SANS | Research Program

2025 SURVEY

SANS 2025 Detection and Response Survey: Unseen Threats Have Security Teams Rethinking Detection

Written by **Josh Lemon**
December 2025

STAMUS NETWORKS

©2025 SANS™ Institute

SANS 2025 STATE OF ICS/OT SECURITY SURVEY

Key Findings

Cloud complexity outpaces expertise.

Cloud detection continues to challenge defenders, with limited cloud security expertise and multicloud complexity as growing barriers. Despite broader adoption of cloud-native and third-party tools, many teams are still struggling to maintain visibility and cohesion across diverse environments.

False positives surge as a persistent pain point.

False positives remain the leading operational burden. This escalation suggests that while detection coverage has expanded, tuning and precision have not kept pace.

Budgets under strain despite rising demands.

Funding pressures are mounting, with budgets that are insufficient, while only very few enjoy surplus resources. Teams are being asked to deliver more capability with less investment, revealing a widening gap between operational expectations and the resources provided to meet them.

Automation is on the rise.

More organizations are automating detection and response workflows to offset staffing shortages and accelerate incident handling, though many still struggle to integrate tools effectively.

Skill and resource gaps persist.

Despite technology advances, teams continue to face constraints around staffing, expertise, and budget, limiting their ability to fully operationalize modern tools.

AI moves from experimentation to execution.

Plans to expand AI and machine learning (ML) surged, marking a decisive shift from proof-of-concept to production use. Automated threat hunting and predictive analytics now form the next frontier of detection, signaling a maturing confidence in AI's role across security operations.

Future outlook is cautious but innovative.

Budgets are growing modestly, but investment in AI-driven threat hunting, predictive analytics, and orchestration signals a strategic push toward more adaptive, resilient security operations.

Survey Author

VIEW PROFILE

Josh Lemon
SANS Principal Instructor

CURRENTLY TEACHING

FOR508: Advanced Incident Response, Threat Hunting, and Digital Forensics

FOR509: Enterprise Cloud Forensics and Incident Response

FOR572: Advanced Network Forensics: Threat Hunting, Analysis, and Incident Response

Josh Lemon is the Chief of Digital Forensics and Incident Response at SoteriaSec, with more than two decades of experience leading complex security investigations for multinational organizations, government agencies, law enforcement, law firms, and local businesses. He specializes in helping organizations detect, investigate, and eradicate cybercriminals and targeted threat actors from their networks, and is frequently called upon to provide expert witness testimony for legal cases involving breaches and incident response. Josh serves as a Principal Instructor for SANS Institute's "FOR508: Advanced Incident Response, Threat Hunting, and Digital Forensics," "FOR509: Enterprise Cloud Forensics and Incident Response," and "FOR572: Advanced Network Forensics: Threat Hunting, Analysis, and Incident Response" courses.

Introduction

The 2025 Detection and Response Survey provides an in-depth look at how organizations across industries are evolving their cybersecurity operations in the face of mounting complexity, resource constraints, and an increasingly sophisticated threat landscape. Building on prior years' insights, this year's results capture perspectives from a globally distributed respondent base spanning banking and finance, technology, cybersecurity, government, healthcare, manufacturing, and other sectors. The diversity of participation underscores that while some industries—particularly those with mature security programs—set operational benchmarks, every sector brings valuable lessons shaped by its unique challenges. As organizations continue to modernize their detection and response capabilities, the findings highlight a growing emphasis on automation, integration, and measurable performance, balanced by an ongoing reliance on skilled human judgment.

Across the data, clear trends emerged: Endpoint detection and response (EDR) tools remain foundational, machine learning (ML) adoption is steady but maturing, and automation continues to expand across both detection and response workflows. Yet, despite these advances, many teams still grapple with familiar barriers such as false positives, limited budgets, and the persistent shortage of skilled personnel.

The survey also reveals how organizations are rethinking team structures, investing in training, and refining metrics to better communicate effectiveness and business impact. Looking ahead, respondents express cautious optimism. Budget growth is expected to be moderate, but innovation in AI-driven threat hunting, predictive analytics, and automated workflows is accelerating. Together, these insights paint a picture of an industry in transition—one that is learning to blend human expertise, machine intelligence, and structured processes to build faster, more resilient security operations for the challenges of 2025 and beyond.

Respondent Demographics

The 2025 survey was led by respondents from banking and finance (17%), technology (17%), and cybersecurity (17%), together representing just over half of all participants. These industries continue to set the pace for detection and response maturity, driven by regulatory scrutiny and constant exposure to advanced threats. Government (10%) and healthcare (8%) followed, with other sectors such as manufacturing, education, and telecommunications contributing valuable perspectives shaped by budget and infrastructure challenges.

Geographically, 46% of respondents are headquartered in the United States, though two-thirds operate there, reflecting the country's central role in global security operations. Europe and Latin America also feature prominently, at 44% and 40% respectively, reinforcing that detection and response have become global, around-the-clock disciplines that must adapt to varied environments and regulatory landscapes (see Figure 1).

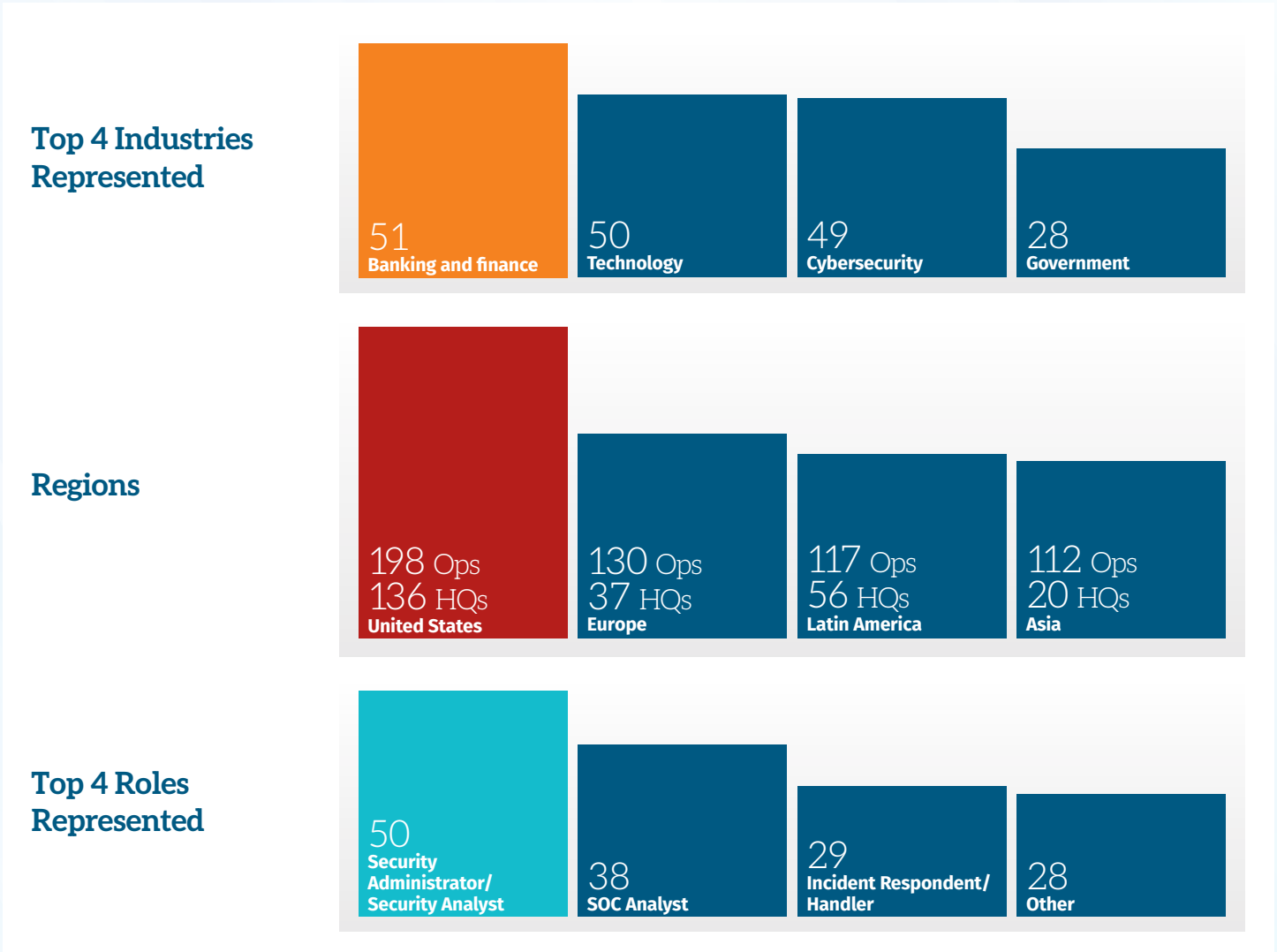

Figure 1. Demographics

Detection

X/EDR solutions once again led the pack, with 43% of respondents rating them as extremely effective and another 46% finding them effective, reinforcing that endpoint visibility remains the cornerstone of modern detection programs. This makes sense because, after all, threat actors must ultimately operate on endpoints to achieve their objectives, whether through lateral movement, credential theft, or data exfiltration.

