MixMode®

State of AI in Cybersecurity Report 2025

Ponemon Institute© Research Report

Sponsored by MixMode

Ponemon INSTITUTE

© MixMode, Inc.

Forward

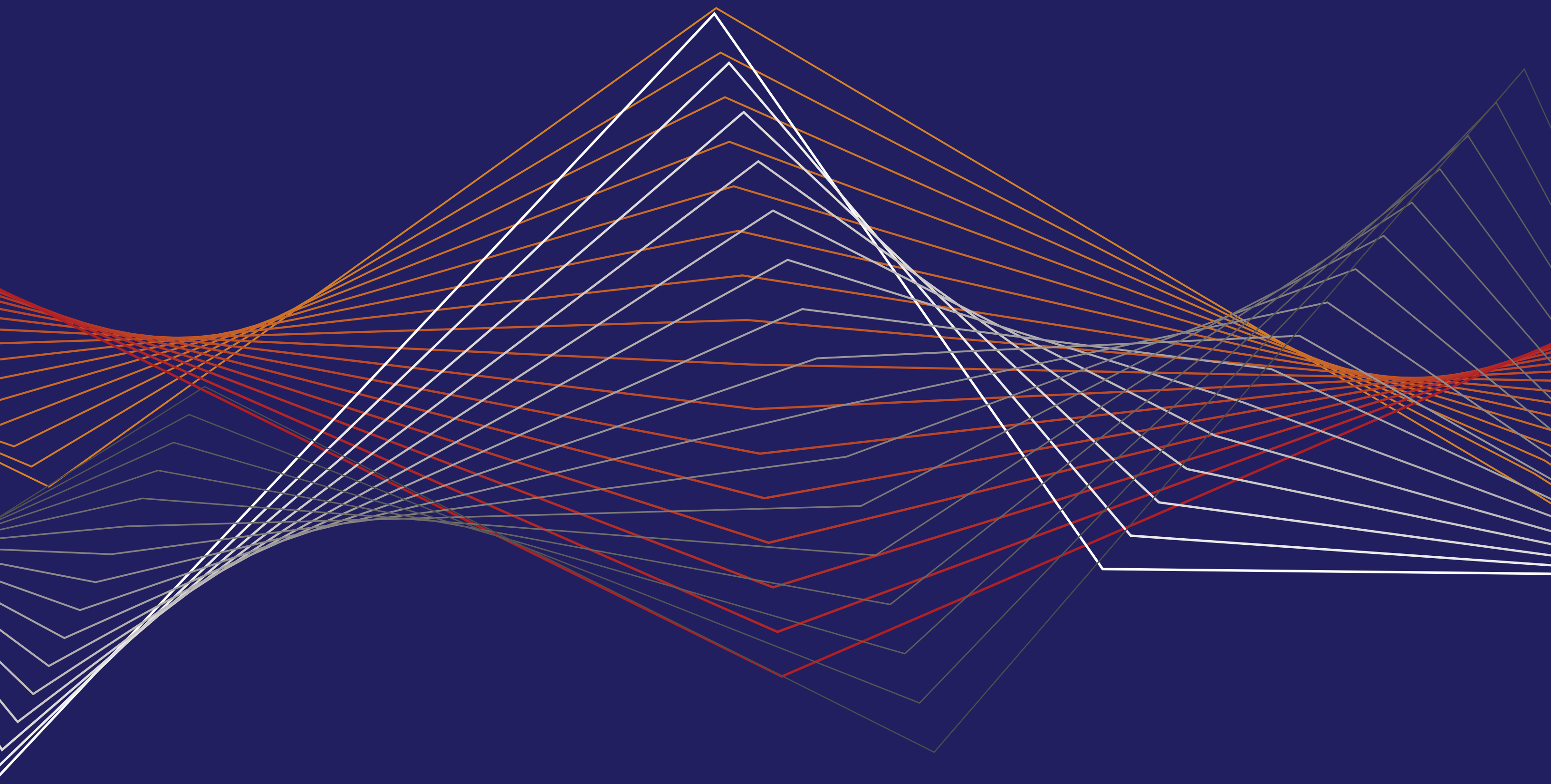
The overall threat from China and other adversaries has only increased over time and has accelerated and been exacerbated with technological innovation and their access to AI. In an article from January 2025, Jen Easterly, former Director of the Cybersecurity and Infrastructure Security Agency (CISA), lays out some of the risks to US critical infrastructure. CISA defines critical infrastructure as encompassing 16 sectors from utilities to government agencies to banks and the entire IT industry.

Outages happen consistently across all sectors and vulnerabilities are everywhere. So, the key for all Cyber programs is continuing to improve upon early detection and early response.

After the Crowdstrike outage in 2024 that affected thousands of hospitals, airports and businesses worldwide, Easterly said, *"We are building resilience into our networks and our systems so that we can withstand a significant disruption or at least drive down the recovery time to be able to provide services, which is why I thought the CrowdStrike incident — which was a terrible incident — was a useful exercise, like a dress rehearsal, for what China may want to do to us in some way and how we react if something like that happens," she said. "We have to be able to respond very rapidly and recover very rapidly in a world where [an issue] is not reversible."* -*https://therecord.media/easterly-china-cyberattacks-crowdstrike-outages.*

What will organizations do to combat persistent threats and cyberattacks from increasingly sophisticated adversaries? A goal of this research MixMode sponsored is to provide information on how industry can leverage AI in their cybersecurity plans to detect attacks earlier (be predictive) and improve their ability to recover from attacks more quickly.

The MixMode Team



Contents

Publication Date: April 2025

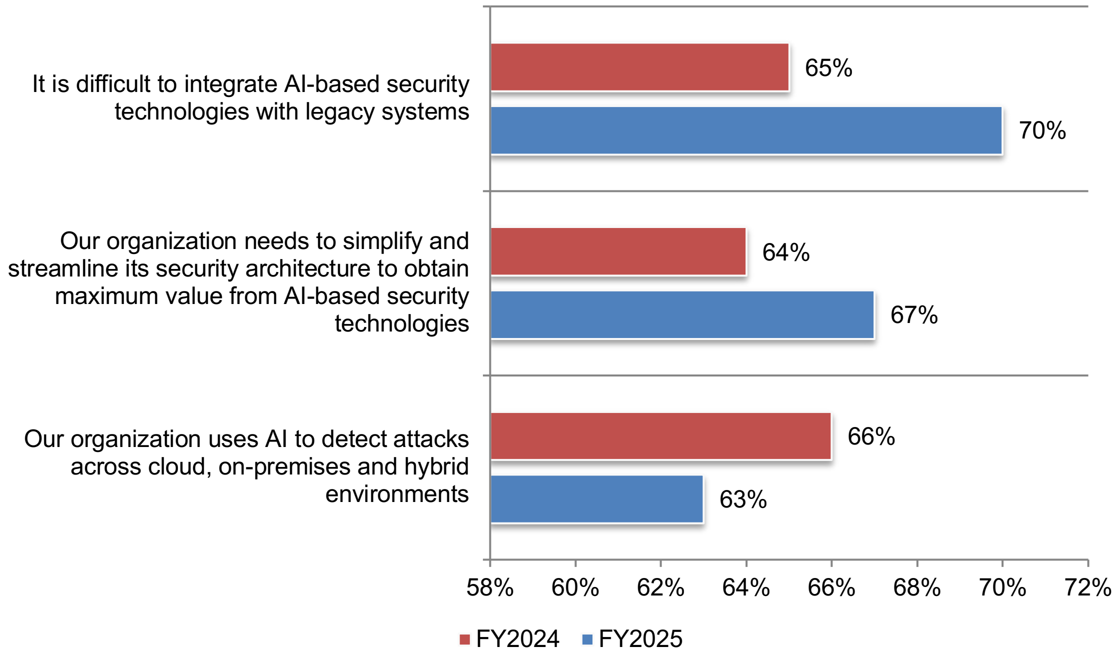
Part 1. Introduction

Organizations are in a race to adopt artificial intelligence (AI) technologies to strengthen their ability to stop the constant threats from cyber criminals. This is the second annual study sponsored by MixMode on this topic. The purpose of this research is to understand since 2024 how organizations are leveraging AI to effectively detect and respond to cyberattacks.

Ponemon Institute surveyed 685 US IT and IT security practitioners in organizations that have adopted AI in some form. These respondents are familiar with their organization's use of AI for cybersecurity and have responsibility for evaluating and/or selecting AI-based cybersecurity tools and vendors.

Since last year's study, organizations have not made progress in their ability to integrate AI security technologies with legacy systems and streamline their security architecture to increase AI's value. According to Figure 1, more respondents believe it is difficult to integrate AI-based security technologies with legacy systems, an increase from 65 percent to 70 percent of respondents. Sixty-seven percent of respondents, a slight increase from 64 percent of respondents, say their organizations need to simplify and streamline its security architecture to obtain maximum value from AI. Most organizations continue to use AI to detect attacks across the cloud, on-premises and hybrid environments.

Figure 1. Trends in AI adoption
Strongly agree and Agree responses combined



The following research findings reveal the benefits and challenges of AI.

How organizations are using AI to improve their security posture.

In just one year since the research was first conducted, organizations are reporting that their security posture has significantly improved because of AI. The biggest changes are improving the ability to prioritize threats and vulnerabilities (an increase from 50 percent to 56 percent of respondents), increasing the efficiency of the SOC team (from 43 percent to 51 percent) and increasing the speed of analyzing threats (from 36 percent to 43 percent).

Since 2024, the maturity of AI programs has increased. Fifty-three percent of organizations have achieved full adoption stage (31 percent of respondents) or mature stage (22 percent of respondents). This is an increase from 2024 when 47 percent respondents said they had reached the full adoption stage (29 percent of respondents) or mature stage (18 percent of respondents).

AI-based security technologies increase productivity and job satisfaction. Seventy percent of respondents say AI increases productivity of IT security personnel, an increase from 66 percent in 2024. Fifty-one percent of respondents say AI improves the efficiency of junior analysts so that senior analysts can focus on critical threats and strategic projects. Sixty-nine percent of respondents say since the adoption of AI, job satisfaction has improved because of the elimination of tedious tasks, an increase from 64 percent.

Forty-four percent of respondents are using AI-powered cybersecurity tools or solutions. By leveraging advanced algorithms and machine learning techniques. AI-powered systems analyze vast amounts of data, identify patterns and adapt their behavior to improve performance over time.

Forty-three percent of respondents are using pre-emptive security tools to stay ahead of cyber criminals. Pre-emptive security tools apply AI-based data analysis to cybersecurity so organizations can anticipate and prevent future attacks. The benefits include the ability to preemptively deter threats and minimize damages, prioritize tasks effectively and address the most important business risks first. Pre-emptive security data can guide response teams, offer insights into the attack's objectives, potential targets and more. The result is continuous improvement to ensure more accurate forecasts and reduce costs associated with handling attacks

Respondents say pre-emptive security is used to identify patterns that signal impending threats (60 percent), assess risks to identify emerging threats and potential impact (57 percent) and is used to harness vast amounts of online metadata from various sources as an input to predictive analytics (52 percent).

Pre-emptive security will decrease the ability of cybercriminals to direct targeted attacks. Fifty-two percent of respondents in organizations that use pre-emptive security say that without it cybercriminals will become more successful at directing targeted attacks at unprecedented speed and scale while going undetected by traditional, rule-based detection. Forty-nine percent say investments are being made in pre-emptive AI to stop AI-driven cybercrimes.

Fifty-eight percent of respondents say their SOCs use AI technologies. The primary benefit of an AI-powered SOC is that alerts are resolved faster, according to 57 percent of respondents. In addition to faster resolution of alerts, 55 percent of respondents say it frees up analyst bandwidth to focus on urgent incidents and strategic projects. Fifty percent of respondents say it applies real-time intelligence to identify patterns and detect emerging threats.

An AI-powered SOC is effective in reducing threats. Human analysts are effective as the final line of defense in the AI-powered SOC. Fifty-seven percent of respondents say AI in the

SOC is very or highly effective in reducing threats and 50 percent of respondents say their human analysts are very or highly effective as the final line of defense in the AI-powered SOC.

More organizations are creating one unified approach to managing both AI and privacy security risks, an increase from 37 percent to 52 percent of respondents. In addition, 58 percent of respondents say their organizations identify vulnerabilities and what can be done to eliminate them.

The barriers and challenges to maximizing the value from AI

While an insufficient budget to invest in AI technologies continues to be the primary governance challenge, more organizations say an increase in internal expertise is needed to validate vendors' claims. The lack of internal expertise to validate vendors' claims increased significantly from 53 percent to 59 percent of respondents. One of the key takeaways from the research is that 63 percent of respondents say the decision to invest in AI technologies is based on the extensiveness of the vendors' expertise.

As the number of cyberattacks increase, especially malicious insider incidents, organizations lack confidence in their ability to prevent risks and threats. Fifty-one percent of respondents say their organizations had at least one cyberattack in the past 12 months, an increase from 45 percent of respondents in 2024.

Only 42 percent say their organizations are very or highly effective in mitigating risks, vulnerabilities and attacks across the enterprise. The attacks that increased since 2024 are malicious insiders (53 percent vs. 45 percent), compromised/stolen devices (40 percent vs. 35 percent) and credential theft (49 percent vs. 53 percent). The primary types of attacks in 2024 and 2025 are phishing/social engineering and web-based attacks.

The effectiveness of AI technologies is diminished because of interoperability issues and an increase in a heavy reliance on legacy IT environments. The barriers to AI-based security technologies' effectiveness are interoperability issues (63 percent, an increase from 60 percent of respondents), can't apply AI-based controls that span across the entire enterprise (59 percent vs. 61 percent of respondents) and can't create a unified view of AI users across the enterprise (56 percent vs 58 percent of respondents). The most significant trend is the increase in the heavy reliance on legacy IT environments, an increase from 36 percent to 45 percent of respondents.

Complexity challenges the preparedness of cybersecurity teams to work with AI-powered tools. Only 42 percent of respondents say their cybersecurity teams are highly prepared to work with AI-powered tools. Fifty-five percent of respondents say AI-powered solutions are highly complex.

