人工智能和安全现状调查报告

Google Cloud

CSA cloud security alliance®

Acknowledgments

Lead Authors

Hillary Baron

Contributors

Josh Buker
Marina Bregkou
Ryan Gifford
Sean Heide
Alex Kaluza
John Yeoh

Graphic Design

Claire Lehnert
Stephen Lumpe

Special Thanks

Jessica Mulreany

About the Sponsor

Google Cloud is the new way to the cloud, providing AI, infrastructure, developer, data, security, and collaboration tools built for today and tomorrow. Google Cloud offers a powerful, fully integrated and optimized AI stack with its own planet-scale infrastructure, custom-built chips, generative AI models and development platform, as well as AI-powered applications, to help organizations transform. Customers in more than 200 countries and territories turn to Google Cloud as their trusted technology partner.

https://cloud.google.com/
https://cloud.google.com/security/ai

Table of Contents

Survey Creation and Methodology

The Cloud Security Alliance (CSA) is a not-for-profit organization with a mission to promote best practices for ensuring cybersecurity in cloud computing and IT technologies. CSA also educates stakeholders within these industries about security concerns in all other forms of computing. CSAs membership is a broad coalition of industry practitioners, corporations, and professional associations. One of CSA's primary goals is to conduct surveys that assess information security trends. These surveys provide information on organizations' current maturity, opinions, interests, and intentions regarding information security and technology.

Google Cloud commissioned CSA to develop a survey and report to better understand the industry's knowledge, attitudes, and opinions regarding artificial intelligence (AI). Google Cloud financed the project and co-developed the questionnaire with CSA research analysts. The survey was conducted online by CSA in November 2023 and received 2,486 responses from IT and security professionals from organizations across the Americas, Asia-Pacific, Europe, and the Middle East. CSA's research analysts performed the data analysis and interpretation for this report.

The Goals of the Study

The primary objectives of the survey were to gain a deeper understanding of:

- Current security challenges
- Perceptions of AI in cybersecurity
- Industry familiarity with AI
- Plans for AI use in the industry
- AI impact on staffing and training

Key Findings and Patterns

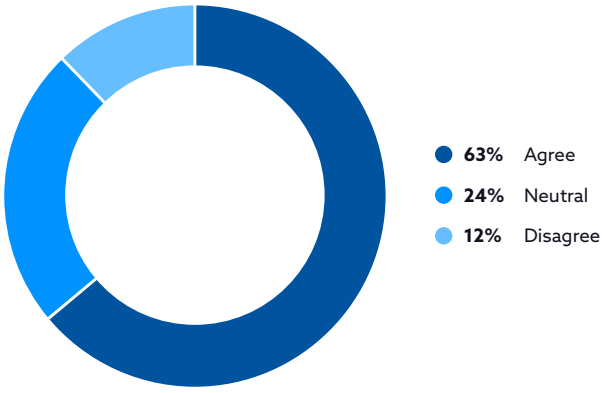
The advent of AI in cybersecurity marks a transformative era in the realm of digital defense, bringing a blend of promising breakthroughs and intricate challenges. AI has the potential to be a vital ally in bolstering security defenses, identifying emerging threats, and facilitating swift responses. However, the journey towards integrating AI into cybersecurity workflows is fraught with obstacles, including the need to mitigate dual-use concerns, bridge skill gaps, and encourage appropriate but not over-reliance on automated systems. Gaining insights into how industry experts view and prepare for AI's evolving role in cybersecurity is pivotal in navigating this transition and ensuring a resilient, forward-looking digital infrastructure.

Key Finding 1:

Cautious Optimism About AI Among Security Professionals

There is a cautious yet optimistic stance among security professionals regarding AI. A majority, 63%, believe in AI's potential to enhance security measures, especially in improving threat detection and response capabilities. However, there's a keen awareness of the potential nefarious use of AI, as evidenced by the divided opinion: 34% see AI more beneficial for security teams, while 31% view it as equally advantageous for both protectors and attackers.

How strongly do you agree or disagree with the following statement: Artificial Intelligence (AI) will improve security within our organization?

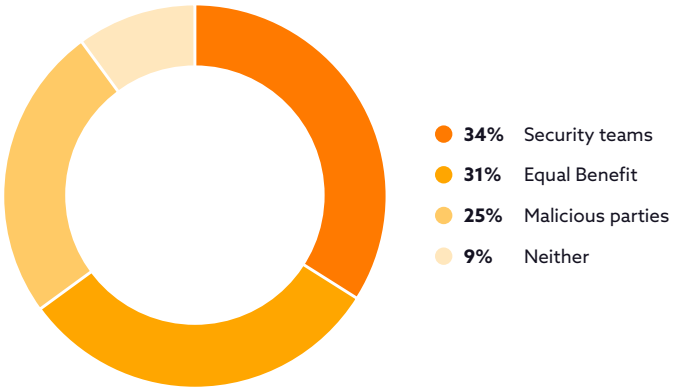


A notable 25% of respondents expressed concerns that AI could be more advantageous to malicious parties, indicating a significant awareness of the potential for advanced AI-enabled cyber threats.

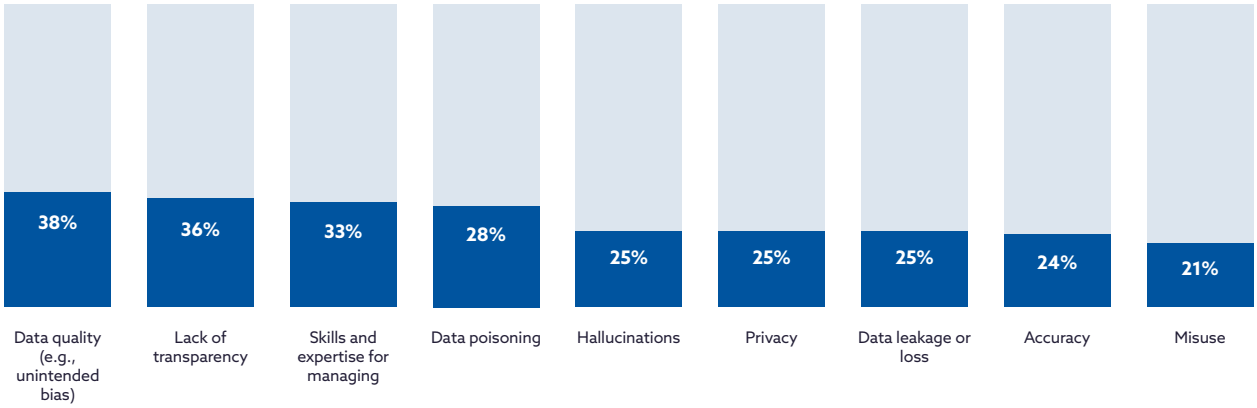
Even though more security professionals view AI as a more beneficial tool for defenders rather than a boon for attackers, there are also some apprehensions about the use of AI in security. These concerns focus on data quality (e.g., data used to train models), which could lead to unintended bias among other issues (38%); the opacity of AI systems (commonly referred to as the 'black box' issue); and skills/expertise gaps for managing complex AI systems.

These findings suggest a balanced perspective in the cybersecurity community. While there's optimism about AI's role in enhancing security, there's also a clear recognition of its potential misuse and the challenges it brings. This calls for evolving security strategies, rigorous data handling, transparent AI models, and continuous vigilance in updating security protocols to stay ahead in the fast-evolving, AI-driven cybersecurity landscape. Additionally, securing AI systems is a critical concern, hinting at the need for comprehensive frameworks to safeguard AI technologies, a topic that was not within the scope of this survey but remains top of mind.

In your opinion, would AI be more beneficial to security teams or malicious 3rd parties?



What are your biggest concerns regarding AI in security? (Select up to 3)

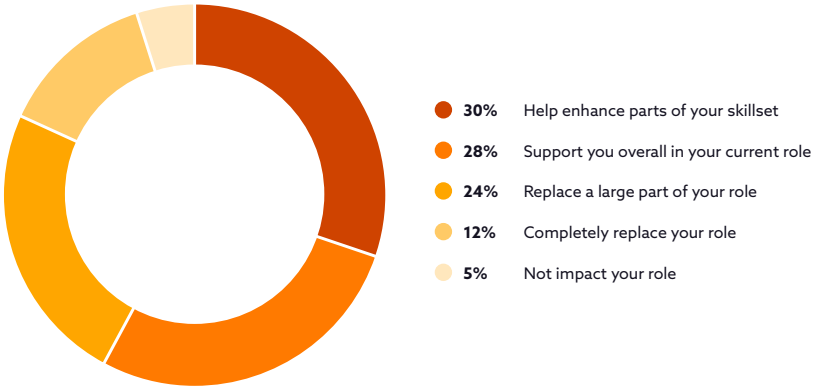


Key Finding 2:

AI Will Empower, not Replace, Security Professionals

AI is seen as an empowering tool rather than a replacement for security professionals. Most professionals acknowledge that there are challenges in threat investigation and response, with only 12% reporting no difficulty with this task in their organization. This sets the stage for AI's role as an empowerment tool. Only a small fraction (12%) of security professionals believe it will completely replace their role. The majority believe it will help enhance their skill set (30%), support their role generally (28%) or replace large parts of their role (24%), freeing them up for other tasks.

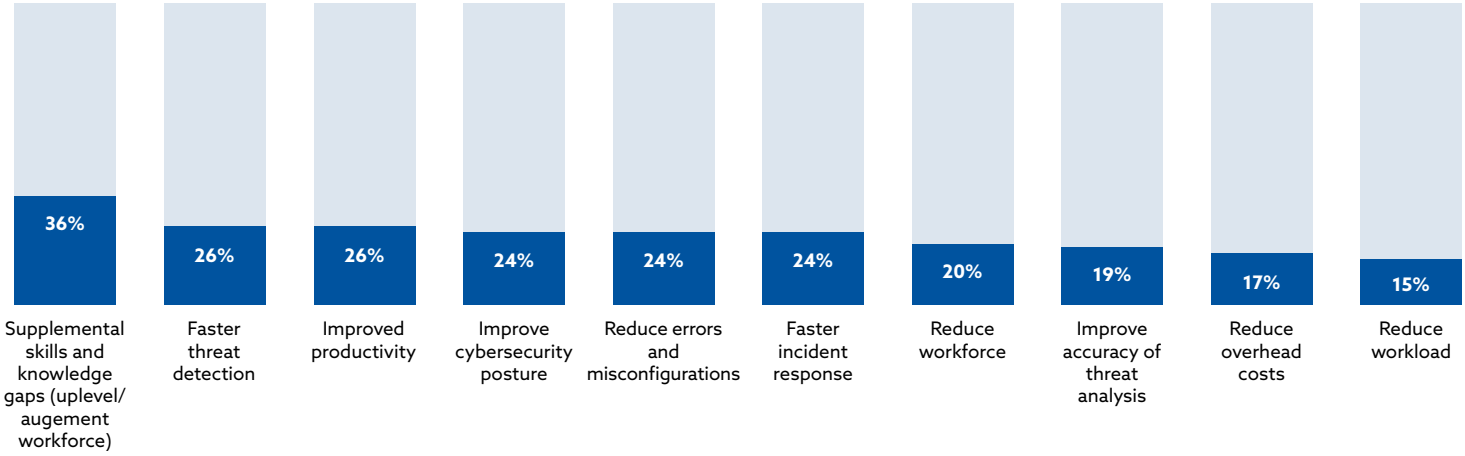
Please select the option that best reflects your opinion about AI's potential impact on your role. Over the next 5 years, AI will...