IDS/IPS and behavior-based analysis tools are still widely seen as effective, though their effectiveness ratings are noticeably lower, suggesting they are now considered foundational but insufficient on their own. AI- and ML-based tools continue to struggle to inspire confidence, with only 16% finding them extremely effective and a relatively high 13% labeling them ineffective, which indicates that while organizations are experimenting with these capabilities, they are still refining their place in operational detection strategies (see Figure 2).

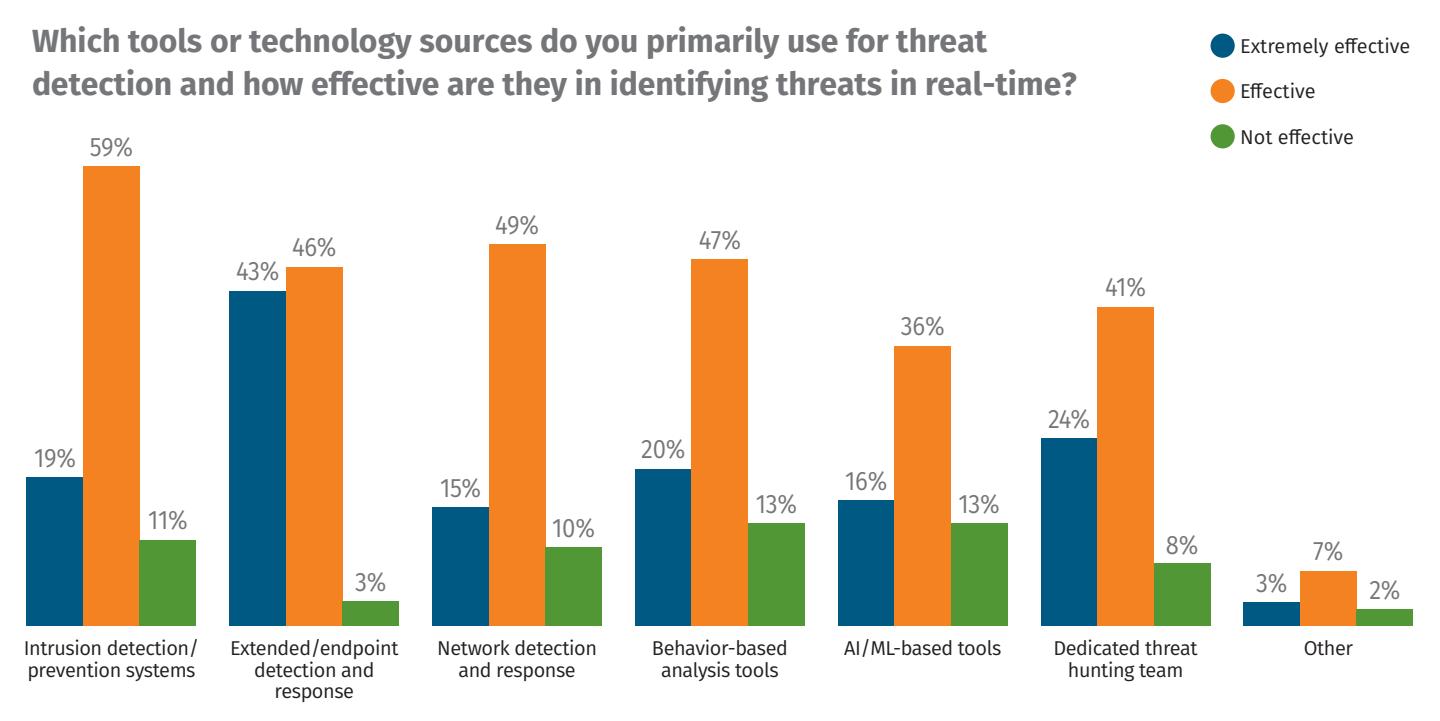

Figure 2. Tools and Technologies in Use and Effectiveness in Threat Identification

Machine Learning

Just over half of respondents (53%) reported using ML algorithms for threat detection in 2025, a slight increase from 51% in 2024, showing that adoption continues to grow but has not surged dramatically. The most notable change in perceived value is that 39% now rate ML as "very useful," a significant jump from 22% last year, suggesting that organizations are gaining confidence as models mature and tuning improves. About a third still consider ML only moderately useful, and nearly 17% remain unsure whether their organization even uses it, highlighting the ongoing challenge of transparency and explainability in these systems. Taken together, the data suggest that ML is finding its footing as a dependable part of detection pipelines, but there is still work to be done before it is seen as transformative across the board (see Figure 3).

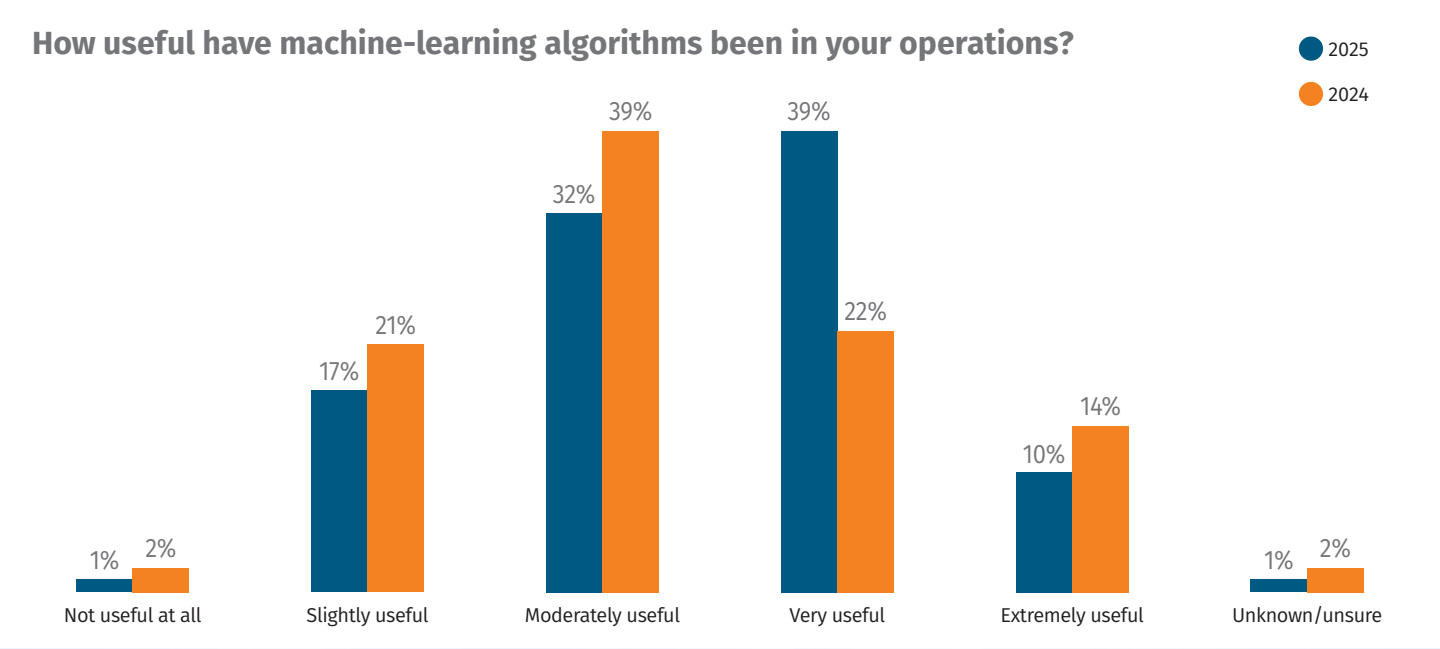

Figure 3. ML Algorithm Usefulness

Automation

Automated tools continued to dominate threat detection in 2025, with nearly 90% of respondents relying on them, up from 87% last year, cementing their role as the backbone of modern SOC operations (see Figure 4). Adoption rises with organization size, reaching near-universal use among enterprises with over 15,000 staff. AI and ML also have gained momentum, now used by 45% of organizations, up from 39% in 2024, signaling a move from experimentation to operational integration. Manual monitoring remains relevant at 63%, indicating that while automation drives efficiency, human analysis remains vital for interpreting complex or context-driven threats.

