skilled staff is the top operational challenge.

The gap between executive intent and practitioner experience is not a morale problem, it is a capability degradation problem. When more than a third of security executives describe an insufficient or absent management relationship with SOC talent, the predictable result is not just high turnover. It is a SOC that cannot build institutional knowledge, cannot develop junior analysts into senior ones, and cannot maintain the continuity of detection and response capability that a sophisticated threat environment requires. The 27-point perception gap is not background noise. It is the mechanism by which staffing problems become operational failures.

The Visibility Blind Spot

When asked to name the single biggest barrier to leveraging SOC capabilities, 24% of cyber leaders name lack of enterprise-wide visibility (See Figure 1). On the other hand, practitioners name a lack of skilled staff first. These are two descriptions of the same dysfunction, one from the top and one from the ground. The executive cannot see the full environment, and the practitioner cannot get the headcount to instrument it.

Lack of automation and orchestration and lack of skilled staff follow visibility as the next-ranked barriers among executives. The ordering reflects an executive perspective: Visibility is a governance problem they feel directly. Staffing is a resourcing problem they believe they are addressing, even when practitioners do not experience it that way.

This matters because visibility is the prerequisite for every other governance decision. Budget prioritization, capability investment, and staffing decisions all flow from leadership's understanding of what the SOC can and cannot see. When that understanding is incomplete, the organization systematically underinvests in the areas it cannot see and overestimates its coverage in the areas it believes it monitors. The visibility gap does not just limit detection. It produces false confidence at the board level and misallocated resources at every level below it.

Cyber Leaders

SANS | Research Program

There is also a loop worth naming. Practitioners cite lack of skilled staff as their top barrier and executives cite lack of visibility. These are not separate problems. The SOC cannot get the headcount to instrument the environment fully, so the environment remains partially visible. That means executives cannot see the full scope of what they are missing, so they cannot make the case for the headcount to fix it. The visibility gap and the staffing gap are the same problem feeding itself. Addressing one without the other will not close either.

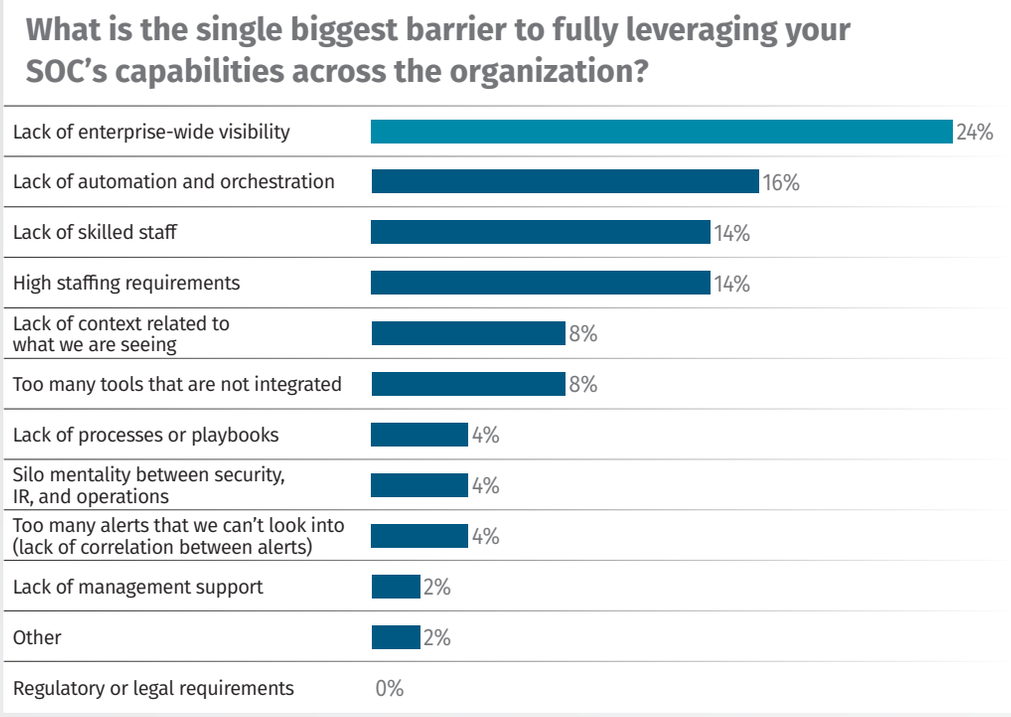


Figure 1. SOC Capability Barrier

Expert Corner

In 15 years of incident response and SOC engagements, the pattern I keep seeing is the one this survey makes hard to ignore: A report covering 444 SOC practitioners in depth mentions identity only once, in passing. Most teams I work with have engineered their endpoint coverage, but they have assumed their identity coverage. The visibility gap executives keep naming is, in large measure, an identity gap—and closing it means treating hybrid identity as a discipline our analysts and responders are deliberately trained in.

VIEW PROFILE

Maxim Deweerdt
SANS Principal Instructor;
Leadership Team at NVISO

COURSES TAUGHT

SEC559:
Cloud and Hybrid Identity Security

Cyber Leaders

SANS | Research Program

Intelligence That Informs Tactics but Not Investment

74% of cyber leaders apply CTI to security operations and threat hunting and 26% use it to inform budget and spending decisions. Intelligence that changes what analysts do today but not what the organization funds tomorrow is only doing half its job. The gap between operational CTI use and strategic application represents an unrealized return on one of the SOC's most mature capabilities.

The "why" is straightforward. CTI tells an organization which threats are active, which assets are targeted, which attack techniques are in use, and where defenses are most likely to fail. That is exactly the information a budget conversation should be built on. Instead, most organizations use it to guide what analysts do on Tuesday, and then set annual budgets based on vendor proposals, historical spend patterns, and executive instinct. The result is a security investment portfolio that is not calibrated to the actual threat environment. The organization knows what it faces. It does not let that knowledge change how it spends.

There is a second consequence worth naming. CTI that does not inform investment eventually loses organizational credibility. If the intelligence function cannot demonstrate that its outputs influence decisions beyond day-to-day operations, it becomes a cost center that leadership tolerates rather than a capability leadership funds. The gap between 74% operational use and 26% strategic application is not just an unrealized return. It is a slow erosion of the case for CTI investment itself.

Understanding Without Funding

75% of cyber leaders say their management understands that technology only works when skilled people run it. Yet when asked what most limits their ability to fund cybersecurity priorities, the same leaders cite human capital as the top constraint. Headcount limits, hiring freezes, and competition for experienced practitioners dominate the answer, indicating that the belief and the budget are not aligned.

51% of cyber leaders describe a funding process where management and SOC leads work closely together. 35% describe a process where management takes SOC recommendations but sometimes overrides them. The technology satisfaction data from the primary survey makes the consequence of that override measurable: SOCs with skilled practitioners score a technology satisfaction GPA of 2.76 compared to 2.14 for low-capability peers. Understanding that people matter is not sufficient. Funding that understanding is what changes outcomes.