This is further supported by the organization's desired outcomes for implementing AI with their security teams. The focus is on AI enhancing the knowledge of security teams skills and knowledge (36%), improving threat detection times (26%), and increasing productivity (26%) rather than reducing the workforce (20%). This aligns with their perceptions of how roles will evolve rather than be replaced, with 74% of organizations planning to create new teams to oversee the secure use of AI within the next five years.

Despite the high value placed on team skills and knowledge enhancement as a desired outcome of AI implementation, when asked to rank their greatest security challenges, respondents placed talent at the bottom, with operational toil and threat detection being ranked higher. This discrepancy may indicate that, while enhancing team capabilities through AI is a priority, the immediate challenges of managing security workloads and identifying threats are perceived as more pressing or perhaps more difficult areas to address. It's evident that AI in cybersecurity is not just transforming existing roles but also paving the way for new specialized positions.

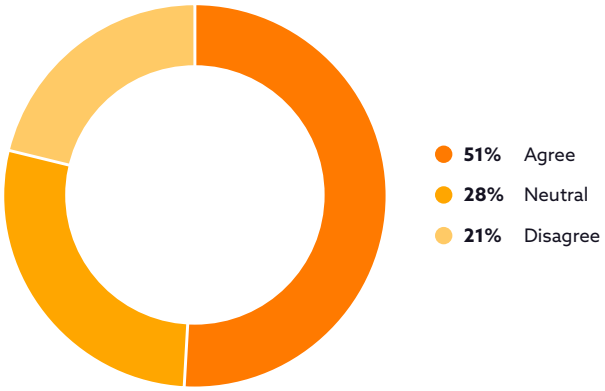
What are your desired outcomes when it comes to implementing AI in your security team?



However, there are concerns about an overreliance on AI, shared by half of the respondents, emphasizing the need for a balance between AI-driven and human-driven security. This concern is particularly relevant given the issues around data quality and lack of transparency in AI systems expressed earlier.

In conclusion, these findings underscore that while AI will bring significant changes to security teams, it's primarily seen as a complementary tool rather than a complete replacement. It's set to assist in bridging skills and knowledge gaps that have plagued the industry, but there are healthy concerns about becoming overly reliant on it. The landscape of cybersecurity is set to evolve with changing roles and the emergence of new positions, indicating a dynamic future for the field influenced heavily by AI integration.

Are you concerned about the potential risks of over-reliance on AI for cybersecurity?

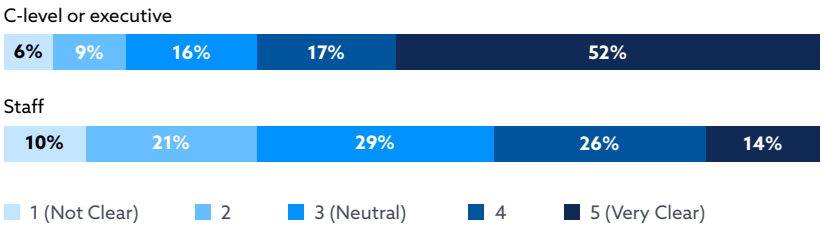


Key Finding 3:

C-Suite Executives Have Different AI Perspectives from Their Staff

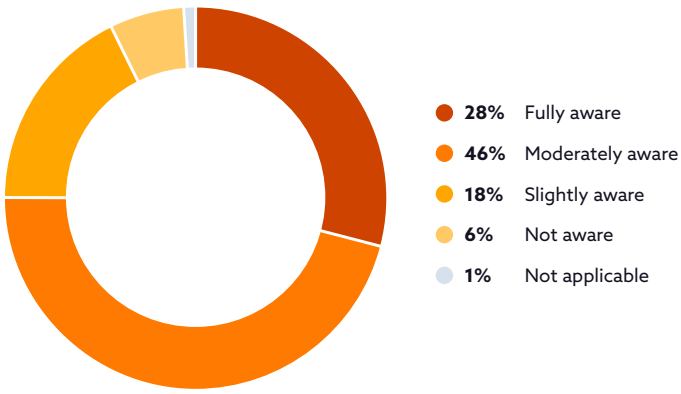
C-level executives and staff responses highlighted a disconnect within a number of areas with respect to AI knowledge and its use within their organizations. C-levels demonstrate a notably higher self-reported familiarity with AI technologies than their staff. For example, 52% of C-suite executives report being very familiar with generative AI (gen AI), in stark contrast to only 11% of staff members.

How clear are you on the potential use cases of AI in cybersecurity?



C-levels report having a clearer understanding of AI use cases, with 51% feeling very clear about them, compared to just 14% of staff. These disparities might indicate a possible overestimation of AI familiarity among C-level executives, or it could suggest a very real difference in knowledge of the topic of AI. This latter implication is supported by the general belief within the industry that leadership is informed and aware of the implications of AI on security, with 74% reporting their leadership is fully or moderately aware. The high levels of awareness are likely due to the keen interest of organizations' leaders in adopting AI within their organizations, with 82% of respondents indicating their executive leadership and boards of directors are pushing for AI adoption.

To what extent is your leadership (e.g., Board of Directors) informed and aware of the implications AI has on security?



This top-down pressure for AI adoption among organizations' leaders indicates that they may have investigated AI technologies and their uses to understand how it could benefit their organization. However, it's worth noting that this approach may not fully align with the actual readiness or understanding at the staff level, potentially leading to implementation challenges, as noted in Key Finding 2.

This may highlight a lack of appreciation for the difficulty and knowledge needed to adopt and implement such a unique and disruptive technology (e.g., prompt engineering).

Overall, the pattern highlights a crucial need for enhanced communication, education, and a more collaborative approach to AI implementation in cybersecurity. The gap between C-suite executives and staff regarding AI technology familiarity and understanding of its implementation necessitates a more inclusive and informed strategy to navigate the evolving landscape of AI in cybersecurity.

Key Finding 4:

2024 Is the Year for AI Implementation – Get Ready for the Revolution

2024 is set to be a revolutionary year for AI implementation in the security sector. Over half (55%) of organizations are planning to implement gen AI solutions.

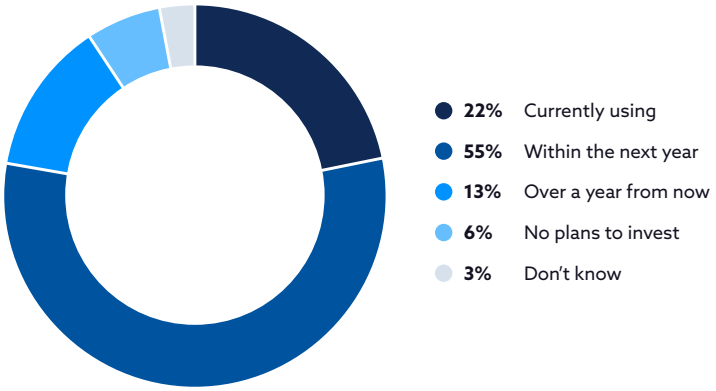
Organizations are exploring a diverse range of use cases for these technologies, with the top use cases being rule creation (21%), attack simulation (19%), and compliance violation detection (19%). However, the distribution of planned use cases is fairly evenly distributed, indicating the potential for AI to have multiple beneficial applications.

How does your organization plan to use Generative AI for cybersecurity? (Select top 3 use cases)

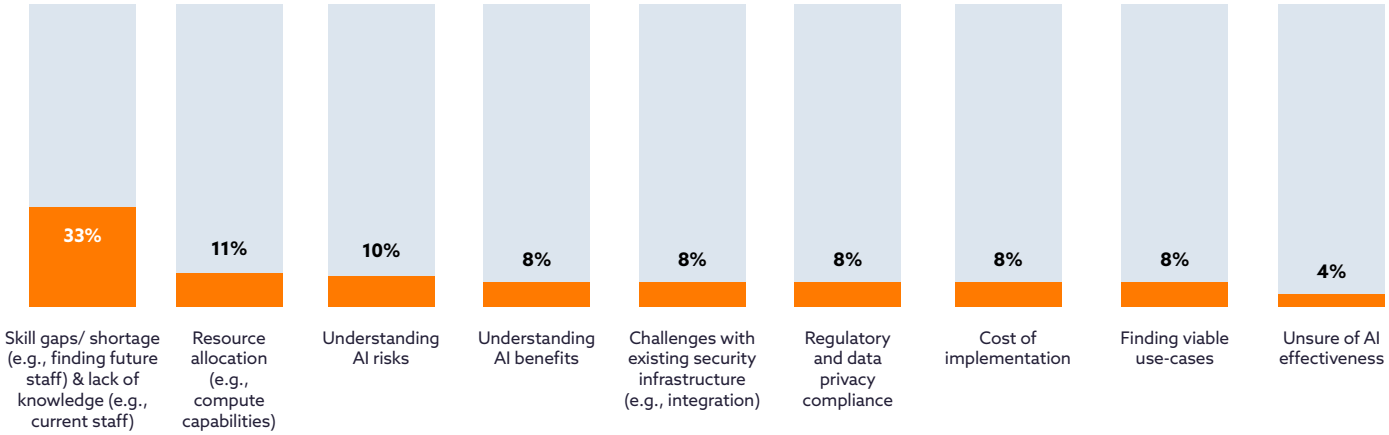
21%	Rule creation	13%	Natural language to search	9%	Forensic analysis
19%	Attack simulation	13%	Threat summarization	9%	Chatbot
19%	Compliance violation monitoring	13%	Data loss prevention, IP protection	8%	Incident summarization
16%	Network detection	11%	User Behavior analysis	8%	Configuration drift
16%	Reduce false positives	10%	Automated report generation	8%	Recommendations for action/ remediation
15%	Training development and support	10%	Endpoint detection	7%	Code analysis
14%	Anomaly classification	9%	Event log summarization		

Despite the excitement and eagerness to implement AI in various ways, there are significant hurdles to overcome. The most prominent challenge is the skills gap and staff shortage, as reported by 33% of respondents - especially high among executives - indicating how top of mind this issue is. Other hurdles were selected far less often: resource allocation (11%) and a full understanding of AI risks (10%). These challenges highlight the need for targeted upskilling, potential hiring of new talent, and a clear strategy for managing advanced AI systems.

