Omdia
by informa techtarget

Human-Centered AI: Redefining the Modern SOC

Author: Andrew Braunberg
July 2025



Commissioned by:

Abnormal

© 2025 TechTarget, Inc. All rights reserved. Unauthorized reproduction prohibited.

Contents

Executive Summary 3

A Moment of AI Transformation 4

The Analyst Reality: Burnout, Bottlenecks, and Newfound Bandwidth 6

The Leadership View: Scaling Without Sacrificing People 10

The Shared Ground: Trust, Transparency, and Impact 14

Future Outlook: Strategic AI in the SOC 19

Conclusion 22

Recommendations 23

Appendix 24

© 2025 TechTarget, Inc. All rights reserved. Unauthorized reproduction prohibited.

Executive Summary

- Cybersecurity leaders and analysts see AI as beneficial. There is, in fact, a surprising consensus regarding the current value of AI tools in the security operations center (SOC) and the expected benefits looking out over the next several years. This survey identifies more than a dozen business objectives for utilizing AI in the SOC, and 100% of respondents have identified implementing AI as their main business objective.
- While cost containment is a primary driver of adopting AI tools for security leaders, 96% say they have no plans to reduce headcount as a result of the broader adoption of AI in the SOC. Instead, they plan to re-allocate talent to higher-value activities, reflecting a belief that AI doesn't replace but improves human work.
- Analysts, who are increasingly overwhelmed with the daily grind of alert triage and other repetitive tasks, view AI tools as a lifeline, and in fact, 75% of analysts report that the adoption of AI tools is already improving their job satisfaction.
- Importantly, analysts also widely (63%) believe AI is helping to improve the accuracy of investigations. And that number increases (69%) among analysts currently using AI every day.
- There is also broad consensus across analysts and leadership that the introduction of autonomous SOCs is both desirable and likely over the next 3-5 years. For CISOs, automating the SOC has long been a key objective to reduce costs and alleviate analyst burnout.
- Omdia fielded a custom survey to support this research, interviewing 493 cybersecurity leaders and analysts to understand the needs of their SOC and how AI is anticipated to play a role. For more information on survey methodology and demographics, please see the appendix.

© 2025 TechTarget, Inc. All rights reserved. Unauthorized reproduction prohibited.

A Moment of AI Transformation

Automating tasks in the security operations center (SOC) has long been a priority, especially as teams face persistent cost pressures and talent shortages. While tools like security orchestration automation and response (SOAR) have helped streamline certain workflows, they haven't kept pace with the volume or complexity of today's threats and as a result SOC teams face widespread and persistent challenges (see Table 1).

Table 1: What are the biggest business challenges your organization experiences in managing SOC operations?

Response	All Leadership	North America	UK/Ireland	Australia
High operational costs	51%	53%	49%	54%
Budget allocation	49%	45%	52%	56%
Talent shortages	48%	48%	48%	49%
Data management challenges	36%	38%	26%	56%
Scalability limitations	29%	28%	34%	17%

As attacks grow more sophisticated and alert fatigue sets in, a new generation of AI-based tools is showing real promise in helping SOC analysts keep up. The immediate goals and perceived benefits of AI tools in the SOC are to automate the repetitive and often mundane tasks of tier-1 SOC analysts but the more strategic goal is to address the broader challenges listed in Table 1.

SOC teams are rethinking how AI can drive real operational impact. Their top business objectives include scaling without adding staff, reducing costs, and enhancing threat intelligence capabilities (see Table 2).

Table 2: What are your main business objectives for utilizing AI within the SOC?

Response	All Leadership	North America	UK/Ireland	Australia
Scaling security operations without increasing headcount	50%	48%	50%	59%
Reducing operational costs through AI-driven automation	47%	42%	44%	73%
Gaining deeper insights through AI-driven threat intelligence	44%	42%	50%	37%

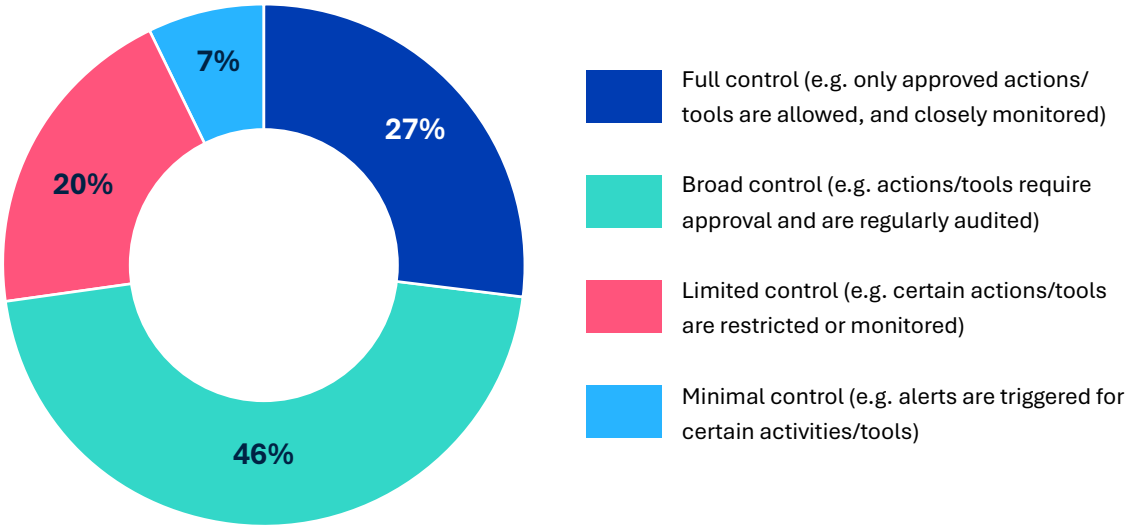
© 2025 TechTarget, Inc. All rights reserved. Unauthorized reproduction prohibited.

Cautious optimism drives thoughtful adoption

Organizations are seeing a clear path forward—one where AI helps scale security operations without requiring a proportional increase in headcount. This would be a major win. Few, if any, leaders or analysts, believe the SOC can, or should, operate with fewer people. The immediate goal is to relieve analysts of the mundane, repetitive tasks that keep them from focusing on higher-value threat investigation, threat hunting, and proactive initiatives.

That is not to say there are no concerns. Almost three-quarters (73%) of organizations report that they have implemented either full or broad control over the use of AI in their organizations (see Figure 1). There is broad recognition of the potential security, regulatory, and privacy risks associated with the use of the current generation of AI tools.

Figure 1: What level of control over AI usage does your organization have in place?