This is important because it closes a specific accountability gap. It is one thing to show that organizations underinvest in people, and it is another to show that the leaders making those investment decisions know better. The 75% "understanding skilled staff are needed" is not a finding about ignorance; it is a finding about revealed preference. When forced to choose between what they believe and what they fund, these executives fund something else.

The technology satisfaction GPA data makes the cost of that choice measurable. The 62-point gap between high and low capability SOCs likely represents the difference between tools that are tuned, integrated, and operationally effective and tools that consume budget without returning value. Every leadership override that protects a technology budget at the expense of headcount investment is making that tradeoff explicitly. The data now quantifies what it costs.

What the Data Asks of Leadership

The data points toward a single requirement: closing the distance between executive intent and practitioner experience. That requires shared metrics, shared accountability, and governance structures that make the practitioner experience visible at the executive level before it becomes a crisis. Four priorities follow directly from the data.

1. **Address visibility as a governance investment, not a technology purchase.** Cross-environment data integration and asset inventory completeness are prerequisites for the visibility executives say they need.
2. **Translate CTI from an operational tool into a strategic one.** Organizations already using threat intelligence to guide daily operations have the input they need to inform annual investment decisions. The step has not been taken.
3. **Close the funding gap on human capital.** Technology budgets move faster than headcount approvals, and that asymmetry shapes every resourcing decision downstream. Automation and AI tooling can extend existing staff capacity in the near term, but they do not replace the practitioners who govern them.
4. **Measure the perception gap directly.** SOC leaders who can quantify the distance between what they need and what management provides—in operational terms—are more likely to close it. Data-free advocacy does not move organizations. Incident costs, detection gaps, and retention

2026 SANS SOC Survey Key Findings

The 2026 SANS SOC Survey tells a story of a function that has absorbed a decade of pressure and is now facing something it cannot absorb at its customary pace. AI adoption has outrun integration, staffing gaps persist despite consistent data on how to close them, and the distance between the SOCs making deliberate decisions and the ones still reacting to whatever arrives next is wider than it has ever been.

AI Has Arrived. Integration Has Not

79% of respondents use AI or ML tools, but only 36% have built them into a defined SOC workflow. The majority use AI individually, without organizational structure, governance, or consistent validation. That gap is not a technology problem but an organizational one.

The Staffing Problem Is Also a Management Problem

Lack of skilled staff is the top operational challenge, cited by 14% of respondents. Yet only 32% say management pays close attention to SOC hiring and retention needs. The data on what retains people is consistent across 10 years of this survey, and largely ignored.

Data Strategy Predicts Technology Satisfaction

SOCs that ingest all data into the SIEM score a technology satisfaction GPA of 2.76, compared to 2.14 for low-capability peers. The difference is not budget. It is intentionality in how data is collected and used before technology is procured.

Meaningful Work Outranks Money

Meaningful work and career progression are the top retention drivers for the third year running. Compensation has fallen to fourth place. SOC professionals stay for purpose and growth, and the organizations that understand this retain their best people.

SIEM and EDR Tell Two Different Stories

EDR earns the highest technology satisfaction rating of any tool. SIEM is the most sought-after skill in hiring, with nearly double the demand of EDR. SOCs are satisfied with their endpoint tools but structurally dependent on their SIEM—and struggling to staff it well.

The leadership perspective above reflects a curated view of the data. The full report that follows provides the complete picture; the survey results, trend analysis, and recommendations that inform it.

Introduction

Ten years of SANS SOC Survey data confirms what practitioners already sense. The SOC evolves deliberately, even as external disruption accelerates around it. This is the 10th year SANS has tracked security operations practice at scale, and three tensions now run through the data clearly enough to name at the outset.

1. **The adoption-integration gap—**AI has entered the SOC faster than any preceding technology, and 79% of respondents are already using it. But only 36% have integrated it into a defined workflow. The rest are using AI individually, without structure, governance, or systematic validation. That gap between adoption and integration is not a technology problem but an organizational one that creates a new category of operational risk: confident, well-formatted output that no one has the expertise to challenge.
2. **The management alignment gap—**The data on what retains SOC staff has been consistent, indicating that key factors such as meaningful work, career growth, and training, outrank compensation. Unfortunately, the data also shows that only about a third of practitioners feel management pays close attention to those needs. This prioritization problem compounds every staffing decision the SOC makes.
3. **The intent-action gap in technology strategy—**More respondents plan to migrate to cloud SOC architecture in the next 12 months than actually made the transition in the prior year. This pattern has held for three consecutive survey cycles. It suggests that announced strategic intent in security operations is a trailing indicator of friction, not a leading indicator of change. The same dynamic appears in data strategy where the SOCs that score highest on technology satisfaction are not the ones with the largest budgets. They are the ones that decided what they needed before they bought it.

The SOC does not resist change. It absorbs it slowly, on its own terms. Ten years of data confirms that has been true in every threat environment, through every technology wave, and across every organizational model this survey has captured.

Beyond those three tensions, the paper examines four additional themes:

- **Threat intelligence maturity—**80% of respondents incorporate CTI into operations, but the gap between operational use and strategic application remains wide. Intelligence drives tactics in most organizations. It rarely drives investment.
- **OT and IoT coverage—**Only 45% of respondents fully or partially monitor nontraditional computing assets through their SOC. As connected systems become a more common attack surface, that gap grows more consequential.
- **Metrics as a measurement problem—**Number of incidents handled has been the top reported SOC metric for 10 consecutive years. It measures volume, not value. The SOC cannot demonstrate business impact with a counter.
- **The executive perception gap—**Security executives and frontline practitioners describe the same organization and reach systematically different conclusions about how well it is managed. That divergence is examined in the Cyber Leaders section and runs through every staffing and funding finding in the primary survey.

These tensions are not new, but the context is. AI is the first external disruption significant enough to potentially resolve them by force rather than by deliberate organizational change. If AI tools mature faster than SOC governance does, the adoption-integration gap becomes a structural vulnerability. If AI reduces headcount demand before organizations have addressed the management alignment gap, the staffing problem does not go away but instead, shifts form. The data in this report establishes the baseline from which those outcomes will be measured.[1]

SOC Capabilities

SOC capabilities this year span a familiar and consistent set of functions. Alerting and triage remain nearly universal, reported by close to 100% of respondents (see Figure 2 on the next page). At the other end of the spectrum, purple team and red team activities, which require more specialized staff, are present in roughly 94% of SOCs. The six-percentage-point spread from the most to least common capability reflects a field where nearly all activities are considered standard requirements.

The narrowest gap between the most and least common SOC capability is just six percentage points. That near-uniformity means organizations are not choosing their capabilities strategically but instead they are adopting everything, and then figuring out what to do with it.

That uniformity has consequences. When capability adoption is effectively universal, the differentiator between SOCs is not *what* they do but *how well* they do it. Organizations that treat capability acquisition as a checklist risk investing in function, they lack the staff or process maturity to operate effectively. The question is not whether the SOC has a threat hunting capability. It is whether anyone is actually hunting.