In general, is your organization using or planning to use Generative AI solutions?



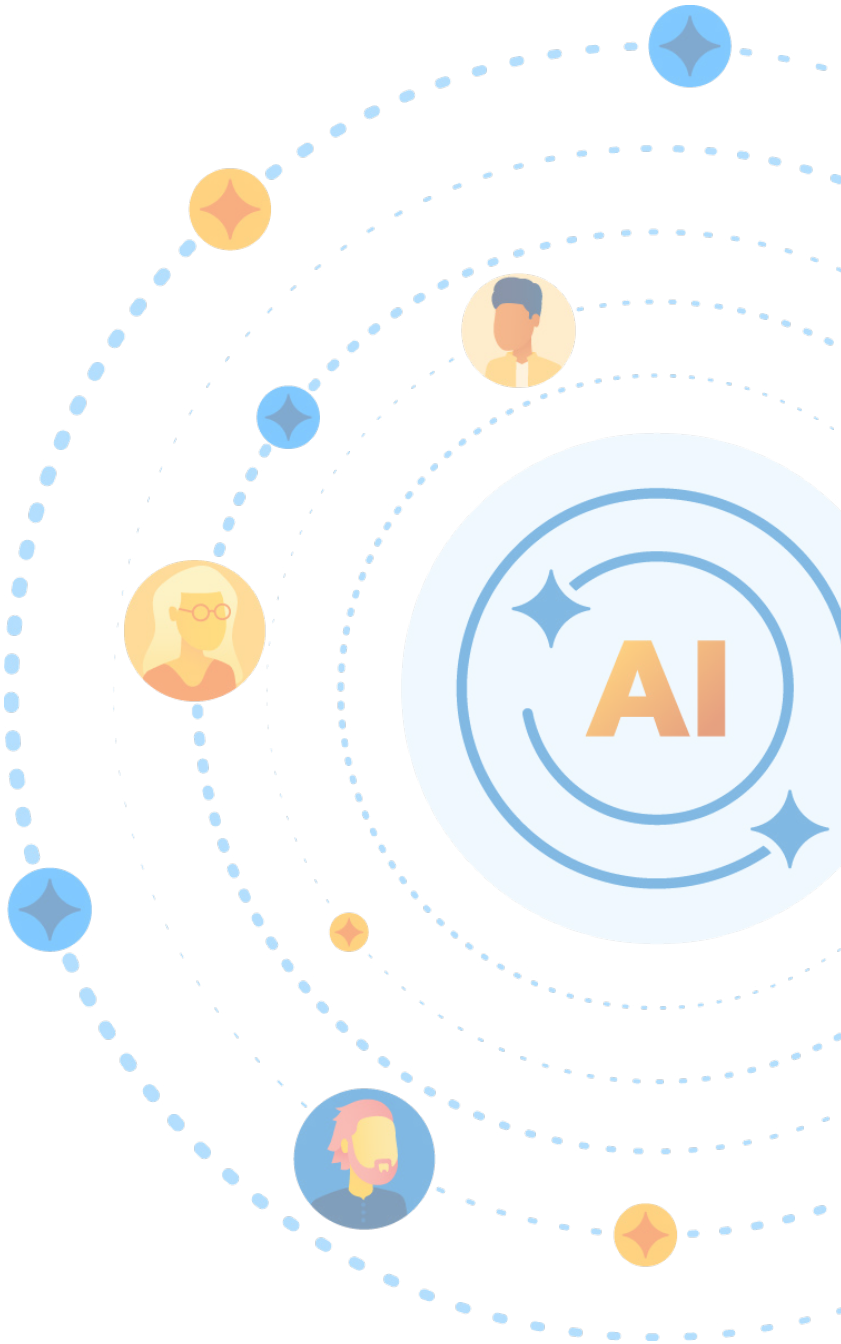
What is the biggest hurdle to getting started with AI in security implementations?



The year 2024 is poised to be pivotal for AI in cybersecurity, driven by growing interests and diverse applications of AI technologies. The push for GenAI adoption is strongly influenced by the board of directors and leadership, underlining the crucial role of executive decision-making in driving technological advancement within organizations. However, the biggest challenges in starting AI initiatives – skills gaps and staff shortages – underscore the need for a strategic approach to developing the necessary expertise and resources for effective AI implementation in cybersecurity.

Conclusion

The current state of AI in cybersecurity is a multifaceted landscape marked by cautious optimism, empowerment over replacement, discrepancies in understanding between C-suite executives and staff, and a strong momentum toward AI implementation in 2024. This complex picture underscores the need for a balanced, informed approach to AI integration in cybersecurity, combining strategic leadership with comprehensive staff involvement and training to navigate the evolving cyber threat landscape effectively.



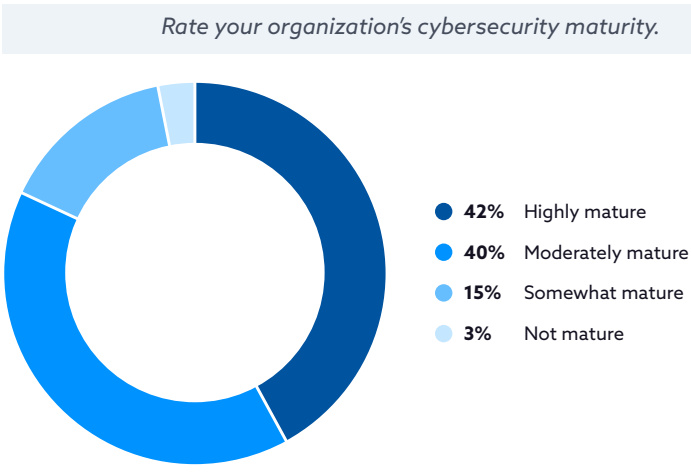
All Survey Findings

Current State of Security

Greatest security challenges for organizations

Most challenges within organizations can be categorized into the "three Ts": toil, threat, and talent. Respondents ranked these challenges within their organization with threat (i.e., threat assessment and prioritization) ranked as the top challenge. This was closely followed by toil (i.e., managing multiple environments and tools). Finally, talent was ranked lowest of these challenges despite the near-constant concern regarding the talent and skills gap in the industry.

Cybersecurity maturity of organizations

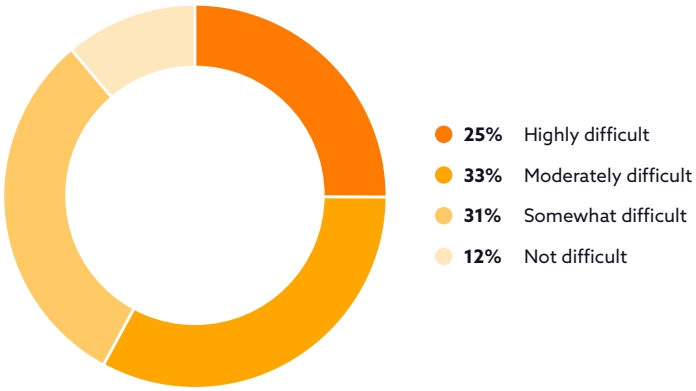


Organizations rated their cybersecurity quite high with 42% rating themselves as highly mature and another 40% as moderately mature. Only 15% reported being somewhat mature and 3% as not mature. It's certainly encouraging to see so few people in the lowest categories, but it is surprising to see so many rating their organization so highly.

Perhaps this is an accurate reflection, but it could also represent over confidence of security professionals in their own work. The latter is potentially supported by the next finding.

Level of difficulty posed by investigating and responding to threats in a timely manner

Rate the level of difficulty of investigating and responding to threats in a timely manner in your organization.

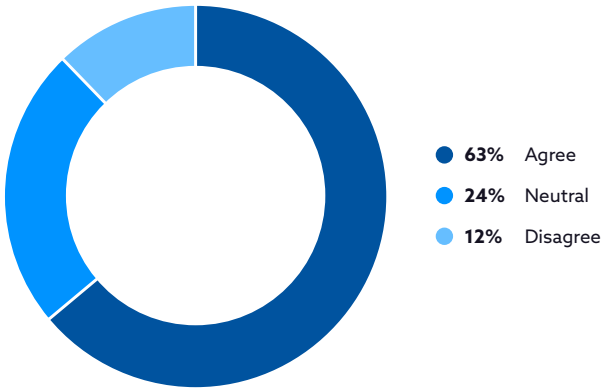


The level of difficulty that investigating and responding to threats poses to organizations seems to vary greatly, but notably despite seeing their organizations are quite mature, very few reported no difficulty (12%) with this task. Relatively even amounts of organizations reported this as somewhat difficult (31%) or moderately difficult (33%). With nearly a quarter reporting this is a highly difficult task. Perhaps security professionals are not considering this metric when assessing their maturity. It also could indicate that this is a difficult task regardless of how mature your organization is.

Perception and Attitudes Towards AI in Cybersecurity

Opinions on AI as a Security Enhancer in Organizations

Artificial Intelligence (AI) will improve security within our organization.

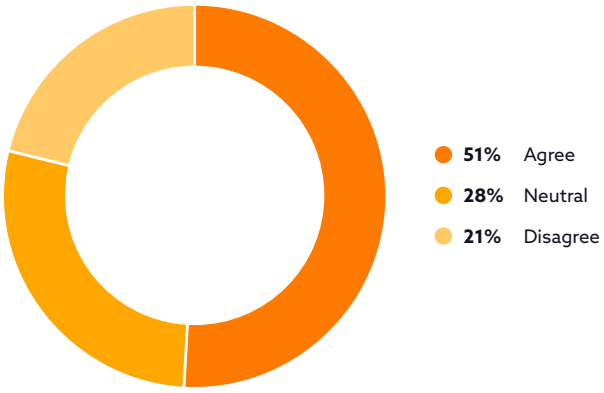


Security professionals have an optimistic view about the impact of AI on improving security within their organizations. A majority (63%) agree that AI will enhance security, largely driven by expectations of increased automation and the technology's potential to assist in security measures. However, there is a notable portion of respondents (24%) who remain neutral, possibly reflecting uncertainty or a wait-and-see approach. This could be attributed to concerns about keeping pace with the rapid advancements and increased complexity of AI technology. A smaller but significant group (12%) disagrees with the notion that AI will improve security, possibly due to concerns about nefarious actors exploiting AI or the challenges in managing such advanced

technology. These mixed responses might also be influenced by the current position in the hype cycle for AI technology, suggesting that expectations and confidence levels may evolve as familiarity and understanding of AI's capabilities in cybersecurity grow.