Note: n=491
Source: Omdia

© 2025 Omdia

© 2025 TechTarget, Inc. All rights reserved. Unauthorized reproduction prohibited.

The Analyst Reality: Burnout, Bottlenecks, and Newfound Bandwidth

The security operations center (SOC) remains a mainstay for most large organizations, but the strain on teams, both financial and operational, are increasingly apparent. Analyst burnout is a well-documented concern, driven by the stress of demanding workloads that require rapid, high-pressure decision-making.

Manual tasks don't just hinder the day-to-day operations, they also make it harder for analysts to "zoom out" and focus on the bigger picture. Nearly three-quarters of analysts report a lack of time for strategic work, a clear sign that SOC teams struggle to effectively automate low-value tasks. As a result, analysts can feel stuck in the weeds—without the capacity to focus on higher-impact initiatives like threat hunting, proactive detection, or professional development.

Threat detection and response remains a last line of defense—and a surprisingly manual one. Analysts still sift through massive volumes of alerts, searching for the proverbial needle in a haystack. As shown in Table 3, alert fatigue is the top challenge analysts face when completing SOC tasks.

Table 3: What are the biggest challenges you face in completing your SOC tasks?

Response	All Analysts
Alert fatigue	49%
Too many tasks/overwhelming workload	44%
Inability to automate repetitive tasks	38%

The pressures of the work environment are clear: analysts are expected to manage too many tasks at a pace that's unsustainable without automating repetitive processes. Furthermore, these manual processes have notably eroded analysts' productivity (see Table 4). The average SOC analyst spends too much time trying to accomplish repetitive tasks. This dynamic is increasing levels of analyst burnout and reducing effectiveness, as seen in the slower mean time to response (MTTR).

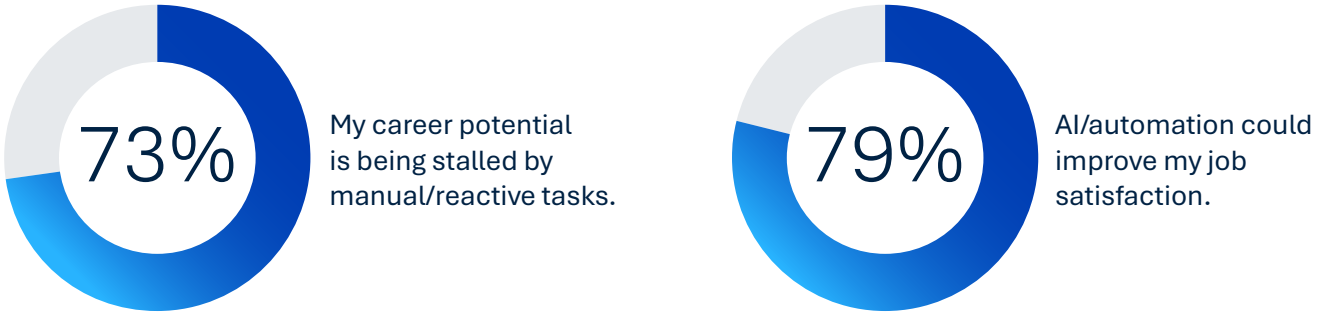
Table 4: How have manual processes negatively impacted your day-to-day activities?

Response	All Analysts
Spending too much time on repetitive tasks	44%
Increased burnout	35%
Slower response time (MTTR)	31%

© 2025 TechTarget, Inc. All rights reserved. Unauthorized reproduction prohibited.

Not surprisingly, career frustration seems to be growing: 73% of analysts say that manual or reactive tasks are stalling their career growth (see Figure 2). With little time left for upskilling, stretch assignments, or pursuing certifications, analysts are caught in a cycle that feels both draining and professionally limiting.

Figure 2: To what extent do you agree with each of the following statements?



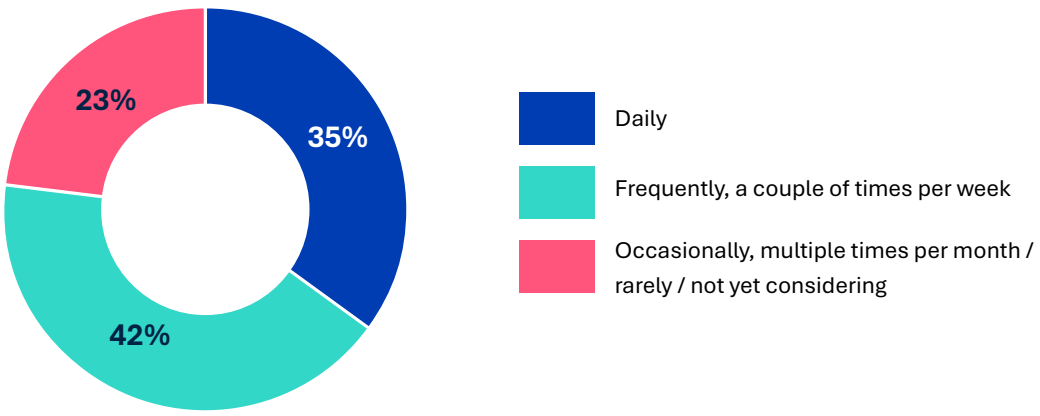
*Percentages indicate strongly agree + agree
Note: n=170 cybersecurity analysts
Source: Omdia

© 2025 Omdia

AI's promise of automation and simplification resonates strongly in the SOC, particularly with analysts who are typically stretched thin. Analysts are busier than ever before, and the daily grind has an impact on their productivity, effectiveness, and overall well-being. It should be no surprise, therefore, that AI use is already prevalent among SOC analysts, with 75% of respondents reporting use of AI at least weekly to support their common tasks. More than a third (35%) of all analysts surveyed already use AI tools daily, and less than a quarter (23%) only use the tools infrequently (see Figure 3).

AI as a relief valve: Benefits for SOC analysts

Figure 3: To what extent are you using AI in your role to support your day-to-day activities?



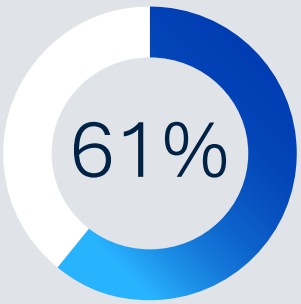
Note: n=170 cybersecurity analysts
Source: Omdia

© 2025 Omdia

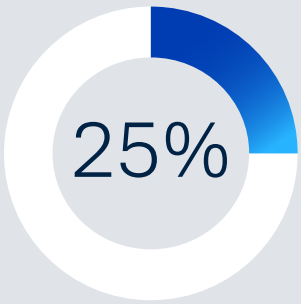
© 2025 TechTarget, Inc. All rights reserved. Unauthorized reproduction prohibited.