[1] Survey demographics are located at the end of this report.

The most commonly outsourced functions remain consistent with prior years: penetration testing, digital forensics, threat intelligence, and 24/7 monitoring. The logic is straightforward. These activities require specialized expertise that is expensive to hire, train, and retain in-house for intermittent demand. Monitoring, in particular, is often transferred to a third party for off-hours coverage or as a first-line triage service that escalates to internal staff.

Outsourcing Patterns

Outsourcing in the SOC has not changed materially in a decade. The pen-test, forensics, threat intelligence, and monitoring portfolio remains the consistent set of externalized functions, with minor annual variation. This stability reflects both the economics of specialized expertise and the operational logic of transferring certain risk and coverage burdens to partners with scale.

Incident response (IR) structure varies across organizations: Some maintain a SOC-based response team, others use a phase-shift model where SOC and non-SOC staff transition into IR roles when needed, and others rely on a separate, independent response function. No single model is optimal across all circumstances. Resource availability and incident frequency determine the right approach for each organization.

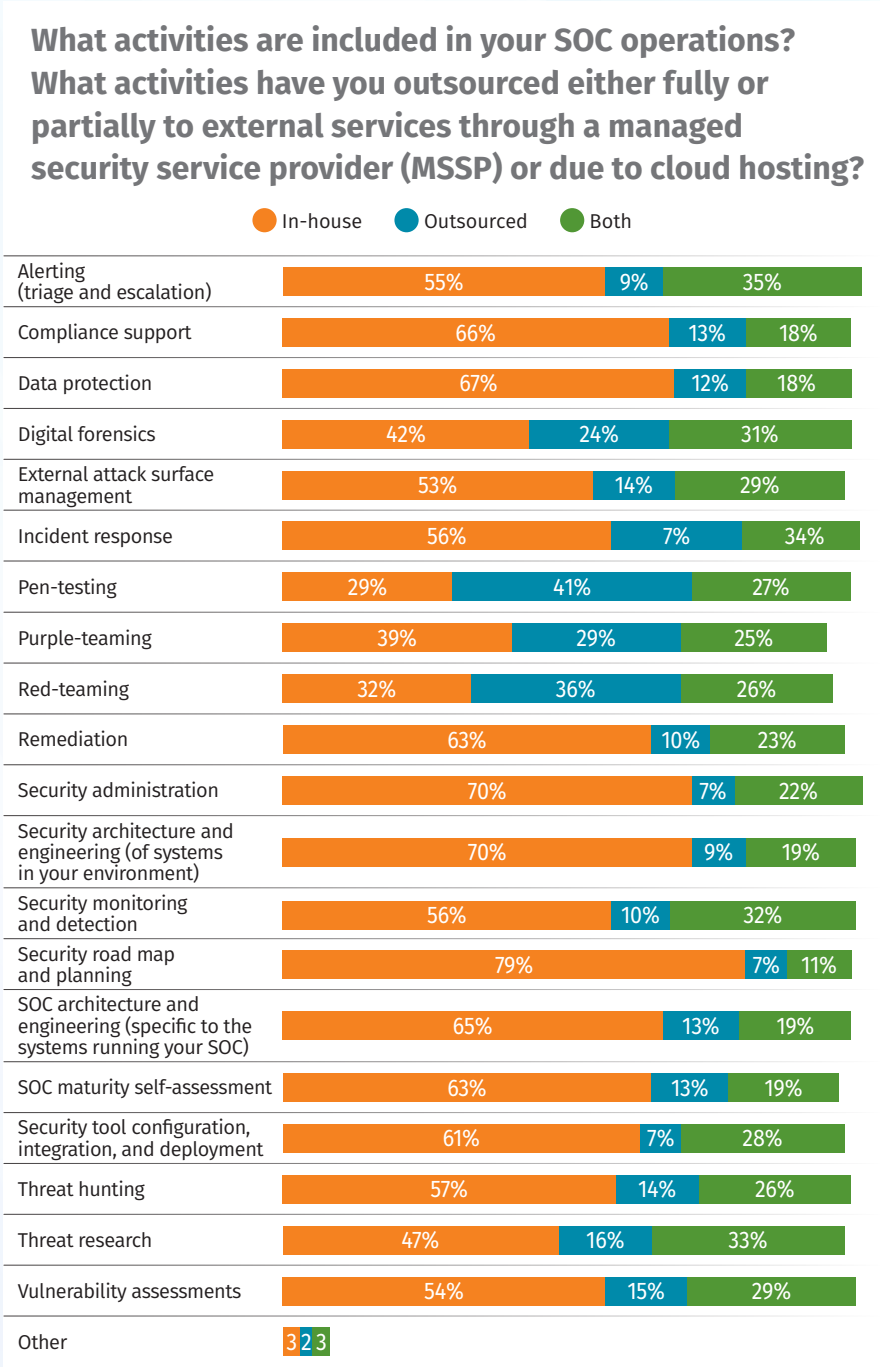


Figure 2. In-House and Outsourced SOC Activities

The stability of the outsourcing portfolio over a decade is worth examining critically. It may reflect genuine operational efficiency, with organizations correctly identifying the functions that benefit from external scale and expertise. It also may reflect inertia, with outsourcing decisions made years ago that have never been revisited as internal capabilities matured. Organizations that have not reviewed their outsourcing model in the past two years should. The threat landscape their current contracts were written against no longer exists.

Regardless of model, all organizations should maintain readiness to integrate external partners for complex or high-impact incidents. External counsel, cyber insurance providers, third-party forensics, MSSP support, and public communications teams all may be required when an incident scales.

Architecture and Infrastructure

The most common current architecture is a single, centralized SOC, followed by cloud-based SOC services and multiple follow the sun model 24 x 7 operations (see Figure 3). When respondents project forward 12 months, cloud-based SOC services rise to 34% and the single centralized SOC drops to 25%. This migration intent is notable but should be interpreted cautiously. Survey data from the past three years shows that more respondents anticipate moving to cloud than actually do so. The gap between planned and realized cloud adoption in SOC operations has remained persistent.

That persistence is not simply a technology adoption lag. It reflects real friction in organizations that have announced cloud migration as a strategic direction without resolving the underlying questions of data sovereignty, staffing for cloud-native tools, and integration with on-premises systems that are not going away. Organizations that have planned cloud migration for three consecutive years without executing it should treat that pattern as a signal that the blockers are organizational, not technical, and address them accordingly.

SOC-NOC integration continues to improve year-over-year, though slowly (see Figure 4). The most common response describes a relationship where the IT or NOC team plays a key role in detection and response without full integration. Fully integrated dashboards and shared workflows represent 24% of respondents. Full convergence of IT, cybersecurity, and physical security monitoring remains rare, and the data suggests it will stay that way for most organizations.