Concerns about over reliance on AI for cybersecurity

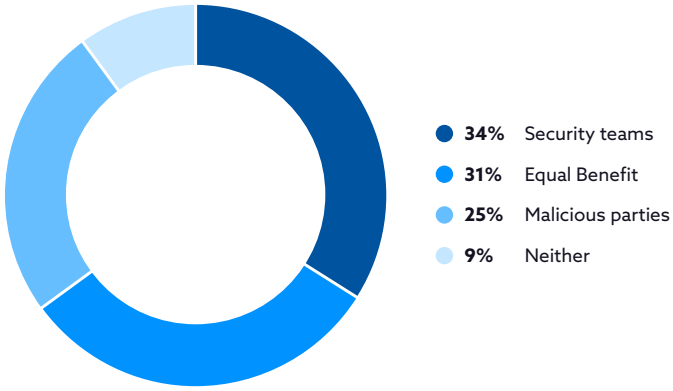
Are you concerned about the potential risks of over-reliance on AI for cybersecurity?



There is some skepticism about AI. Some security professionals see the potential risks of over-reliance on AI for cybersecurity, revealing a nearly even split in opinion among respondents. About 51% agree that there are concerns about depending too much on AI, reflecting a degree of skepticism about removing significant human elements from cybersecurity. This concern likely stems from the recognition that AI systems, while advanced, are not infallible and may require human oversight for monitoring and resolving issues. Additionally, there's an awareness that unforeseen challenges may emerge as AI is more widely used in cybersecurity contexts. A notable 28% of respondents remain neutral, indicating either uncertainty or a balanced view of AI's benefits and risks. Meanwhile, 21% disagree with the concern, possibly suggesting confidence in AI's reliability or a belief in the sufficiency of existing safeguards and response mechanisms to address potential AI shortcomings. This division of opinion highlights the complexity of integrating AI into cybersecurity, balancing technological advancement with the need to retain critical human judgment and oversight.

Security benefits and risks with AI

In your opinion, would AI be more beneficial to security teams or malicious 3rd parties?



Security professionals have a cautious and potentially nuanced perspective of who will benefit from AI more: security professionals or malicious parties. About 34% believe that AI will primarily benefit security teams, suggesting a general optimism about AI's role in bolstering cybersecurity defenses. However, a closely matched 31% see AI as offering equal benefits to both security

teams and malicious actors, highlighting an awareness of the dual-use nature of AI technologies in cybersecurity. This is further underscored by the 25% who think AI might be more advantageous to malicious parties, acknowledging the potential threat if AI is used with malicious intent.

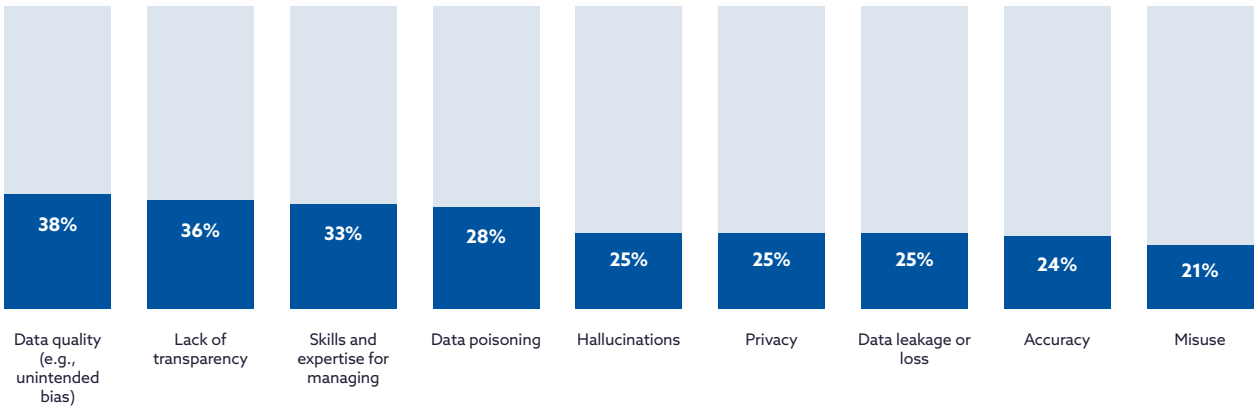
A smaller segment (9%) feels that it's neither clearly beneficial to security teams nor malicious 3rd parties, or it's too early to tell. This reflects an underlying sentiment that, given the early stage of AI's integration into cybersecurity, there's still a lot of unknowns about its full impact and potential. The results indicate a cautious optimism where respondents generally lean towards AI helping security teams slightly more, but there's a clear recognition of the significant risks if AI tools fall into the wrong hands or are exploited by adversaries.

Greatest concerns with AI in security

Security professionals express a range of concerns regarding the implementation of AI in cybersecurity, reflecting the complexity and multifaceted nature of AI integration. The top concern, cited by 38%, is data quality, specifically the risk of unintended bias, which is closely linked to concerns about accuracy (24%). This connection is significant, as AI is often perceived as an objective tool; thus, the quality and integrity of data fed into AI systems directly influence the accuracy and reliability of their outputs. Similarly, 36% are wary of the lack of transparency in AI systems, highlighting the 'black box' nature of some AI algorithms that can make understanding and trust in AI decisions challenging.

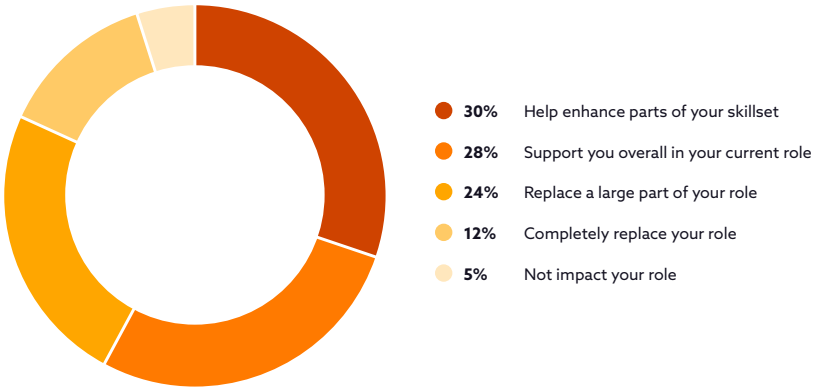
Other notable concerns include skills and expertise for managing AI, mentioned by 33% of professionals, indicating an awareness of the need for specialized knowledge to effectively integrate and oversee AI technologies. Data poisoning and hallucinations, concerns for 28% and 25% respectively, are closely related issues, along with data leakage or loss, and privacy concerns, each noted by 25% of respondents. These issues are relatively less understood but nonetheless acknowledged as potential risks that could emerge with more extensive AI usage. The broad range of concerns suggests that security professionals are cautiously considering all possible implications of AI, recognizing that the technology's rapid evolution means that today's secondary concerns could become tomorrow's primary challenges.

What are your biggest concerns regarding AI in security? (Select up to 3)



Impact of AI on current cybersecurity roles

Please select the option that best reflects your opinion about AI's potential impact on your role. Over the next 5 years, AI will...



Within the cybersecurity field, professionals widely anticipate that AI will have a significant impact on their roles over the next five years. This sentiment reflects the disruptive nature of AI in the workplace. A substantial number (58%) perceive AI as a tool that will support and enhance their current roles. Specifically, 30% believe AI will help enhance certain aspects of their skillset, while 28% see it as an overall support to their existing functions. This perspective underscores the potential of AI to augment human capabilities, especially in automating manual and routine tasks. Technologies like AI-driven chatbots and analytical tools are expected to streamline operations and increase efficiency, assisting security professionals in more effectively managing their workload. Freeing their time up from more menial tasks to focus on more complex and creative elements of their job role.

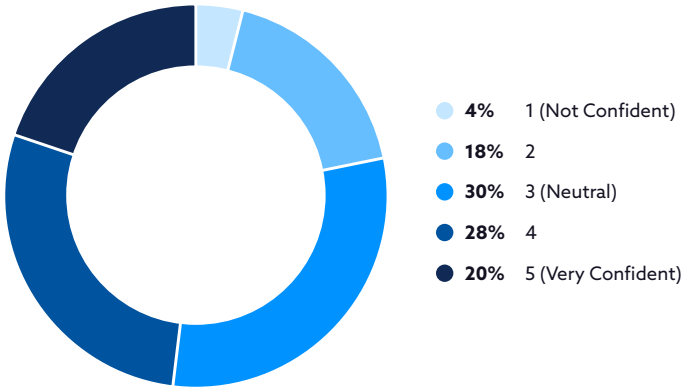
There's a notable concern among these professionals about AI's ability to replace human roles. About 24% foresee AI replacing significant parts of their job, and 12% even predict a complete replacement of their role. This apprehension is more pronounced in aspects of cybersecurity work that are heavily manual or repetitive, where AI's capabilities for automation are most directly applicable. It's important to recognize that while AI is seen as a supportive and enhancing tool, its potential to disrupt existing job structures in cybersecurity is also a key consideration. Security professionals are thus faced with the dual challenge of leveraging AI for its benefits while also preparing for the shifts it may bring in the job market, highlighting the importance of adaptability and continuous skill development in this rapidly evolving field.

Confidence in organizations' skills to execute a security strategy leveraging AI

In the cybersecurity sector, there's a cautiously optimistic view regarding organizations' readiness to leverage AI. About 48% of professionals express confidence in their organization's ability to implement AI strategies effectively, with 28% feeling reasonably confident and 20% very confident. This level of assurance is intriguing, considering the nascent stage of AI in this field. It suggests that many professionals might be optimistic about their preparedness or overlook the intricacies of AI integration, a classic scenario of an unknown unknown.

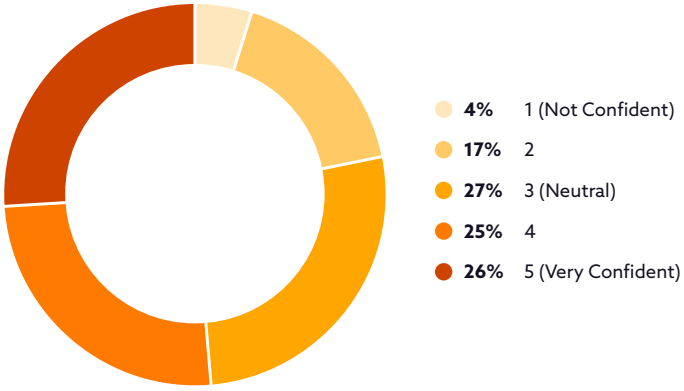
Conversely, a notable 30% remain neutral, indicating either a balanced recognition of their capabilities or uncertainty about the challenges AI might pose. The remaining 22% show less confidence, including 18% who are somewhat unconfident and 4% who are not confident at all. This spread in confidence levels across the cybersecurity community points to a complex landscape where some AI applications are seen as straightforward and readily deployable, while others, more complex and novel, evoke caution and uncertainty.