The data shows that analysts spending the most time on the most repetitive tasks are more likely to use AI tools today, suggesting that many are operating at maximum capacity and have turned to AI out of necessity.

For example, of the 35% of analysts using AI daily:

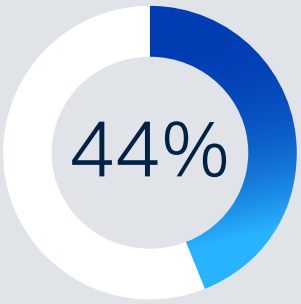


61% report spending more than 75% of their day triaging alerts.

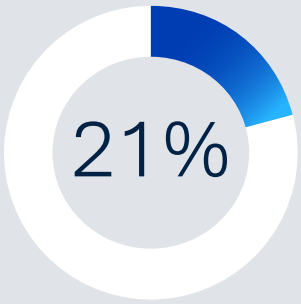


25% report spending 51%-75% of their day triaging alerts.

The 23% of analysts who use AI only a couple times a month or less, report spending less time on average on triaging alerts:



44% report spending more than 75% of their day triaging alerts.



21% report spending 51%-75% of their day triaging alerts.

The data suggests that analysts suffering from alert fatigue are more likely to be early adopters of AI tooling. While alert fatigue is reported by 49% of all analysts, 56% of analysts currently using AI tools everyday report alert fatigue.

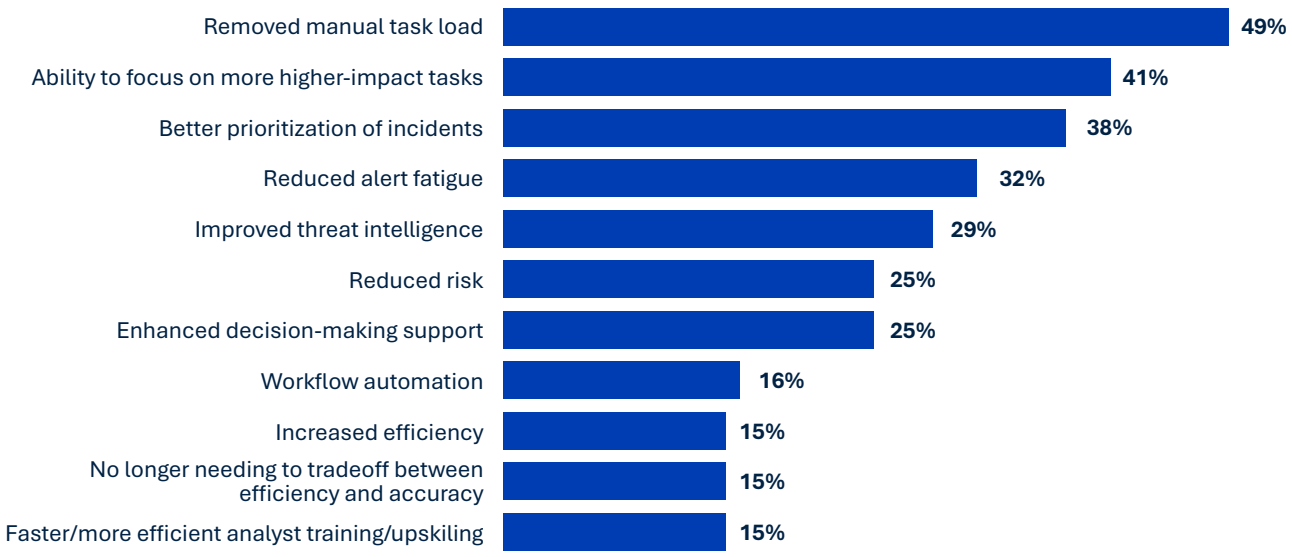
For many, AI offers much-needed relief. As seen in Table 5, more than three-quarters of analysts believe AI and automation could improve their job satisfaction. One hundred percent of analysts surveyed report that AI has driven significant change to their daily activities. For example, 63% of analysts believe AI is helping to improve the accuracy of results. And that number increases (69%) among analysts currently using AI every day.

© 2025 TechTarget, Inc. All rights reserved. Unauthorized reproduction prohibited.

Table 5 : How has AI influenced your work and perspective since you started utilizing it in your daily activities?		
Response	All Analysts	Analysts (Daily use)
Improved accuracy	63%	69%
Increased focus on strategic decision-making	60%	59%
More time to dedicate to continuous learning/upskilling	46%	41%
Able to adopt new role responsibilities	43%	54%
Able to advance my career	42%	47%
Spend less time on manual tasks	42%	47%
Increased my trust in AI-driven recommendations	41%	39%
Ability to transition to a different role	36%	34%
Fewer attacks to remediate	33%	32%
I haven't experienced any significant changes.	0%	0%

The introduction of AI can help alleviate the pressure of keeping up with manual tasks, freeing up time for analysts to pursue tasks that require higher mental load. Analysts who use AI daily are more likely (54% of daily users vs 43% of all analysts) to believe that AI will make it easier for them to adopt new role responsibilities. The data already demonstrates that AI tools are allowing analysts to redirect time saved to higher-value tasks. For example, 39% of all analysts use more than half of their saved time on these higher-impact tasks. In fact, as seen in Figure 4, the ability to focus on higher-impact tasks is seen as a chief benefit of adopting AI tools in the SOC.

Figure 4: Where do you see AI being most beneficial to your role?



Note: n=170 cybersecurity analysts
Source: Omdia

© 2025 Omdia

© 2025 TechTarget, Inc. All rights reserved. Unauthorized reproduction prohibited.

The Leadership View: Scaling Without Sacrificing People

Generally speaking, there is another strategy for dealing with alert overload and threat detection, and that is to take a proactive approach to maintaining security posture. Take for example, an alert that indicates a suspicious email with a malicious attachment was delivered to an executive's inbox. Could that email threat have been detected and quarantined before the recipient had a chance to open it? Could the compromised credentials resulting from a successful phishing email have been identified before the attacker used them to access sensitive company data and exfiltrate confidential information? Proactive security can take many forms. Email filtering technologies, such as advanced threat protection and sandboxing, can proactively reduce exposures by automatically analyzing attachments and links for malicious content before delivery to the end user.

These proactive actions and threat hunting scenarios are often described as shifting security left (of breach). In other words, taking action that prevents or limits attacker action. A more proactive approach sounds great but historically the limitation has been that there are so many vulnerabilities and other potential exploits (e.g., misconfigurations), that it has been hard to prioritize which represent the most risk. That problem is beginning to be solved, often with the aid of machine learning based analytics, and many organizations are investing more of their security budget in proactive solutions (e.g., exposure management).