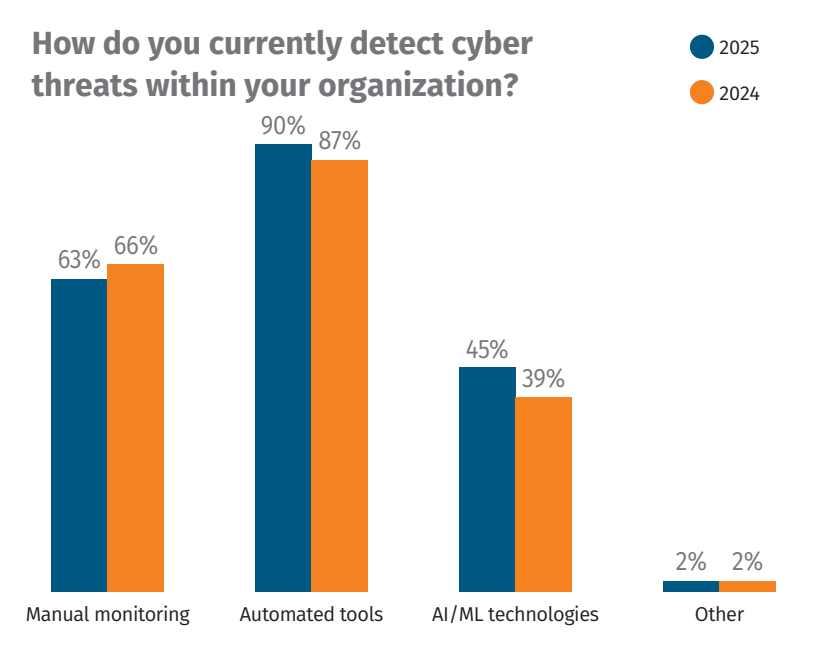

Figure 4. Current Cyber Threat Detection Trends

Detection Rules

In 2025, 37% of respondents reported sharing detection rules or indicators with other entities, a slight decrease from 39% in 2024 (see Figure 5). Nearly half still do not share externally, reflecting continued hesitation around legal, operational, or resource challenges. Another 13% remain unsure whether sharing occurs at all, underscoring that although collaboration is valued in theory, consistent and practical intelligence exchange remains limited across many organizations.

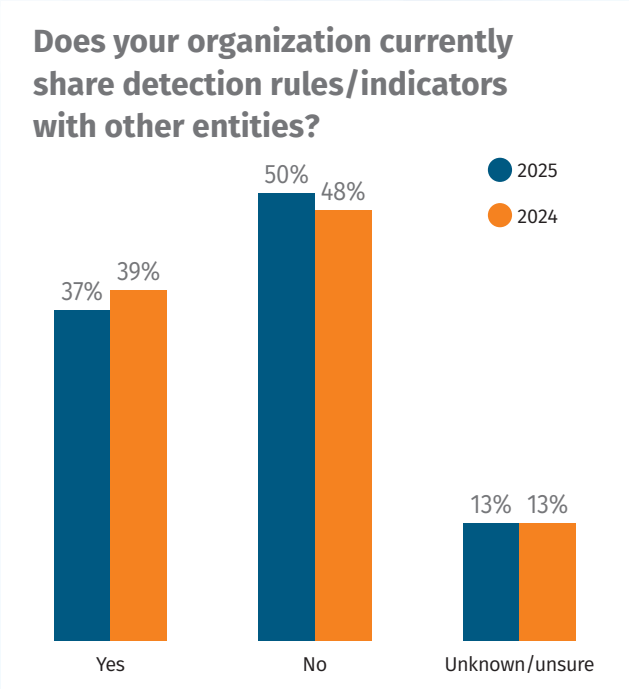

Figure 5. Detection Rule Sharing

Among organizations that share data, 85% cite improving overall security posture as their main motivation, up sharply from 65% last year (see Figure 6). Reciprocity remains important at 72%, reflecting a continued belief in mutual benefit through shared intelligence. Community contribution (59%) and business partnerships (44%) also play key roles, indicating that collaboration is viewed not just as compliance, but as a collective effort to strengthen the wider security ecosystem.

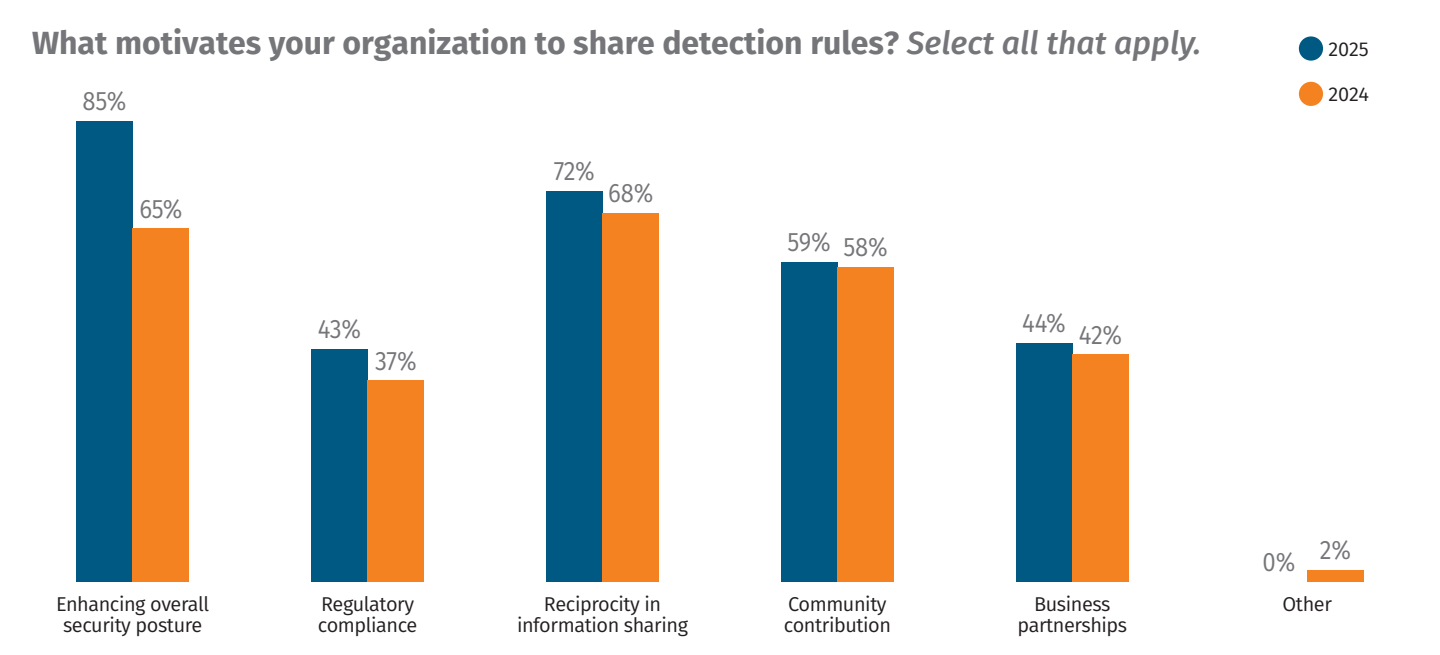

Figure 6. Drivers for Sharing Detection Rules

Most sharing still occurs internally, with 34% of organizations exchanging detection rules daily through internal teams or collaboration tools, underscoring the value of rapid knowledge flow within SOCs. Industry-specific threat intelligence platforms also see regular use, with just over 20% sharing daily or weekly. In contrast, exchanges with government agencies and vendors are largely ad hoc, 32% and 26% respectively, suggesting these relationships are primarily activated during major incidents rather than routine operations.

Security vendors remain the leading source for detection rules in 2025, selected by 73% of respondents, up from 59% last year, reflecting growing trust in vendor-provided detections and their ability to scale coverage quickly. Open source communities also rose to 56%, underscoring the continued role of community-driven intelligence in identifying emerging threats early.

Cloud Detection

Third-party security solutions stood out in 2025, with 20% of respondents rating them as "extremely effective," up from 17% last year, while "not effective" responses dropped to 11% (see Figure 7). This improvement shows growing confidence in specialized vendors that bridge visibility gaps across complex cloud environments. Cloud-native tools remain widely used, with 57% rating them effective, though their top-tier effectiveness score dipped slightly to 20%, suggesting performance is steady but no longer improving at the same pace. In contrast, in-house tools have fallen sharply, with "extremely effective" ratings down to 14% from 19% and "effective" responses dropping to 37% from 59%. The findings suggest that organizations are moving away from resource-heavy, homegrown solutions and leaning more on scalable, vendor-supported cloud and third-party tools.