AI continues to make it difficult to comply with privacy and security mandates and to safeguard confidential and personal data in AI. Forty-eight percent of respondents say it is highly difficult to achieve compliance and 53 percent of respondents say it is highly difficult to safeguard confidential and personal data in AI

Part 2. Key findings

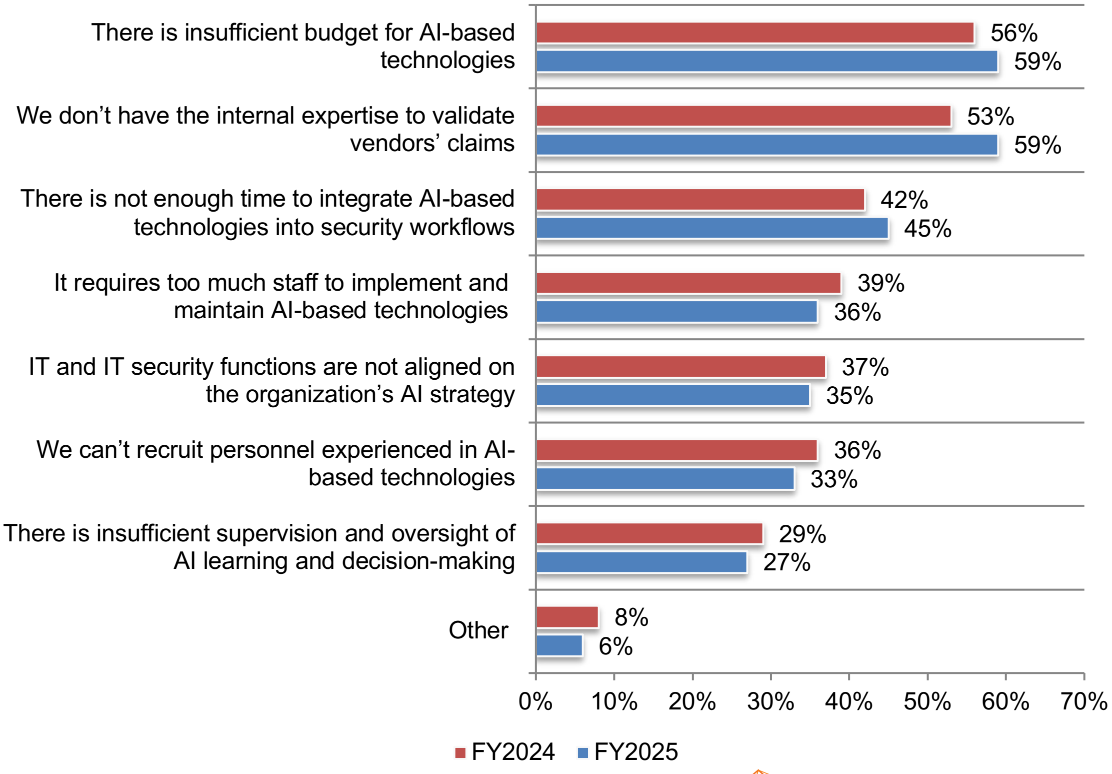
In this section, we provide a deeper dive into the research. The complete research findings are presented in the Appendix. The report is organized according to the following topics.

- Is AI making a difference?
- AI-powered cybersecurity tools
- Getting ahead of cyber criminals with pre-emptive AI solutions
- The use of AI in the SOC
- Privacy, security and ethical considerations

Is AI making a difference?

While an insufficient budget to invest in AI technologies continues to be the primary governance challenge, more organizations say an increase in internal expertise is needed to validate vendors' claims. According to Figure 2, 59 percent of respondents say an insufficient budget to invest in AI-based technologies continues to be a challenge, an increase from 56 percent. The lack of internal expertise to validate vendors' claims increased significantly from 53 percent to 59 percent of respondents. This challenge can affect investments in AI technologies because 63 percent of respondents say the decision to invest in AI is based on a review of a vendor's extensive expertise.

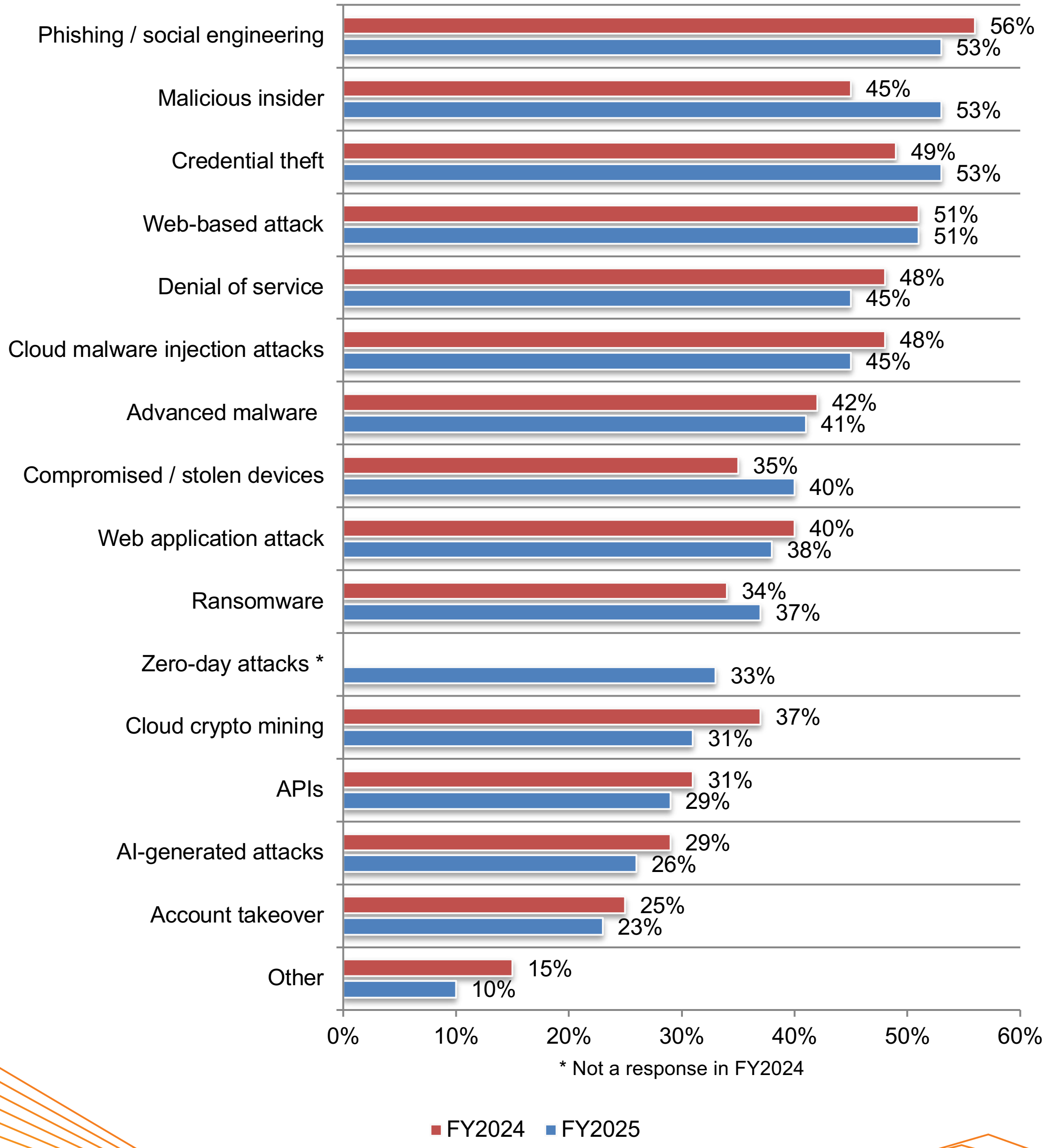
Figure 2. Organizational or governance challenges
Three responses permitted



Malicious insider attacks increased significantly since 2024. Fifty-one percent of respondents had at least one cyberattack in the past 12 months, an increase from 2024 of 45 percent of respondents. Accordingly, when asked to rate the effectiveness of their IT security posture in terms of its effectiveness at mitigating risks, vulnerabilities and attacks across the enterprise on a scale of 1 = not effective to 10 = highly effective, only 42 percent say their organizations are very or highly effective (7+ on the 10-point scale).

As shown in Figure 3, the attacks that increased are malicious insiders (53 percent vs. 45 percent), compromised/stolen devices (40 percent vs. 35 percent) and credential theft (49 percent vs. 53 percent). Phishing/social engineering continues to be a primary security threat.

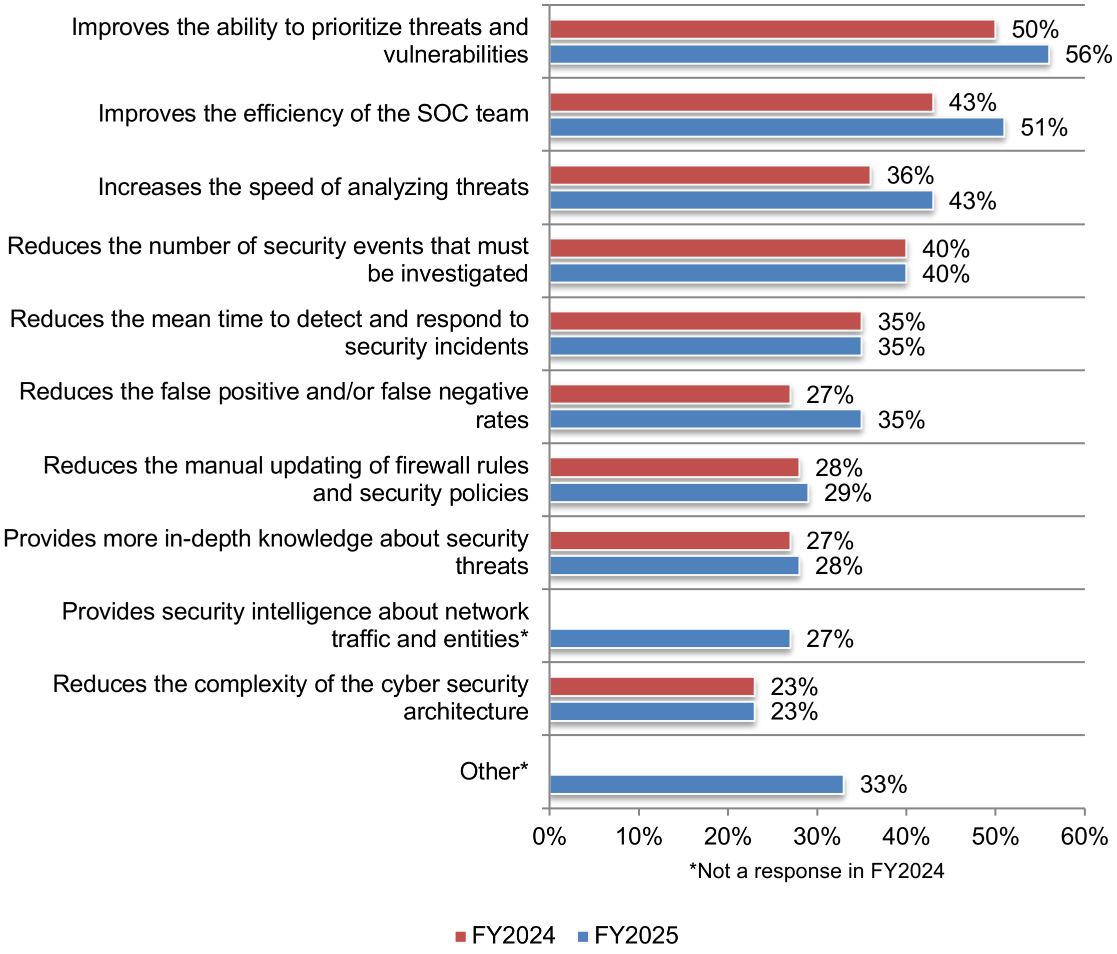
Figure 3. What best describes the type of attacks experienced by your organization?
More than one response permitted



* Not a response in FY2024

A positive finding is that despite the challenges in adoption, more organizations in the 2025 research believe AI is making a difference in their security posture. According to Figure 4, AI improves organizations' security posture by improving the ability to prioritize threats and vulnerabilities (56 percent, an increase from 50 percent), the efficiency of the SOC team (51 percent, an increase from 43 percent) and the speed of analyzing threats (43 percent, an increase from 36 percent).

Figure 4. How does AI improve your organization's security posture?
More than one response permitted

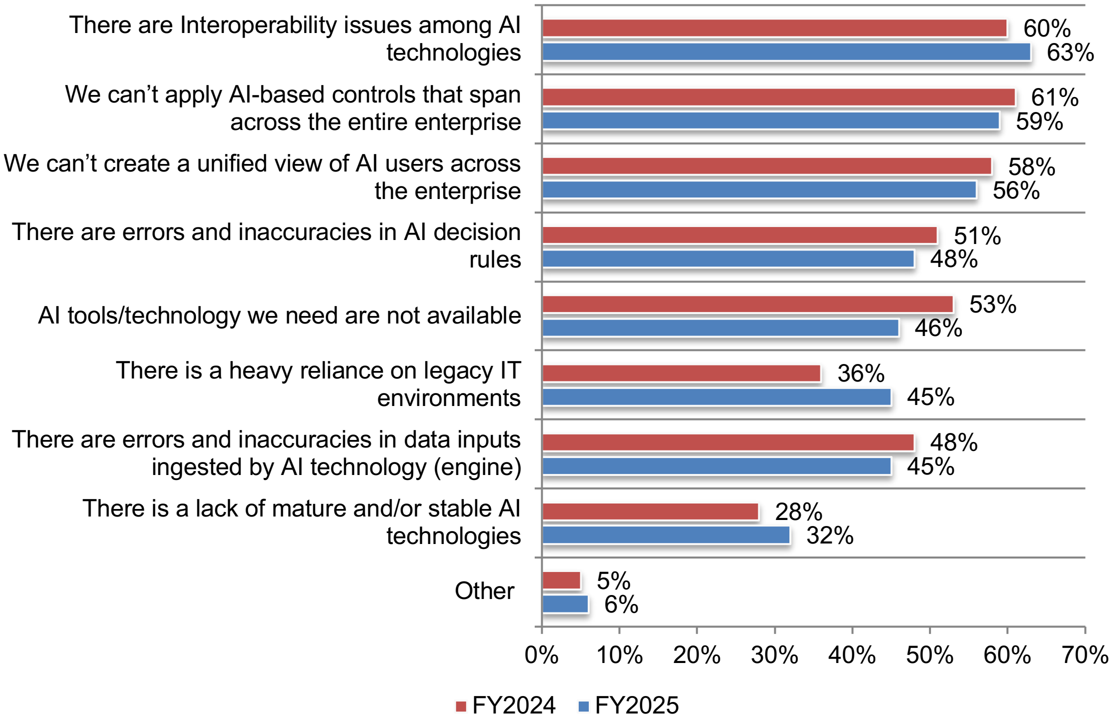


*Not a response in FY2024

The effectiveness of AI technologies is diminished because of interoperability issues and an increase in a heavy reliance on legacy IT environments. According to Figure 5, the barriers to AI-based security technologies' effectiveness are interoperability issues (63 percent, an increase from 60 percent), can't apply AI-based controls that span across the entire enterprise (59 percent vs. 61 percent) and can't create a unified view of AI users across the enterprise (56 percent vs 58 percent).

