Osterman Research

WHITE PAPER

White Paper by Osterman Research
Published **November 2024**
Sponsored by **Abnormal Security**

Using AI to Enhance Defensive Cybersecurity

Executive summary

The cyberthreat landscape is transforming rapidly as threat actors exploit artificial intelligence (AI) to drive attack sophistication and evasion techniques. As a result, security leaders are increasingly turning to AI-powered defensive tools to effectively combat the growing volume and sophistication of AI-enabled attacks.

This report explores the evolving use of AI in both offensive and defensive cybersecurity operations, providing actionable insights based on recent survey data from 125 security leaders in the United States. Three conclusions stand out:

- **AI is already a key enabler of advanced cyberattacks**
  Attackers are leveraging AI to automate and scale attacks, increase the evasion of current security controls, and accelerate attack velocity. Generative AI in particular is giving attackers the ability to create highly targeted, polymorphic phishing campaigns and more sophisticated malware strains that evade detection.
- **Defenders are moving quickly but face challenges**
  While 80% of security leaders agree that AI is essential for countering malicious AI, the deployment of effective AI defenses remains uneven. Defensive AI technologies like behavioral analysis and semi-supervised machine learning are gaining traction, but cybercriminals maintain a clear lead in areas like generative adversarial networks (GANs).
- **AI's impact on cybersecurity professionals is transformative**
  AI offers the potential to automate routine tasks, freeing cybersecurity professionals to focus on strategic initiatives such as threat hunting, incident response, and defense hardening. However, there is still work to be done in integrating AI into a cohesive long-term cybersecurity strategy, with only 70.4% of leaders ranking strategic alignment as a high priority.

Security leaders are increasingly turning to AI-powered defensive tools to effectively combat the growing volume and sophistication of AI-enabled attacks.

KEY TAKEAWAYS

- **Attackers have the early advantage in generative AI and GANs**
  Generative AI and GANs are tipping the scales in favor of attackers, but defensive AI tools are catching up, especially in behavioral AI and supervised machine learning.
- **Integrate AI strategically into cybersecurity frameworks**
  Strategic integration of AI into cybersecurity frameworks is essential to fully leverage the technology's potential. Organizations should focus on aligning AI investments with core business objectives and risk management practices.
- **AI is a force multiplier for cybersecurity teams**
  AI enables cybersecurity teams to focus on high-impact activities. However, this requires appropriate training, organizational alignment, and investment in the right tools.
- **The time for embracing AI in defensive cybersecurity is now**
  As AI reshapes both offensive and defensive cybersecurity, organizations must act swiftly to secure their infrastructures, adopt AI-powered defenses, and prepare their teams for the next generation of AI-enabled threats.

ABOUT THIS WHITE PAPER

Abnormal Security sponsored this white paper. Information about Abnormal Security is provided at the end of this paper.

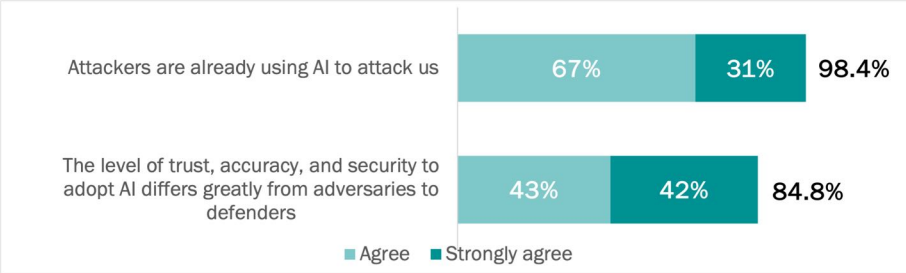
Cybercriminals are using AI in cyberattacks

The use of AI in cyberattacks is a current reality for almost all organizations.

AI IS ALREADY WIDELY USED IN CYBERATTACKS

Security leaders say that AI is already being widely used by attackers in cyberattacks against their organization. Most security leaders agree that adversaries and defenders face differing standards of trust, accuracy, and security when adopting AI. See Figure 1.

Figure 1
Use of AI by attackers in cyberattacks
Percentage of respondents



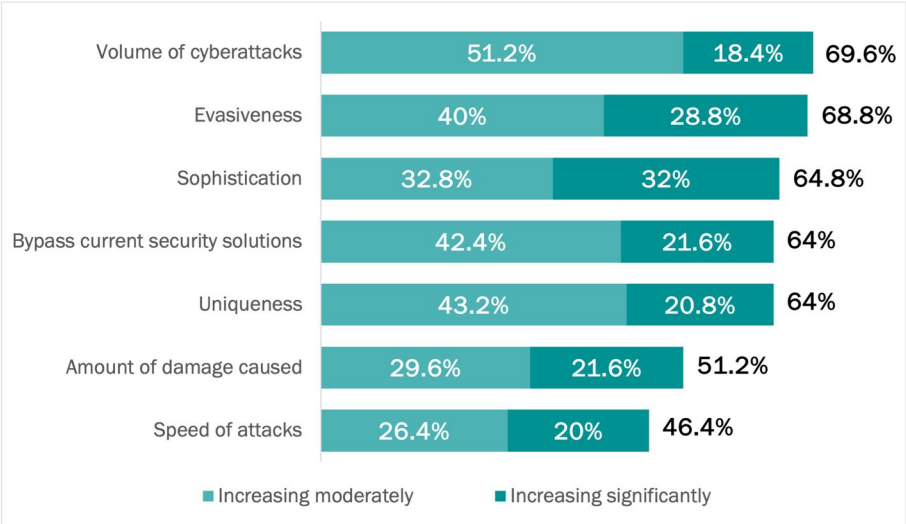
Source: Osterman Research (2024)

AI DRIVES ATTACK VOLUME, EVASIVENESS, AND SOPHISTICATION

The data from this research says that the use of AI by cybercriminals has led to an increased volume of attacks that are harder to detect. On average, 89% of security leaders say that seven characteristics of AI-enhanced cyberattacks have increased compared to two years ago. The most significant increases have been seen for attack sophistication (32%), attack evasiveness (28.8%), and the ability of attacks to bypass current security solutions (21.6%). See Figure 2.

The use of AI by cybercriminals is driving an increased volume of harder-to-detect attacks.

Figure 2
Impacts of AI as an adversarial or offensive threat compared to two years ago
Percentage of respondents



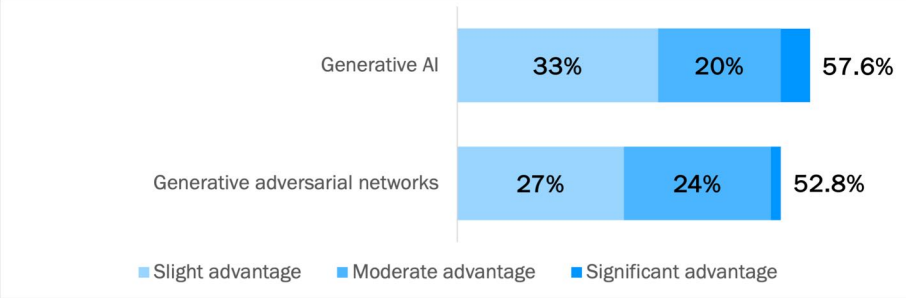
Source: Osterman Research (2024)

CYBERCRIMINALS HAVE THE ADVANTAGE IN TWO AREAS OF AI

Security leaders see differences in where cybercriminals and defenders have the advantage in using AI. Cybercriminals lead in two out of seven areas (see Figure 3):

- **Generative AI**
  Stimulates the creation of a higher volume of sophisticated and unique attacks, driving mass customization and hyper-personalization. Early examples include hyper-polymorphic phishing messages; creating and writing relevant content for realistic fake personas on social media platforms; and summarizing content to streamline decisions in data exfiltration attacks.[1]
- **Generative adversarial networks**
  A method of using neural networks to find ways to bypass current security controls.