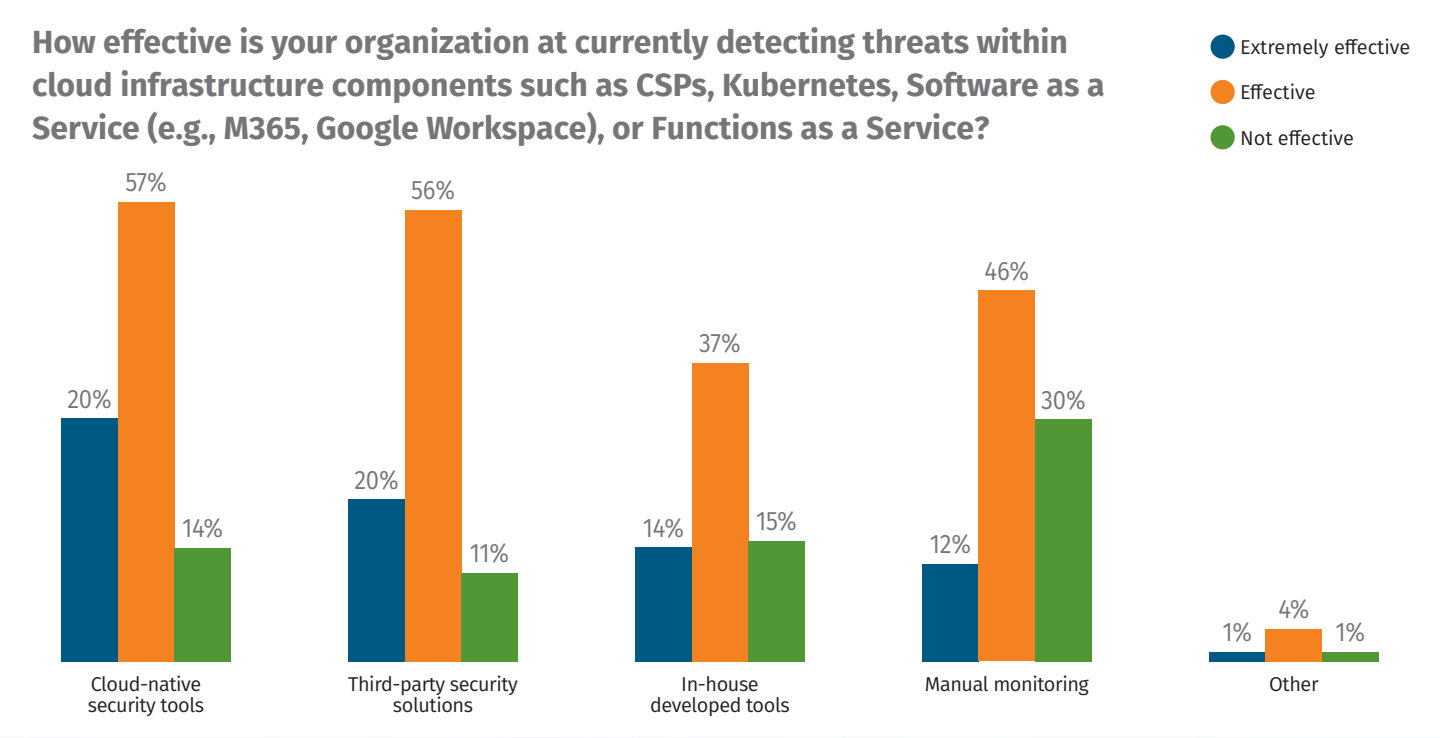

Figure 7. Threat Detection Effectiveness

Response

EDR remained the dominant tool for threat response in 2025, with 89% of respondents using it, a slight increase from 82% last year, highlighting its role as the backbone of post-detection investigation and containment (see Figure 8). SOAR platforms are slowly gaining traction, with 62% of respondents now using them, indicating their adoption is very slow-moving from year to year. Network detection and response (NDR) usage has dipped slightly to 44%, perhaps as more response actions shift to the endpoint layer. NDR technology may be becoming more challenging to implement as organizations move to a work-from-home culture, leaving NDR more useful for production environments or cloud environments.

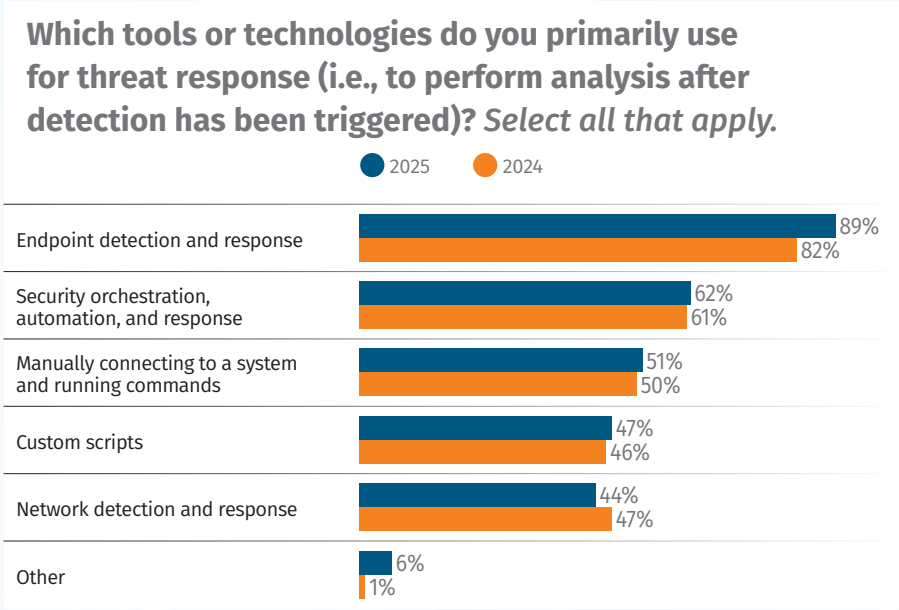

Figure 8. Threat Response Tools

Most organizations still respond to confirmed threats within minutes (40%), but this year's data shows a shift toward slower reaction times (see Figure 9). Those responding within hours rose to 38% from 33%, while near-instant responses dropped to just 3% from 8%. This measure reflects the time between detection and response (not attacker dwell time), and the change likely points to growing incident complexity, where teams must validate and scope issues carefully before acting, particularly in cloud environments.

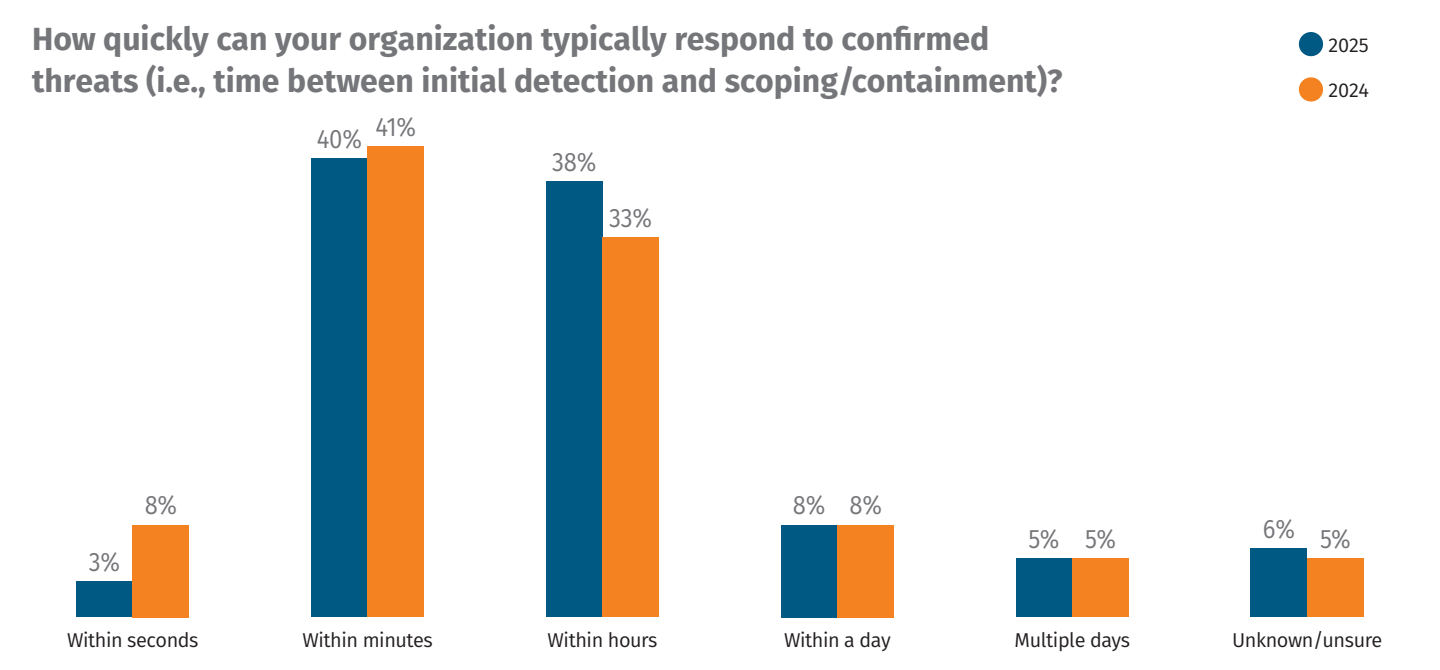

Figure 9. Threat Response Times

Partial automation remained the norm in 2025, with 66% of organizations using at least some automated response, up slightly from 64% last year (see Figure 10). Full automation has slipped to 13% from 16%, likely reflecting ongoing caution around false positives and business impact. About 15% still rely entirely on manual response, a figure largely driven by smaller organizations. In contrast, full automation is most common among large enterprises, where 24% or more report fully integrated automated response mechanisms.