The most significant trend is the increase in the heavy reliance on legacy IT environments, an increase from 36 percent to 45 percent. As discussed in this report, 70 percent of respondents say it is difficult to integrate AI- based security technologies with legacy systems.

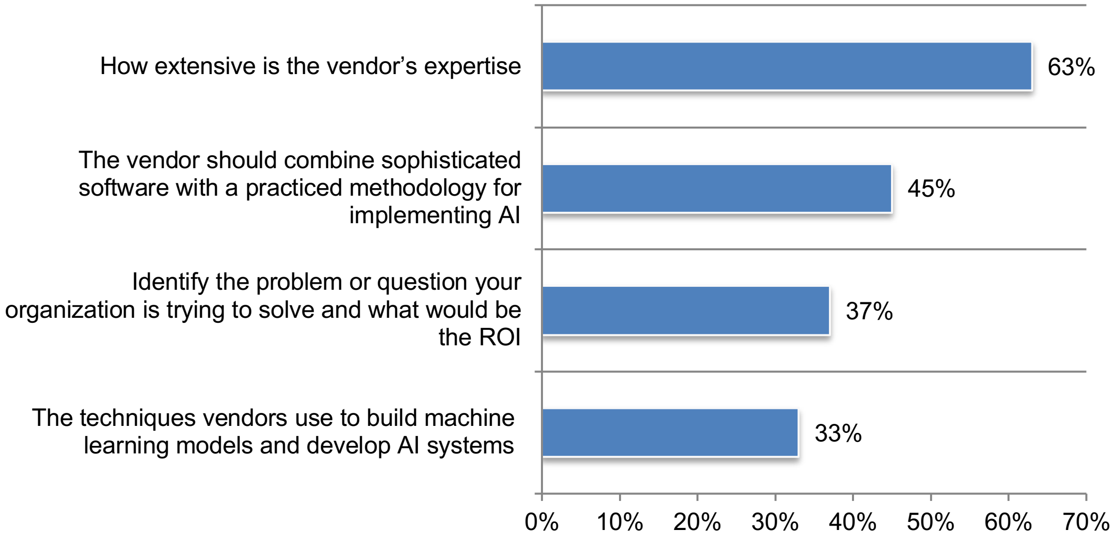
Figure 5. Barriers to the effectiveness of AI-based security technologies used today
Four responses permitted

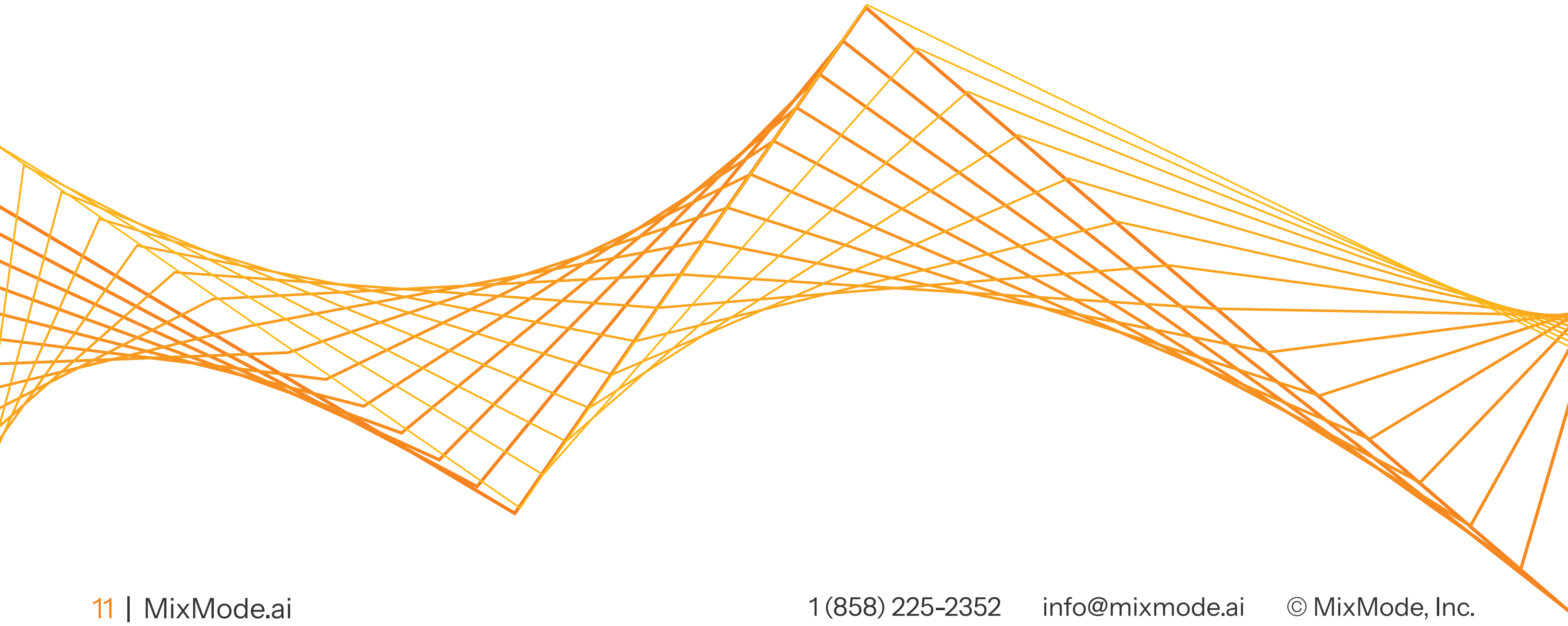


When investing in AI technologies, most organizations consider the expertise of vendors. As shown in Figure 6, 63 percent of respondents say extensive expertise is important followed by the vendor's ability to combine sophisticated software with a practiced methodology for implementing AI (45 percent of respondents). However, as shown in the research 56 percent of respondents say their organizations do not have the necessary internal expertise to validate vendors' claims.

The average IT security budget for 2025 is $36.8 million and an average of 21 percent or $7.9 million is allocated to AI/ML investments.

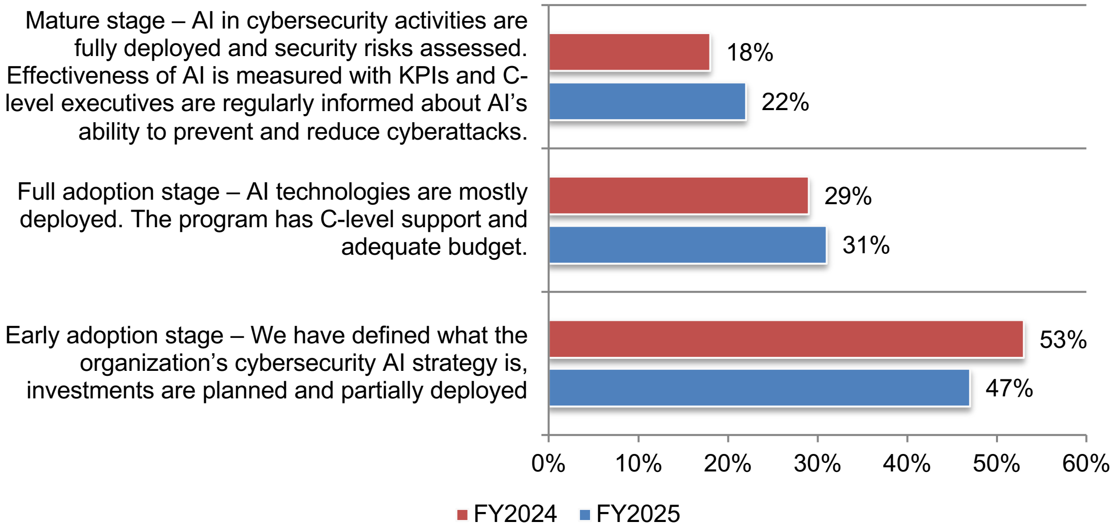
Figure 6. Which of the following factors are most important when investing in AI security technologies?
More than one response permitted





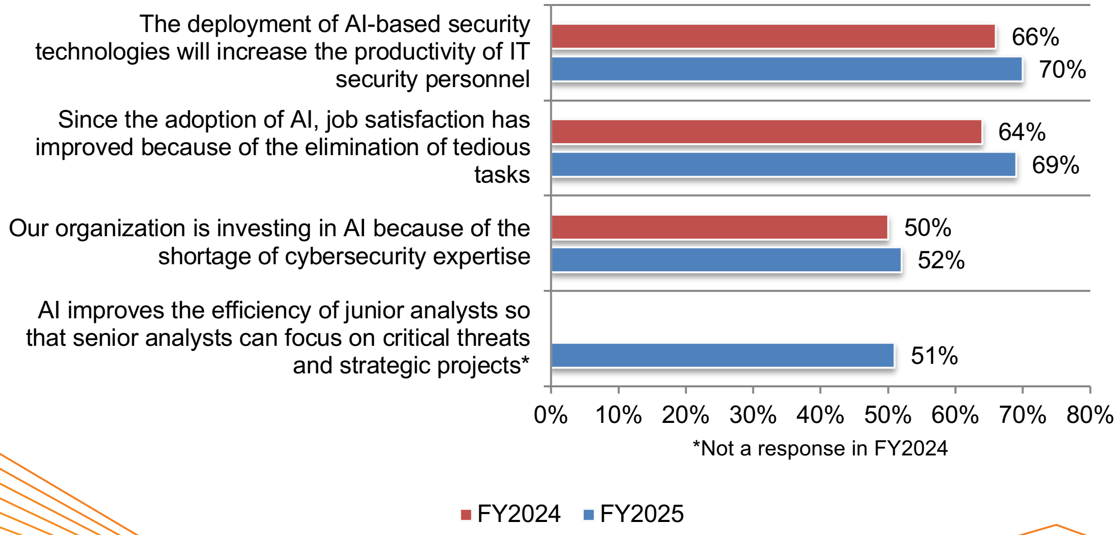
Since 2024, the maturity of organizations' use of AI has increased. As shown in Figure 7 2025, 53 percent of organizations have achieved full adoption stage (31 percent) or mature stage (22 percent), as described below. This is an increase from 2024 when 47 percent say they have reached the full adoption stage (29 percent) or mature stage (18 percent).

Figure 7. What best describes the maturity of your organization's use of AI?



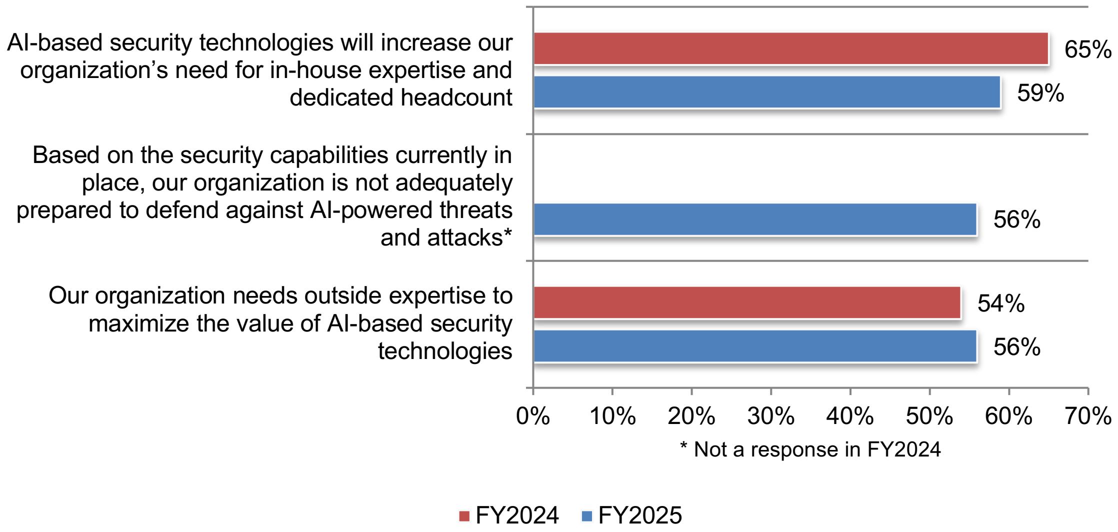
AI-based security technologies improve productivity and job satisfaction. According to Figure 8, 70 percent of respondents say AI increases productivity of IT security personnel, an increase from 66 percent in 2024. Fifty-one percent of respondents say AI improves the efficiency of junior analysts so that senior analysts can focus on critical threats and strategic projects. Sixty-nine percent of respondents say since the adoption of AI job satisfaction has improved because of the elimination of tedious tasks, an increase from 64 percent.