Figure 3
Advantage in using AI capabilities: Cybercriminals lead
Percentage of respondents

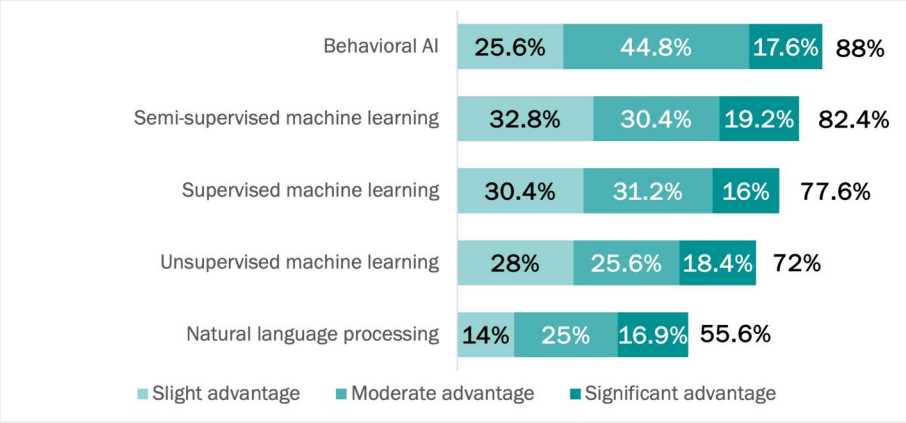


Source: Osterman Research (2024)

Defenders are seen as having the advantage in five of the seven capability areas. The greatest advantage for defenders is with behavioral AI—which analyzes patterns of behavior and flags deviations and anomalies that are likely to indicate threat activity. Security leaders rank all areas as having much clearer significant advantage compared to the cybercriminal areas above. See Figure 4.

Defenders have a strong advantage with behavioral AI for detecting and responding to threats, while cybercriminals excel in using generative AI to create advanced attacks.

Figure 4
Advantage in using AI capabilities: Defenders lead
Percentage of respondents



Source: Osterman Research (2024)

SIMILAR FINDINGS FROM ACROSS THE INDUSTRY

Other industry research corroborates the rise of AI in adversarial attacks:

- **Generative AI drives attack sophistication and volume**
  Security leaders express the highest concern for the risks of increased sophistication of email attacks, increased sophistication of malware, and the increased volume of email attacks from generative AI services used by cybercriminals.[2]

- **Generative AI gives cyber attackers an advantage**
  A survey by the World Economic Forum found that generative AI gives attackers the advantage over defenders, noting that *generative AI advances adversarial abilities in undertaking actions that defenders are already fighting against, e.g., phishing, malware, misinformation*.[3]

- **Threat actors designing malware with weaponized AI frameworks**
  Weaponized AI frameworks are being used by threat actors to design malware that bypasses current security controls in EDRs (endpoint detection and response), anti-virus tools, and other security solutions.[4] For example, threat actors use AI to generate a malware package and test it against an AI engine. If the package is detected as malicious, the generative malware service gains a learning point and then generates another attempt at bypassing current controls.

- **Threat actors designing malware with autonomous adaptation capabilities**
  Threat actors are also developing new malware strains with capabilities for autonomous adaptation to bypass security controls. Threat data often identifies malware with AI smarts that adapt when probed by cybersecurity defenses. Such malware variants adjust their behavior in response to security tools, hiding their malicious intent behind new evasive smokescreens.[5]

- **Malicious generative AI services reduce the required skill levels for threat actors**
  The availability of malicious generative AI services decreases the required skill levels for an attacker, making highly performant cybercrime methods available to a much larger pool of cyberthreat actors.[6]

- **High concern about deepfakes, a uniquely AI-created problem**
  Recent research found that almost all IT professionals expressed concern around the threat posed by deepfakes, an emerging type of AI-enabled cyberthreat.[7] 74% of survey respondents reported the highest level of concern for the future of weaponized deepfakes, and less than half had high confidence in their current defensive solutions to counteract deepfake attacks. 64% of respondents believe the volume of deepfake-enabled attacks will increase in the next 12-18 months, surpassing ransomware and account takeovers.

Weaponized AI frameworks are being used by threat actors to design malware that bypasses current security controls in EDRs and anti-virus tools.

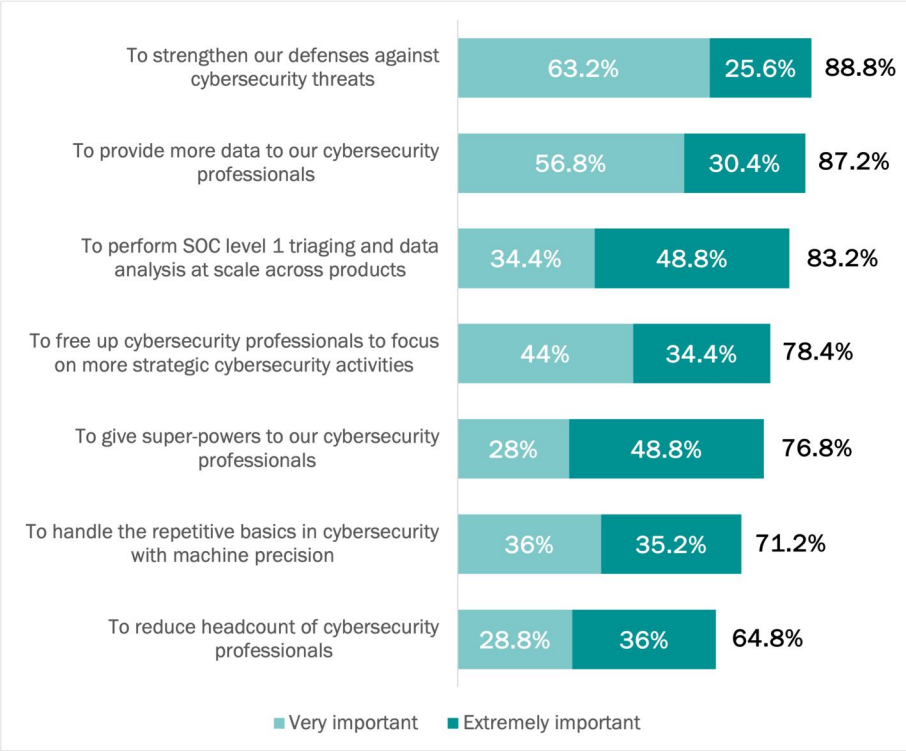
The strategic viewpoint on using AI to enhance defensive cybersecurity

This section looks at the drivers for using AI, defender expectations of AI, and addressing the risks of using AI in cybersecurity, among others.