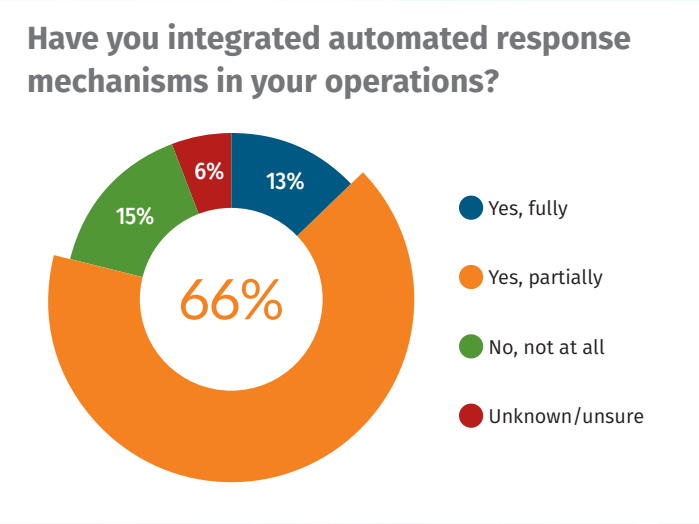

Figure 10. Automated Response Integration

Predefined playbooks remained the leading method for automating detection-to-response workflows, adopted by 76% of organizations, up from 74% last year. Custom scripts declined to 61%, suggesting a gradual move toward standardized, lower-maintenance solutions. Integration with SOAR tools also fell to 57%, suggesting a more selective approach as teams refine automation strategies. ML continues its steady rise, now used by 36%, showing that while AI is gaining ground, most still rely on structured, rule-based automation as the operational backbone.

When asked what factors most influence incident prioritization, respondents overwhelmingly pointed to business risk, with 47% ranking potential business impact as their top consideration and another 30% ranking it second. Severity of the threat closely followed, taking the highest priority for 37% of respondents and second for 34%. Resource availability, litigation, and regulatory impact were much less likely to drive first-line prioritization, with over half of respondents ranking legal considerations near the bottom of the list.

Detection and Response Team Structure

This year, most organizations (53%) reported that detection and response functions are now integrated within a single team, up from 48% last year (see Figure 11). The move toward unified structures reflects a push for faster coordination and reduced handoff delays during incidents. Separate teams have declined to 44%, although they remain common among the largest enterprises (those with over 100,000 employees), where scale demands more distributed responsibilities. Overall, the shift suggests growing confidence in integrated operational models that streamline the detection-to-containment process.

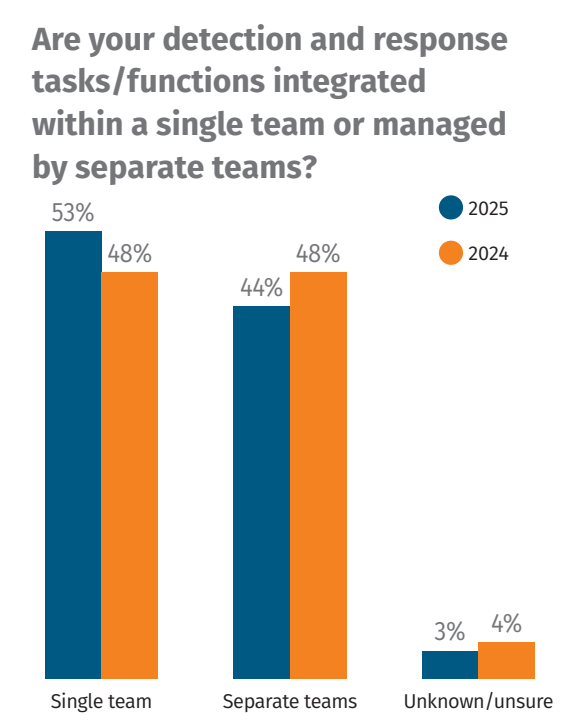

Figure 11. Integration of Detection and Response Tasks/Functions

Training and Skill Development

Training remains the leading approach to closing skill gaps, with 78% of organizations investing in structured programs to build internal expertise rather than relying solely on external hiring (see Figure 12). Recruitment still plays a key role at 57%, but many are shifting focus toward developing existing talent. Outsourcing, used by 42% of respondents and 61% of large enterprises, continues to supplement internal capacity, particularly during major incidents. Internal rotations, selected by 29%, highlight a growing emphasis on cross-training and strengthening team resilience.

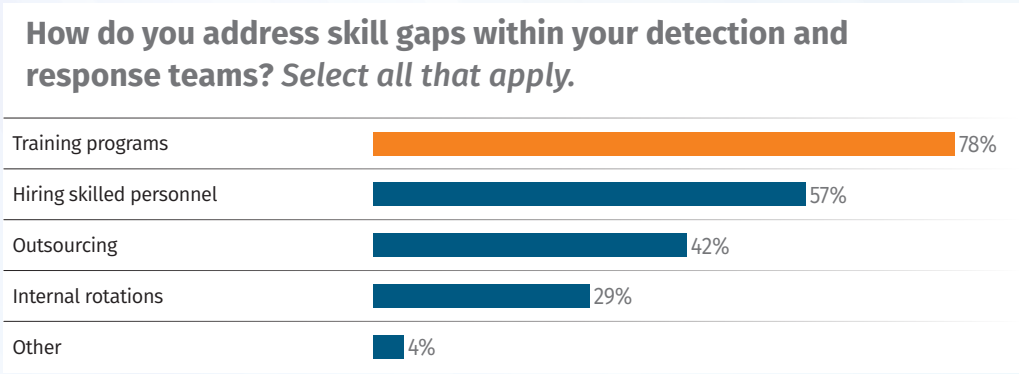

Figure 12. Addressing Skill Gaps in Detection and Response

On-the-job training remains the top development focus for detection and response teams in 2025, with 75% of respondents prioritizing it, followed closely by certification programs at 72% (see Figure 13). Regular workshops have grown to 53%, reflecting greater emphasis on hands-on learning, while conference attendance holds steady at 50%. The trend suggests a shift toward continuous, practical training that strengthens day-to-day operational skills within security teams.

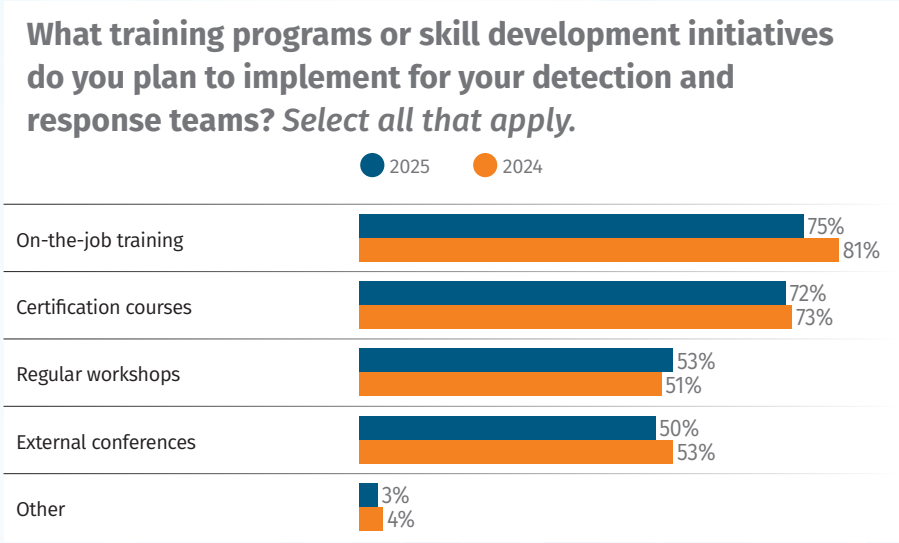

Figure 13. Training Options for Detection and Response Skills

Budget and Resource Allocation

Budget sentiment in 2025 reflected mounting strain on detection and response teams, with 28% of respondents describing their funding as "insufficient," up from 22% in 2024 (see Figure 14). Smaller organizations and those with 10,000 to 15,000 staff report the highest shortfalls at 52% and 53%, respectively. "Adequate but limited" budgets fell to 38%, while fully "sufficient" funding remains steady at 25% and "more than sufficient" dropped to 3%. The data underscores a growing resource divide, where many teams are being asked to do more with less amid an increasingly complex threat landscape.