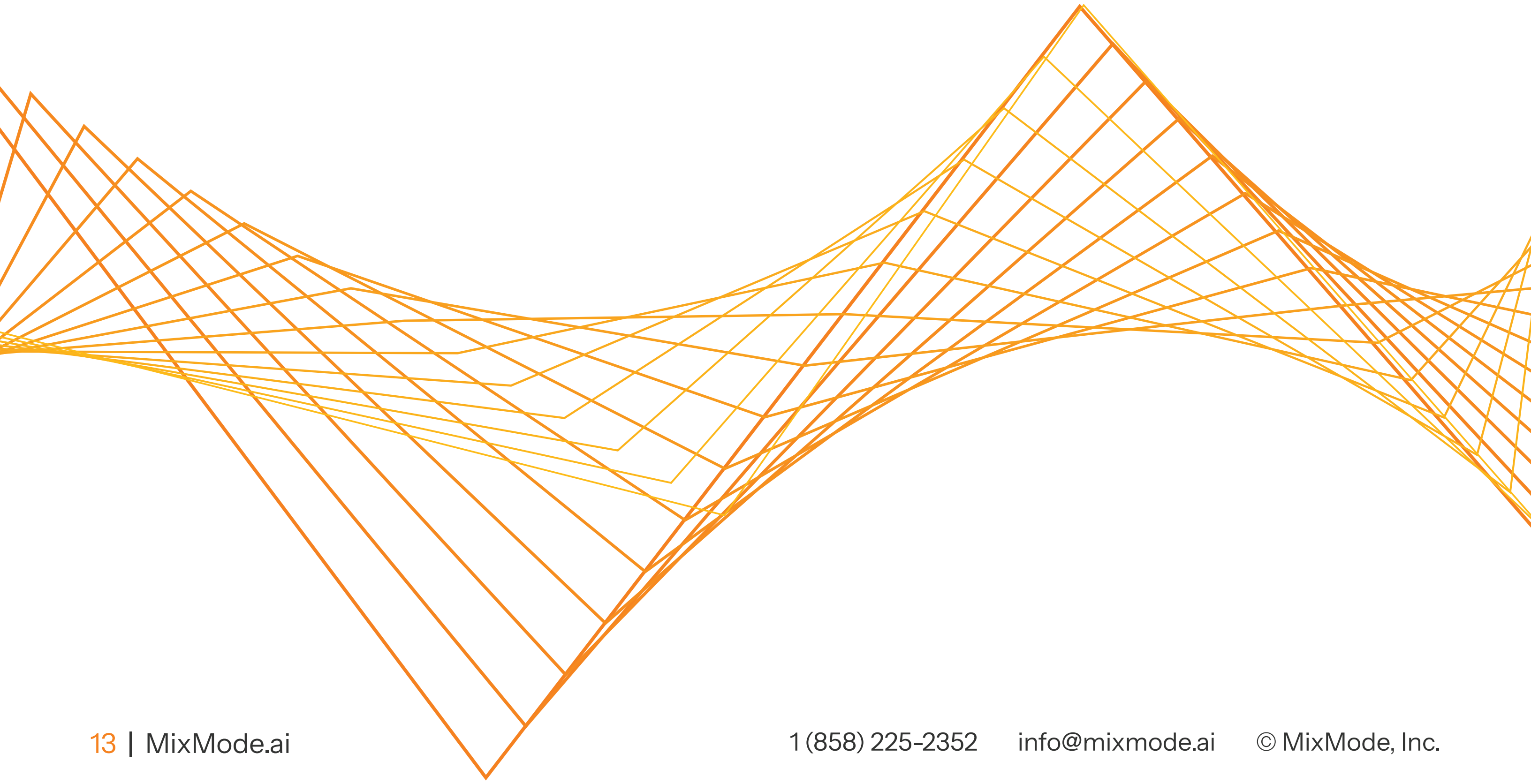
Figure 8. The impact of AI on productivity and job satisfaction
Strongly agree and Agree responses combined



The need to increase in-house expertise and dedicated headcount has declined significantly. However, outside expertise is needed to maximize the value of AI-based technologies. According to Figure 9, in 2024 65 percent of respondents said they would need more in-house expertise and dedicated headcount because of AI-based security technologies. In 2025, 59 percent of respondents say more staffing is needed. The decline could be attributed to evidence in the research that AI improves productivity. Fifty-six percent of respondents say their organizations need outside expertise to maximize the value of AI-based security technologies, a slight increase from 54 percent of respondents.

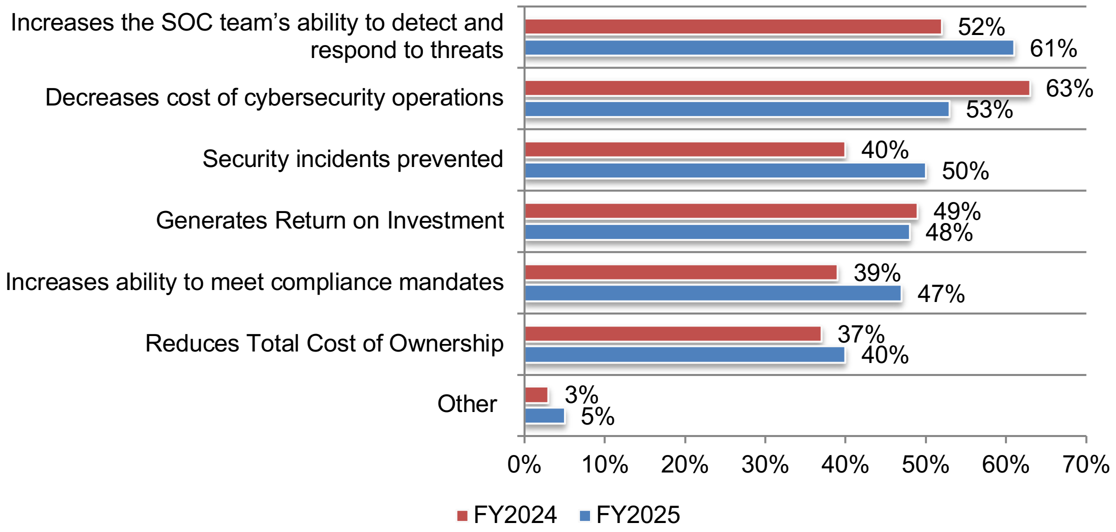
Figure 9. The impact of AI on staffing
Strongly agree and Agree responses combined





To determine AI's effectiveness, more organizations are measuring the SOC team's increased ability to detect and respond to threats, an increase from 52 percent of respondents to 61 percent of respondents. As shown in Figure 10, an important measure is the cost of cybersecurity operations. However, the use of this measure decreased from 63 percent to 53 percent of respondents. The prevention of security incidents as a measure increased significantly from 40 percent to 50 percent of respondents.

Figure 10. How does your organization determine the effectiveness of AI?
More than one response permitted



In AI there are a variety of technologies and respondents were asked if they are very familiar or familiar with them as defined below.

Unsupervised learning in artificial intelligence is a type of machine learning that learns from data without human supervision. Unlike supervised learning, unsupervised machine learning models are given unlabeled data and allowed to discover patterns and insights without any explicit guidance or instruction.

Supervised machine learning is a machine learning technique that uses labeled data to train algorithms to predict outcomes. The goal is to create a model that can accurately predict outputs on new data.

Generative AI produces new content, such as text, images or music applications. Machine learning is used for tasks like recommendation systems, predictive analytics and diagnostic tools

Self-supervised learning (SSL) is a machine learning technique that trains models to learn from unlabeled data. It's a middle ground between supervised and unsupervised learning.

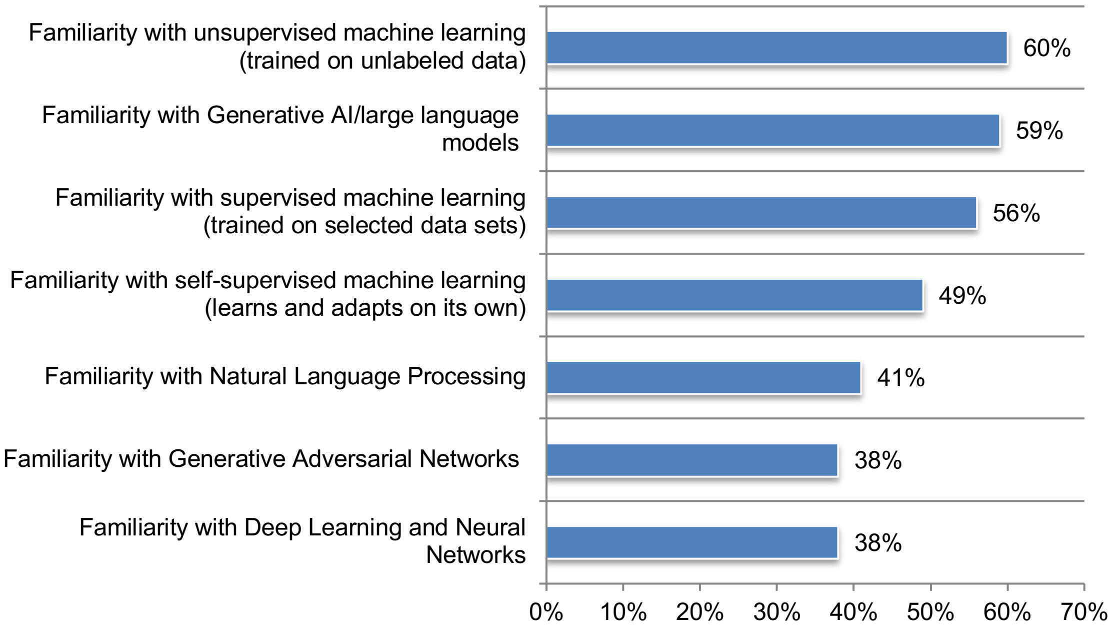
Natural language processing (NLP) is a technology that enables computers to understand human language. It's a key part of AI and is used in many applications, such as Chatbots and machine translation.

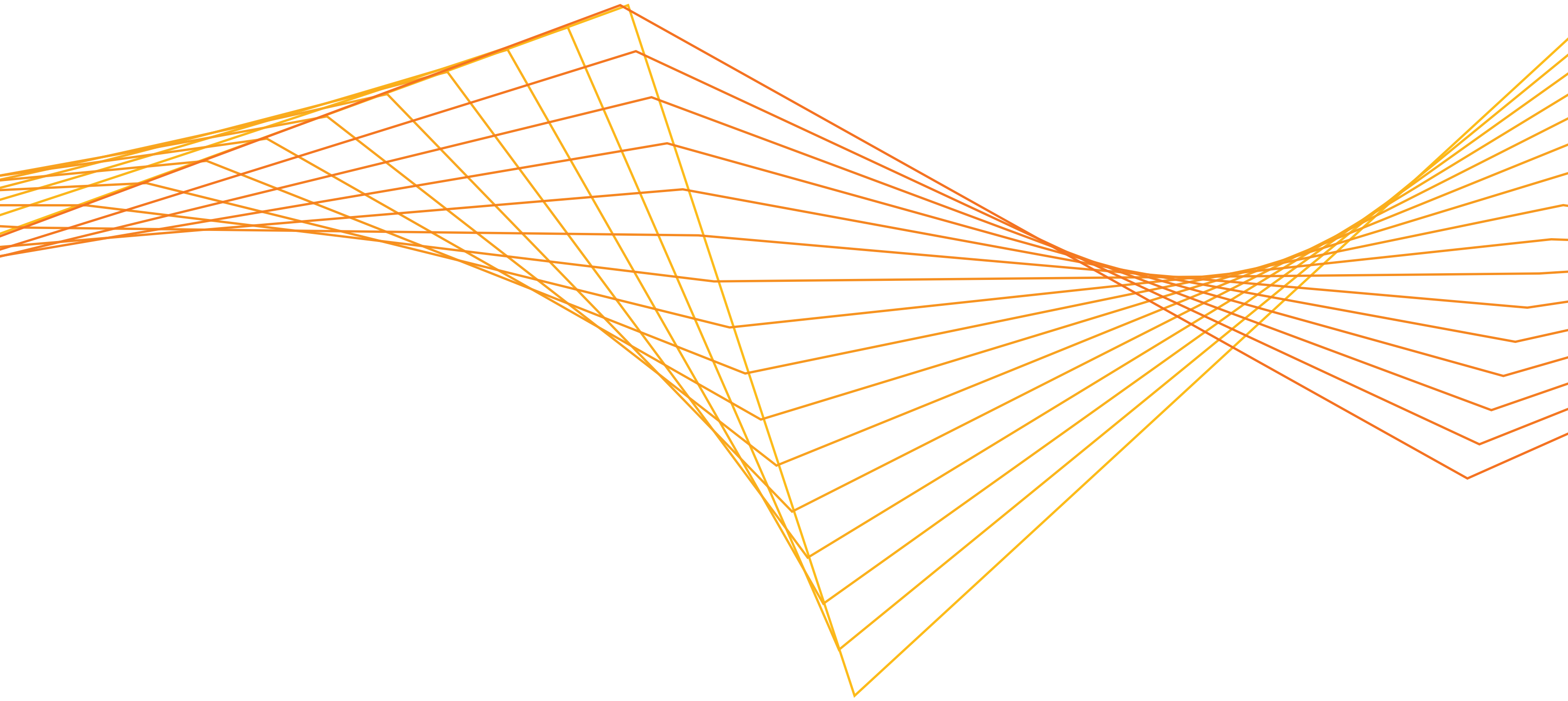
Generative adversarial networks (GANs) are machine learning models that create new data that resembles real data. GANs are made up of two neural networks that compete against each other.

Deep learning models can recognize data patterns like complex pictures, text, and sounds to produce accurate insights and predictions. A neural network is the underlying technology in deep learning. It consists of interconnected nodes or neurons in a layered structure.

As shown in Figure 11, respondents are most familiar with unsupervised machine learning and generative AI/large language models, 60 percent and 59 percent of respondents, respectively.

Figure 11. Familiarity with AI-based technologies
Very familiar and Familiar responses combined





AI-powered cybersecurity tools

AI-powered cybersecurity tools or solutions incorporate AI to perform tasks or make decisions typically requiring human intelligence. By leveraging advanced algorithms and machine learning techniques. AI-powered systems analyze vast amounts of data, identify patterns and adapt their behavior to improve performance over time.

Forty-four percent of respondents say their organizations use AI-powered tools or solutions. Thirty-six percent of these respondents say their organizations have fully deployed and 64 percent of respondents say these tools are partially deployed. Figure 12 lists the AI-powered tools or solutions their organizations use or plan to use.

Extended Detection and Response (XDR) is a cybersecurity technology that monitors and responds to threats. XDR is a unified security platform that combines data from various security tools into a single console and is used by 44 percent of organizations. Endpoint Detection and Response (EDR) is a cybersecurity technology that monitors devices for cyber threats. EDR can help prevent cyber criminals for using devices to access data and networks and is used by 40 percent of organizations.

Network Detection and Response (NDR) is a cybersecurity technology that monitors network traffic for threats, uses machine learning and analytics to identify suspicious activity can be delivered through hardware, software or SaaS and is used by 38 percent of organizations.