In practice, however, many SOCs still have trouble carving out analyst time to pursue these techniques and strategies. As is often the case, tactical requirements can crowd out more strategic goals. As seen in Table 6, over the next 12 to 24 months, leadership is more focused on scaling threat detection, investigation, and response (TDIR) operations and securing more of its digital infrastructure.

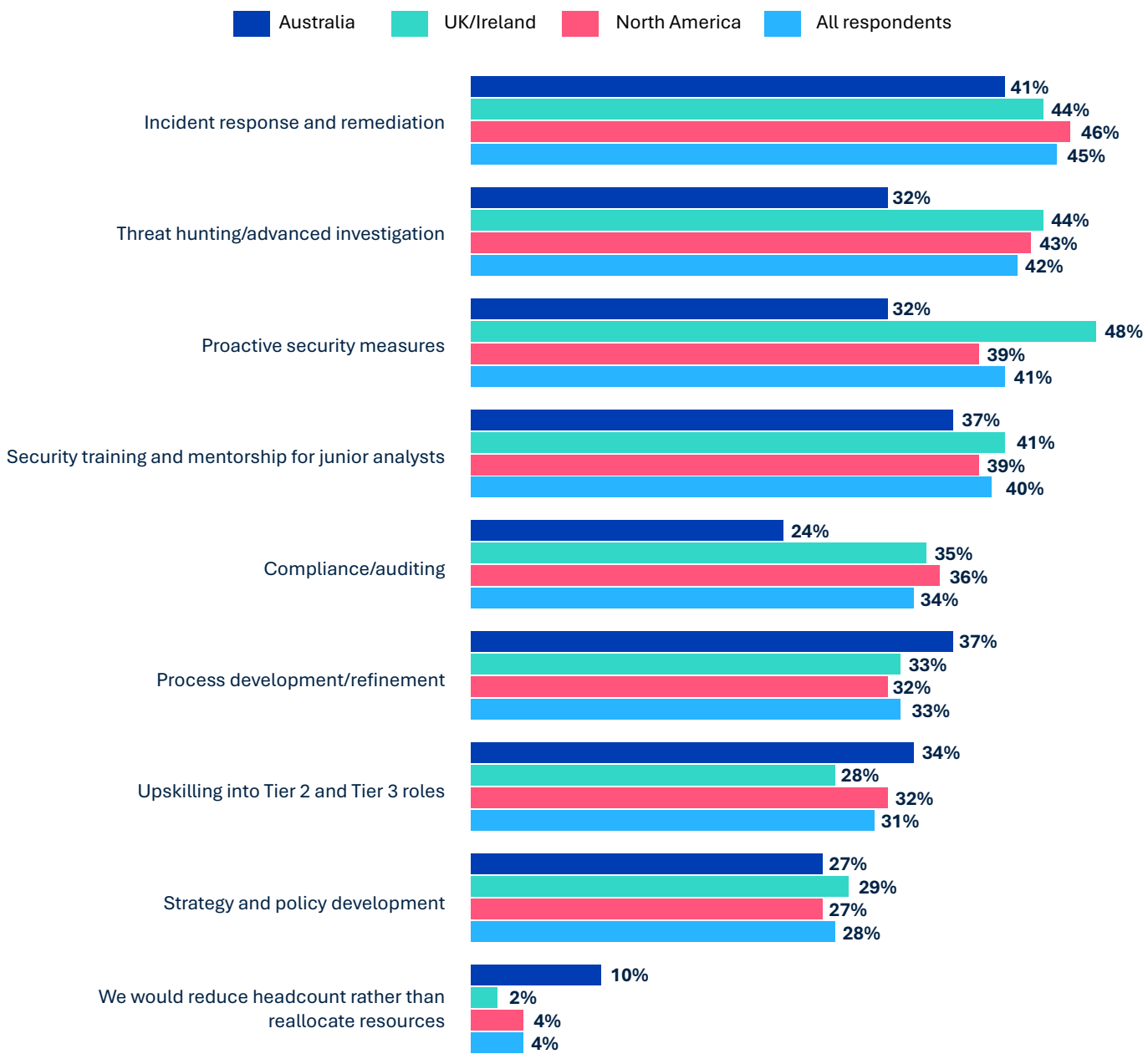
Table 6: What are your top cybersecurity priorities over the next 12-24 months?

Response	All Leadership	North America	UK/Ireland	Australia
Improving threat detection capabilities	40%	36%	42%	49%
Increasing automation to reduce manual workloads	36%	35%	39%	29%
Securing IoT and OT environments	26%	29%	22%	29%
Managing AI-related security risks	25%	28%	24%	20%
Enhancing cloud security posture	25%	24%	24%	32%

© 2025 TechTarget, Inc. All rights reserved. Unauthorized reproduction prohibited.

But an interesting finding in the survey shows that security leaders view the adoption of AI not just as a cost containment tool but also as a strategic enabler. When asked where saved analyst hours would be reallocated after broader adoption of AI tools in the SOC, the three most popular focus areas (across all geographies) were threat hunting, proactive security, and analyst mentorship (see Figure 5).

Figure 5: If AI could effectively reduce the need for tier-1 analysts, where would you ideally reallocate those resources?