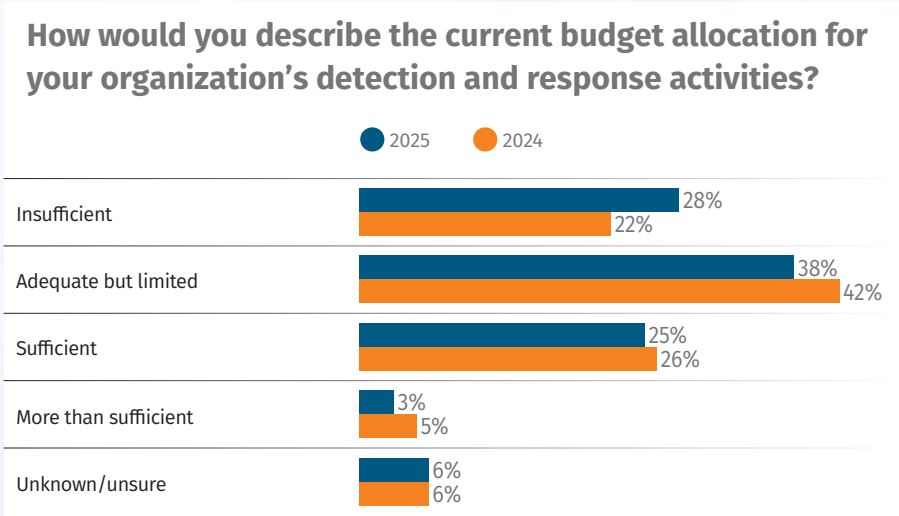

Figure 14. Budget Allocation for Detection and Response

Future budget outlooks for detection and response remained cautiously optimistic in 2025, with 44% of respondents expecting a moderate increase in funding, up slightly from 42% in 2024 (see Figure 15). However, only 5% anticipate a significant increase, continuing a downward trend from 7% last year, suggesting that most organizations are pursuing steady, incremental growth rather than dramatic investment. Overall, the data suggests that while funding will hopefully trend upward, most organizations are planning for gradual enhancements rather than transformative spending increases. The only challenge with these plans—based on current budget allocation data—is that detection and response teams will remain under-resourced for another year.

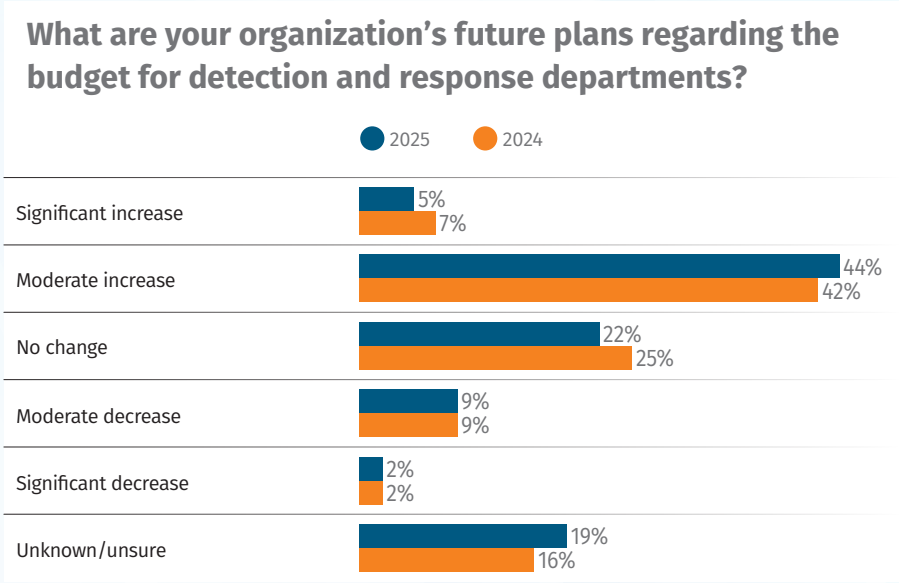

Figure 15. Future Budget Plans for Detection and Response

Metrics and Performance Evaluation

Organizations are clearly leaning into quantitative measurement of their detection and response performance, with 64% tracking the number of incidents detected and 62% measuring mean time to respond (MTTR), although the latter has dropped slightly from 67% in 2024 (see Figure 16). Mean time to detect (MTTD) rose to 56% from 52%. This is a positive sign, as the goal should be that the time to detect a threat actor gets shorter as you become more efficient as a team. False positive rate and mean time to closure (MTTC) both increased to 43% and 41% respectively, reflecting a growing interest in measuring efficiency and precision, not just volume and velocity. Organizations with 5,000 employees or fewer were our predominant respondents who said they did not conduct any KPI tracking. This is not entirely unexpected and may result from a lack of resources and time for smaller teams. However, I caution readers in small organizations that don't track metrics. These metrics help communicate to leadership teams when additional resources or funding are needed.

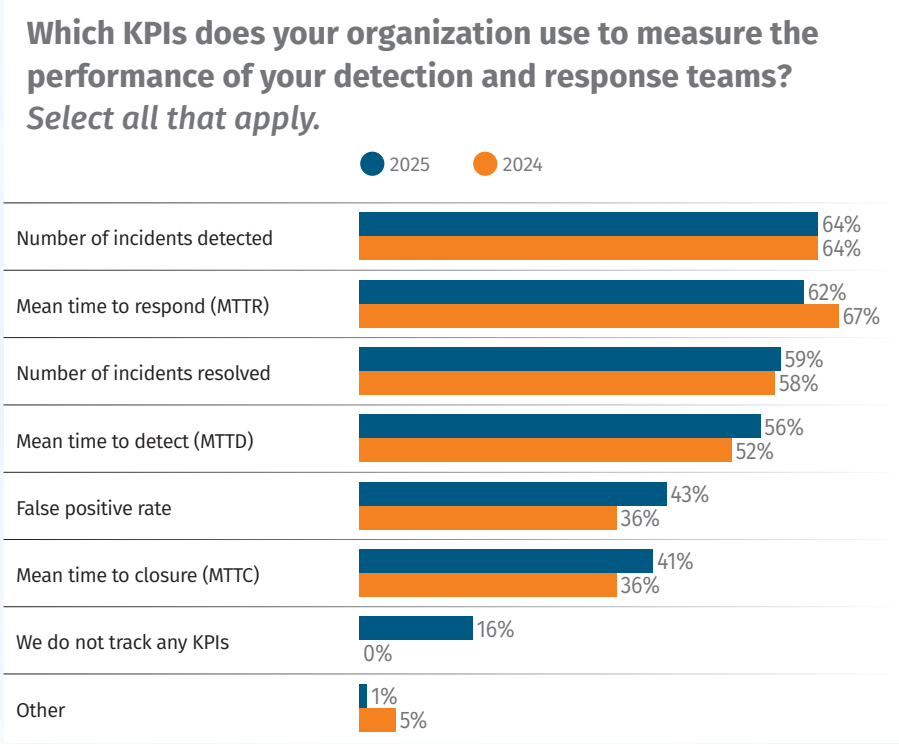

Figure 16. KPIs Used to Track Detection and Response Performance

Among the 57% of respondents who actively assess their detection coverage, the MITRE ATT&CK® Matrix remains the most widely used approach, with 78% leveraging it, up from 74% in 2024, highlighting its role as the de facto framework for mapping and validating detection capabilities. Threat intelligence reports follow closely at 75%, showing that many teams continue to align their coverage with the latest adversary behaviors and campaigns. Overall, the results point to a maturing approach in which security teams use structured frameworks and intelligence-driven methods to ensure their detection programs remain current and comprehensive. The other thing we need to see now is more than 57% of organizations assessing detection coverage.

Only 17% of organizations reported regularly benchmarking their detection and response metrics against industry standards (see Figure 17), a decline from 23% in 2024, suggesting that while measurement of internal coverage is improving, external comparison remains less common. Encouragingly, 24% of respondents say they plan to begin benchmarking, up from 18% last year, suggesting growing recognition of the value of understanding performance in a broader industry context.

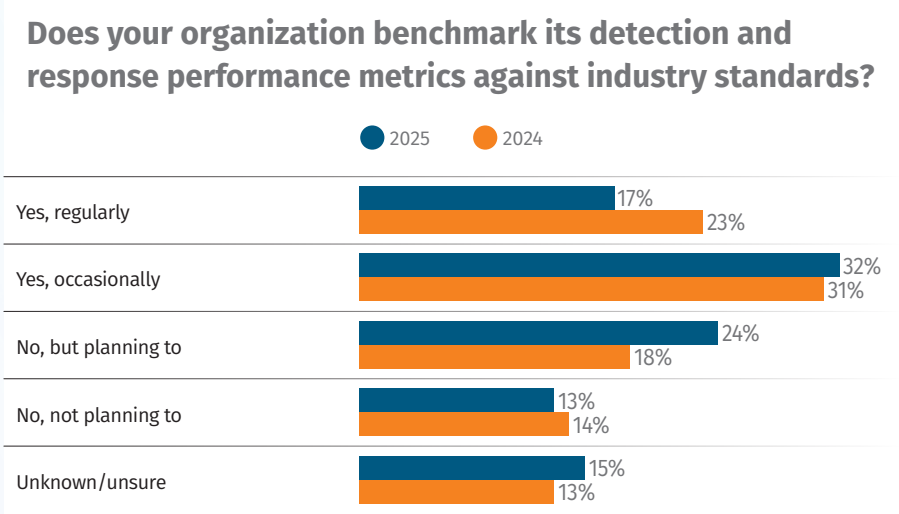

Figure 17. Benchmarking of Detection and Response Metrics

Most organizations (43%) rated their performance metrics as "moderately effective," up from 39% last year, indicating steady but incomplete progress in measurement maturity (see Figure 18). Those viewing metrics as "very effective" dipped slightly to 20%, and fewer than 1% consider them "extremely effective," revealing that few teams believe their data provides a complete picture of performance. Overall, although metrics are improving, many programs still lack the depth needed to translate measurement into actionable insight.