MULTIPLE DRIVERS FOR USING AI IN DEFENSIVE CYBERSECURITY

Security leaders place highest priority on using AI in defensive cybersecurity for counteracting emerging AI-powered cyberthreats and strengthening the ability to detect what is anomalous or out of place in the ocean of signal and threat data. See Figure 5.

Figure 5
Drivers for using AI in defensive cybersecurity
Percentage of respondents



Source: Osterman Research (2024)

Four drivers in Figure 5 relate to cybersecurity professionals and AI. The highest one places AI in the role of redesigning work, so that cybersecurity professionals can focus on more strategic cybersecurity activities. Enabling this transition is the gift of cybersecurity super-powers and handling the repetitive basics in cybersecurity.

Of the four drivers, the least important is reducing headcount among cybersecurity professionals. Security leaders primarily want AI to improve the ability of the security team to engage in more important and strategic work—which involves changes in how work is carried out—rather than merely reducing headcount.

Strengthening defenses with richer data and a more skilled security team drives growing interest in defensive AI.

DEFENDERS HAVE HIGH EXPECTATIONS FOR MANY USE CASES OF AI

Security leaders have high expectations for how AI can strengthen defensive cybersecurity. 80% of leaders gave high ratings to 13 use cases. The rankings are closely aligned, with only small variations across the top use cases. See Figure 6.

Several areas stand out with high rankings:

- **Enhancing threat response processes**
  The top three use cases focus on improving how security operations centers (SOCs) handle critical threats. These include assembling reports for analysts, proposing steps to resolve incidents, and prioritizing critical alerts for investigation.

- **Prioritizing critical alerts for investigation received the highest "extremely important" ranking**
  Prioritizing critical alerts was rated as the most "extremely important" use case by security leaders. Prioritization, however, just scratches the surface. There is room to further develop AI's role in investigating alerts autonomously.

- **Predicting attacker activity received the second highest "extremely important" ranking**
  44% of leaders rated predicting attacker activity as "extremely important." AI's ability to analyze large data sets could help prevent attacks by detecting patterns early and enhancing defense strategies.

Other areas stand out for not having higher ratings:

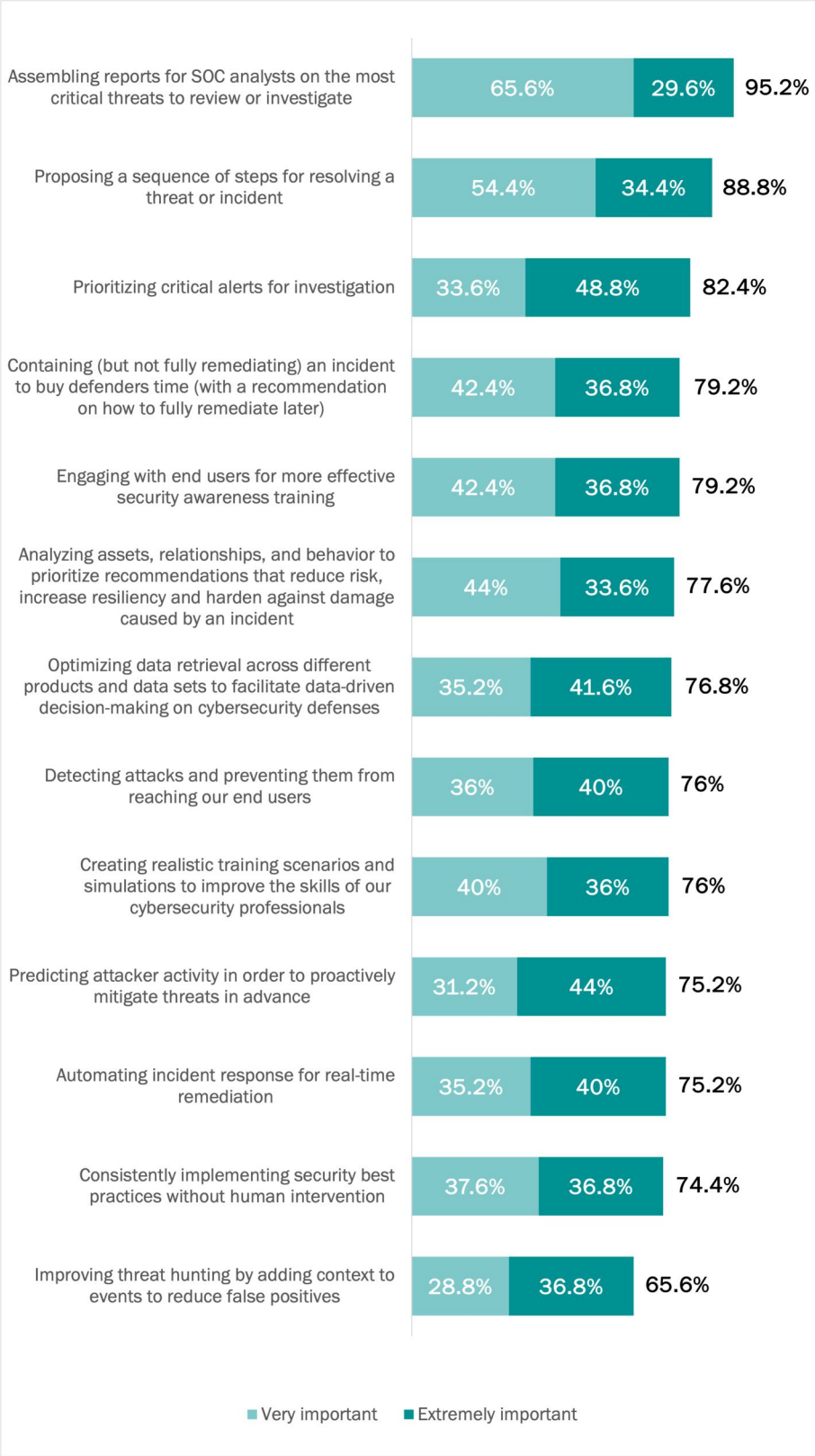
- **Analysis of assets, relationships, and behavior to make recommendations**
  The ability of AI to crunch through large datasets to identify the best approaches for reducing risk seems underweighted in these answers. This is a more strategic use of AI than using it for prioritizing critical alerts for investigation. It should be rated as more important.

- **Blocking attacks from reaching end users**
  With strengthening cybersecurity defenses the highest rated driver in Figure 5 above, we would have expected to see "detecting attacks and preventing them from reaching our end users" ranked much closer to 100% on the importance scale. It currently ranks at 76%. Stopping attacks from getting through to where they may be activated should be a critically important use case for all organizations.

- **Consistently implementing security best practices**
  If best practices can be defined, using AI to ensure they are consistently implemented with appropriate adaptability is a strong use case. This reduces the need for human intervention in day-to-day security workflows.

There is across-the-board interest in using AI to strengthen cybersecurity capabilities.