How confident are you about your organization's skills to execute a strategy for leveraging AI in security?



Confidence in organizations' skills to execute a security strategy to protect AI systems

How confident are you about your organization's skills to execute a security strategy for protecting AI used in your core business/mission?



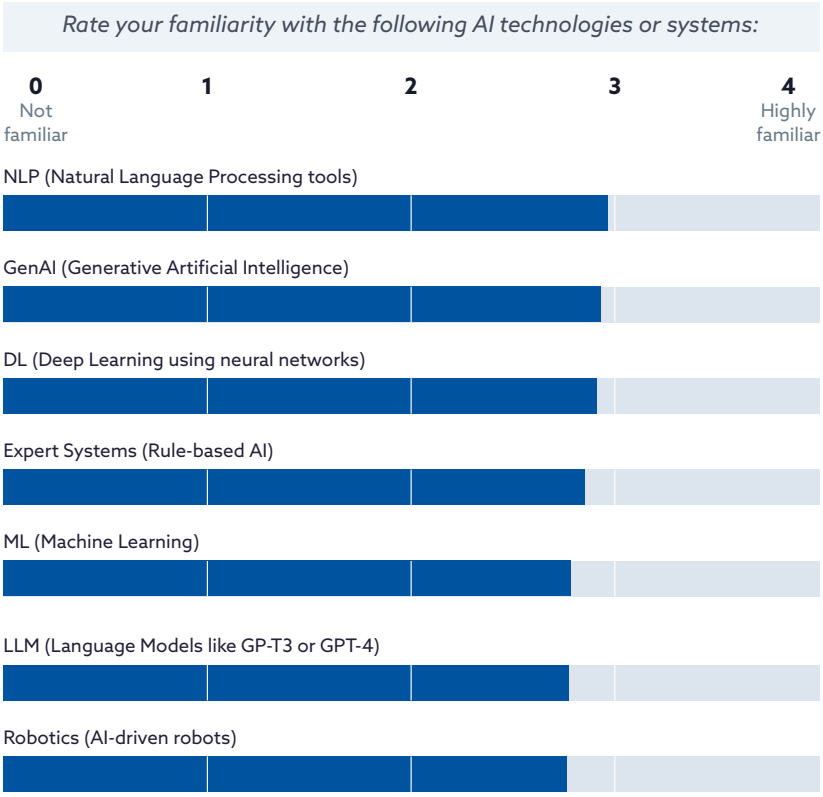
In assessing confidence levels regarding the execution of a security strategy for protecting AI within core business or mission functions, there is a comparable yet slightly more confident stance among professionals compared to their views on leveraging AI in security. About 51% of respondents lean towards confidence, with 25% feeling reasonably confident and 26% very confident. This slightly higher confidence level, particularly in the 'very confident' category, is notable. However, it also suggests a potential underestimation of the unique challenges and threats associated with securing AI systems, possibly due to a perception of AI as just another application in the business environment.

On the other hand, 27% of respondents adopt a neutral stance, perhaps reflecting a cautious acknowledgment of the complexities involved or an uncertainty about the emerging threats specific to AI. The lower confidence spectrum includes 17% who are somewhat unconfident and 4% who are not confident at all. The overall trend indicates that while many professionals are confident in their organization's ability to protect AI systems, there's still a significant portion that recognizes the unknowns and potential underestimation of threats.

Industry Familiarity with AI

Familiarity with AI technologies and systems

The survey results regarding familiarity with various AI technologies and systems across the cybersecurity sector show a general trend of moderate to somewhat familiarity. Weighted averages for technologies like Natural Language Processing (NLP), Generative Artificial Intelligence (gen AI), Deep Learning, Expert Systems, Machine Learning, LLM (Language Models like Gemini or GPT-4), and Robotics fall within a narrow range. This indicates that, generally, if professionals are familiar with one of these technologies, they likely have a comparable understanding of the others.



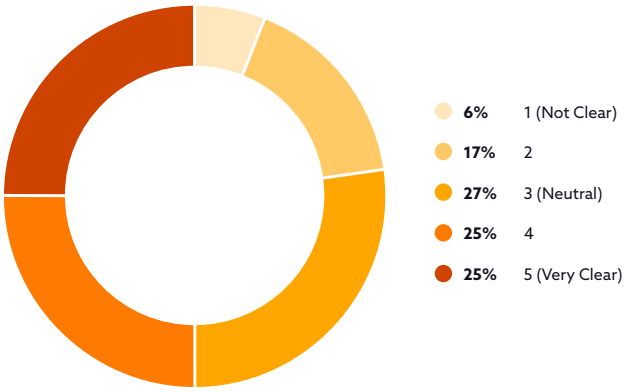
Interestingly, there's a slight inclination towards older, more established terms like NLP and Deep Learning, which score marginally higher than newer terms like LLM and gen AI. This could suggest a conflation between gen AI and popular tools like ChatGPT, indicating that while such tools are well-known, there may not be a deep understanding of the broader category of gen AI. This surface-level familiarity across various AI technologies might also contribute to the observed overconfidence in implementing AI strategies, as professionals might not fully grasp the complexities of these technologies.

This lack of deep understanding raises questions about the effectiveness of current strategies and the need for further education in these areas. Comparatively, C-level executives report higher familiarity with all AI categories compared to staff. This discrepancy in familiarity may be due to the pressure from leadership within organizations to explore adoption of AI. It likely requires leadership in the C-suite to familiarize themselves with a wide variety of AI technologies to identify which may provide the greatest benefits to their organizations. This gap in understanding underscores the importance of comprehensive education and training in AI technologies to ensure their effective and secure implementation especially for staff that is responsible for the implementation.

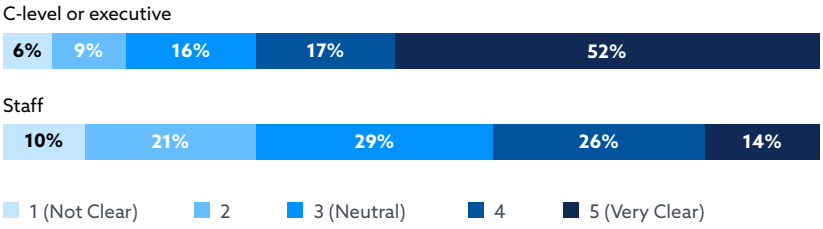
Clarity of potential AI use cases in cybersecurity

The understanding of potential AI use cases in cybersecurity shows a split perspective, with professionals divided on their clarity regarding AI applications. Overall, 50% of respondents feel clear about AI use cases, with 25% somewhat clear and another 25% very clear. However, the other half of the respondents express less certainty, with 27% neutral, 17% somewhat unclear, and 6% very unclear about AI's potential roles.

How clear are you on the potential use cases of AI in cybersecurity?



How clear are you on the potential use cases of AI in cybersecurity?

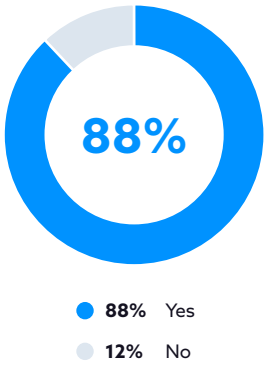


A notable difference emerges when comparing responses from C-level executives and staff. Among C-level executives, a significant 52% report being very clear on AI use cases in cybersecurity, compared to only 14% of staff feeling the same. This stark contrast might suggest that C-level executives have a more aspirational or vision-oriented understanding of AI, focusing on broader goals and potentials, whereas staff, who are typically closer to the practical implementation, might be more aware of the complexities and uncertainties involved. It's interesting to note that staff usually tend to buy into new technologies like AI earlier than the C-suite, yet in this case, their lower clarity could be influenced by the operational challenges they foresee. The high level of awareness and clarity among C-level executives aligns with the increasing presence of AI in the news and its growing significance in the corporate zeitgeist.

Awareness of AI security frameworks

A significant 88% of security professionals are aware of existing AI security frameworks, such as those based on NIST guidelines in the US. However, it's crucial to note that awareness does not necessarily equate to usage or deep understanding of these frameworks. Only 12% of respondents report not being aware of any AI security frameworks, highlighting the widespread recognition of these standards in the cybersecurity community yet leaving room for further exploration of their practical application and comprehension.

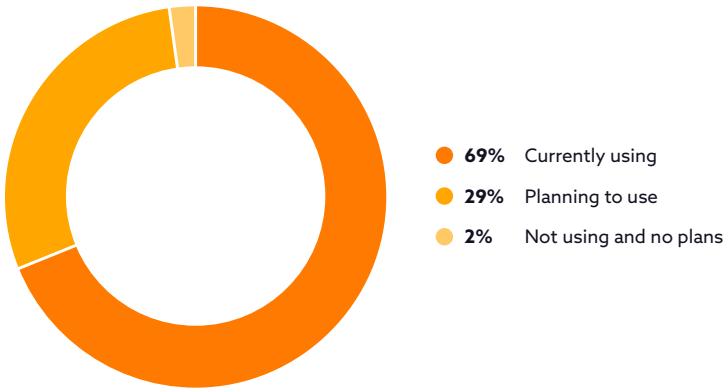
Are you aware of any existing AI security frameworks?



General Plans to Use AI

Current use of AI products in general

Does your organization use or plan to use AI products in general?

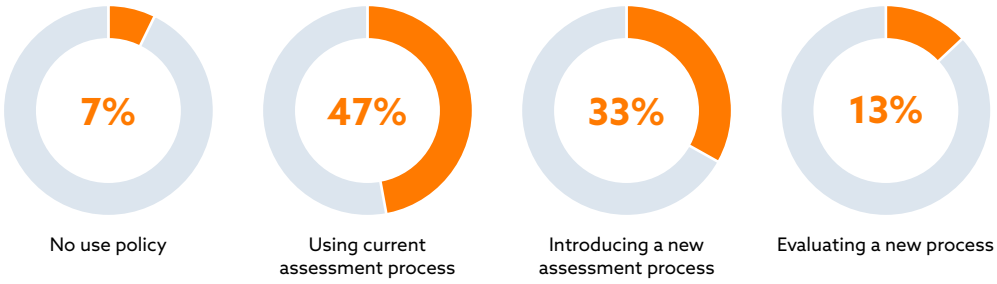


The use or planned use of AI products in organizations suggests a few possibilities: AI may be integrated into many products that organizations are using, but staff might not be fully aware of this integration or may not recognize these as AI-driven products. Alternatively, it could indicate a gap in understanding or communication within the organization, where C-level executives believe they are utilizing AI more extensively than their staff are aware, or they might overestimate their actual use of AI technologies. This discrepancy underscores the need for clearer communication and education about AI applications and usage within organizations, ensuring that executives and staff consistently understand how AI is being leveraged in their work environment.