Figure 12. What AI-powered cybersecurity tools or solutions does your organization use or plan to use?
More than one response permitted

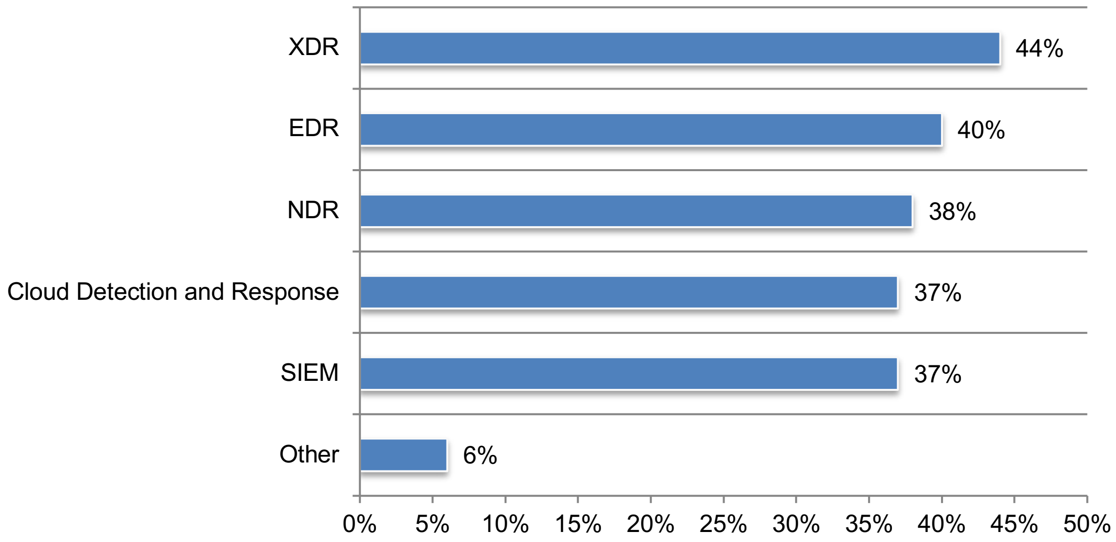
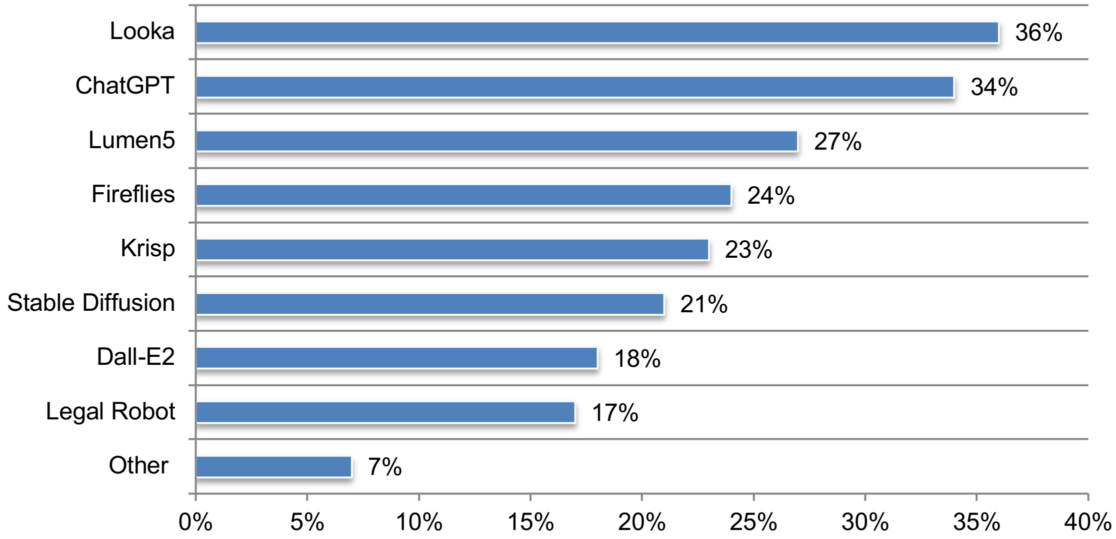
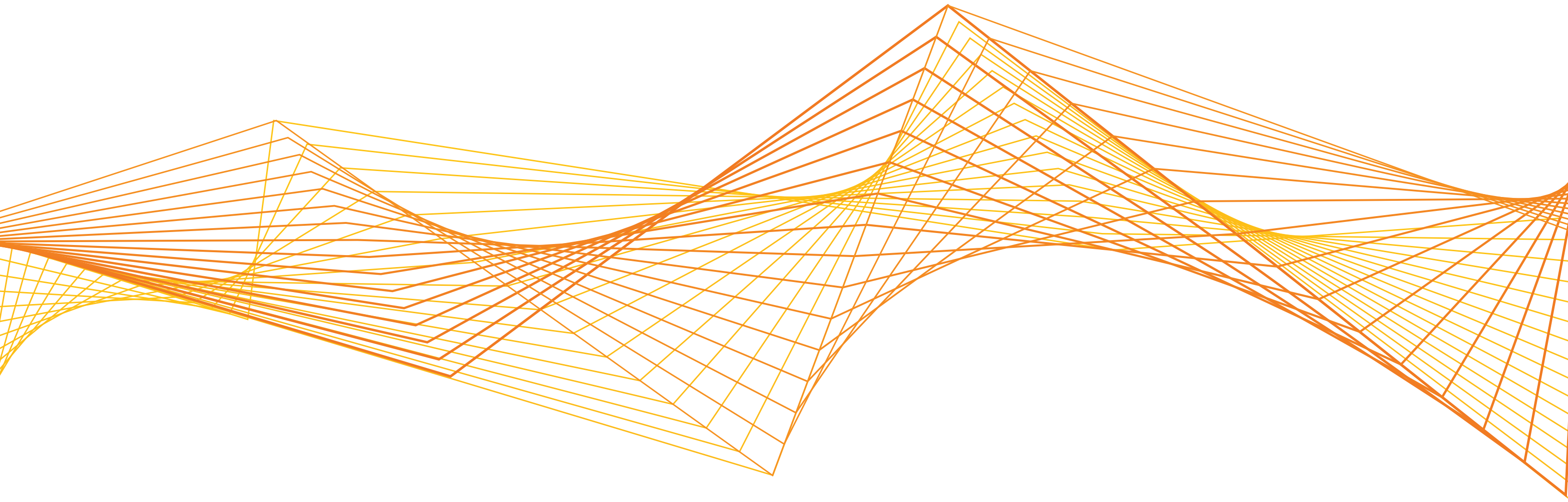


Figure 13 lists the other AI-powered tools organizations use or plan to use. As shown, Looka and ChatGPT are the most frequently used according to 36 percent and 34 percent of respondents, respectively.

Following are descriptions of AI-powered tools or solutions used. Looka's AI powered platform is used to design logos. ChatGPT is a generative AI Chatbot developed by open AI. Lumen5 is a video creation platform powered by AI. Fireflies transcribes, summarizes and analyzes team conversations. Krisp is AI-based audio processing software that offers real-time noise and voice suppression technology. Stable Diffusion is a generative AI model that produces unique photo realistic images from text and images. Dall-E2 is an AI system that can create realistic images and text for a desig. Legal Robot provides automate analysis of legal documents and linguistic/statistical analysis to help understand potential issues.

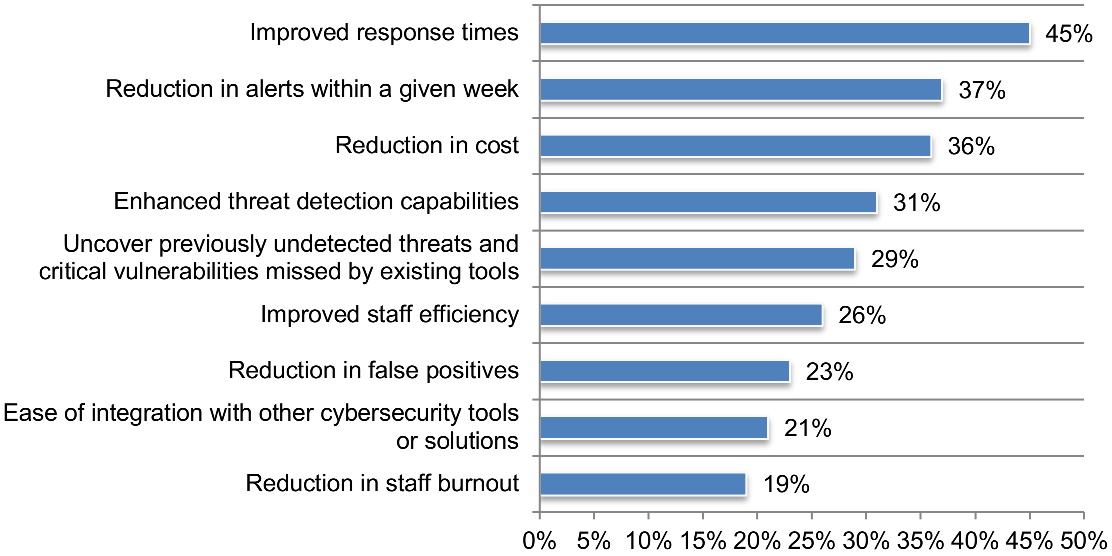
Figure 13. What other AI-powered tools or solutions does your organization use or plan to use?
More than one response permitted

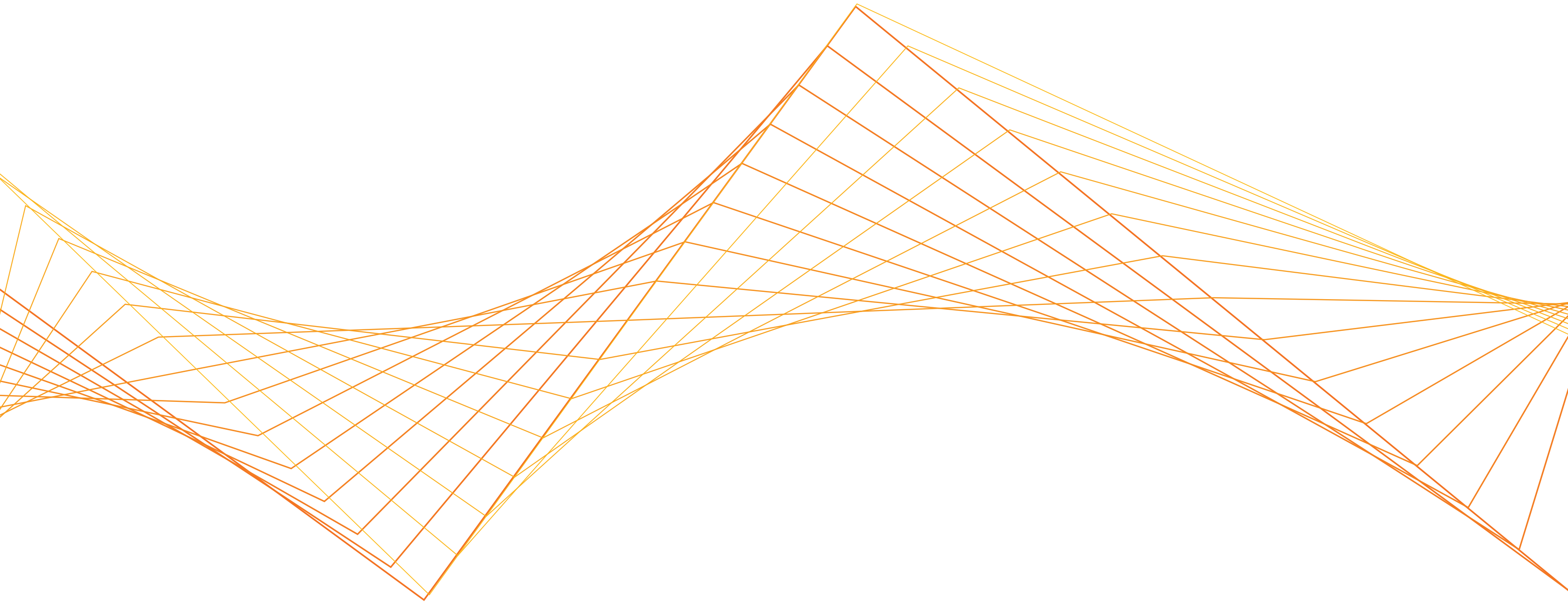




To evaluate effectiveness of AI-powered cybersecurity solutions, organizations measure improved response times (45 percent), reduction in alerts within a given time (37 percent) and reduction in cost (36 percent), as shown in Figure 14.

Figure 14. How does your organization evaluate the effectiveness of your AI-powered cybersecurity solutions?
More than one response permitted



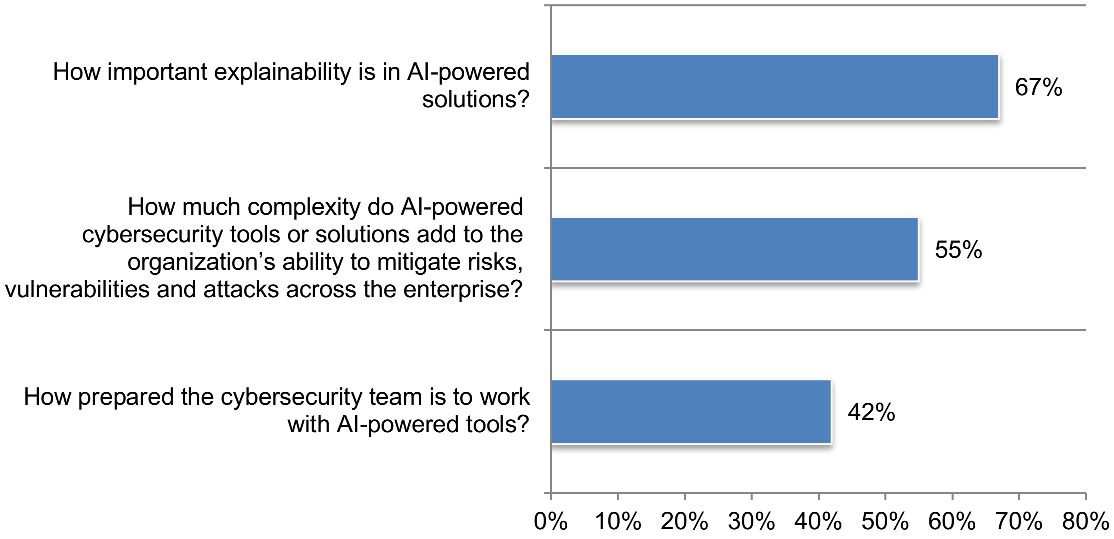


Complexity challenges the preparedness of cybersecurity teams to work with AI-powered tools. Respondents were asked to rate the complexity of AI-powered cybersecurity tools when attempting to mitigate risks, vulnerabilities and attacks across the enterprise on a scale from 1 = not complex to 10 = highly complex and how prepared the cybersecurity team is to work with AI-powered tools on a scale from 1 = low preparedness to 10 = high preparedness.