Figure 6
Importance of using AI in defensive cybersecurity use cases
Percentage of respondents



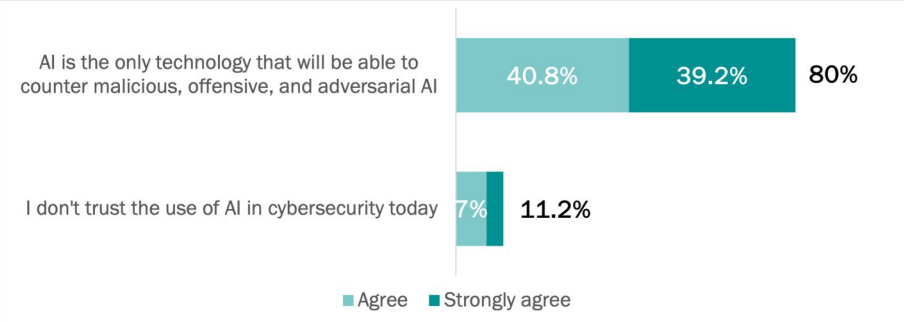
Source: Osterman Research (2024)

There is much to be done to embrace the full potential of AI across multiple use cases.

DEFENDERS HAVE HIGH EXPECTATIONS FOR USING AI TO DETECT AND RESPOND TO AI-POWERED CYBERTHREATS

Security leaders have very high expectations for the role of AI in counteracting malicious, offensive, and adversarial AI attacks, with 80% viewing it as the only technology that will work. Only 11.2% of security leaders distrust the use of AI in cybersecurity today. See Figure 7.

Figure 7
The importance of AI in cybersecurity today
Percentage of respondents



Source: Osterman Research (2024)

Security leaders see a significant role for AI-powered defenses to detect and respond to many types of AI-enabled cyberthreats (see Figure 8). Notable expectations include:

- **Detecting attacks enabled by AI top the list**
  Security leaders anticipate the highest role for AI-powered defenses will be to detect and respond to new attacks made possible by the malicious use of AI by cybercriminals, such as the creation of deepfakes, hidden logic bombs, and evasive malware. What AI used for malicious purposes can create or enable, security leaders insist that AI on the defensive side must be able to identify and stop. Without the use of AI, defenders don't have highly performant security capabilities to counter these new types of attacks.

- **Complex attacks are especially important to detect**
  Advanced multi-stage attacks that unfold across multiple platforms received the highest rating for "extremely important," followed by hidden logic bombs in second place. Threat signals from discrete systems treated in isolation will not uncover advanced multi-stage attacks.

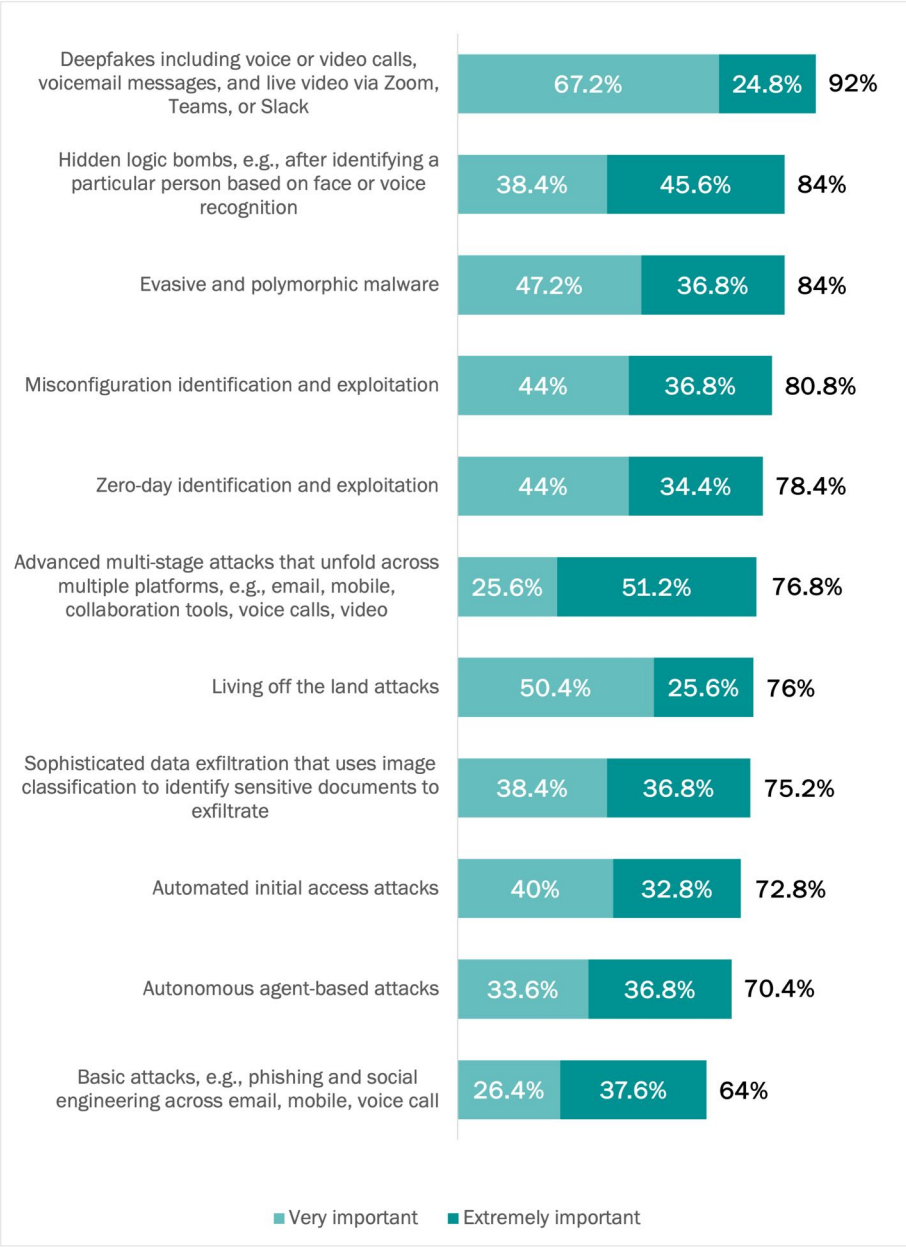
  To achieve such an outcome, AI-powered solutions that can aggregate, correlate, and determine anomalous patterns across multiple systems are essential.

  The detection of hidden logic bombs is an equally complex challenge, requiring deep analysis of software code and differential run-time execution pathways to ascertain behavior that doesn't make sense.

80% of security leaders say that AI is the only technology that will be able to counter malicious, offensive, and adversarial AI.

- **Additive detection capabilities for common types of attacks**
  Using defensive AI is expected to make a net positive improvement to the detection of current types of cyberattacks, including identifying misconfigurations and zero-days. The detection of basic phishing and social engineering attacks is also expected to benefit from AI, with the third highest rating for "extremely important" across all types (37.6%). It is unclear why basic attacks ranked in last place overall, since this remains a very common attack vector that results in costly incidents. One potential reason is that, comparatively speaking, the other types of attacks in Figure 8 are newer and not so well addressed by current security solutions. Hence AI is seen as making a more substantial difference in security defenses across the other areas.