Evaluation, assessment, or procurement process of AI products or services

In assessing the adoption of evaluation, assessment, or procurement processes for GenAI and AI-specific products, survey results show a divide in organizational strategies. Nearly half of the respondents (47%) rely on their current assessment processes, suggesting a level of adaptability of existing frameworks to AI technologies. However, almost an equal proportion (46%)—comprising those introducing new assessment processes (33%) and those evaluating new processes (13%)—are actively seeking or developing AI-specific evaluation methods. This indicates a recognition of AI's unique challenges that might not be fully addressed by traditional approaches. The divergence in strategies is more pronounced when considering organization size: larger organizations, particularly those with over 100 employees, predominantly use current processes (87%), while smaller organizations (48%) are more inclined to develop new approaches, highlighting the varying capacities and needs in AI integration across different scales of business operations.

Do you have an evaluation, assessment, or procurement process designed for Gen AI or AI-specific products and services?



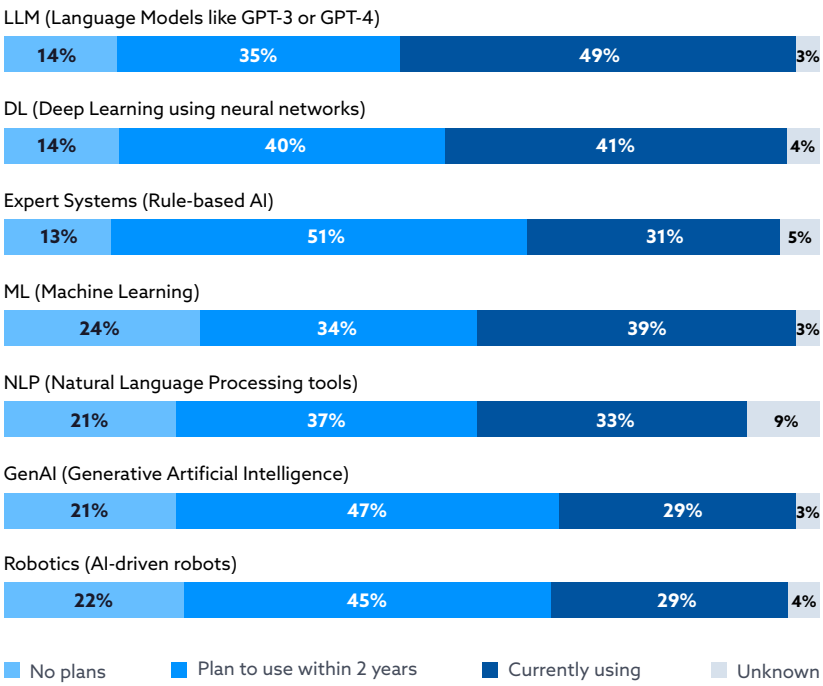
Current and planned use of AI technologies

The survey on AI technology usage within organizations reveals diverse adoption patterns across different AI systems. Large Language Models are currently in use by 49% of the respondents, while 35% plan to use them within the next two years, and 14% have no plans for their adoption. This trend of current usage and future planning is similar across other technologies: Deep Learning is currently used by 41%, with 40% planning future use. Expert Systems are currently at 31% usage, with a notable 51% planning to implement them. Machine Learning and Natural Language Processing tools show a balanced mix of current usage (39% and 33%, respectively) and future plans (34% and 37%, respectively).

Interestingly, there seems to be a sense of obligation to keep pace with technological advancements, as indicated by the consistent number of respondents planning to adopt various AI technologies within two years. This could explain why 47% are planning to use Generative AI (GenAI) and 45% are looking at Robotics, despite 21% and 22% respectively having no plans to use these technologies. This highlights a potential trend where organizations feel the need to stay technologically relevant, even if they currently do not see an immediate application for these

AI systems. Additionally, there's a perceptible discrepancy between C-level executives and staff in their understanding of AI usage within their organizations. C-level executives tend to report higher current use of these tools, whereas staff members are more inclined to believe that their organizations are planning to adopt these technologies in the next two years. This difference suggests a gap in awareness or communication about the actual stage of AI integration within their organizations.

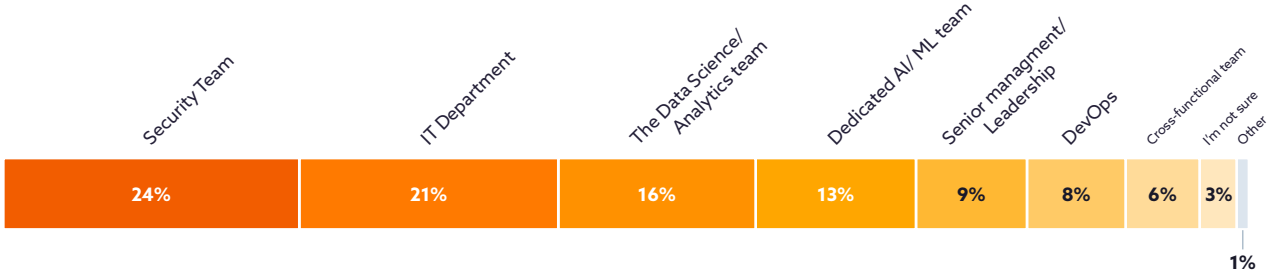
Which of the following AI technologies or systems are you using in your organization? (Select all that apply)



Primary team responsible for AI deployment

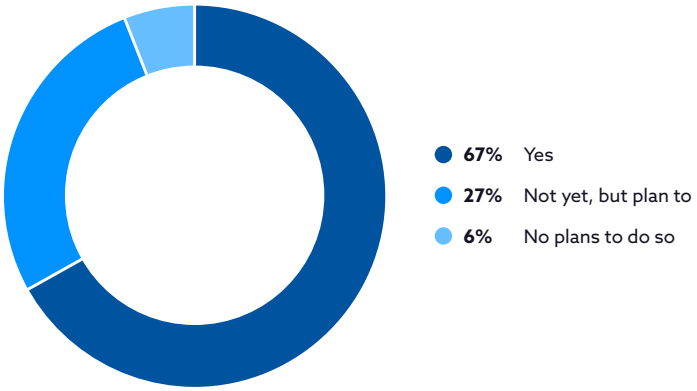
In the realm of AI deployment in security products, the responsibility predominantly falls on the Security Team and IT Department, with 24% and 21%, respectively taking the lead. This is followed by the Data Science/Analytics team and a Dedicated AI/ML team, handling the task in 16% and 13% of organizations. Interestingly, Senior Management/Leadership and DevOps teams play a smaller yet significant role, at 9% and 8%, respectively. This distribution highlights a trend where AI deployment is often managed by teams directly involved in technical and security aspects, although cross-functional collaboration and senior leadership also play crucial roles in guiding AI strategies.

Which team is primarily responsible for AI deployment in your organization?



Testing AI capabilities for security

Have you tested any AI capabilities for security in your organization?

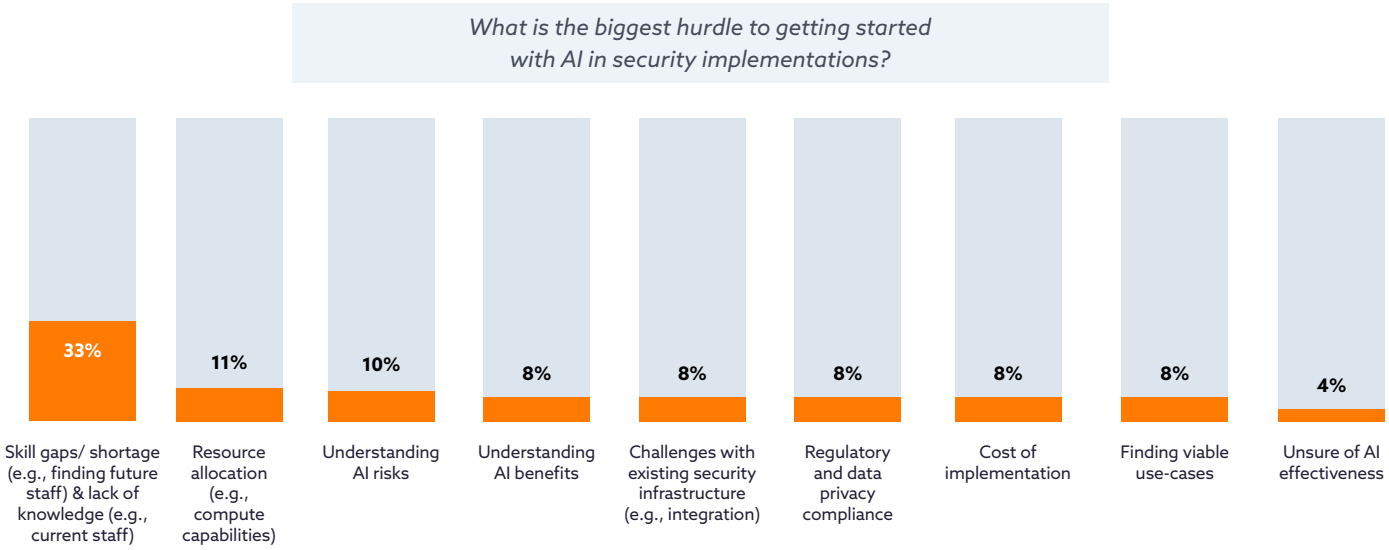


A high number of security professionals report testing AI capabilities for security in organizations, with 67% affirming that they have tested AI for security purposes specifically. This significant percentage suggests that AI integration into cybersecurity is not just a concept but a practical reality for many. This widespread testing could be attributed to AI functionalities being incorporated into existing product suites, making it more accessible and easier for organizations to adopt and experiment with or use LLM agents. Furthermore, 27% of respondents are in the planning stages of testing AI capabilities, indicating a growing trend and recognition of AI's potential in enhancing security measures. On the other hand, a small portion (6%) have no plans to engage with AI for security, possibly due to lack of resources, expertise, or skepticism about AI's effectiveness in their specific context.