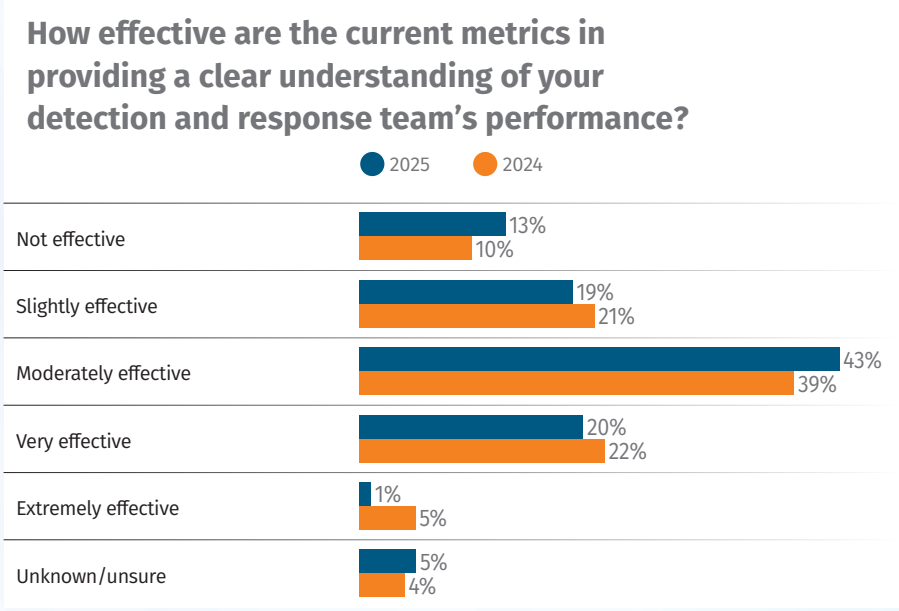

Figure 18. Effectiveness of Detection and Response Metrics

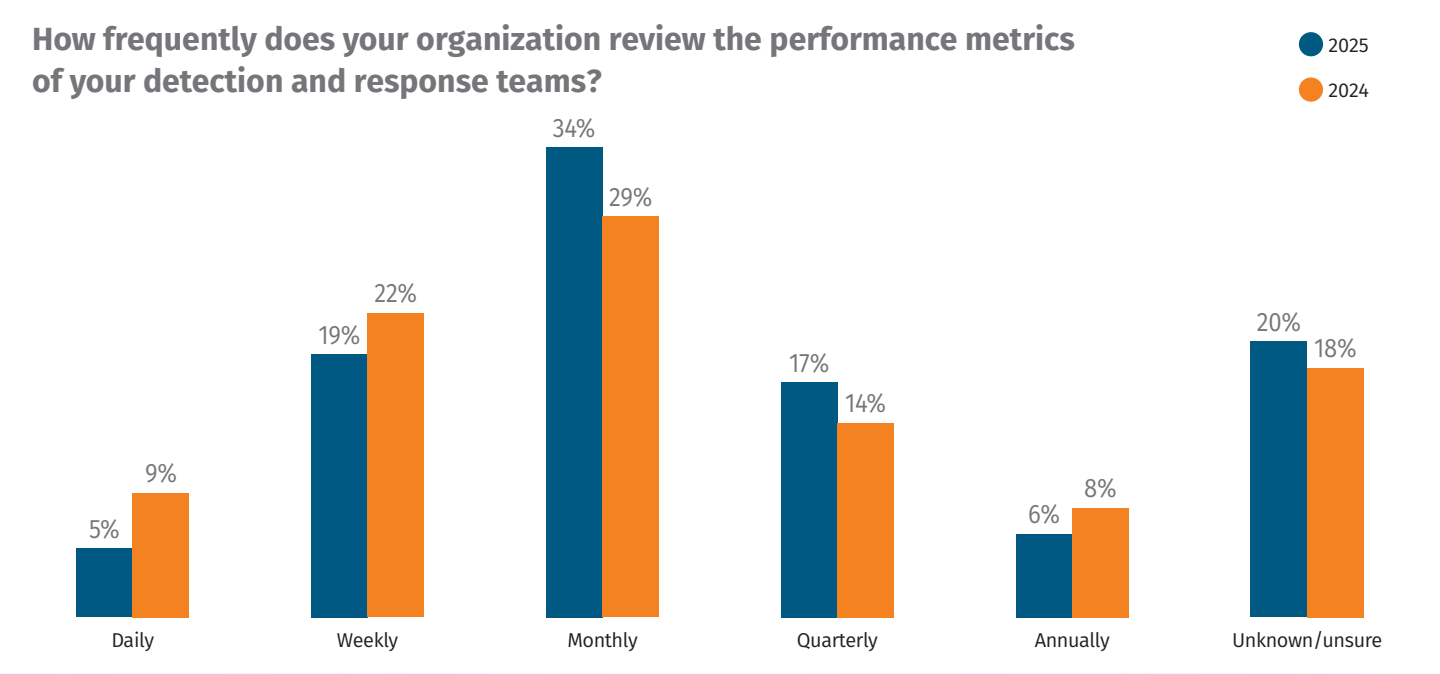

Figure 19. Frequency of Detection and Response Metric Monitoring

Monthly reviews have become the most common cadence for evaluating detection and response performance, with 34% of respondents selecting this approach, up from 29% in 2024 (see Figure 19). The decline in weekly reviews to 19% indicates a preference for more deliberate, trend-focused assessments rather than reactive checks. When it comes to improving KPI measurement, real-time monitoring remains the leading priority, with 31% of respondents placing it first, highlighting a strong demand for more immediate visibility into detection and response performance.

Challenges and Barriers

Detection

False positives remained the leading challenge in 2025, cited by 73% of respondents (up sharply from 64% last year), highlighting the ongoing difficulty of separating signal from noise (see Figure 20). The volume of data remains a concern for 60%, while the shortage of skilled personnel persists at 59%, reinforcing how staffing constraints compound detection inefficiencies. Together, these findings show that, despite progress in tooling, many teams continue to struggle with the scale and sophistication of modern threats.

Figure 20. Challenges in Detecting Cyber Threats

More than 60% of respondents reported encountering false positives frequently or very frequently, with those facing them at very high rates climbed to 20% from 13% last year (see Figure 21). This rise highlights ongoing tuning challenges and the strain it places on analysts. It also underscores the need for stronger detection engineering and training, as excessive noise provides attackers with greater cover and erodes defenders' ability to respond swiftly.

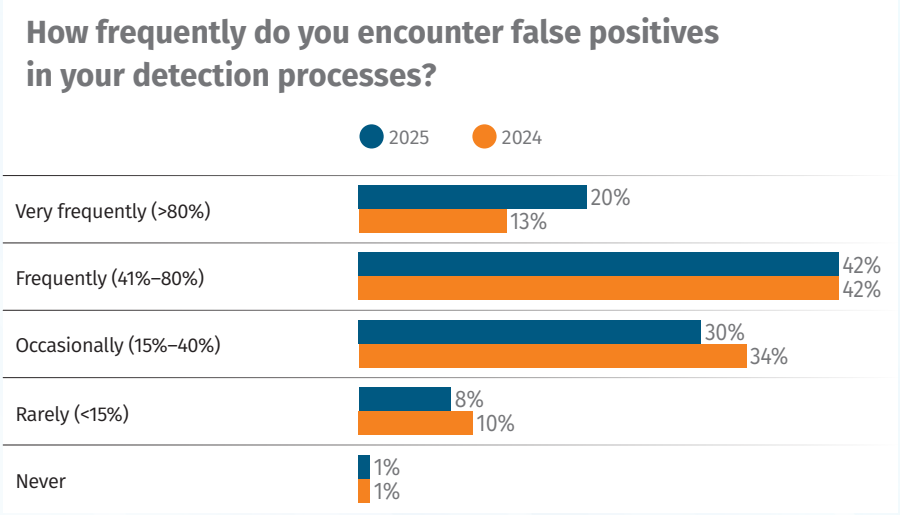

Figure 21. Frequency of False Positive Detection

Cloud

Cloud threat detection continues to challenge security teams, with 58% citing limited cloud expertise, up from 56% last year, underscoring a persistent skills gap as adoption grows (see Figure 22). The complexity of multicloud environments and tool integration, both reported by 53%, further underscores the friction of managing visibility across fragmented systems. Combined with alert fatigue affecting 35% of respondents, these findings reveal that although cloud maturity is improving, expertise and operational cohesion still lag behind the pace of cloud expansion.