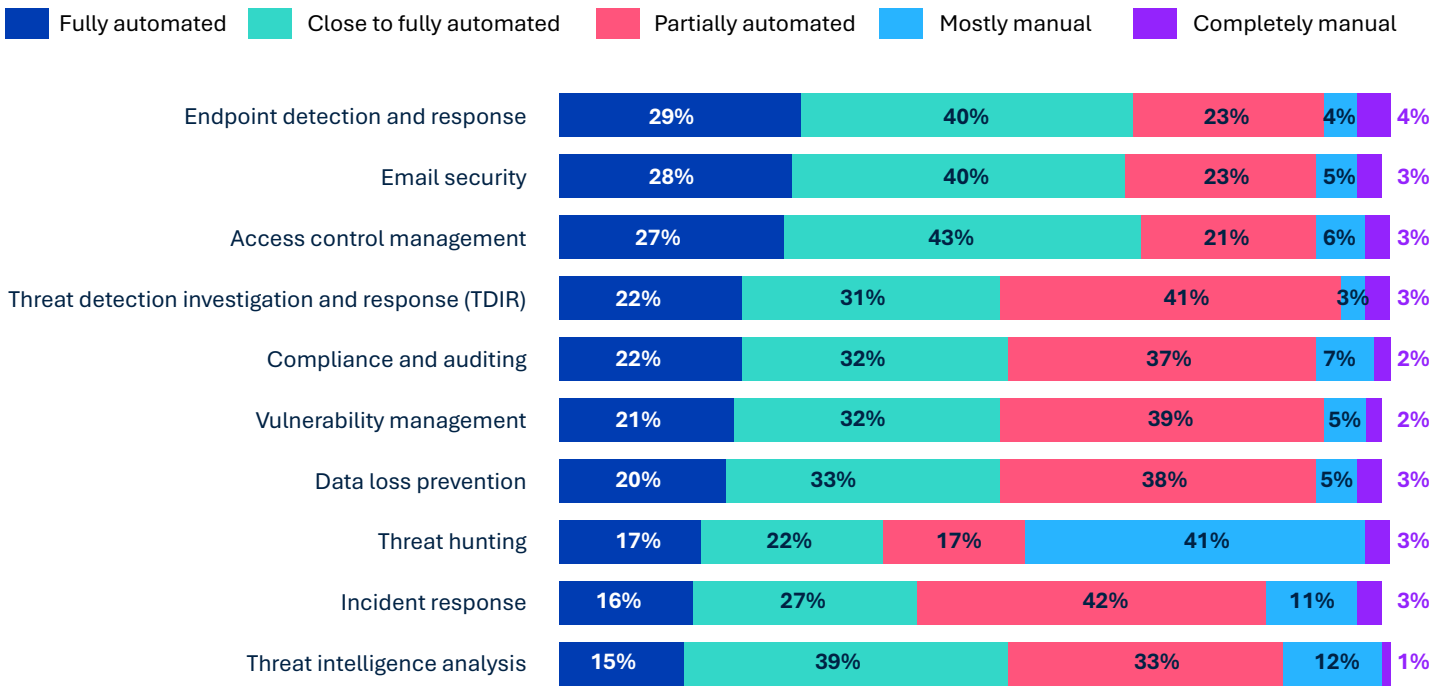
Note: n=321 cybersecurity leaders (C-level, VP, directors)
Source: Omdia

© 2025 Omdia

© 2025 TechTarget, Inc. All rights reserved. Unauthorized reproduction prohibited.

The question of whether the adoption of AI was driven chiefly by a desire to reduce headcount has been a persistent one. These responses suggest that repurposing analyst time to address more strategic tasks is the primary driver for these initiatives. As can be seen in Figure 6, these more strategic tasks, such as threat hunting and incident response, have also tended to be more difficult to automate.

Figure 6: How manual/automated are the following processes in your Security Operations Center (SOC)?



Note: n=491 cybersecurity decision makers
Source: Omdia

© 2025 Omdia

© 2025 TechTarget, Inc. All rights reserved. Unauthorized reproduction prohibited.

Leaders acknowledge AI for analyst engagement

Today, organizations are already seeing tactical and strategic value from the adoption of AI tools. When asked how AI has helped empower or engage SOC analysts to date, the most cited responses by security leaders were to complement/enhance analyst expertise, allow analysts to investigate more threats, and to focus on more complex threat investigations (see Table 7). These are impressive early results from tools that are maturing rapidly.

Table 7: How has AI helped empower/engage your SOC analysts?

Response	All Leadership
Provided tools that complement and enhance analysts' expertise	54%
Allowed analysts to handle a higher volume of threats without feeling burnt out	52%
Allowed analysts to focus on more complex threat investigation	50%
Improved team efficiency/reduced time spent on manual tasks	47%
Provided analysts more time to focus on continuing education or career progression	45%
Improved analyst effectiveness in threat response	44%
Improved analyst job satisfaction and/or reduced analyst burnout	43%
Enabled analysts to work at scale without sacrificing quality	43%

Security leaders are in a very tough spot. They need to contain (or reduce) costs, scale operations, and improve detection accuracy. The latest generation of AI tools are broadly seen as a means to achieve these goals. And in one of the most widely held findings of the survey, 96% of leadership wants to retain their current analyst headcount and pivot those analysts into more strategic (often more proactive) activities. This represents a significant win for SOC teams, demonstrating the evolution of the SOC from a reactive cost center to a strategic business enabler.

As we will see, there is strong alignment between security leaders and security analysts regarding where AI can be applied in the SOC, the value it can bring, and the future it can enable.

© 2025 TechTarget, Inc. All rights reserved. Unauthorized reproduction prohibited.

The Shared Ground: Trust, Transparency, and Impact

AI adoption in the SOC is still in its early stages, but so far, both security leaders and analysts agree on the value these tools are delivering. When asked which tasks AI is currently addressing to provide the most benefit, responses were closely aligned across roles (see Table 8). As shown, that value is largely tied to solving today's tactical challenges.

Table 8: Where do you think AI is most valuable in the SOC currently?

Response	Leadership	Analysts
Threat intelligence enrichment and correlation	38%	37%
Threat detection and anomaly identification	39%	35%
Reducing false positives and alert fatigue	36%	39%

There's also strong consensus around AI's positive impact on risk management within the SOC, especially among analysts who use these tools daily (see Table 9). The one exception is the effect of AI tools on reducing response times. As can be seen below, leadership is twice as confident in that benefit, compared to daily users, perhaps because those daily users have a more realistic view of what these tasks entail, compared to traditionally more idealistic leaders. On the other hand, analysts using AI daily tend to be more bullish than leadership on the ability of these tools to reduce false positives in alerts (49% of analyst daily users vs. 37% of all leadership). These discrepancies may reflect differences in expected benefits and early experience with actual benefits.

Table 9: How does AI impact risk management in your SOC?

Response	Leadership	Analysts (daily)
Improves accuracy of risk identification	59%	56%
Enhances detection capabilities	47%	47%
Improves threat intelligence analysis	47%	46%
Automates routine security tasks	41%	42%
Reduces response times	40%	19%

© 2025 TechTarget, Inc. All rights reserved. Unauthorized reproduction prohibited.

Analysts also tend to be more optimistic on the future value of AI tools in the SOC. When asked to look out over the next three to five years, both security leaders and analysts see these tools providing more strategic value, but analysts are more confident in the ability to achieve autonomous SOC operations over that period (see Table 10). This gap likely stems from the different vantage points of these groups; analysts directly experience AI's capabilities in their daily operations and can envision its full potential, whereas leaders tend to remain cautious due to accountability concerns and historical trust issues with AI solutions. Both groups expect AI tools to aid proactive threat protection, and the thorny problem of insider threat detection.

Table 10: Where do you think AI will be most valuable in the SOC in the next 3-5 years?