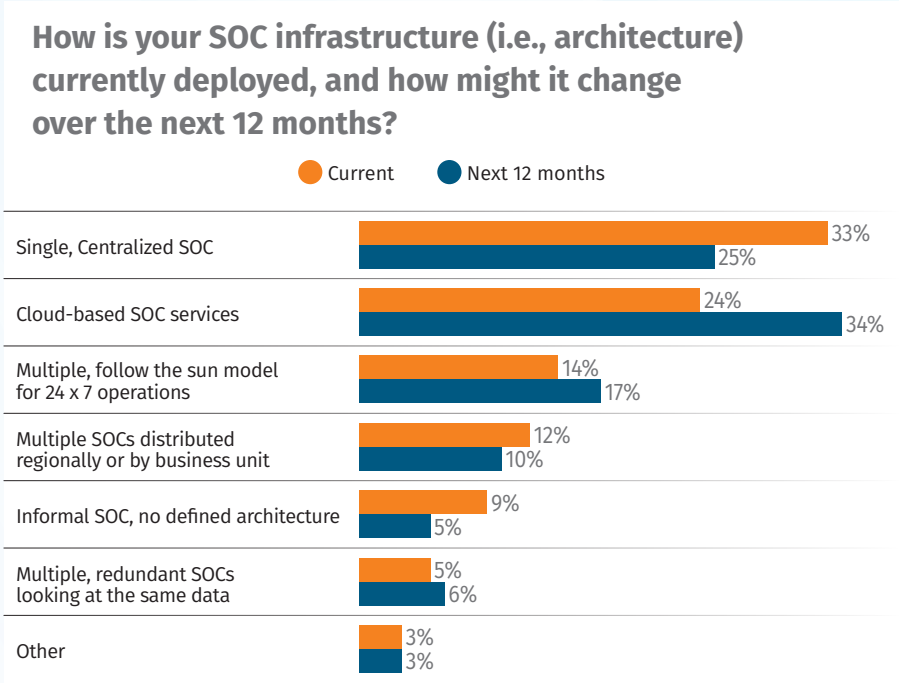


Figure 3. Current and Anticipated SOC Infrastructure

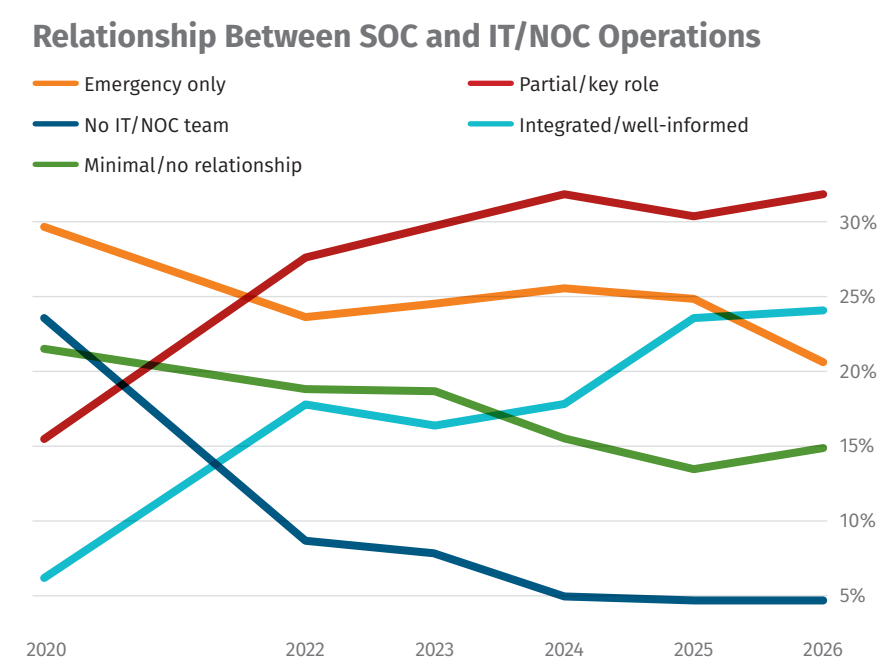


Figure 4. Year-over-Year SOC-NOC relationship

OT and IoT Coverage

Coverage of nontraditional computing assets, such as industrial control systems, smart sensors, building systems, and IoT devices, remains a meaningful gap. A small portion (16%) of respondents say their SOC fully supports all at-risk smart systems, and another third of respondents indicate partial coverage (see Figure 5).

For organizations that do monitor OT, the approaches vary. Some use entirely separate monitoring infrastructure staffed by the same team; others integrate OT telemetry into the IT SOC using shared resources. The right model depends on the organization's risk profile, the nature of its OT environment, and the maturity of its IT SOC, but the choice of model matters far less than the decision to make one.

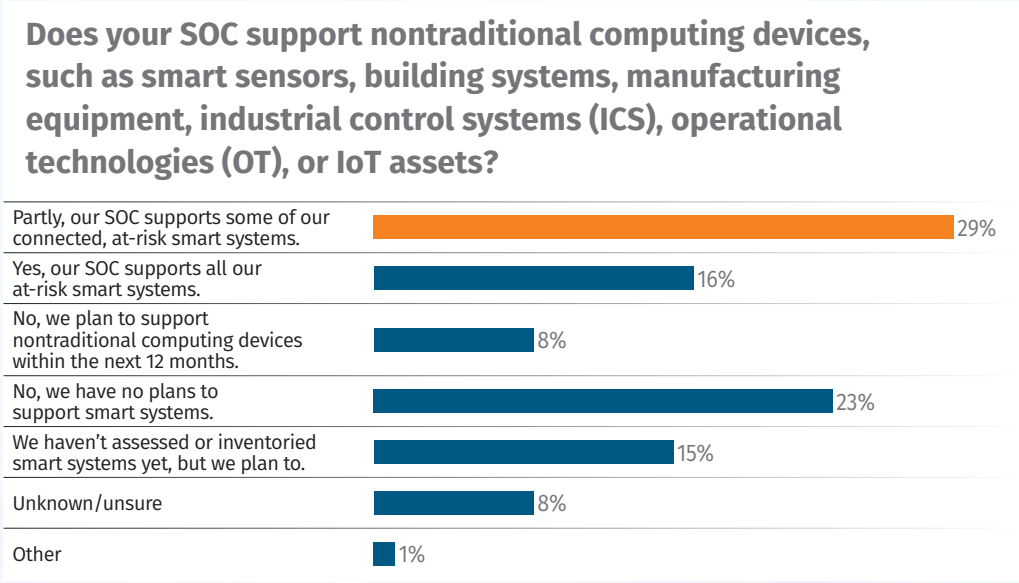


Figure 5. OT/IoT Coverage in the SOC

OT and IoT environments are now a primary attack surface. Ransomware operators, nation-state actors, and opportunistic attackers all have demonstrated the ability to move from IT networks into operational technology, disrupting physical processes, production systems, and critical infrastructure. Unlike a compromised workstation, a compromised industrial controller or building management system can have consequences that extend well beyond data loss. The SOC that cannot see its OT environment cannot detect that lateral movement, cannot measure its exposure, and cannot respond before the damage reaches systems where recovery is measured in days or weeks rather than hours. The 55% of organizations with no full OT coverage are not just missing telemetry. They are operating without visibility into the part of their environment where a breach is most likely to cause irreversible harm.