Figure 8
Importance of AI defenses in detecting and responding to AI-enabled cyberthreats
Percentage of respondents



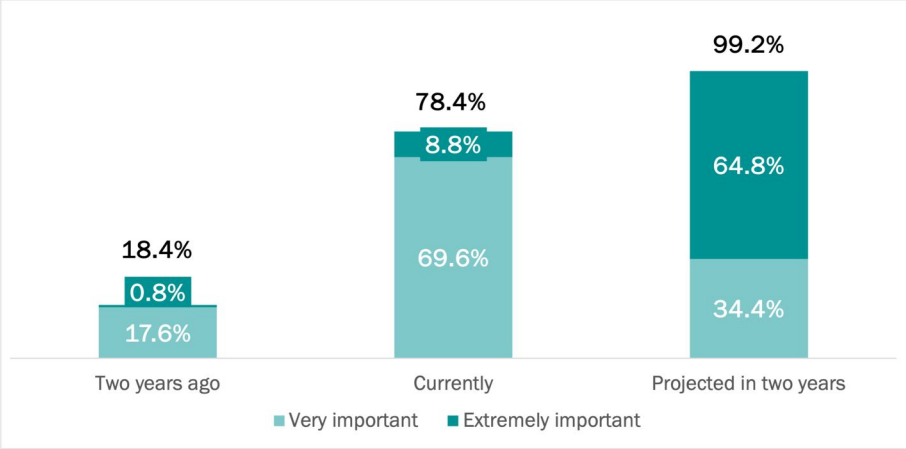
Source: Osterman Research (2024)

Security leaders are looking to AI-powered defenses to counteract threats made possible by the malicious use of AI.

DEFENDERS AIM TO FLIP ATTACKER-DOMINATED CAPABILITIES

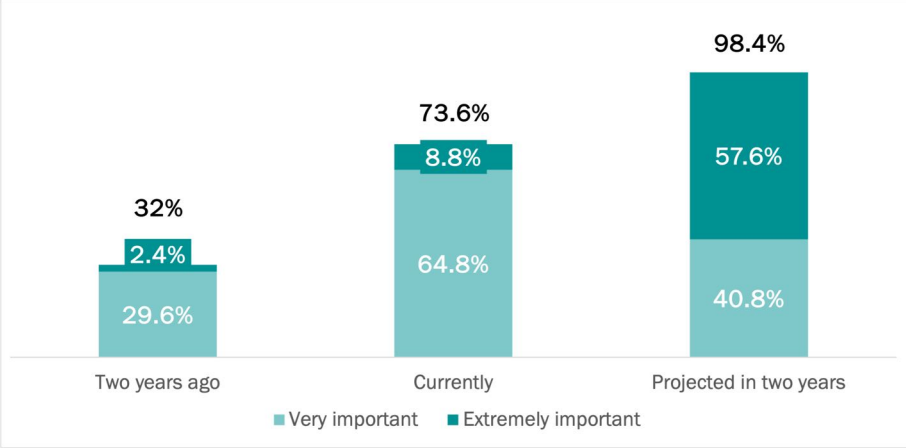
Cybercriminals have established an early advantage over defenders in the use of generative AI and generative adversarial networks (see page 4). The security leaders in this research aim to neutralize this advantage. They indicate that the importance of both capabilities for use in defensive activity is growing rapidly and significantly. There is a five times' increase in overall importance from two years ago to projected importance in two years' time for generative AI (see Figure 9) and a three times' increase over the same timeframe for generative adversarial networks (see Figure 10). The strength of the importance rating is growing quickly, too, with 64.8% and 57.6% respectively of security leaders saying that generative AI and generative adversarial networks will be "extremely important" in two years' time, up from essentially nothing for both capabilities two years ago.

Figure 9
Importance of generative AI to defenders
Percentage of respondents



Source: Osterman Research (2024)

Figure 10
Importance of generative adversarial networks to defenders
Percentage of respondents



Source: Osterman Research (2024)

Generative AI and generative adversarial networks are becoming increasingly important in defensive cybersecurity.

ADDRESS THE RISKS OF EMBRACING AI FOR DEFENSIVE CYBERSECURITY

Many security leaders are increasingly concerned about the risks AI poses to their organizations, both in the short and long term. Over the next 12 months, the top issues include threat actors gaining access to sensitive data used for training machine learning models and bypassing the safety features of AI systems. These risks threaten the day-to-day effectiveness of AI-powered cybersecurity solutions. Given the relative newness of AI-powered defenses, significant unknowns remain. Looking five years ahead, bypassing AI safety features is expected to be the most significant risk, followed by false attribution from nation-state attacks. For more details, see Figure 11.

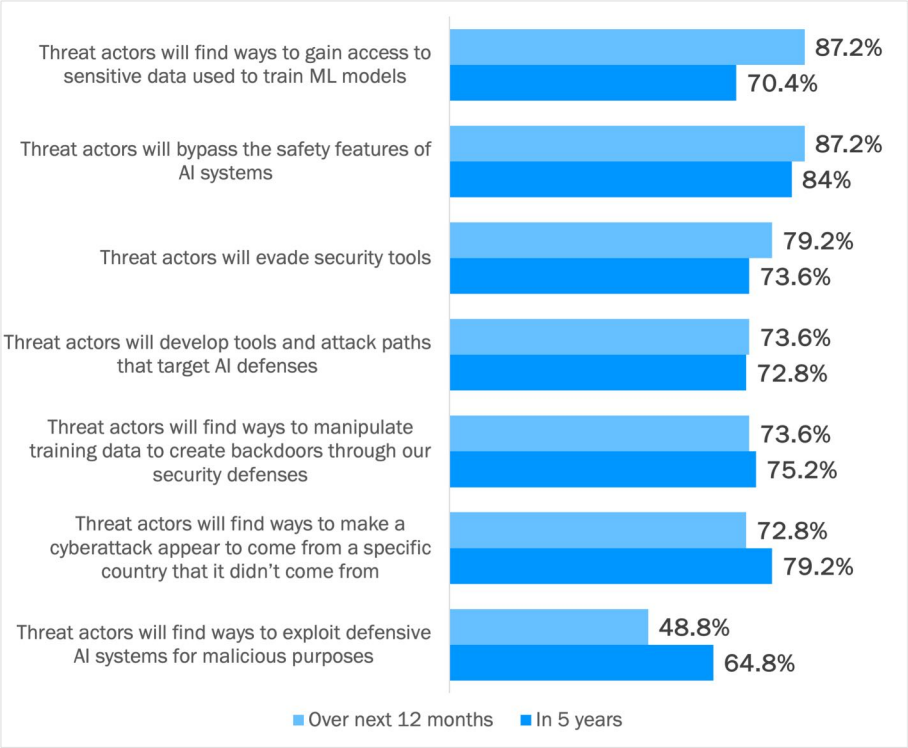
The two risks that intensify the most over the next five years. are:

- **Exploiting defensive AI systems for malicious purposes (32.8% increase)**
  Security leaders say the concern of greatest change over the next five years is defensive AI systems being exploited for malicious purposes. No security leader wants to see their bolstered defenses turned against them, especially as AI-powered tools refactor both their defenses and how their security team works. However, despite the significant increase, this is still rated as the lowest risk of the seven both in 12 months and five years.

- **False attribution from nation-state attacks (8.8% increase)**
  A key principle of defense is knowing who the attacker is. When AI is used to disguise the true source of a cyberattack by making it appear to come from a different country, it leads to a series of missteps. This can harm trade and business while allowing the real attackers to remain hidden.

Security leaders are highly concerned that threat actors will find ways to undermine the day-to-day efficacy of AI-powered defensive cybersecurity solutions to perform as expected.