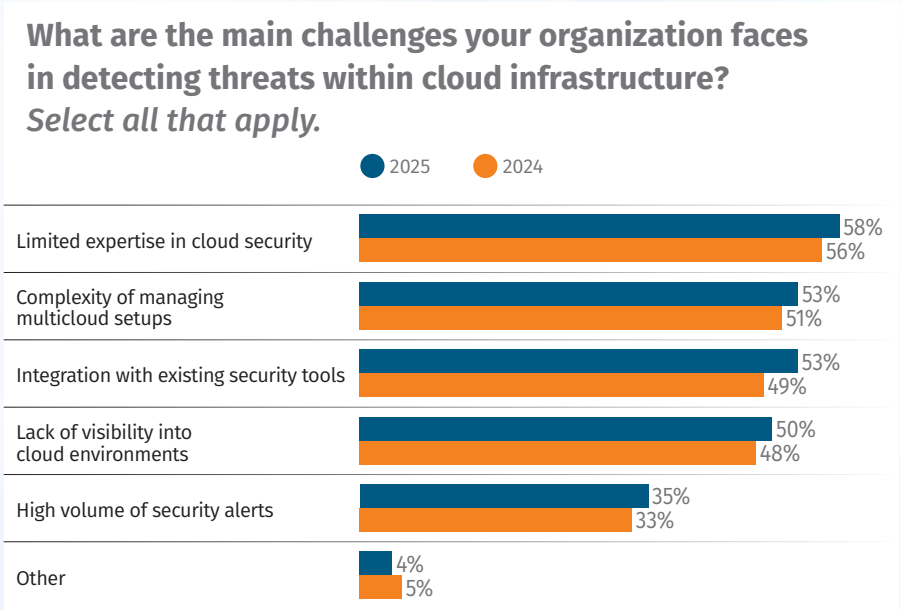

Figure 20. Challenges in Detecting Cyber Threats

Response

Responding to cyber threats remains complex, with skill gaps (56%) and team coordination (55%) continuing to top the list of challenges (see Figure 23). Response time has risen sharply to 53%, up from 45% last year, signaling that many teams are struggling to keep pace with faster, more intricate threats. Tooling limitations (39%) and regulatory pressures (26%) are also gaining ground, underscoring that both operational agility and compliance demands are testing even mature programs.

Figure 23. Challenges in Responding to Cyber Threats

Budget constraints remain the dominant obstacle to maintaining effective detection and response, with 56% ranking it first and another 25% second, reflecting ongoing struggles to fund staffing, tooling, and process improvements. Talent acquisition and retention follow closely, with more than half of respondents ranking them among their top two challenges, underscoring that both money and skilled people remain essential ingredients for advancing operational maturity.

Future Trends and Innovations

Adoption of AI and ML in detection and response continues to accelerate, with 76% of respondents planning to expand their use, up from 67% last year. Automated threat hunting saw the largest increase, to 73%, while predictive analytics (68%) and advanced correlation engines (65%) also gained traction, reflecting a shift toward more proactive, intelligence-driven operations. These findings suggest that AI is no longer experimental but increasingly embedded as a core enabler of faster and more adaptive security response.

Expectations for automation in detection and response are stronger than ever in 2025, with 47% of respondents anticipating a significant increase in its role over the coming years, up notably from 36% last year (see Figure 24). Moderate increases remain steady at 37%, reinforcing that most organizations see automation as a key driver of future capability rather than a marginal enhancement. If these plans eventuate, it should allow teams to handle growing alert volumes and increasingly complex threats with greater speed and consistency.

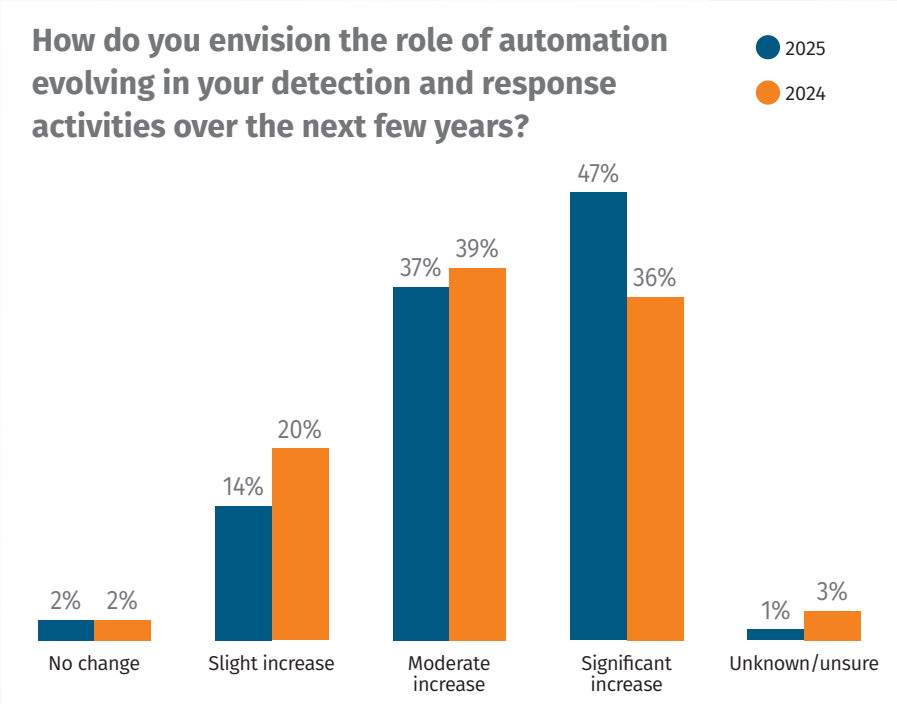

Figure 24. Evolution of Automation in Detection and Response

Organizations continue to prioritize workforce readiness in cloud detection and response, with 68% planning enhanced training for security teams, though slightly down from last year (see Figure 25). The biggest surge is in AI and ML integration, rising to 64% from 52%, reflecting a shift toward more automated and adaptive defense strategies. Meanwhile, custom solution development has declined to 31% from 37%, suggesting that many teams are favoring scalable, vendor-supported approaches over resource-intensive in-house builds.

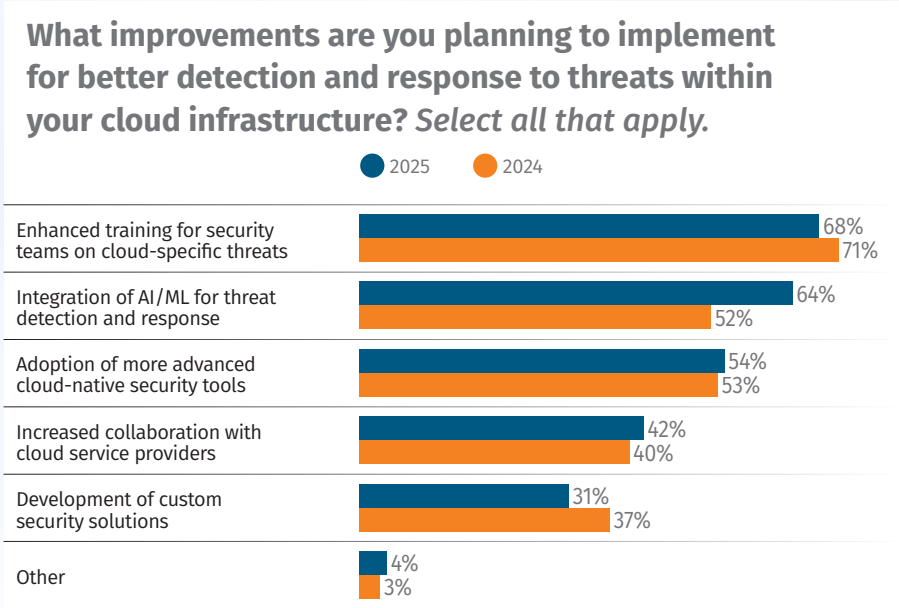

Figure 25. Planned Improvements to Detection and Response

Conclusion

The 2025 Detection and Response Survey shows a community that is not standing still but steadily evolving to meet the threats it faces. Across industries and regions, teams continue to refine how they detect and respond, blending automation, human expertise, and emerging technologies to keep pace with adversaries who are constantly changing their tactics. Endpoint detection tools and dedicated threat hunters remain at the heart of modern security operations. Still, this year's findings make it clear that organizations are also moving toward smarter, more adaptive approaches, with many exploring AI, behavioral analytics, and automation to stay ahead of attackers rather than simply react to them.

Response practices are likewise maturing, with most organizations now combining automated workflows with the judgment of experienced analysts to contain threats quickly and confidently. Our respondents made it clear that speed is no longer their only goal. They are seeking to respond precisely and to balance quick action with the need to avoid unnecessary business disruption. Skill gaps, coordination challenges, and resource constraints remain significant hurdles, but there is an evident willingness to invest in training and process improvements to close those gaps over time.

The most encouraging finding is that defenders are increasingly looking forward, not just fighting today's fires. Plans to expand automation, integrate ML, and improve collaboration with cloud providers show a shift toward a more proactive and resilient security posture. While challenges such as false positives and alert fatigue are still with us, the direction of travel is unmistakable. Security teams are becoming faster, more capable, and more collaborative. And the message is clear: Detection and response may never be "finished," but the progress made this year suggests that the community is better positioned than ever to meet what comes next.

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, content, and in-person or virtual events, email us at **Sponsorships@sans.org** or go to **www.sans.org/sponsorship**.