Response	Leadership	Analysts
Autonomous SOC operations	37%	51%
Behavioral analytics for insider threat detection	42%	37%
Predictive analytics for proactive threat prevention	37%	43%
SOC workflow automation and case management	38%	38%
Cloud security monitoring and response	36%	38%
Threat detection and anomaly identification	36%	32%
Security compliance and audit automation	33%	35%
Threat intelligence enrichment and correlation	32%	33%
Endpoint and network security optimization	34%	29%
Phishing and email attack threat detection	34%	28%
Forensic investigations and root cause analysis	33%	29%
Security awareness training	30%	28%
Phishing simulations	28%	29%
Automated incident response and remediation	26%	33%
Reducing false positives and alert fatigue	24%	18%

© 2025 TechTarget, Inc. All rights reserved. Unauthorized reproduction prohibited.

Trust but verify

As we saw above, there is strong agreement that AI tools are already improving risk management in the SOC. That is not to say there are no concerns associated with the adoption of these tools. Only 3% of all respondents reported no concerns about adopting AI in the SOC. A consistent set of concerns was reported across all geographies (see Table 11).

Table 11: Top 3 concerns regarding AI adoption in the SOC (by region)

Response	All respondents	North America	UK/Ireland	Australia
Concerns over data privacy and security	39%	34%	42%	47%
Regulatory and compliance challenges with AI adoption	32%	30%	30%	44%
Introduce new security risks	29%	29%	29%	29%

All three of these concerns relate to potential new liabilities for the organization or its employees. Contrary to the common concern across industries about AI displacing employees, few of the SOC analysts surveyed reported this as a concern. Only 16% of analysts voiced concerns about AI replacing them, in stark contrast to the 47% of analysts using these tools daily that believe AI can help advance their careers.

Not surprisingly, respondents across all regions and job titles want to see strong data privacy and security measures in place; training and upskilling programs for analysts that work with AI; and clear communications about the specific limitations of AI. And looking just at analysts, daily users of AI were more likely to report feelings of reassurance surrounding clear communication from leadership regarding the specific limitations of these tools, and not allowing the AI agent to be the final decision maker (see Table 12).

Table 12: Which initiatives would offer reassurance regarding these concerns about AI adoption in the SOC?

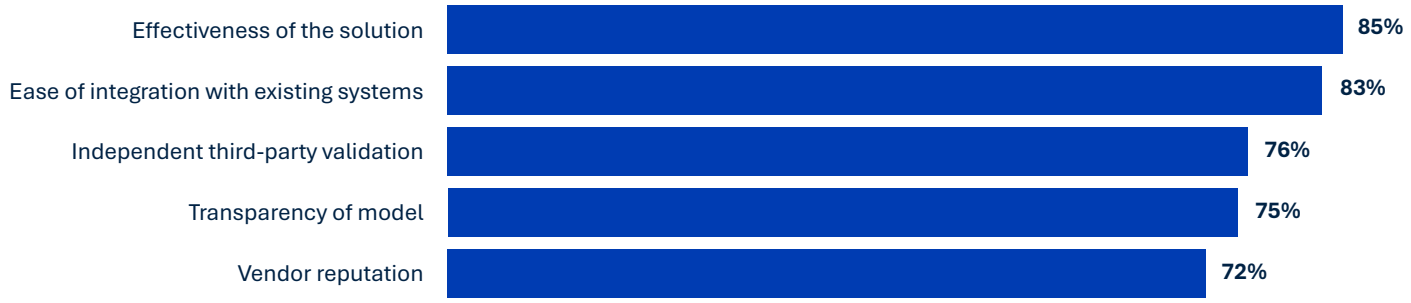
Response	All Analysts	Analysts (daily)	Analysts (frequently)	Analysts (Occasionally)
Clear communication about the specific limitations of AI technology at my organization from my leadership team	38%	51%	36%	23%
AI solutions keeps a human analyst as the final decision maker	40%	44%	39%	36%

© 2025 TechTarget, Inc. All rights reserved. Unauthorized reproduction prohibited.

Buying criteria

Security leaders and analysts are closely aligned on the top factors to consider when evaluating AI security vendors or solutions (see Figure 5).

Figure 5: Which factors are most important when evaluating AI security vendors (or solutions)?



*Percentages indicate critical + important
Note: n=170 cybersecurity decision makers
Source: Omdia

© 2025 Omdia

Except for "transparency of model," these are very similar criteria seen for any new security control or tooling introduced into the SOC. The importance of understanding AI models and not being presented with a black box approach became even more apparent when respondents were asked how they evaluate the trustworthiness of an AI-powered security solution. As seen in Figure 6, vendor transparency regarding how AI models are built and trained is the primary means for customers to determine if they can trust an AI security solution.

Figure 6: How do you evaluate trustworthiness of an AI-powered security solution?



Note: n=491 cybersecurity decision makers
Source: Omdia

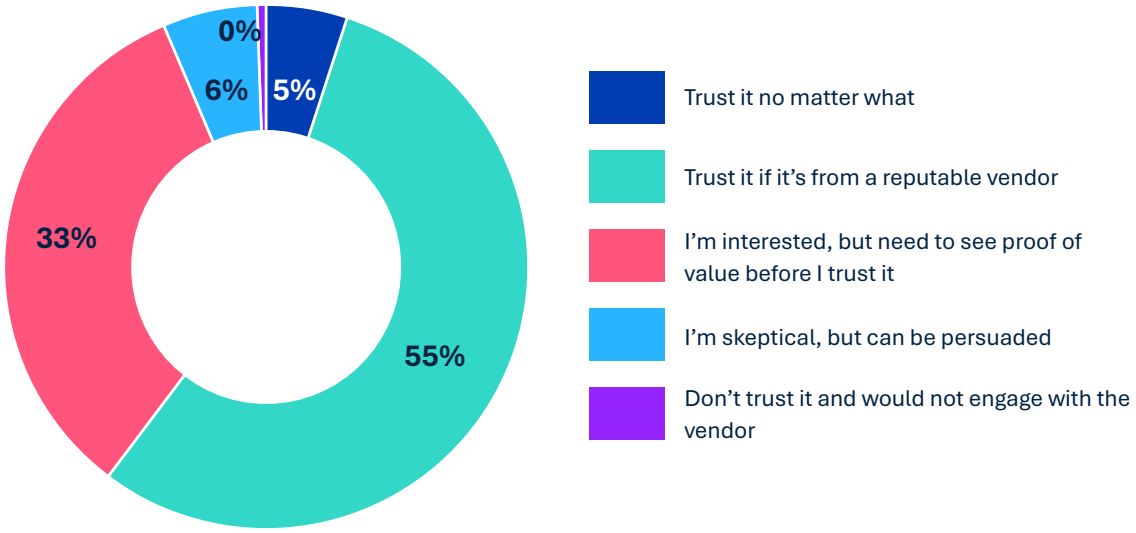
© 2025 Omdia

© 2025 TechTarget, Inc. All rights reserved. Unauthorized reproduction prohibited.