Figure 15 shows the 7+ responses on a 10-point scale. Only 42 percent of respondents say their cybersecurity teams are highly prepared to work with AI-powered tools. Fifty-five percent of respondents say AI-powered solutions are highly complex.

Sixty-seven percent of respondents say explainability in AI-powered solutions is highly important (7+ on the 10-point scale of 1 = low importance to 10 = highly important). Explainability in AI is the ability to understand how an AI system makes decisions or predictions, and why it made them. It is also known as explainable machine learning or explainable AI (XAI).

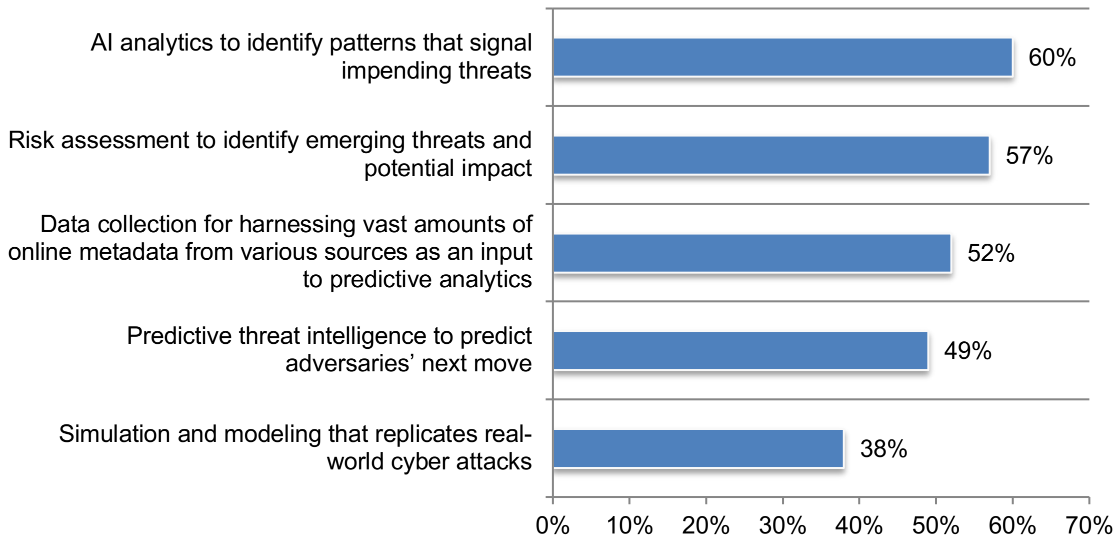
Figure 15. How prepared are organizations to deal with complexity of AI-powered solutions?
On a scale from 1 = not important/complex/prepared to 10 = highly important/complex/prepared, 7+ responses presented



Pre-emptive security tools apply AI-based data analysis to cybersecurity so organizations can anticipate and prevent future attacks. The benefits include the ability to preemptively deter threats and minimize damages, prioritize tasks effectively and address the most important business risks first. Pre-emptive security data can guide response teams, offer insights into the attack's objectives, potential targets and more. The result is continuous improvement to ensure more accurate forecasts and reduce costs associated with handling attacks

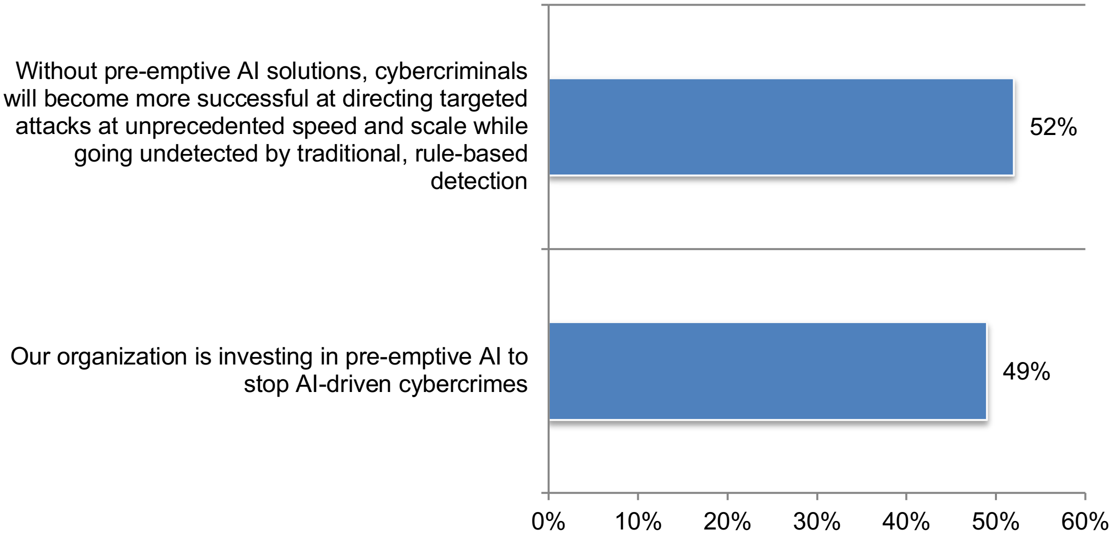
Forty-three percent of respondents say their organizations have adopted pre-emptive security. According to Figure 16, respondents say pre-emptive security is used to identify patterns that signal impending threats (60 percent), assess risks to identify emerging threats and potential impact (57 percent) and is used to harness vast amounts of online metadata from various sources as an input to predictive analytics (52 percent).

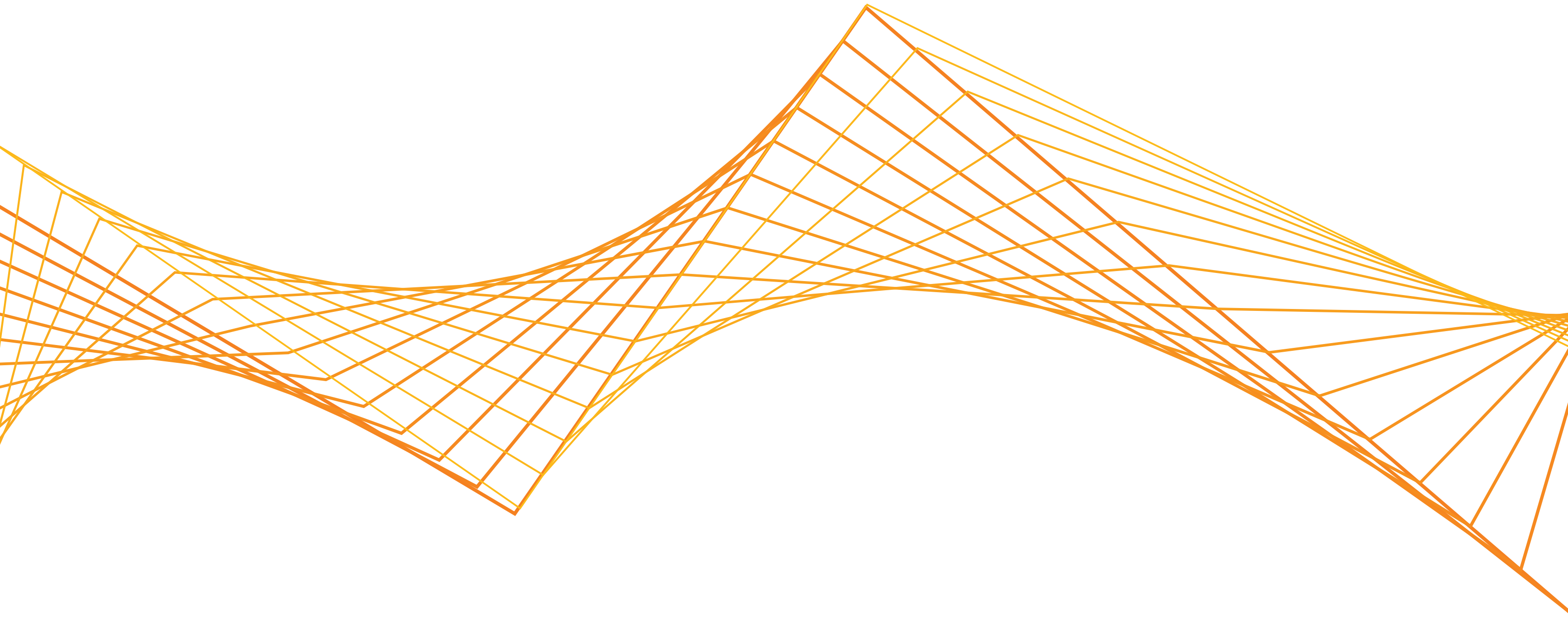
Figure 16. How does your organization use pre-emptive security?
More than one response permitted



Pre-emptive security will decrease the ability of cybercriminals to direct targeted attacks. According to Figure 17, 52 percent of respondents that use pre-emptive security say that without it, cybercriminals will become more successful at directing targeted attacks at unprecedented speed and scale while going undetected by traditional, rule-based detection. Forty-nine percent say investments are being made in pre-emptive AI to stop AI-driven cybercrimes.

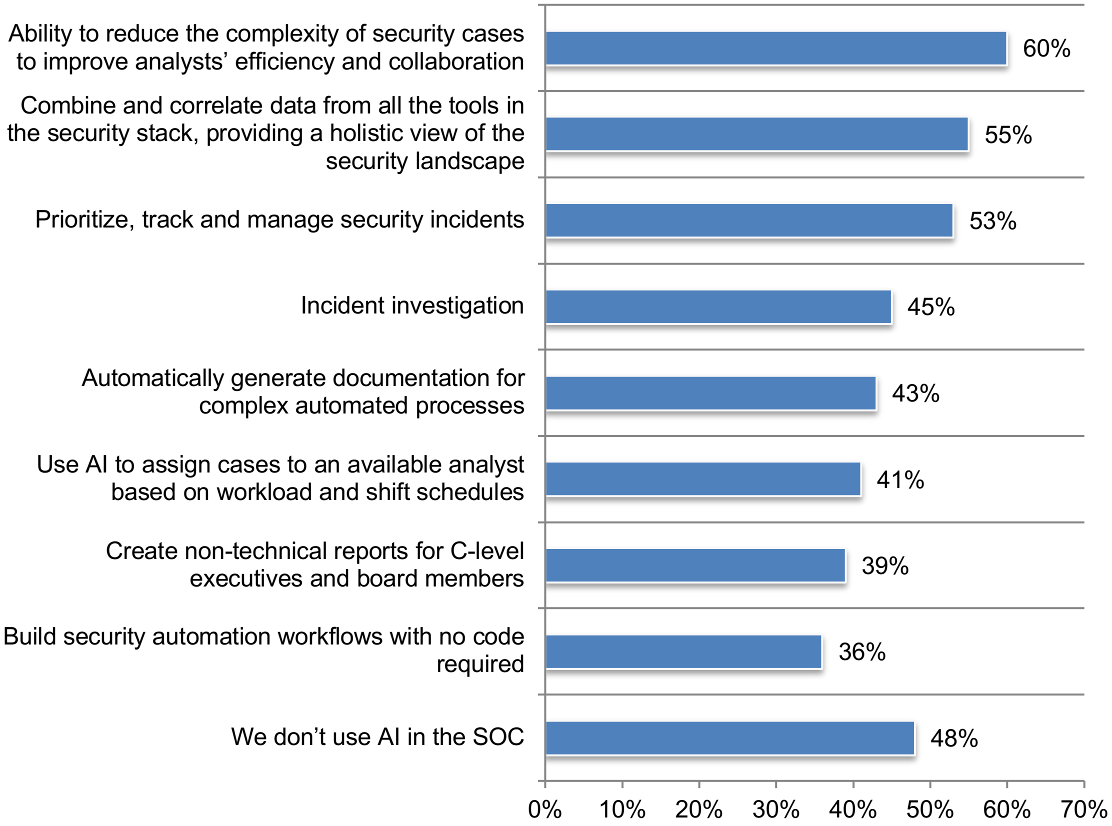
Figure 17. The benefits of pre-emptive AI security
Strongly agree and Agree responses combined





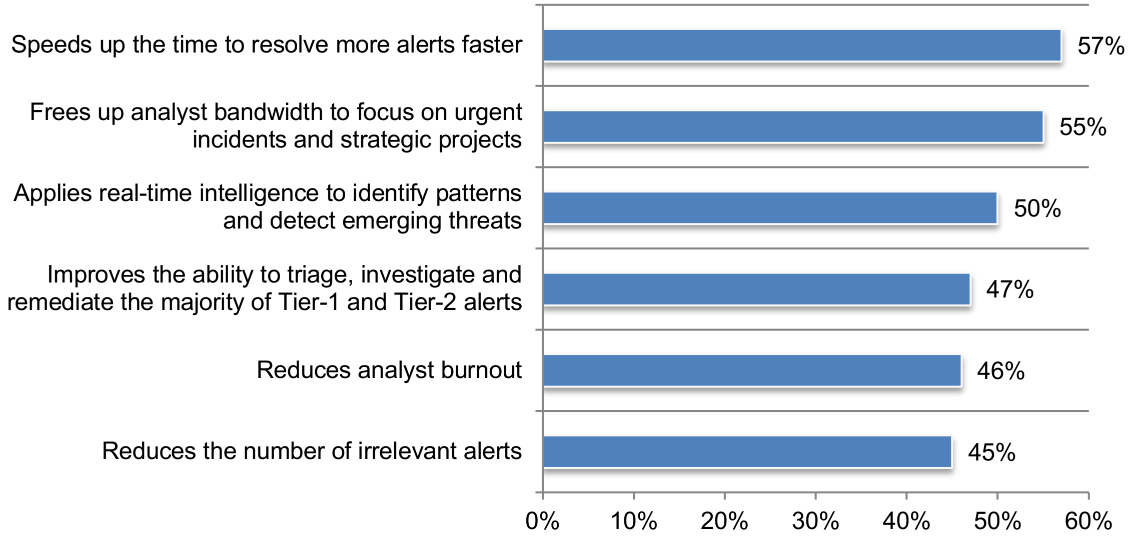
Fifty-two percent of respondents say their organizations use AI in the SOC. According to Figure 18, organizations use AI in the SOC to reduce the complexity of security cases to improve analysts' efficiency and collaboration (60 percent), combine and correlate data from all tools in the security stack, providing a holistic view of the security landscape (55 percent) and prioritize, track and manage security incidents (53 percent).