Figure 11
Concerns about risks from AI systems
Percentage of respondents indicating “highly concerned” or “extremely concerned”



Source: Osterman Research (2024)

Effectiveness of early investments in AI

The results of early investments in AI for defensive cybersecurity are highly promising, leading to an appetite for greater investment in coming years.

AI-POWERED CYBER DEFENSES ARE VIEWED AS THE ESSENTIAL TO STOP AI-ENABLED ATTACKS

Four out of five security leaders agree or strongly agree with three statements about cybersecurity tools that leverage AI for defensive purposes:

- Such tools are better equipped to stop attacks of all kinds, not just AI-enabled attacks.
- There are solutions currently available on the market that use defensive AI effectively.
- Finding the right approaches or solutions takes work to break through the noise and see what makes a difference to the cybersecurity defenses in their organization.

Of the three, the highest rating on both the "strongly agree" and "disagree" scale is for breaking through the noise to see what makes a difference. AI as a defensive cybersecurity play is still in its early years, and for many vendors and organizations, there remains a lot to deliver and comprehend. Organizations will work with their vendors to say what is and isn't working with these new tools, and vendors will adjust as more real-world experience is gained across a greater number of customer environments. Ideally, greater clarity will emerge over the next three to five years on what solutions make a difference and where. On the other hand, the higher "disagree" rating for this option (9.6% versus 3.2% for each of the other two) indicates that some security leaders are already finding it easier to identify the approaches and solutions that make a difference.

See Figure 12.

Security leaders see AI-powered defensive tools as a strategic play for all kinds of attacks, not only for attacks that leverage AI.

Figure 12
Statements about cybersecurity tools that leverage AI for defensive purposes
Percentage of respondents

Source: Osterman Research (2024)

DEFENDERS ARE ALREADY USING AI IN CYBERSECURITY ...

Security leaders say they are already using AI for an average of 10 cybersecurity tasks out of a list of 24 tasks we queried. The highest uses of AI currently are for detecting phishing attacks, account (or identity) takeover, and accidental data exposure. At the low end of adoption, AI is barely scratching the surface on source code and vulnerability checks. With an average adoption rate of only 44.3%, there is still a ton of room to grow.

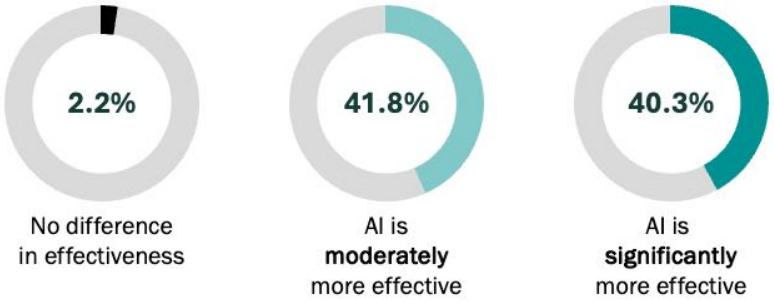
... AND REAPING HIGHER EFFECTIVENESS FOR CYBERSECURITY TASKS

For each of the cybersecurity tasks they are currently enhancing with AI, we asked security leaders to assess how much better AI-powered cybersecurity solutions were versus what they were using previously. Nearly 98% of security leaders say AI-powered tools are outperforming their previous solutions—40.3% say they are "significantly more effective," and 41.8% say "moderately more effective." No security leaders said AI-powered cybersecurity solutions were "less effective," and only an average of 2.2% said there was no difference. See Figure 13.

- **Highest ratings for significantly more effective**
  The effectiveness of AI-powered cybersecurity solutions for nine tasks is ranked by around half of security leaders as being "significantly more effective" than previous approaches. This includes detecting financial fraud attempts (52.9%) and detecting malware (51.9%) at the high end of the list of nine and developing adaptive responses to incidents in ninth place (47.5%).
- **Deepfakes is in the top nine**
  Earlier, we saw that deepfakes received the highest rating for how AI can be used to detect and respond to AI-enabled cyberthreats (see Figure 8). 48.1% of security leaders said their AI-powered cybersecurity solutions to address deepfakes were "significantly more effective" than previous solutions, and in total, 98.8% said AI-powered solutions were more effective to some degree. With deepfakes being a modern AI-enabled cyberthreat, AI-powered cybersecurity solutions are essential for identifying attacks.
- **The overall trendlines are in the right place**
  With 97.8% of security leaders saying that their early experiences with AI-powered cybersecurity solutions across a whole set of solution categories have already proven to be more effective than previous approaches, the trendline for AI in cybersecurity is in the right place. Clearly, we would like to see the "significantly more effective" ratings significantly higher than they are currently, but the numbers are already highly net positive.

97.8% of security leaders say that AI-powered cybersecurity solutions are more effective compared to their previous cybersecurity solutions.

Figure 13
AI-powered cybersecurity solutions are more effective
Percentage of respondents (average per rating option)



Source: Osterman Research (2024)

SECURITY LEADERS SEE A DIVERSE SET OF BEST USE CASES WITH AI FOR STRENGTHENING OR ENHANCING DEFENSIVE CYBERSECURITY

In an open-ended question, we asked security leaders to share the best use of AI they had seen for strengthening or enhancing defensive cybersecurity. We analyzed the free text answers and added a classification label to summarize each. Many of the answers prepended the phrase "AI-powered," "ML-powered" or "AI-enabled," as in "AI-powered cloud security" or "ML-powered threat detection," but we excluded those from the classification label for readability.

A word cloud of the answers—with larger phrases indicating higher frequency in the answers—is shown in Figure 14.

- **Dominant use cases**
  Several use cases clearly dominate the word cloud, with network traffic analysis, threat detection, and phishing email identification the top three. A second-tier group includes cloud security, threat hunting, and predictive threat detection.

- **Emphasis on enhancing current cybersecurity processes**
  All the answers in the word cloud focus on enhancing processes that are currently undertaken in cybersecurity. AI is an additive play with various degrees of contribution—offering ways of rethinking, reimagining, or even fundamentally rearchitecting how cybersecurity processes are undertaken.

- **A diverse set of best use cases indicates wide applicability**
  The security leaders in this research offer a diverse collection of best use case ideas. AI has wide applicability across many areas for enhancing defensive cybersecurity, not just an isolated set of limited use cases.

Security leaders approach AI as an additive play, offering new ways of rethinking, reimagining, or fundamentally rearchitecting how cybersecurity processes are undertaken.

Figure 14
Best use of AI for strengthening or enhancing defensive cybersecurity

Source: Osterman Research (2024)

FUTURE INVESTMENT PRIORITIES FOR DEFENSIVE AI

More than 70% of security leaders said there is a high priority for investing in many AI capabilities to strengthen defensive cybersecurity over the next 12 months. See Figure 15.

Figure 15
Investment priorities for defensive AI capabilities over the next 12 months
Percentage of respondents

Source: Osterman Research (2024)

In looking at Figure 15 above:

- **Detecting malware heads the list**
  Using AI to detect malware is the highest rated priority for the next 12 months, with 98.4% of security leaders saying it is a high or extreme priority at their organization. Earlier in this report, we mentioned the trends of threat actors designing malware with weaponized AI frameworks and with autonomous adaptation capabilities to bypass security controls (see page 5). Detecting this next generation of AI-enabled malware with AI-powered defensive capabilities is seen as being highly important.