Threat Intelligence

Threat intelligence has completed its transition from emerging capability to SOC standard. The majority of respondents report that CTI activities are part of their SOC operations, continuing a multi-year increase. This reflects the maturation of vendor products, the widespread adoption of MITRE ATT&CK® as a common framework, and the normalization of intelligence sharing across the industry.

The top applications for CTI data are incident response (68%), threat hunting (61%), security operations and network defense (56%), and vulnerability management (50%). These are operational uses. Budget and spending prioritization, a more strategic application, is reported by only a small subset of organizations, suggesting that CTI has been deeply operationalized, but not yet fully integrated into investment planning.

That gap matters more than it might appear. CTI that informs daily operations but not annual budgets mean organizations are absorbing threat data without letting it change their resource decisions. The intelligence confirms what defenders are facing. The investment does not follow. That is a structural disconnection between what an organization knows and what it is willing to pay to address.

Threat Hunting

Threat hunting is active in most organizations, though the approach varies considerably. Vendor-provided tools are the dominant delivery mechanism in a partially automated model (see Figure 6).

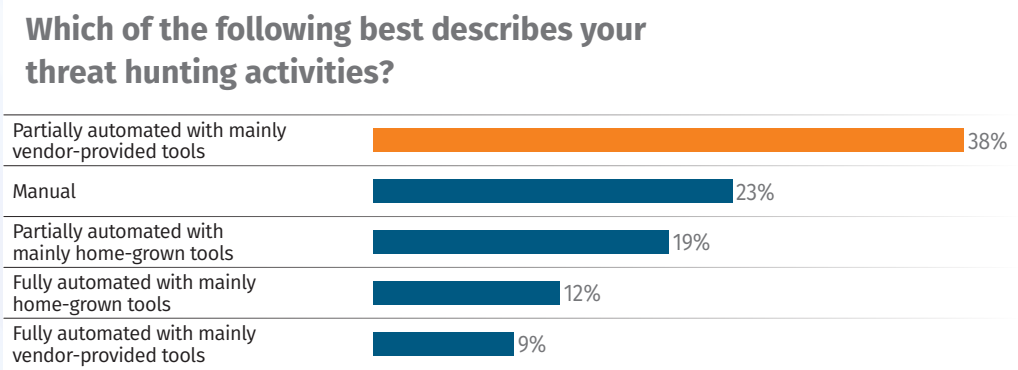


Figure 6. Threat Hunting Approach

Prioritization practices are split. The most common approach is formal prioritization based on SOC guidelines and available threat intelligence, reported by 22% of respondents. An additional 20% have analysts determine priorities independently, and 17% respond to emerging threat information on an ad hoc basis. About 16% do not prioritize hunts at all.

Hunting typically occurs across SIEM, EDR, and identity telemetry, with priorities set by recent campaigns, high-value asset designations, and identified detection gaps. The dependence on vendor-provided tools and the relatively informal prioritization structure in much of the field suggests that hunting is widespread but not yet systematically governed in most SOCs.

That matters because ungoverned hunting is not just inefficient, it is a missed opportunity. Threat hunting is one of the few SOC activities that is genuinely proactive. When it is ad hoc and individually driven, its findings rarely feed back into detection engineering, playbook updates, or coverage gap analysis in a systematic way. The value of a hunt that is not documented, reviewed, and acted on is limited to the analyst who ran it.

Artificial Intelligence in the SOC

AI has entered the SOC with a speed and impact that exceeds any prior technology adoption in security operations. The large majority of the respondents report using AI or ML tools but a much smaller portion of them (36%) have integrated these tools into a defined SOC workflow (see Figure 7).

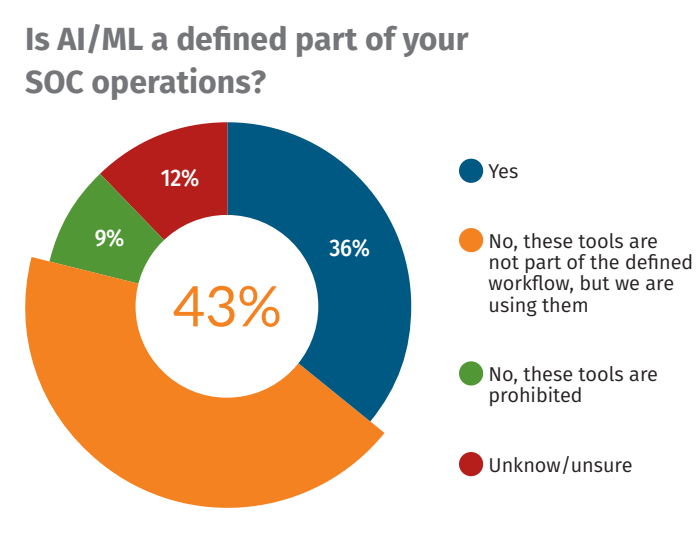


Figure 7. AI/ML Integration Status

The gap between use and integration is the defining AI story in this year's data. Analysts are reaching for AI tools individually, often without organizational structure around how they are used, validated, or governed. This is not surprising given how quickly the technology arrived. But it does represent a maturation gap that carries operational risk.

The dominant approach to AI tooling is using pre-existing vendor products without customization, cited by 38% of respondents. Another 31% customize existing tools, and 20% build their own AI or ML capabilities using frameworks such as PyTorch or TensorFlow. The build-your-own approach requires significant technical maturity and is not accessible to most SOC teams.

Guidance for AI Adoption

For organizations at early stages of AI integration, a use-modify-build progression provides a practical framework. Most SOCs should start by identifying vendor-provided AI tools that address documented capability gaps, deploy them operationally, and measure results against existing metrics. Once the obvious use cases are covered, organizations can explore customization and, where justified, purpose-built solutions.

The biggest AI risk in the SOC is not a bad tool. It is an analyst who trusts one.

The risk of an unstructured AI approach is not just inefficiency. Analysts who produce results they cannot validate represent a new kind of operational error. The SOC has always depended on expert human judgment to interpret what tools produce. As AI-generated outputs become more prevalent, the ability to verify and challenge those outputs becomes more important, not less.

AI is also reshaping the staffing conversation. The generalist analyst with strong AI skills is emerging as an anticipated role, though the transition is not yet reflected in current hiring data. Organizations that build AI governance structures and training programs now are likely to be better positioned when the transition accelerates.

Expert Corner

One of the findings that resonates most with me is the risk of analysts accepting AI-generated output without the skills, context, or confidence to challenge it. AI can absolutely help SOC teams move faster, especially as agentic capabilities become more common, but its value depends on analysts being able to validate what it produces. It does not replace core investigative skills; it builds on them.