Figure 18. How does your organization use AI in the SOC?
More than one response permitted



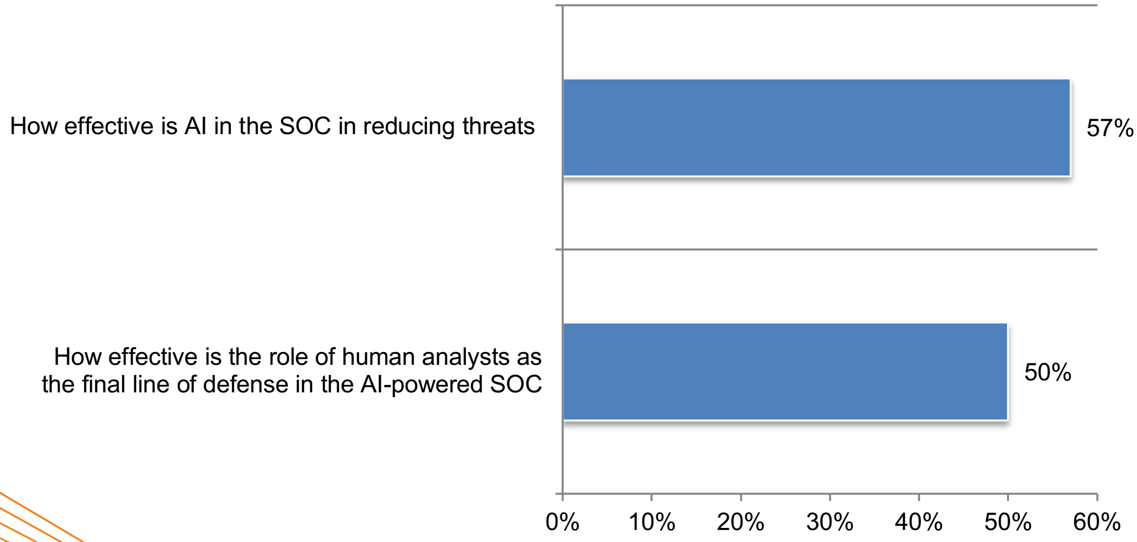
The primary benefit of an AI-powered SOC is that alerts are resolved faster, according to 57 percent of respondents. As shown in Figure 19, in addition to faster resolution of alerts, 55 percent of respondents say it frees up analyst bandwidth to focus on urgent incidents and strategic projects. Fifty percent of respondents say it applies real-time intelligence to identify patterns and detect emerging threats.

Figure 19. What are the primary benefits of an AI-powered SOC?
Three responses permitted



An AI-powered SOC is very or highly effective in reducing threats. Human analysts are very or highly effective as the final line of defense in the AI-powered SOC. Respondents were asked to rate the effectiveness of the SOC in reducing threats and the effectiveness of human analysts as the final line of defense on a scale from 1 = not effective to 10 = highly effective. Fifty-seven percent of respondents say AI in the SOC reduces threats and 50 percent of respondents say their human analysts are highly effective in the SOC.

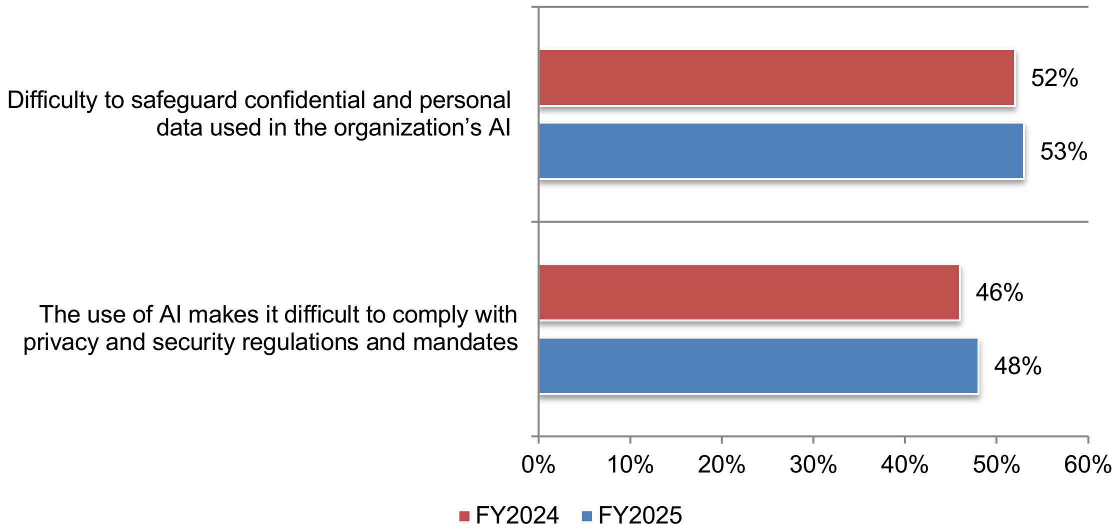
Figure 20. How AI increases security in the SOC
On a scale from 1 = not effective to 10 = highly effective, 7+ responses presented



Privacy, security and ethical considerations

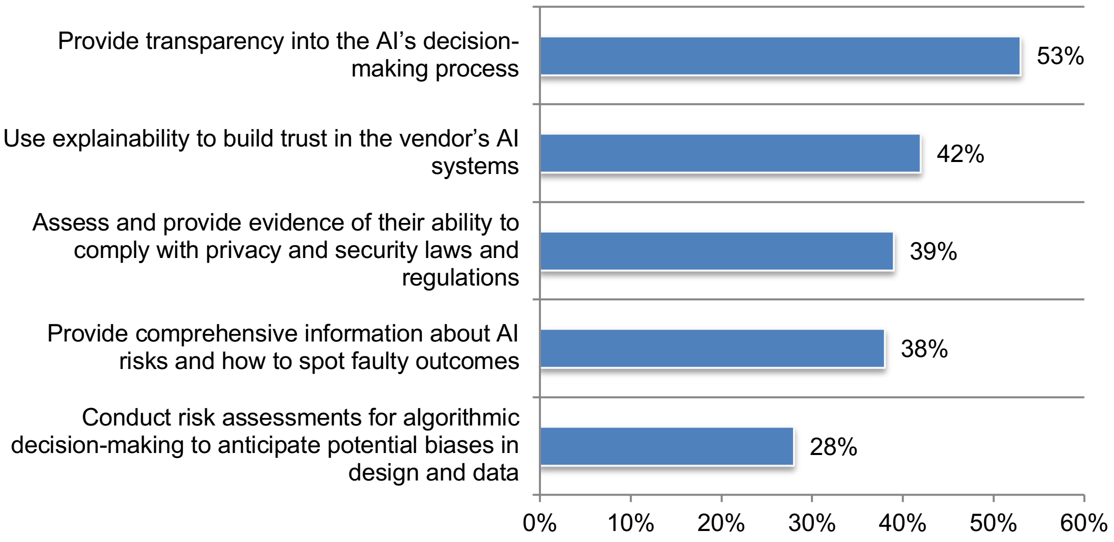
AI continues to make it difficult to comply with privacy and security mandates and to safeguard confidential and personal data in AI. Respondents were asked to rate the difficulties created by AI in organizations' privacy and security objectives on a scale of 1 = not difficult to 10 = highly difficult. According to Figure 21, 48 percent of respondents say it is highly difficult to achieve compliance and 53 percent of respondents say it is highly difficult to safeguard confidential and personal data in AI

Figure 21. The impact of AI on privacy and security regulations
On a scale from 1 = not difficult to 10 = highly difficult, 7+ responses presented



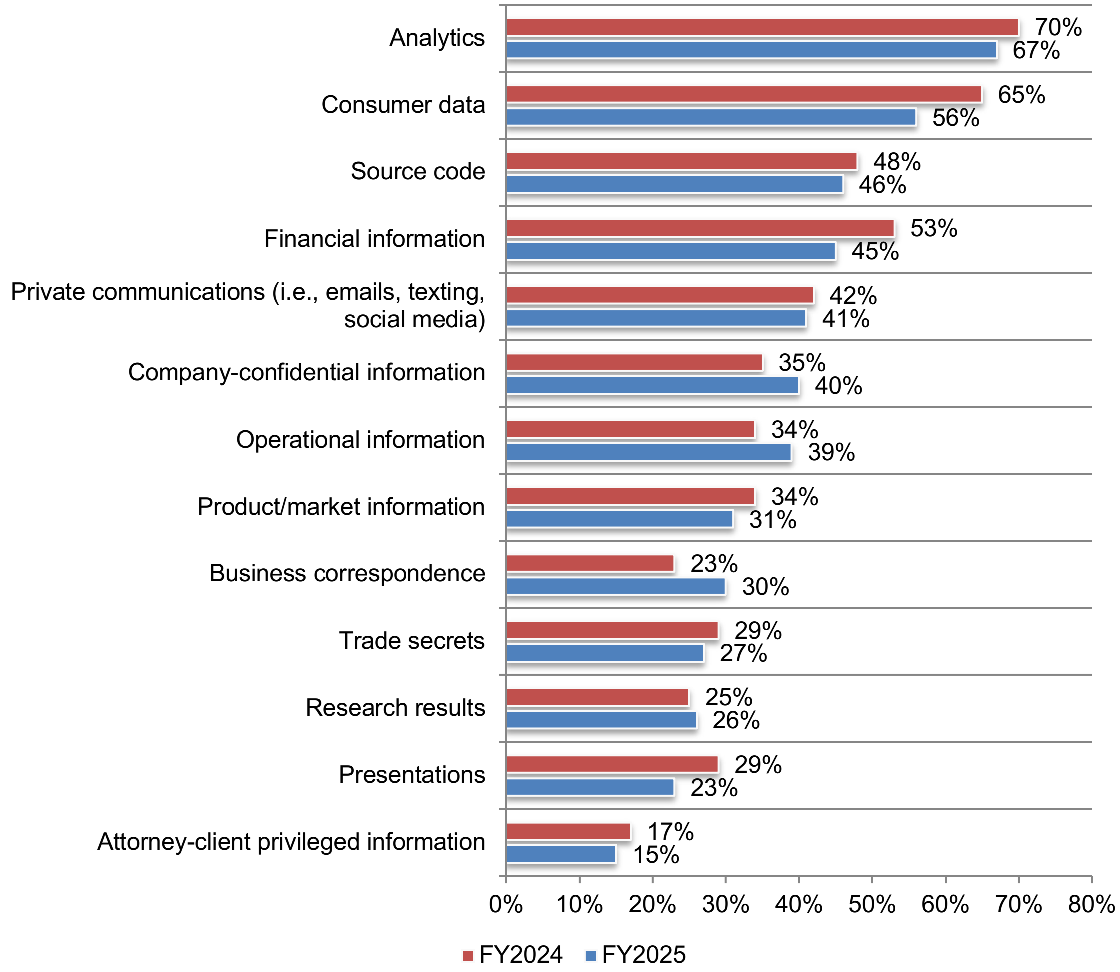
Transparency and explainability can help AI vendors build trust in their systems. According to Figure 22, 53 percent of respondents say providing transparency into the AI's decision-making process builds trust and 42 percent of respondents say the use of explainability builds trust.

Figure 22. How can AI vendors build trust in their systems?
Two responses permitted



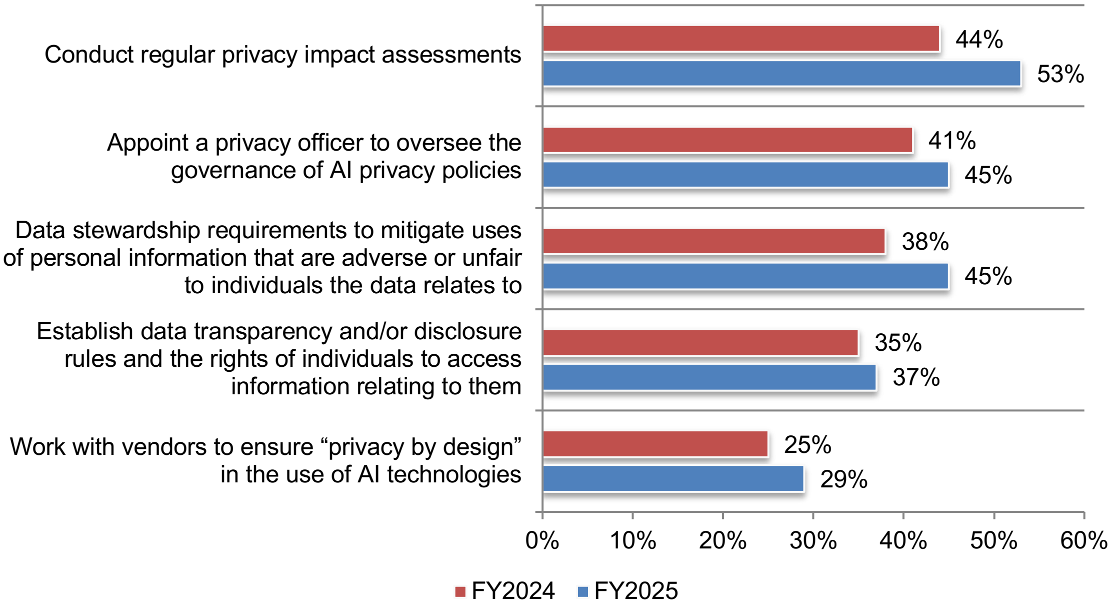
As the research shows, consumer data in AI is difficult to safeguard and has declined in usage. According to Figure 23, analytics is most often used in AI (67 percent of respondents). The use of consumer data and financial information have both declined from 65 percent to 56 percent and 53 percent to 45 percent, respectively.