Analysts and security leaders agree, for the most part, on how to evaluate trustworthiness, but there are a few areas of emphasis on both sides. Analysts put more weight on third-party evaluations (65% to 57%) while leadership is more likely to want to work with a vendor that has a proven record of responsiveness to security concerns (57% to 40%).

Given how quickly AI tooling is emerging and evolving, it is likely that many of the traditional resources for product evaluation, such as industry standards, may be having trouble keeping up with market developments. This makes model transparency an even more important metric. Organizations seem willing to give vendors the benefit of the doubt regarding their marketing claims, for now at least, see Figure 7.

Figure 7: What is your perception of vendors' marketing of AI solutions?



Note: n=491 cybersecurity decision makers
Source: Omdia

© 2025 Omdia

© 2025 TechTarget, Inc. All rights reserved. Unauthorized reproduction prohibited.

Future Outlook: Strategic AI in the SOC

What might be possible if analysts didn't feel like they were chasing their tails all day? On this topic, there is also strong alignment between security leaders and analysts that there needs to be a fundamental shift in SOC strategy, toward more strategic tasks. These include advanced threat hunting and proactive security initiatives. Analysts currently using AI tools daily are more inclined to increase their focus on advanced threat hunting (see Table 13). This is not surprising given that threat hunting is typically performed by more senior analysts within the SOC. If basic tasks can be automated, analysts can be freed up to tackle more interesting work.

Table 13: What tasks would you be most likely to focus on if AI could handle routine/manual tasks? (top three responses)

Response	All Analysts	Daily	Frequently	Occasionally
Advanced threat hunting	52%	59%	50%	46%
Incident response and forensics	47%	56%	42%	44%
Proactive security initiatives	42%	41%	42%	46%

Security leaders have the same goal. The data makes clear that automation is seen as a jumping off point for a reorientation of effort within the SOC (see Table 14). Good help remains hard to find, and automation is seen as an effective strategy to reduce burn out and repurpose analysts into more interesting roles.

Table 14: If AI could effectively reduce the need for Tier 1 analysts, where would you ideally reallocate those resources?

Response	All Leadership
Incident response and remediation	45%
Threat hunting/advanced investigation	42%
Proactive security measures	41%
Security training and mentorship for junior analysts	40%
Compliance/auditing	34%
Process development/refinement	33%
Upskilling into Tier 2 or Tier 3 roles	31%
Strategy and policy development	28%
We would reduce headcount rather than reallocate resources	4%

© 2025 TechTarget, Inc. All rights reserved. Unauthorized reproduction prohibited.

Anticipating disruption

While neither security leaders nor analysts plan or expect a strategy of headcount reduction because of this evolution, there is broad agreement that organizational disruption is likely, and that SOC evolution is going to require significant changes to how analysts work. Perhaps the most obvious is the need to create new roles or specialized positions within the SOC for AI management, with 57% of security leaders identifying this as a requirement. More significantly, 43% of leaders believe this evolution demands a complete rethinking of the overall structure and staffing of the SOC (see Table 15). This indicates that many organizations recognize AI integration requires fundamental changes, not just incremental additions.

Table 15: How does the use of AI in the SOC influence your overall planning and strategy?

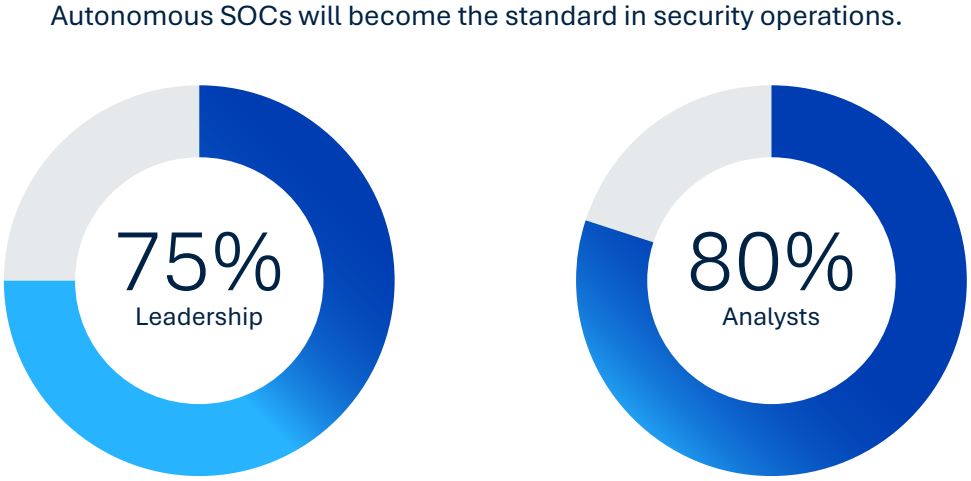
Response	All Leadership
Need to create new roles or specialized positions responsible for AI management	57%
Adjustments to team dynamics or role responsibilities overall	50%
Impact on training opportunities for new SOC hires (e.g. reduced shadowing and hands-on experience)	50%
Changes to Tier 1 analyst responsibilities/career paths	44%
Migration plans for Tier 1 analysts to Tier 2-3 roles	44%
Rethinking the overall structure and staffing of the SOC	43%
Reduced need for additional headcount	28%
I don't expect any changes.	0%

© 2025 TechTarget, Inc. All rights reserved. Unauthorized reproduction prohibited.

AI-powered but human focused

As discussed, security leaders are motivated to adopt AI tools in the SOC primarily to achieve the goals of cost-effectively increasing the scalability of TDIR processes while also obtaining additional risk reduction through deeper insights gained with AI-driven threat intelligence. The early success of the latest generation of AI tools in meeting these goals is driving an optimistic view of the future of the SOC. In fact, 80% of all analysts believe the autonomous SOC will become standard in security operations. Three-quarters of security leaders agree with that prediction (see Figure 8).

Figure 8: To what extent do you agree with each of the following statements?



*Percentages indicate strongly agree + agree
Note: n=491 cybersecurity decision makers
Source: Omdia

© 2025 Omdia

© 2025 TechTarget, Inc. All rights reserved. Unauthorized reproduction prohibited.

Conclusion

When considered in total, the survey suggests a future where much of the traditional tier 1 analysts' work is automated, and work within the SOC shifts left of breach into more proactive and strategic initiatives. While it is likely that AI agents will be able to fully automate tasks such as alert triage, the need for analysts to remain in the loop of many SOC actions will not change in the foreseeable future. Remember that the primary concerns associated with the adoption of these tools involve liability associated with privacy, compliance, and security.