- **Detecting—and stopping—data loss is seen as an extreme priority**
  The two capability areas with the highest ratings for "extreme priority" are both about data loss. Detecting accidental data exposure is in second place overall in the list (87.2%), but first for the extreme rating (56.8%). Detecting data breach incidents is 23rd in the list overall, but second for the extreme rating (48%). Data protection regulations across the world have raised the level of awareness of the damage caused by data breaches and have set higher minimum expected standards for organizations of all kinds.

- **Security leaders want AI to improve almost everything**
  There is not a lot of variation between the ratings across the 24 capability areas in Figure 15, with all but three of the areas being within 10% of the average. Security leaders say they want everything to get better with AI.

  On the one hand, that isn't a problem because cybersecurity vendors with AI solutions are more than willing to help. On the other hand, it sets a very high bar for the industry to meet in order to prevent expectations from crashing dramatically.

  We would expect to see a greater level of variation between these ratings as the use of AI for defensive cybersecurity matures over the next several years.

Security leaders want everything in cybersecurity to get better with AI.

What AI means for cybersecurity personnel

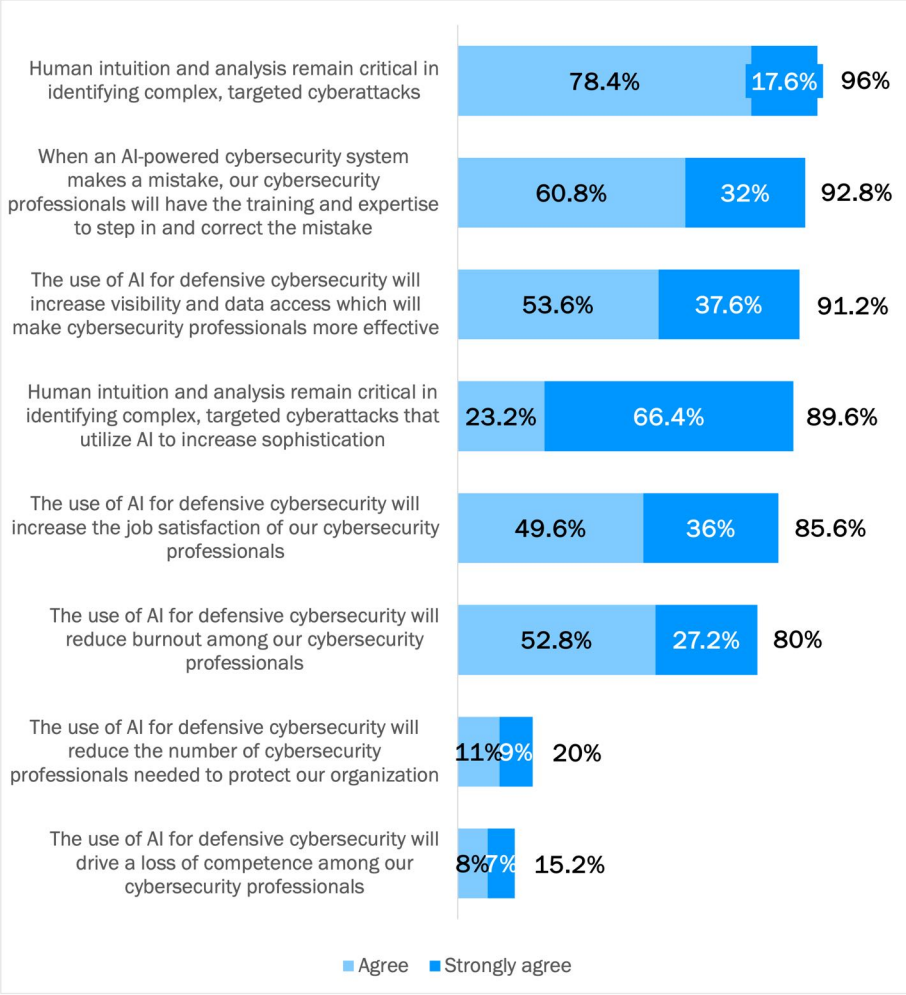
Cybersecurity professionals are affected by the security solutions used by their organization. Let's look at how AI impacts these dynamics.

AI AND CYBERSECURITY PROFESSIONALS ARE A COMPLEMENTARY PLAY

Nine out of ten security leaders see a complementary relationship between defensive AI solutions and cybersecurity professionals, rather than one in which AI replaces security personnel. In the opinion of these respondents, AI doesn't eliminate the need for human intuition and analysis to identify complex attacks, cybersecurity professionals will have the training and expertise to correct AI mistakes, and the visibility gifted by AI makes cybersecurity professionals more effective. In other words, few security leaders believe they will need fewer cybersecurity professionals and loss of competence among cybersecurity professional is not anticipated.

See Figure 16.

Figure 16
Relationships between defensive AI solutions and cybersecurity professionals
Percentage of respondents



Source: Osterman Research (2024)

Security leaders see a complementary relationship between defensive AI solutions and cybersecurity professionals.

It remains to be seen whether the strength of the beliefs in Figure 16 is fair or unfounded. For example:

- **Cybersecurity professionals will have the training and expertise to correct mistakes made by AI-powered cybersecurity systems**
  Believing this to be true sets a very high standard of performance from cybersecurity professionals and the organizations they work for. If this belief is to translate into reality, cybersecurity professionals will require deep training in AI model troubleshooting, along with organizational decision processes to ensure the selection of AI systems with high interpretability.

- **Reducing burnout of cybersecurity professionals**
  Let's do a thought experiment. If current attack dynamics remain unchanged on the offensive side, then logically the adoption of AI for defensive cybersecurity will increase detection efficacy, dramatically shrink the workload, and reduce burnout.

  By contrast, if attack dynamics scale and morph as they are expected to do with AI-enabled cyberattacks (for example, in volume, attack evasiveness, and attack sophistication as explored on page 3), it is likely that cybersecurity professionals will find themselves just as busy fighting new types of attacks with new types of solutions.

  Finally, if attack dynamics scale and morph as they are expected to do but organizations do not embrace AI-powered defenses, cybersecurity professionals are likely to be completely overwhelmed by attacks they can't detect, evade, or mitigate.

- **Changing the nature of competence**
  Only 15.2% of security leaders believe that cybersecurity professionals will lose competence due to using AI for defensive cybersecurity. If defensive cybersecurity solutions make greater use of AI to augment or eliminate tasks that current cybersecurity professionals have the competence to complete without AI, then over some time period, cybersecurity professionals will lose their hard-won ability to complete these tasks without the help of AI. This will create a new level of dependence between machines and people in cybersecurity, although this general principle is true across all professions embracing AI to augment human intelligence.

  However, while the competence to execute current tasks may decline, the need to develop new areas of competence to work effectively with AI-powered solutions will grow. On balance, it seems fair to conclude that competence to complete current tasks will diminish as AI-powered solutions step in, but in terms of an overall assessment of human competence, levels will at minimum remain the same, if not increase.

Cybersecurity professionals will develop new areas of competence to work effectively with AI-powered solutions.