Biggest hurdles for implementing AI in security

The survey results reveal that the most significant hurdle to implementing AI in security is the skill gaps and shortage of knowledgeable staff, which is highlighted by 33% of respondents. This dual challenge of finding future staff with the necessary skills and enhancing the knowledge of current staff reflects the complex nature of AI in cybersecurity, requiring both specialized cybersecurity knowledge and a continuous understanding of evolving AI technologies. Addressing these skill-related issues is fundamental, as it could potentially alleviate other downstream challenges such as understanding AI risks and benefits, integrating AI with existing security infrastructure, and effectively managing regulatory and data privacy compliance.

Other notable hurdles include resource allocation (11%), understanding AI risks (10%), and the cost of implementation (8%), among others. Surprisingly, concerns like regulatory and data privacy compliance and the cost of implementation, which are traditionally viewed as significant barriers, are not the foremost concerns in this context. This might indicate an anticipation of long-term cost savings and a focus on current rather than future regulatory scenarios. The responses also show a general concern across almost all options, indicating that while there is no single overwhelming obstacle, the journey to AI integration in cybersecurity is multifaceted and complex. This widespread concern across various aspects of AI implementation underscores the need for a holistic approach in adopting AI in security, one that addresses skill gaps, resource needs, and regulatory challenges in a balanced manner.

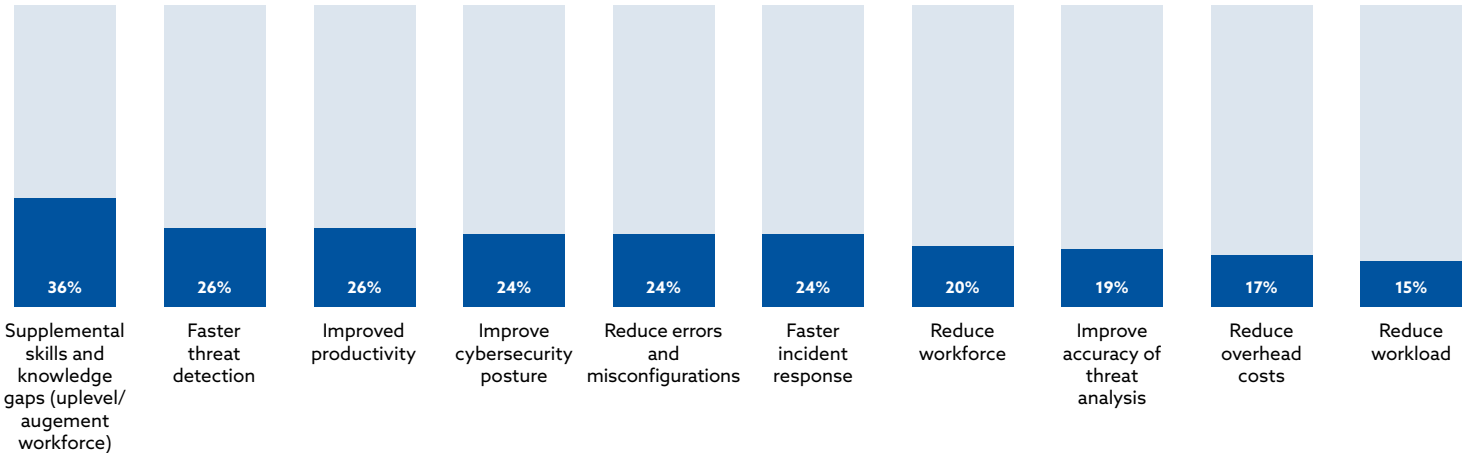


Desired outcomes from AI implementations

Organizations' desired outcomes for implementing AI in security teams highlight a strong inclination towards supplementing skills and knowledge gaps, with 36% of respondents identifying this as a key goal. This aligns with the previously noted challenge of skill gaps and lack of knowledge in AI applications within cybersecurity. This also aligns with the previous finding that AI is expected to support job roles rather than replace them completely. By integrating AI, organizations aim to uplevel and augment their workforce, addressing these gaps and enhancing their team's capabilities. This focus on enhancement rather than outright replacement of the workforce is further evidenced by the lower priority given to reducing the workforce (20%), indicating a preference for AI as a tool for empowerment and support.

Other significant desired outcomes include faster threat detection and improved productivity, each selected by 26% of respondents, as well as enhancing the overall cybersecurity posture, reducing errors and misconfigurations, and accelerating incident response, each at 24%. These goals underscore a desire for AI to bring efficiency and effectiveness to cybersecurity operations. Interestingly, while improved productivity is a key expectation, it is not the dominant outcome, possibly reflecting a nuanced view where the focus is more on quality (such as accurate threat detection and response) rather than quantity of work. However, the fact that a notable portion of respondents (15% to 20%) also look for AI to reduce workforce, overhead costs, and workload suggests a balanced expectation where AI is seen as a means to optimize and streamline security operations while also enhancing the performance and capabilities of the existing human workforce.

What are your desired outcomes when it comes to implementing AI in your security team?

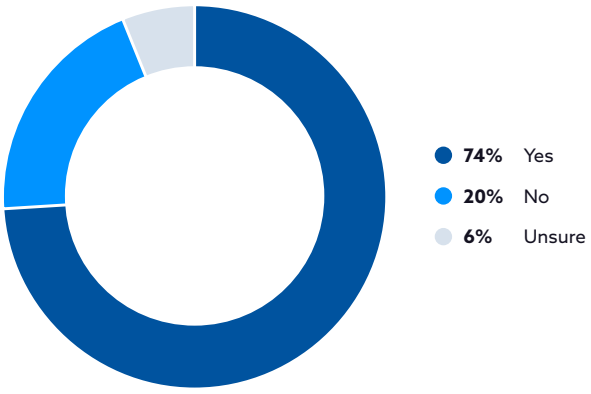


AI Staff, Leadership, and Training

Creating a team for governing the secure use of AI

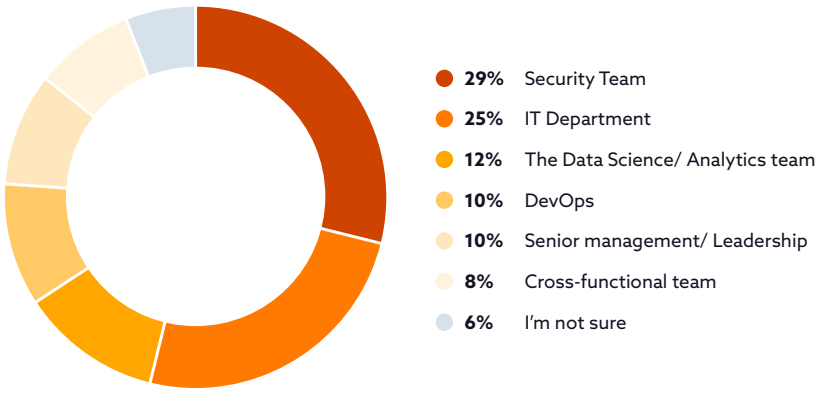
A substantial 74% of organizations are planning to create teams dedicated to governing the secure use of AI, emphasizing the serious consideration companies are giving to AI integration. This move towards establishing specialized teams for policy development, AI product procurement, and ensuring responsible and ethical use, signals a clear recognition of AI's transformative impact on security roles. Rather than replacing existing functions, AI is leading to the evolution and expansion of organizational roles, requiring new governance structures and expertise. This approach underscores the shift in the security landscape where AI is not merely an additional tool, but a significant factor that necessitates thoughtful integration and management. The fact that only 20% are not forming such teams, and 6% are unsure, further highlights the widespread acknowledgment across the industry of the need for dedicated oversight and specialized skills to harness AI's potential effectively and securely.

Are you creating a team to govern the secure use of AI within your organization? (e.g., policy development, AI features/ product procurement, responsible/ ethical use of)



Team responsible for securing AI systems

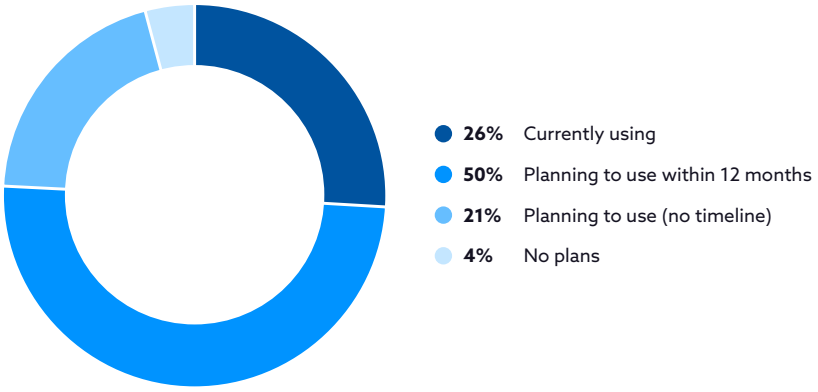
Which team will be responsible for securing AI systems within your organization?



The responsibility for securing AI systems within organizations predominantly falls to the Security Team and IT Department, with 29% and 25% respectively taking the lead. These figures mirror the similar distribution seen in AI deployment responsibilities, reflecting a consistent approach where the primary technical teams are entrusted with both implementing and securing AI technologies. This allocation of responsibilities underscores the crucial role these departments play in the effective and safe integration of AI into organizational infrastructures.

Current or planned use of training programs related to AI and cybersecurity

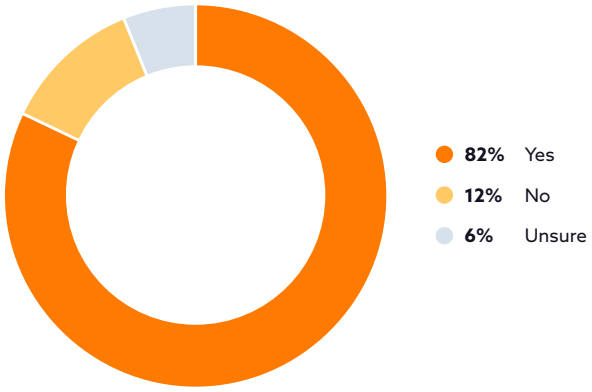
Is your organization using or planning to use training programs for staff related to AI and cybersecurity?



The survey indicates a strong inclination towards investing in training programs for staff on AI and cybersecurity within organizations. A notable 26% of organizations are already using such training programs, demonstrating a proactive approach to equipping their workforce with the necessary skills and knowledge. A significant 50% plan to implement these training programs within the next 12 months and 21% of organizations have plans to introduce such training, although without a specific timeline. This highlights the widespread recognition of the importance of continuous learning in the rapidly evolving fields of AI and cybersecurity. Only a small fraction (4%) have no plans for such training, suggesting that most organizations are focused on solving the skills and knowledge gaps they've previously identified as concerns with AI use.