Security leaders view AI as a strategic lever to scale operations while cutting costs and increasing analyst autonomy. Analysts see AI tools as a lifeline to reduce job burnout and provide a new avenue toward professional growth. Security leaders and analysts have long agreed on the challenges facing the SOC, but agreement on the best solution has been elusive, given sometimes divergent priorities and constraints. While these groups will continue to have different motivations, the data demonstrates agreement that an AI-based tooling is an important component of future SOCs.

© 2025 TechTarget, Inc. All rights reserved. Unauthorized reproduction prohibited.

Recommendations

Based on the data findings from this survey, Omdia has five key recommendations for organizations looking to adopt a human-centric approach to AI:

- **Develop an AI-enabled SOC transformation roadmap:** Analysts and leaders agree that autonomous SOCs will become standard. Create a comprehensive three- to five-year strategic plan for transitioning to an autonomous SOC model that includes clear milestones for technology adoption, organizational restructuring, GRC integration, and skills development to ensure a coordinated evolution rather than piecemeal implementation.

- **Establish a human/AI collaboration framework:** AI's primary value is complementing analyst expertise and human analysts should always be your final decision makers. Design operational models that optimize the complementary strengths of human analysts and AI systems. Define which decisions require human judgment versus which can be fully automated, with governance protocols that evolve as AI capabilities mature. This should also include a thoughtful approach to redesigning SOC roles or career paths to include specialized positions for AI management.

- **Implement risk-based resource allocation:** Organizations support shifting resources to proactive security and threat hunting. Ensure you're setting yours up for success in order to do so. Develop metrics to quantify how AI implementation affects risk reduction and operational efficiency. Use these metrics to justify strategic reallocation of resources from reactive to proactive security measures. Prioritize the low-hanging fruit and the automation of high-volume repetitive tasks first.

- **Create centers of excellence for AI security operations:** Establish specialized teams responsible for evaluating, implementing, and continuously improving AI capabilities across the security organization. These teams should focus on addressing the top concerns around AI adoption: data privacy (39%), regulatory compliance (32%), and new security risks (29%), while ensuring alignment with business objectives.

- **Develop a talent transformation strategy:** Create a comprehensive plan to evolve security talent alongside AI implementation, addressing the 43% of leaders who believe AI requires rethinking the overall structure and staffing of the SOC. Include upskilling pathways for current analysts, new hiring profiles, and retention strategies that leverage AI to improve job satisfaction (important to 79% of analysts).

© 2025 TechTarget, Inc. All rights reserved. Unauthorized reproduction prohibited.

Appendix

Methodology

In May 2025, Omdia conducted an online survey of 491 cybersecurity decision makers regarding their priorities, challenges, and needs in their SOC. Survey participants included respondents in manager-level positions and higher, across global geographies. Surveys were fielded using a double-blind methodology to ensure anonymity.

Geography	
North America (US, Canada)	50%
UK/Ireland	39%
Australia	11%

Company size (Employees)	
3,000 – 4,999 employees	40%
5,000 – 9,999 employees	37%
10,000+ employees	23%

Respondent level	
Leadership (C-Level, VP, Director)	65%
Analyst (Manager, Individual Contributor)	35%

Industry (Top 5)	
Software/SaaS	13%
Banking, financial services, insurance	13%
Retail and eCommerce	11%
Technology services/consulting	10%
Manufacturing, construction, and materials	10%

© 2025 TechTarget, Inc. All rights reserved. Unauthorized reproduction prohibited.

About Abnormal AI

Abnormal AI is the leading AI-native human behavior security platform, leveraging machine learning to stop sophisticated inbound attacks and detect compromised accounts across email and connected applications. The anomaly detection engine leverages identity and context to understand human behavior and analyze the risk of every cloud email event—detecting and stopping sophisticated, socially-engineered attacks that target the human vulnerability.

You can deploy Abnormal in minutes with an API integration for Microsoft 365 or Google Workspace and experience the full value of the platform instantly. Additional protection is available for Slack, Workday, ServiceNow, Zoom, and multiple other cloud applications. Abnormal is currently trusted by more than 3,200 organizations, including over 20% of the Fortune 500, as it continues to redefine how cybersecurity works in the age of AI. Learn more at abnormal.ai.

Author:

Andrew Braunberg
Principal Analyst, Security Operations
askananalyst@omdia.com

Omdia consulting

Omdia is a market-leading data, research, and consulting business focused on helping digital service providers, technology companies, and enterprise decision makers thrive in the connected digital economy. Through our global base of analysts, we offer expert analysis and strategic insight across the IT, telecoms, and media industries.

We create business advantage for our customers by providing actionable insight to support business planning, product development, and go-to-market initiatives.

Our unique combination of authoritative data, market analysis, and vertical industry expertise is designed to empower decision-making, helping our clients profit from new technologies and capitalize on evolving business models.

Omdia is part of Informa TechTarget, a B2B information services business serving the technology, media, and telecoms sector. The Informa group is listed on the London Stock Exchange.

We hope that this analysis will help you make informed and imaginative business decisions. If you have further requirements, Omdia's consulting team may be able to help your company identify future trends and opportunities.

Get in touch

www.omdia.com
askananalyst@omdia.com

Copyright notice and disclaimer

The Omdia research, data, and information referenced herein (the "Omdia Materials") are the copyrighted property of TechTarget, Inc. and its subsidiaries or affiliates (together "Informa TechTarget") or its third-party data providers and represent data, research, opinions, or viewpoints published by Informa TechTarget and are not representations of fact.

The Omdia Materials reflect information and opinions from the original publication date and not from the date of this document.

The information and opinions expressed in the Omdia Materials are subject to change without notice, and Informa TechTarget does not have any duty or responsibility to update the Omdia Materials or this publication as a result.

Omdia Materials are delivered on an "as-is" and "as-available" basis. No representation or warranty, express or implied, is made as to the fairness, accuracy, completeness, or correctness of the information, opinions, and conclusions contained in Omdia Materials.

To the maximum extent permitted by law, Informa TechTarget and its affiliates, officers, directors, employees, agents, and third-party data providers disclaim any liability (including, without limitation, any liability arising from fault or negligence) as to the accuracy or completeness or use of the Omdia Materials. Informa TechTarget will not, under any circumstance whatsoever, be liable for any trading, investment, commercial, or other decisions based on or made in reliance of the Omdia Materials.

© 2025 TechTarget, Inc. All rights reserved. Unauthorized reproduction prohibited.