VIEW PROFILE

Cristian-Mihai Vidu
SANS Certified Instructor;
Cyber Security Consultant

COURSES TAUGHT

SEC450:
SOC Analyst Training – Applied Skills for Cyber Defense Operations

Staffing, Hiring, and Retention

The staffing story in 2026 is not about numbers. It is about a persistent gap between what SOC leaders know and what their organizations do about it. Only 32% of respondents say management pays close attention to SOC hiring and retention needs. That figure has not moved meaningfully in a decade of this survey. The data on what retains skilled practitioners is public, consistent, and widely cited and the organizational response has been none of these.

This matters because the SOC cannot staff its way out of a management attention problem. Competitive compensation, recruiting investments, and onboarding programs are all downstream of a leadership structure that treats the SOC talent needs as a priority. 68% of respondents are working in organizations where that priority does not exist.

What Actually Retains People

Meaningful work is the top retention factor for the third consecutive year, followed by career progression and training (see Figure 8), and compensation has fallen to fourth place. Analysts stay when the work is challenging, when they can see a career path, and when their organization invests in their development. Organizations that cannot compete on compensation can still compete on all three of those factors. The ones that lead with salary increases while underinvesting in meaningful assignments and growth opportunities are solving the wrong problem.

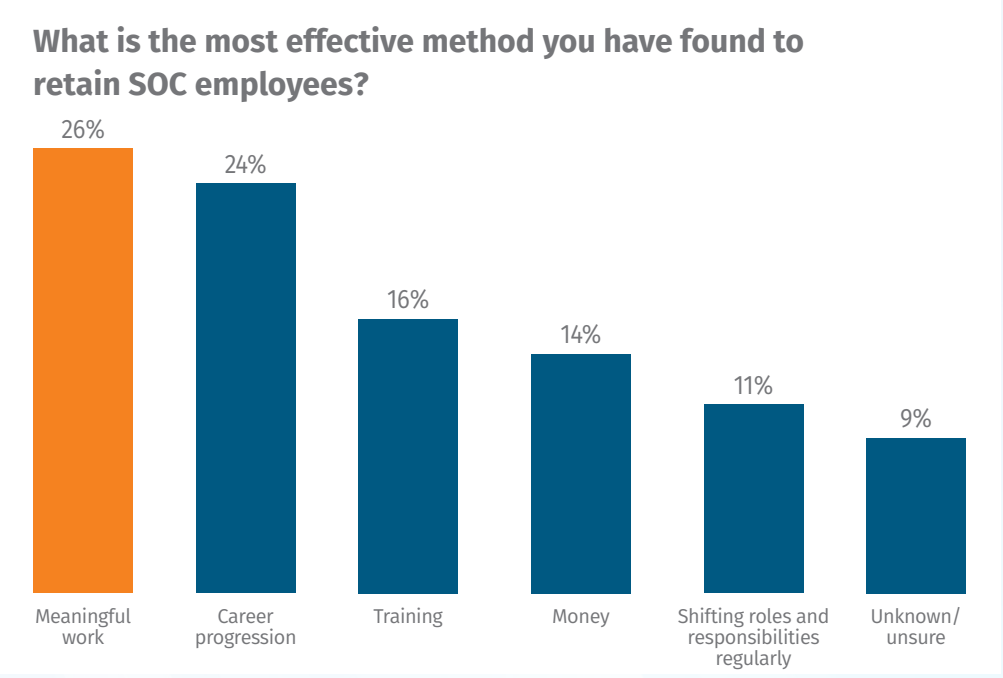


Figure 8. Employee Retention Methods

The Hiring Paradox

SIEM proficiency is the most requested technology skill in new hires. EDR is second and earns the highest technology satisfaction rating of any tool in the survey. SIEM does not.

SOCs are staffing for the tool they are most dependent on, not the tool that performs best. This is rational in the short term. A SIEM without skilled operators is a liability, but it reflects a resourcing posture oriented toward maintenance rather than improvement. Organizations that want to advance their detection capability need to ask whether their hiring priorities are pointed at where they are or where they want to be.

The retention answer has not changed in 10 years. Organizations still leading with salary increases are solving the wrong problem.

Technology and Tools

Technology satisfaction in the SOC is not evenly distributed, and the pattern of where it is high and where it is low tells a more useful story than any ranked list. The tools that earn the highest satisfaction scores are not always the most sophisticated or the most expensive. They are the ones SOCs have the staff, the process maturity, and the data discipline to operate well. Where satisfaction is lowest, the explanation is rarely about product quality. It is about the distance between what a tool requires to deliver value and what the team running it can consistently provide.

That gap has direct implications for how organizations should think about procurement, staffing, and data strategy together rather than in sequence. The sections below examine three dimensions of that relationship: how most SOCs discover threats and what that reveals about detection posture, why data strategy predicts technology satisfaction more reliably than budget does, and where the overall pattern of tool performance points for organizations trying to improve outcomes without simply adding to their stack.

How Incidents Are Found

Most SOCs find threats because something flagged them, not because someone went looking. Endpoint alerts (86%), automated SIEM alerts (78%), and user-reported issues (77%) dominate incident discovery (see Figure 9). Proactive threat hunting ranks lower at 63%. That gap is not a failure of current practice—reactive detection is necessary and the coverage is broad. But adversaries who know how to stay below the alerting threshold are exactly the ones that proactive hunting is designed to find. Organizations that rely entirely on passive triggers are defending against the threats they have already anticipated.