THE PROMISE OF PIVOTING FROM BASIC TO STRATEGIC ACTIVITIES

The promise of being able to focus on "more strategic activities" is commonly posited as a benefit of investing in new cybersecurity and other IT solutions. These are generally undefined, however, but the security leaders in this research have a clear picture. If the promise of AI to enhance defensive cybersecurity is achieved, security leaders want cybersecurity professionals to spend more time on:

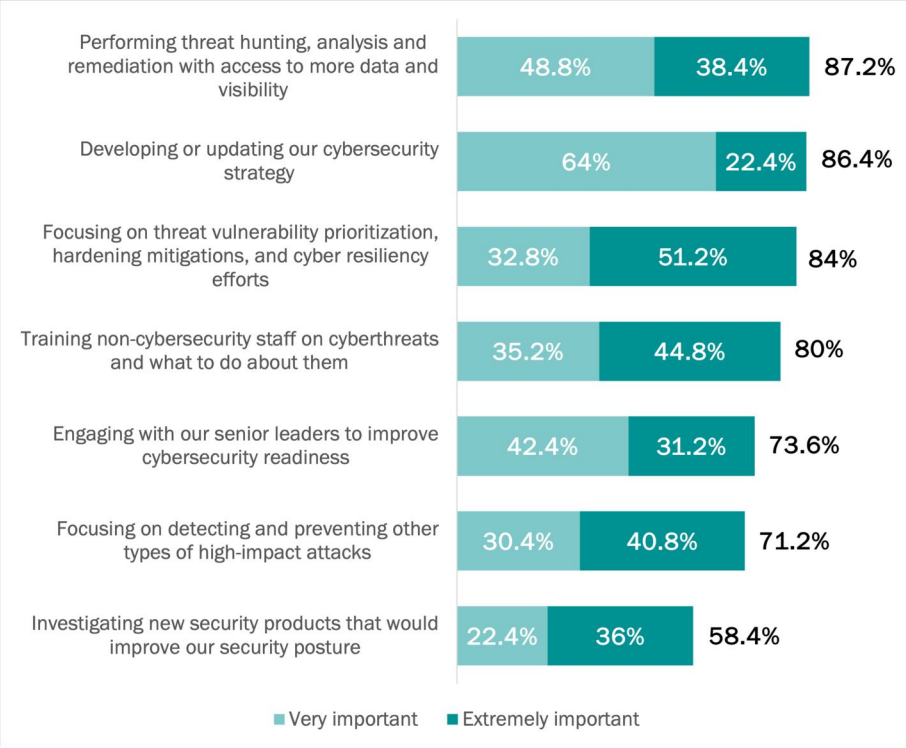
- **Threat hunting and response**
  Two of the highest rated strategic activities are seen as more effective threat hunting and efforts at hardening defenses. For threat hunting, security leaders see having access to more data and visibility with AI as driving higher efficacy response, which means outcomes such as hardened mitigations and better cyber resiliency. It appears that regardless of what tools you have and what capabilities they offer, dealing with threats is an enduring strategic responsibility for cybersecurity professionals.

- **Strategy development and engaging with senior leaders on cybersecurity**
  Strengthening the cybersecurity strategy and engaging with senior leaders to improve cybersecurity readiness are usually viewed as strategic activities. Security leaders ranked these in second and fifth places overall. However, both activities received the lowest "extremely important" ratings of the seven listed, indicating that other strategic activities will probably rise to the top of the list in practice.

Dealing with threats is an enduring strategic responsibility for cybersecurity professionals. AI isn't going to change that.

See Figure 17.

Figure 17
Preferred strategic activities for cybersecurity professionals
Percentage of respondents



Source: Osterman Research (2024)

Conclusion

As AI reshapes both offensive and defensive cybersecurity, organizations must act swiftly to secure their infrastructures, adopt AI-powered defenses, and prepare their security teams for the next generation of AI-enabled threats. Early investments in AI-powered defenses are already paying off in higher effectiveness against emerging attack methods, and organizations that embrace these new defenses quickly and prepare their security teams to leverage the best of what AI offers will be the best positioned to address the next waves of AI-enabled cyberthreats.

Organizations must act swiftly to secure their infrastructures against emerging AI-enabled threats.

Sponsored by Abnormal Security

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

You can deploy Abnormal in minutes with an API integration for Microsoft 365 or Google Workspace and experience the full value of the platform instantly. Additional protection is available for Slack, Workday, Salesforce, ServiceNow, Zoom, Amazon Web Services and multiple other cloud applications.

abnormalsecurity.com

Abnormal

abnormalsecurity.com

@AbnormalSec

Methodology

This white paper is based on findings from a survey conducted by Osterman Research. One hundred twenty-five (125) respondents who have high levels of responsibility for cybersecurity and AI at their organization were surveyed during September 15 to 21, 2024. To qualify, respondents had to work at organizations with at least 500 employees and/or have at least 50 people on their security team. All surveys were conducted in the United States. The survey was cross-industry, and no industries were excluded or restricted.

JOB ROLE

IT manager or director	25.6%
Security manager or director	24.0%
CISO, or some other role that has this responsibility	20.0%
Cybersecurity manager or director	16.8%
CIO, or some other role that has this responsibility	13.6%

ORGANIZATION SIZE

500 to 2499 employees	52.8%
2500 to 4999 employees	38.4%
5000 to 9999 employees	7.2%
10,000 or more employees	1.6%

INDUSTRY

Healthcare	12.0%
Professional services (law, consulting, etc.)	10.4%
Life sciences or pharmaceuticals	9.6%
Retail or ecommerce	9.6%
Data infrastructure or telecom	8.0%
Energy or utilities	7.2%
Information technology	7.2%
Computer hardware or computer software	6.4%
Financial services	6.4%
Hospitality, food or leisure travel	6.4%
Media or creative industries	4.8%
Education	3.2%
Industrials (manufacturing, construction, etc.)	3.2%
Transport or logistics	2.4%
Public service or social service	1.6%
Agriculture, forestry or mining	0.8%
Government	0.8%

[1] Darktrace, The CISO's Guide to Cyber AI: Categorizing the Use of AI in Cyber Security, December 2023, at https://darktrace.com/resources/the-cisos-guide-to-cyber-ai

[2] Abnormal Security, The State of Email Security in an AI-Powered World, October 2023, at https://abnormalsecurity.com/resources/state-of-email-security-ai-powered-world

[3] World Economic Forum, Global Cybersecurity Outlook 2024, January 2024, at https://www.weforum.org/publications/global-cybersecurity-outlook-2024/

[4] SentinelOne, Impacts of AI in Security: A New Era in Defense, March 2024, at https://assets.sentinelone.com/defendnext/impacts-ai-security-en

[5] Constella Intelligence, 2024 Identity Breach Report, August 2024, at https://constella.ai/wp-content/uploads/2024/08/Constella_IdentityBreachReport-2024.pdf

[6] Osterman Research, The Role of AI in Email Security, August 2023, at https://ostermanresearch.com/2023/08/21/orwp_0358/

[7] Ironscales, New Research From IRONSCALES Reveals Deepfake Dread Looms Large Among IT Professionals: Over 74% "Very Concerned"With What Future Holds, October 2024, at https://ironscales.com/news/new-research-from-ironscales-reveals-deepfake-dread-looms-large-among-it-professionals-over-74-very-concerned-with-what-future-holds