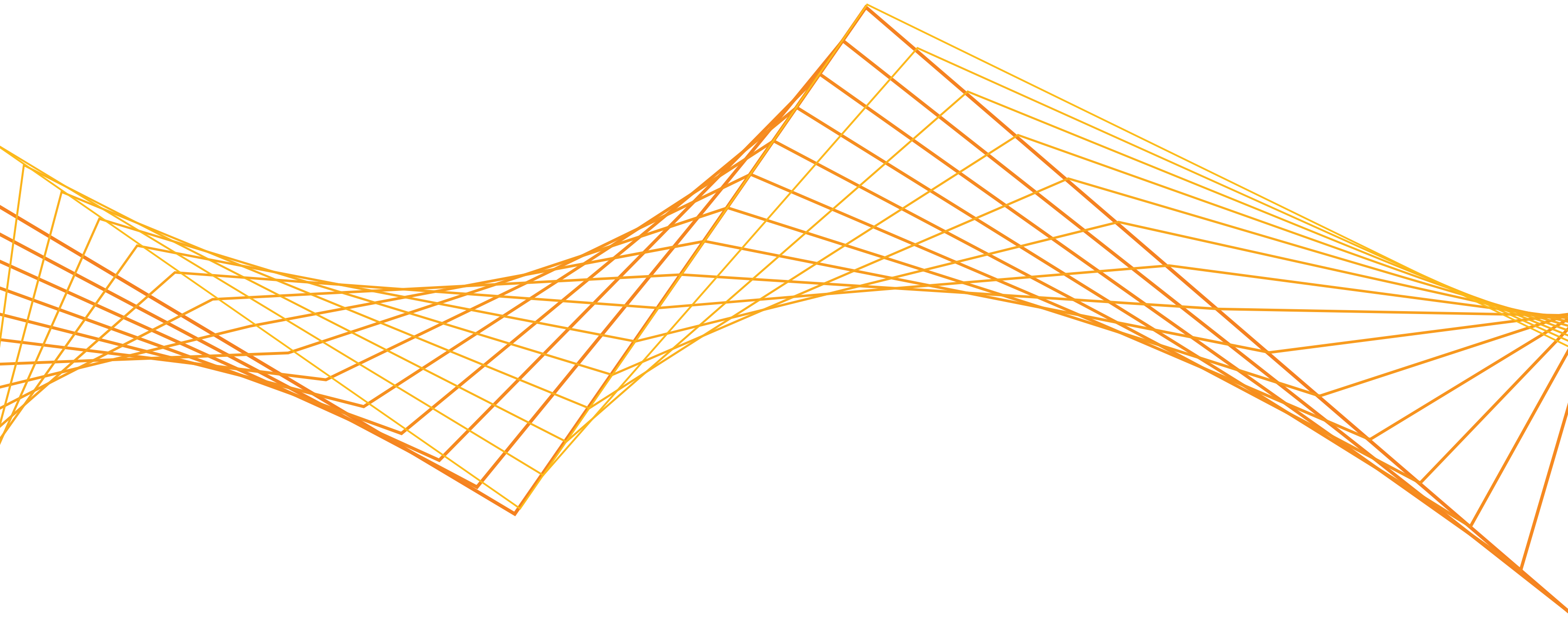
Figure 23. What confidential and personal data is used by your organization's AI?
More than one response permitted



Conducting regular privacy impact assessments is the number one practice in ensuring the privacy of sensitive and confidential data in AI. Forty-one percent of respondents say their organizations have privacy policies specifically for the use of AI. Figure 24 lists what is included in privacy policies. Regular privacy impact assessments have increased from 44 percent to 53 percent and data stewardship requirements to mitigate uses of personal information that are adverse or unfair to individuals the data relates to, an increase from 38 percent of respondents to 45 percent of respondents.

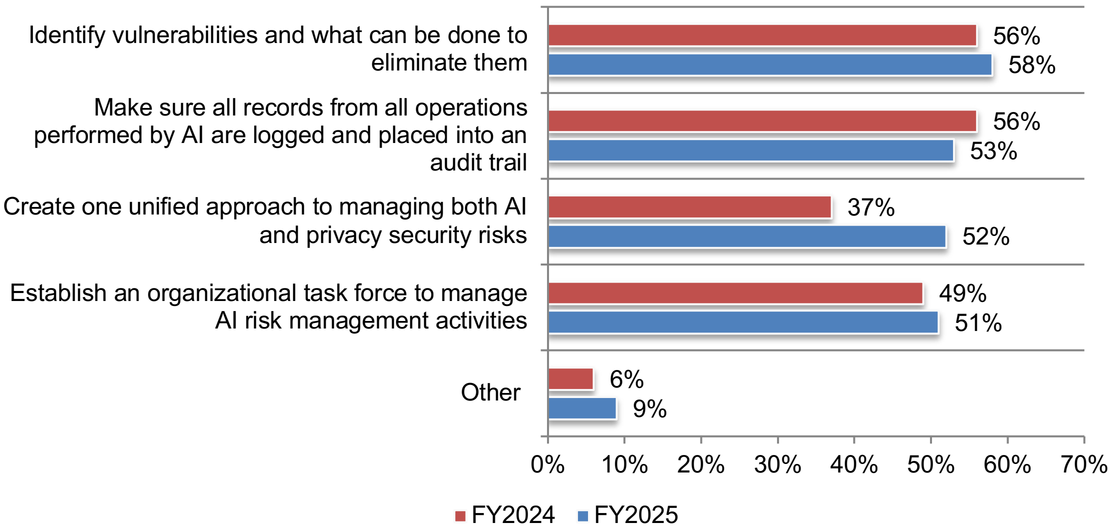
Figure 24. What is included in privacy policies?
More than one response permitted





More organizations are creating one unified approach to managing both AI and privacy security risks, an increase from 37 percent to 52 percent of respondents. Fifty-eight percent of respondents say their organizations identify vulnerabilities and what can be done to eliminate them, according to Figure 25.

Figure 25 Does your organization take any of the following steps to manage AI security risks?
More than one response permitted



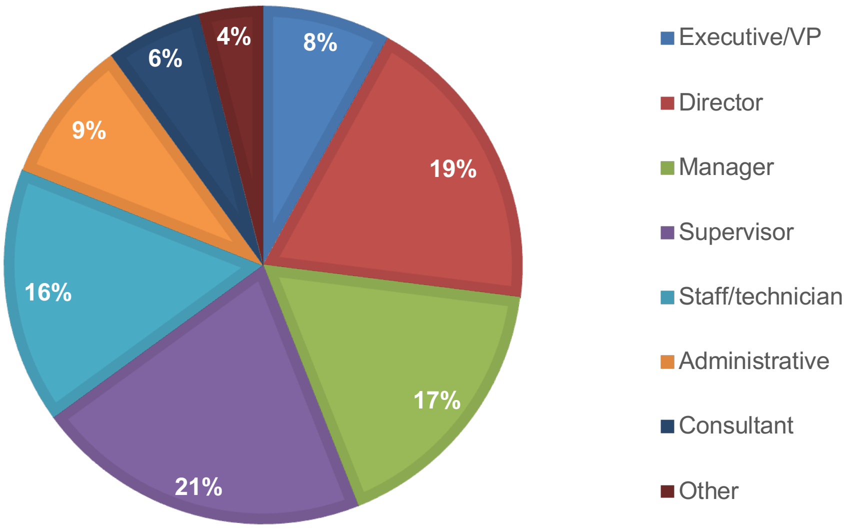
Part 3. Methodology

A sampling frame of 17,022 IT and IT security practitioners in organizations that are at some stage of AI adoption were selected as participants to this survey. Table 1 shows 717 total returns. Reliability checks required the removal of 76 surveys. Our final sample consisted of 641 surveys or a 3.8 percent response rate.

Table 1. Sample response	Freq	Pct%
Sampling frame	16,775	100.0%
Total returns	756	4.5%
Rejected or screened surveys	71	0.4%
Final sample	685	4.1%

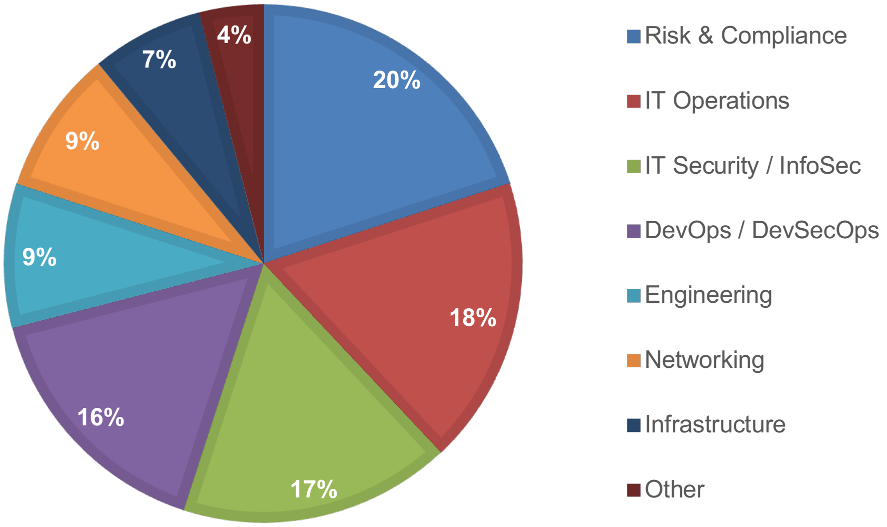
Pie chart 1 reports the respondent's organizational level within participating organizations. By design, more than half (65 percent) of respondents are at or above the supervisory levels.

Pie chart 1. Current position within the organization



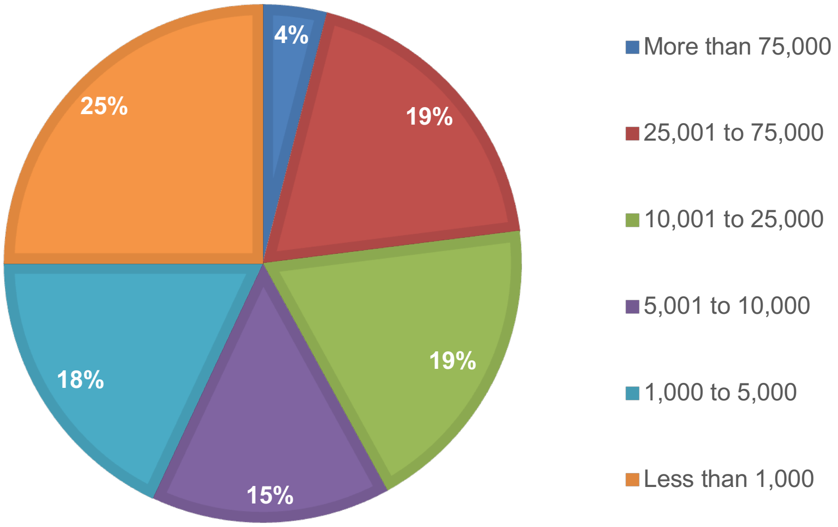
Pie chart 2 identifies the department or team the respondents are located in. Twenty-two percent of respondents are in IT operations, this is followed by IT security. InfoSec (20 percent of respondents), DevOps/DevSecOps (17 percent of respondents), risk and compliance (16 percent of respondents), and engineering (8 percent of respondents).

Pie chart 2. What best describes your department or team?



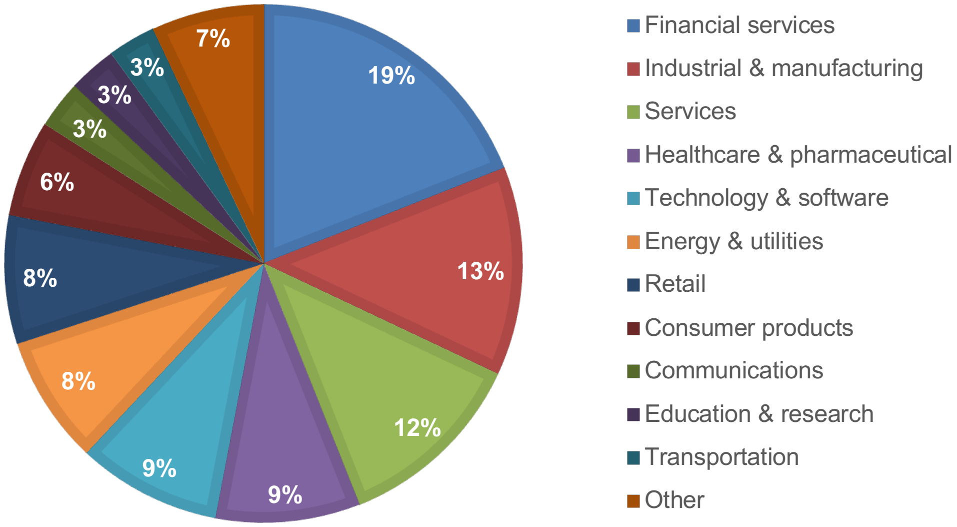
As shown in Pie chart 3, 69 percent of respondents are from organizations with a global headcount of more than 5,000 employees. The largest group is organizations with a headcount between 5,000 and 10,000 (26 percent of respondents).

Pie chart 3. Global full-time headcount



Pie chart 4 reports the industry classification of respondents' organizations. This chart identifies financial services (19 percent) as the largest industry focus, which includes banking, investment management, insurance, brokerage, payments and credit cards. This is followed by industrial and manufacturing (13 percent of respondents), services (12 percent of respondents), healthcare and pharmaceuticals (9 percent of respondents), technology and software (9 percent of respondents), energy and utilities and retail, (each at 8 percent of respondents).

Pie chart 4. Primary industry classification



Part 4. Caveats to this study

There are inherent limitations to survey research that need to be carefully considered before drawing inferences from findings. The following items are specific limitations that are germane to most web-based surveys.

- Non-response bias: The current findings are based on a sample of survey returns. We sent surveys to a representative sample of individuals, resulting in a large number of usable returned responses. Despite non-response tests, it is always possible that individuals who did not participate are substantially different in terms of underlying beliefs from those who completed the instrument.

- Sampling-frame bias: The accuracy is based on contact information and the degree to which the list is representative of individuals who are IT or IT security practitioners. We also acknowledge that the results may be biased by external events such as media coverage. Finally, because we used a web-based collection method, it is possible that non-web responses by mailed survey or telephone call would result in a different pattern of findings.

- Self-reported results: The quality of survey research is based on the integrity of confidential responses received from subjects. While certain checks and balances can be incorporated into the survey process, there is always the possibility that a subject did not provide accurate responses.

MixMode®

MixMode.ai

1 (858) 225-2352 info@mixmode.ai © MixMode, Inc.