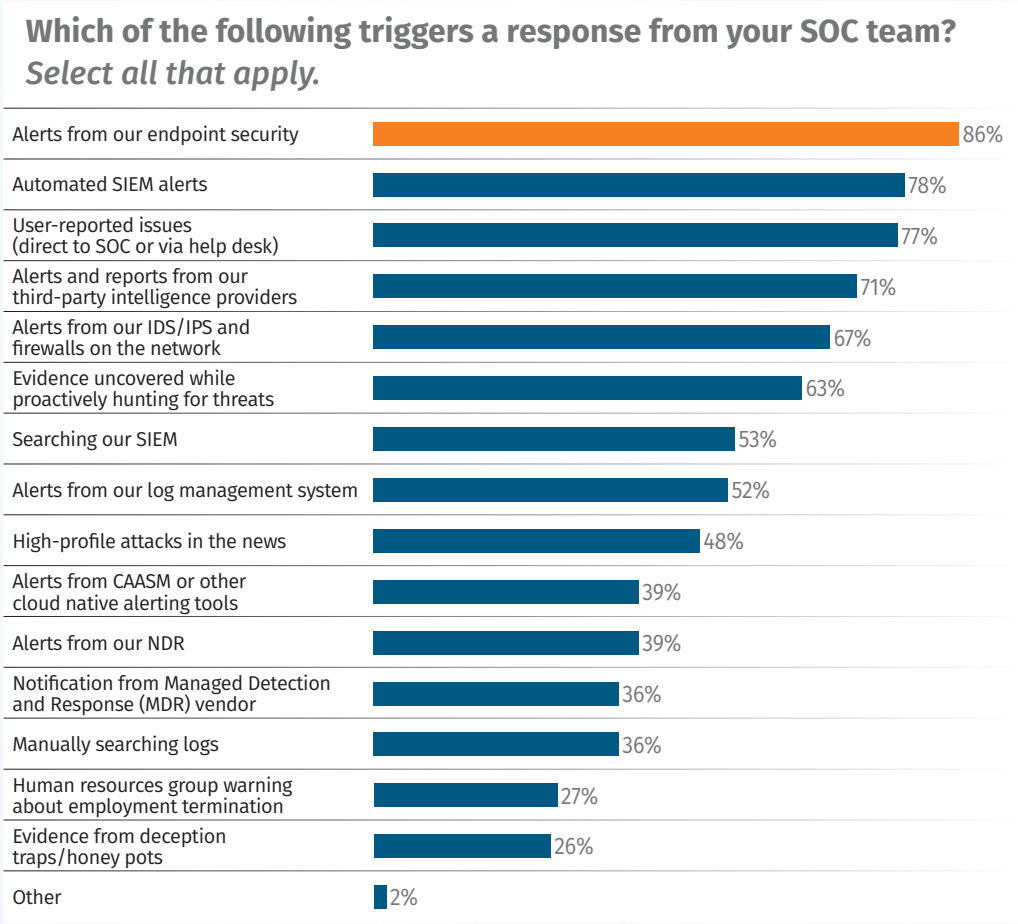


Figure 9. Top SOC Response Trigger

Data Strategy Is the Differentiator

The most important technology finding in this year's survey is not about a specific tool. It is about how the most capable teams approach technology differently from everyone else. The difference is not budget, and it is not the tools themselves. High-capability teams decide what they need before they buy. They use data to drive procurement and tune their environment against specific, documented problems. Lower-capability teams acquire tools and then determine their use. That sequence—buy first, justify later—produces lower satisfaction, lower value realization, and a technology stack that grows without improving.

Metrics and Reporting

Number of incidents handled has been the top reported SOC metric for 10 consecutive years, cited by 70% of respondents. It is also the top metric used to define SOC budget. That consistency is not evidence of measurement maturity. It is evidence of measurement inertia.

Incident counts measure how busy the SOC is. They say nothing about whether the right threats were caught, whether they were caught early enough, or whether they will recur. An organization that presents its board with a rising incident count cannot tell from that number alone whether its SOC is improving or whether the threat environment is getting worse. Both explanations fit the same data.

SOCs that want to demonstrate business impact need metrics that answer the questions leadership actually cares about. Time from detection to containment, thoroughness of eradication, and avoidability rate tell a more complete story than volume alone. The organizations that have not changed their primary metric in a decade should treat that consistency as a problem worth solving, not a baseline worth defending.

Conclusion

Ten years of tracking the same field through the same instrument leads to one honest conclusion. The three tensions named at the start of this report do not resolve in the data, they sharpen instead.

The adoption-integration gap is wider now than it was before AI arrived. SOCs have absorbed new technologies before: SIEM, EDR, SOAR. Each followed a similar arc from disruption to integration. But AI is moving faster, and the organizational structures for governing AI use, validating AI output, and building AI competency are not keeping pace with deployment. The risk is not that AI performs badly. The risk is that no one will know when it does.

The management alignment gap is as persistent as it has ever been. Cyber leaders, surveyed separately, believe they are responsive to SOC staffing needs. Practitioners do not experience it that way. That 27-point perception gap is not a communication problem that better reporting will fix. It is a structural misalignment between how security organizations are governed and what they actually require to function. The SOC has the data to make the case. What it lacks is the organizational standing to act on it.

Expert Corner

The greatest threat to a modern SOC is not the sophistication of the adversary—it is the quiet comfort of the dashboard that shows green. As AI-driven platforms consolidate alerts, correlate signals, and suppress noise with increasing confidence, we risk engineering ourselves into a dangerous paradox: The more automated our visibility becomes, the more invisible our blind spots grow. An AI model trained on known threat patterns will, by design, be most confident precisely where it is most deceived. And in security, misplaced confidence is not a feature, it is a vulnerability.

VIEW PROFILE

Nick Mitropoulos
SANS Certified Instructor;
Cybersecurity Consultant

COURSES TAUGHT

SEC555:
Detection Engineering and SIEM Analytics

The intent-action gap in technology strategy is the most tractable of the three, and the data points toward a clear answer. The SOCs that score highest on technology satisfaction are not defined by what tools they have. They are defined by how deliberately they chose them. Intentionality in data strategy predicts satisfaction more reliably than budget. That finding is replicable. It does not require more resources. It requires different decisions.

The overarching message of this 10th survey is not that the SOC is failing. It is that the SOC is absorbing a decade of external pressure with the same deliberate pace it has always used, and that pace is being tested. The next few years will determine whether the organizational structures that govern security operations can adapt quickly enough to match the speed of the technology they are being asked to manage. The data will follow.

De-identified response data and analysis notebooks will be available for download at soc-survey.com following the release of this report and webcast. Respondents and researchers are encouraged to submit their own analysis.

Survey Demographics

The 2026 SANS SOC Survey received 444 qualified responses from IT and security professionals actively working in monitoring or security operations roles. Figure 10 provides the demographic details. This survey was conducted in two parts. The first section, completed by all 444 respondents, covers SOC structure, operations, staffing, and technology. The second section, completed by approximately 150 respondents, covers technology deployment, satisfaction, metrics, and threat intelligence in greater depth. A parallel instrument completed by 69 CISOs and senior security executives is addressed in the Cyber Leader Perspectives section.