Pressure from executive leadership to adopt AI

Is your executive leadership (e.g., Board of Directors) pushing for AI adoption?

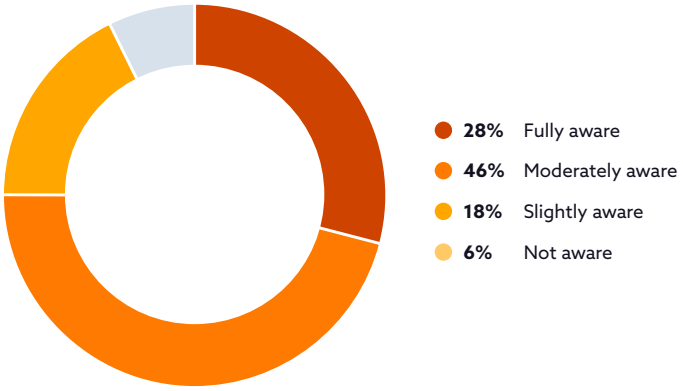


The push for AI adoption from executive leadership, as indicated by 82% of respondents, sheds light on why many C-level executives report higher levels of familiarity with AI technologies and their applications. This top-down pressure likely stems from a recognition of AI as a competitive advantage in the modern business landscape. When executive teams, including Boards of Directors, prioritize AI integration, it creates an organizational culture that values and focuses on AI capabilities, thereby encouraging a deeper understanding and engagement with AI at all levels of the organization. This focus at the top echelons of management not only drives the strategic adoption of AI but also likely influences the reporting of higher familiarity with AI among C-level executives.

Perception of leadership's knowledge of AI implications on security

There is a tendency among organizational leadership to be more informed and aware of AI's implications on security than not. Approximately 28% of leaders are reported as being fully aware, showing a proactive initiative among a significant portion of upper management to deeply understand AI's impact on security. An additional 46% are moderately aware, suggesting that while they have a general understanding, there may be gaps in their full comprehension of AI's complexities and nuances in the security domain. This awareness may be informed by information from security teams and current news, highlighting the importance of continuous and high-level communication within organizations. An interesting point to note is that there is no substantial difference in this awareness between C-level executives and staff, indicating a unified perception of leadership's awareness. This collective view is a point-in-time measurement and is subject to change as rapidly as the AI and cybersecurity landscape itself evolves.

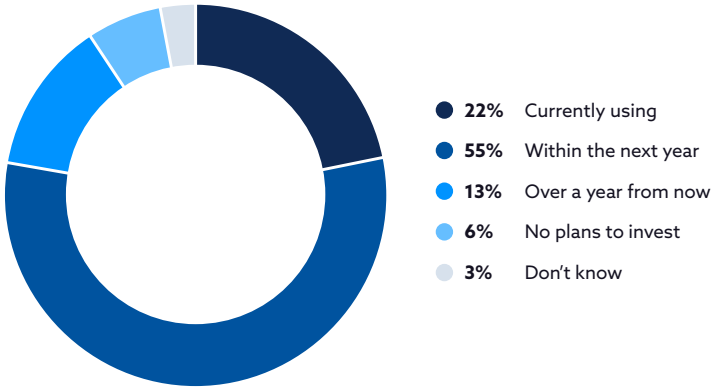
To what extent is your leadership (e.g., Board of Directors) informed and aware of the implications AI has on security?



GenAI Plans for Cybersecurity

Current and planned use of GenAI solutions

In general, is your organization using or planning to use Generative AI solutions?



The anticipation for 2024 as a significant year for the adoption of Generative AI (GenAI) solutions is evident from the survey results. Currently, 22% of organizations are using GenAI, but a remarkable 55% plan to adopt these solutions within the next year, signaling a substantial surge in GenAI integration. An additional 13% expect to use GenAI solutions over a year from now, while only 6% have no plans to invest in this technology. Regardless, the data points to 2024 as a pivotal year, with a significant movement towards embracing GenAI across various organizations.

Planned uses for GenAI in cybersecurity

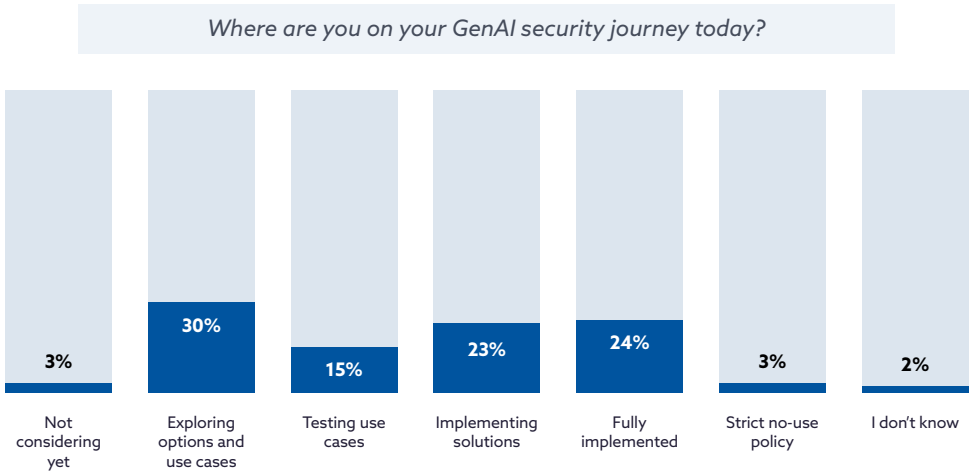
The planned use of GenAI in cybersecurity reflects a broad exploration of potential applications across various organizations. The survey results show a relatively even distribution among the top five use cases, indicating a diverse range of areas where GenAI is expected to make an impact. Rule creation emerges as the leading use case, with 21% of organizations aiming to leverage GenAI to develop more sophisticated security protocols. This is closely followed by attack simulation and compliance violation monitoring, each at 19%, highlighting GenAI's potential to enhance proactive security measures and regulatory adherence. Additionally, 16% of respondents are looking to use GenAI for network detection, aiming to improve the identification of network threats. Another 16% focus on using GenAI to reduce false positives, underscoring its potential to refine alert accuracy and efficiency. This spread of interest across different use cases suggests that organizations are not only eager to adopt GenAI but are also keen on customizing its applications to meet specific security needs, thereby maximizing its benefits in the evolving landscape of cybersecurity.

How does your organization plan to use Generative AI for cybersecurity? (Select top 3 use cases)

21%	Rule creation	**13%**	Natural language to search	**9%**	Forensic analysis
19%	Attack simulation	**13%**	Threat summarization	**9%**	Chatbot
19%	Compliance violation monitoring	**13%**	Data loss prevention, IP protection	**8%**	Incident summarization
16%	Network detection	**11%**	User Behavior analysis	**8%**	Configuration drift
16%	Reduce false positives	**10%**	Automated report generation	**8%**	Recommendations for action/ remediation
15%	Training development and support	**10%**	Endpoint detection	**7%**	Code analysis
14%	Anomaly classification	**9%**	Event log summarization		

Current status of GenAI security journey

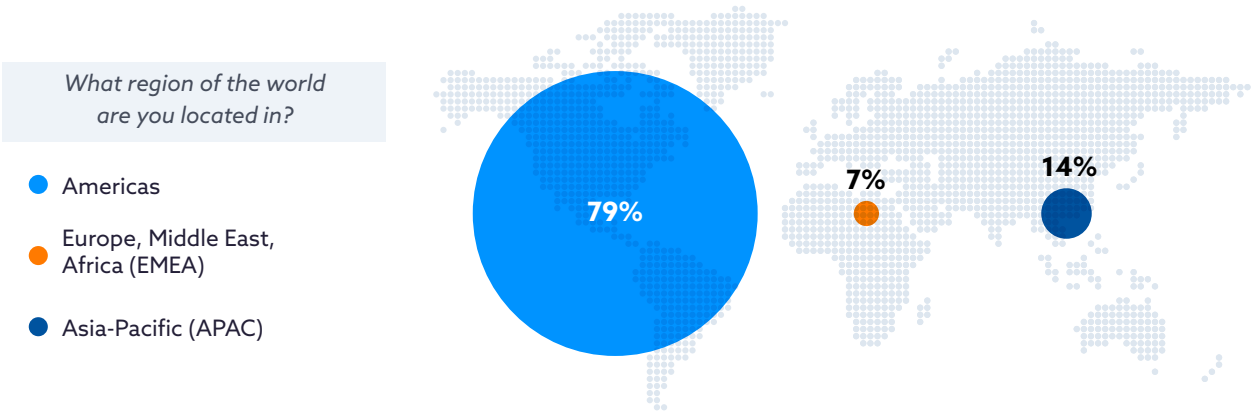
The majority of organizations are in the early stages of their GenAI journey in the realm of cybersecurity, with a strong focus on exploration and implementation. Approximately 30% are currently exploring options and use cases, indicating a proactive approach to understanding the potential of GenAI in enhancing their security posture. This phase of exploration is crucial as it lays the groundwork for practical applications. Additionally, 15% are in the testing phase, experimenting with specific use cases to gauge the effectiveness and applicability of GenAI solutions. The implementation phase sees a combined 47% of organizations, with 23% currently implementing solutions and 24% having fully implemented GenAI, suggesting a rapid advancement from theoretical exploration to practical deployment. A negligible 3% are not considering GenAI yet, and an equal 3% maintain a strict no-use policy. These findings reflect a trend towards embracing GenAI in cybersecurity, with most organizations actively engaged in the initial phases of exploring and integrating these innovative solutions.



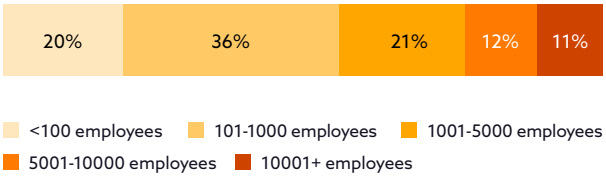
Demographics

The survey was conducted online by CSA in November 2023 and received 2,486 responses from IT and security professionals from organizations of various sizes across the Americas, APAC and EMEA.

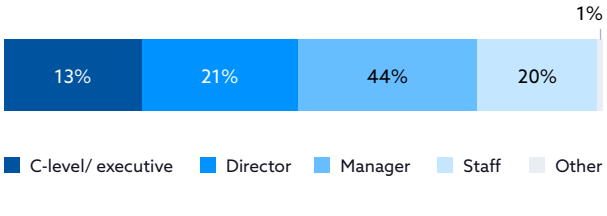
What region of the world are you located in?



What is the size of your organization?



What is your position within your organization?



Which of the following best describes the principal industry of your organization?