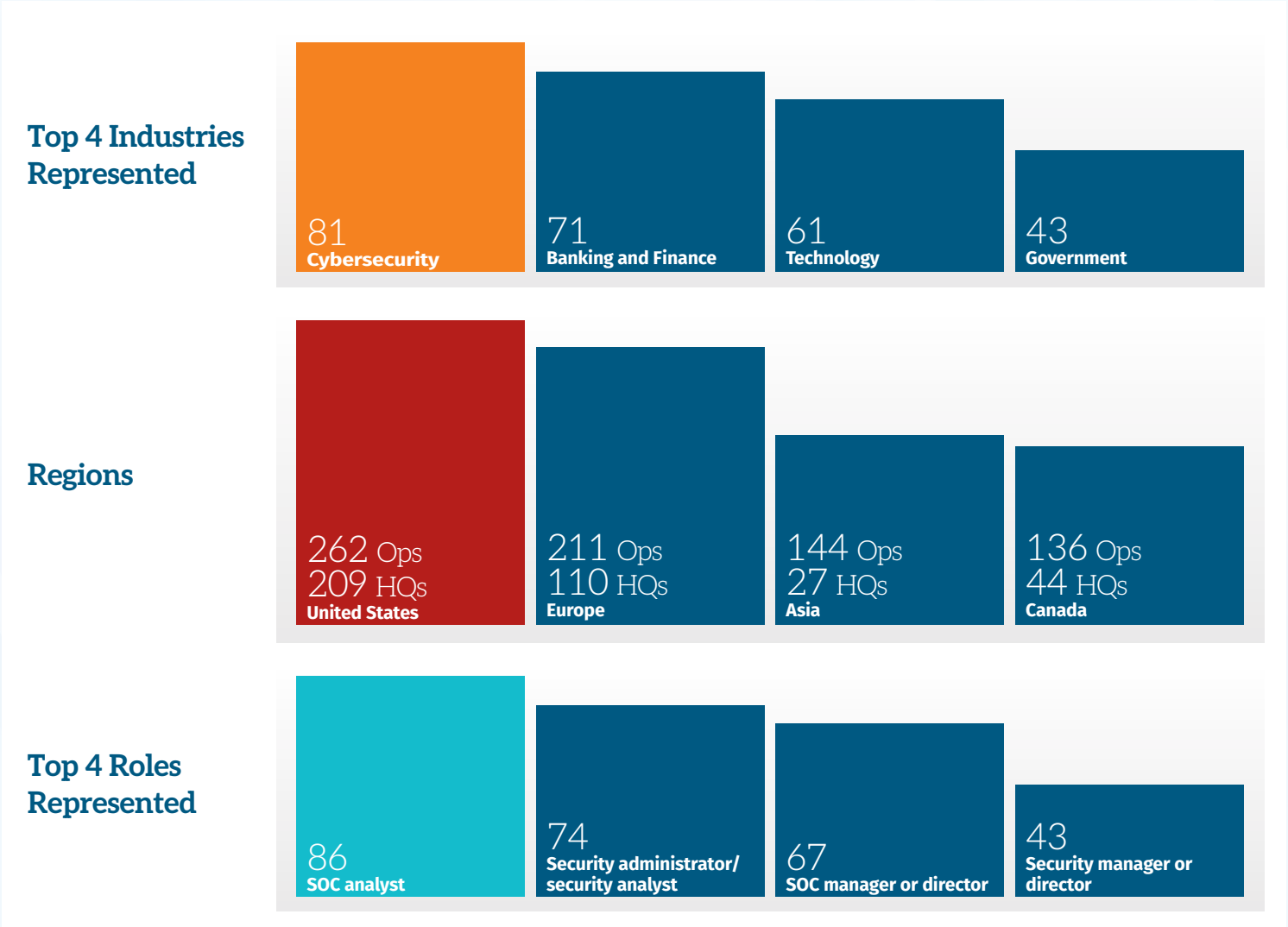


Figure 10. Demographics of Survey Respondents

Sponsor

SANS would like to thank this survey's sponsor:

HORIZON3.ai

SANS | Research Program

About the SANS Research Program

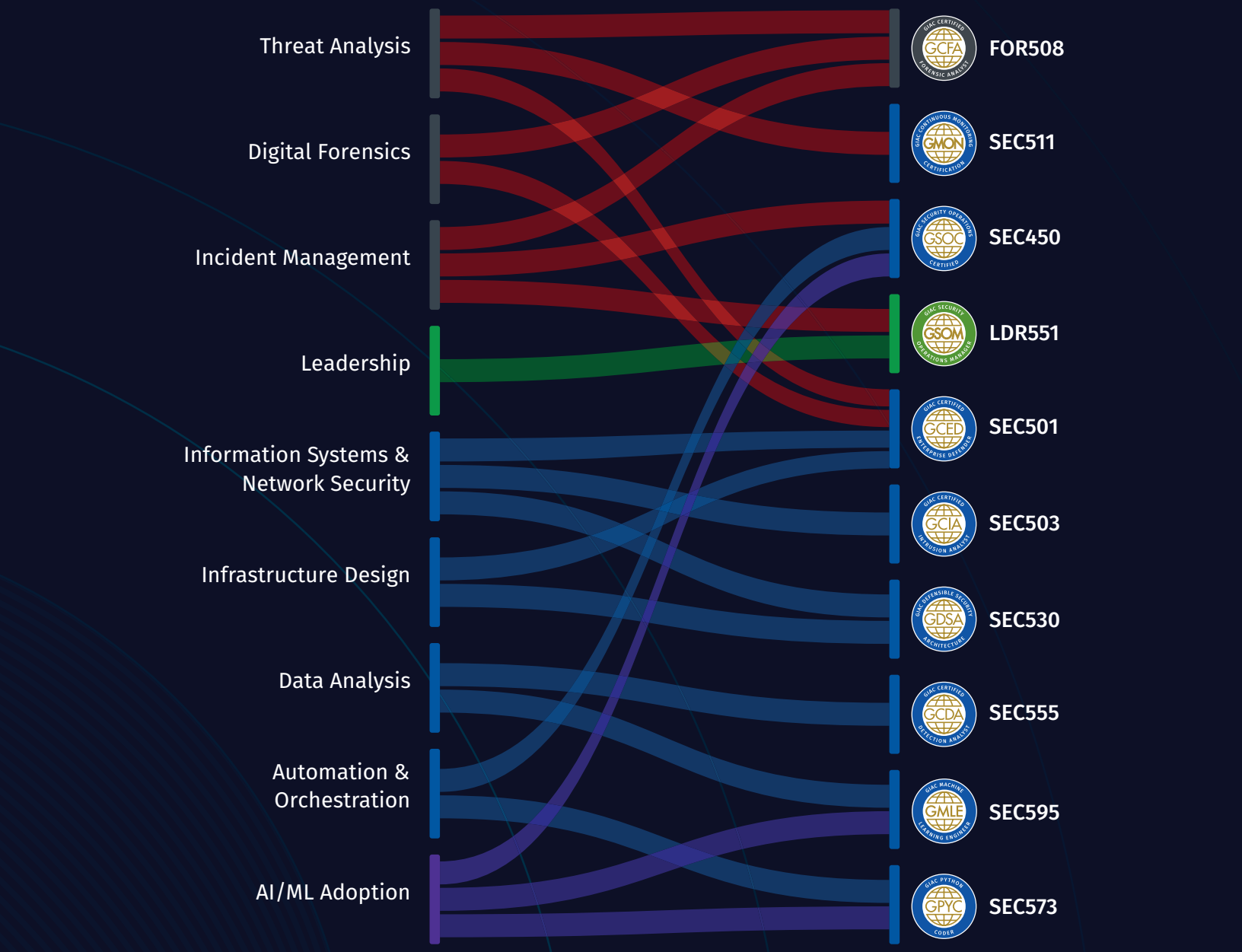
The SANS Research Program is a key initiative by the SANS Institute and a premier global provider of cybersecurity research and information. SANS Research Program is designed to provide cybersecurity practitioners and leaders with data-driven insights, thought leadership, and solutions that help them 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, content, and in-person or virtual events, email us at **Sponsorships@sans.org** or go to **www.sans.org/sponsorship**.

SANS | GIAC CERTIFICATIONS

The Skills Behind a Stronger SOC

Security operations teams are only as strong as the skills behind them. SANS offers purpose-built courses that close the most critical SOC skill gaps – from threat analysis and digital forensics to AI/ML adoption and automation. Monitor, detect, and respond with confidence.



sans.org/soc