March 2025

Fighting AI Cyber Crime with AI Cyber Defense

How IT leaders are leveraging AI to defend against AI-powered cyber threats

The Register®

Introduction

Cyber threats continue to be a big problem, and an ongoing headache for the IT professionals responsible for fighting them. According to the Global Cybersecurity Index 2024 published by the International Telecommunications Union (ITU), 8bn records worldwide were breached in 2023 across 2,800 separate incidents. And the cost of cleaning up after those data breaches expanded by 15% per incident compared to the same period three years earlier.

There's clearly a lot of cyber crime about, so how can organizations best marshal their defenses and often limited expert resources to thwart it?

Cyber criminals tend to be more agile than the average enterprise when it comes to harnessing new technologies for their purposes, and artificial intelligence (AI) has proved no different. Many now use personalized and highly realistic AI-generated emails, SMS messages, and social media posts to steal sensitive information, gain access to systems, or trick users into installing malicious files for example. And these techniques often employ levels of automation and self learning which allow the hackers to scale up their attacks to target much higher numbers of victims than would have been possible using manual processes.

97%

of businesses believe AI-powered threats will have a significant impact on their organizations in future.

According to Darktrace's State of AI Cyber Security 2024 report, almost three quarters of organizations (74%) agree that AI is already having a major impact on the cyber threats they face. All the signs suggest the menace will escalate, with 87% of businesses believing AI-powered threats will have a significant impact on their organizations for months and years to come. The fifth edition of Deep Instinct's Voice of SecOps report tells a similar story, estimating that 97% of security professionals are concerned that their organization will suffer an AI-generated cybersecurity incident in the future.

The good news is that AI can be equally advantageous to organizations trying to protect themselves against those attacks as it is for the hackers launching them.

Cyber security companies are busy integrating AI into their products and services to help IT departments improve their defensive capabilities, but important questions on which specific tasks to tackle (or tackle first) from the perspective of individual organizations remain.

We surveyed 879 readers of The Register representing a variety of different company sizes and industry verticals spread across North America (NA); Europe, The Middle, East and Africa (EMEA); and Asia Pacific (APAC) for answers. The results give us a better idea of how IT decision makers think AI can help them stop AI-generated cyber attacks from disrupting their operations, or at least help them clean up afterwards to minimize the damage. Here's what they told us.

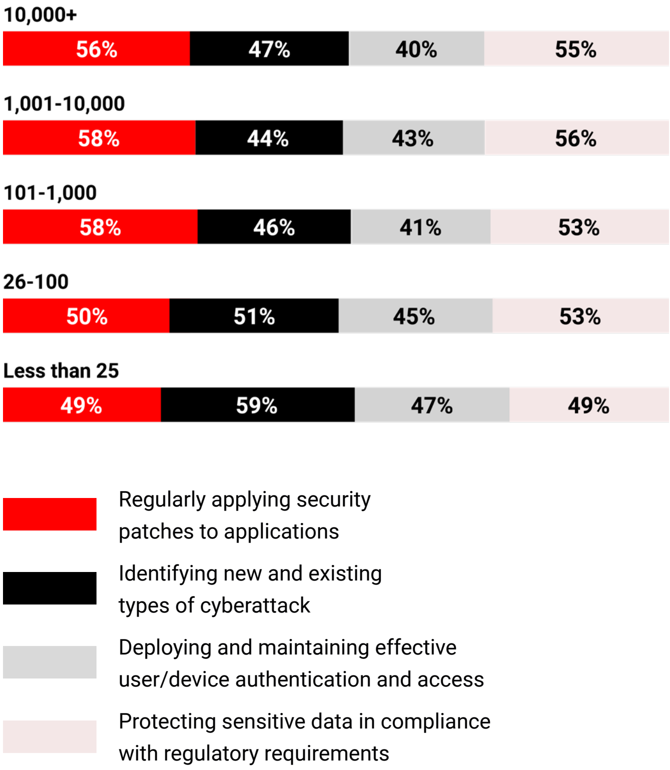
Clear challenges in defense maintenance

There are challenges galore, but two clear priorities stood out when it comes to maintaining adequate cyber security defenses. The majority of those taking part in the survey highlighted regularly applying security patches to applications (54%) and protecting sensitive data in compliance with regulatory requirements (53%) as ongoing issues. Half (50%) reported hurdles in identifying new and existing types of cyberattack, while a comparatively fewer number reported deploying and maintaining effective user/device authentication and access to be a problem.

Organizations in the NA and EMEA regions were consistent in their opinions here, but there were marked differences from APAC respondents. Less than half (49%) found regular security patches to be a challenge, and only 42% struggled to identify new and existing types of cyberattack (the average for EMEA and NA was 52%). At the same time, more APAC respondents (57%) cited difficulties in protecting sensitive data in compliance with regulatory requirements.

This particular challenge also appears to be more prevalent amongst organizations in education and training (66%) & financial services (62%) compared to other verticals, possibly because these industries handle so much sensitive personal & financial information & are therefore more highly regulated in the first place. Along with technology & telecoms, respondents from these verticals are also more likely to struggle with configuring regular security patches to their applications & services. But in the manufacturing industry it's identifying new and existing types of cyberattack which causes more concern than most.

Q1: What challenges does your organization face in maintaining adequate cyber security defenses?



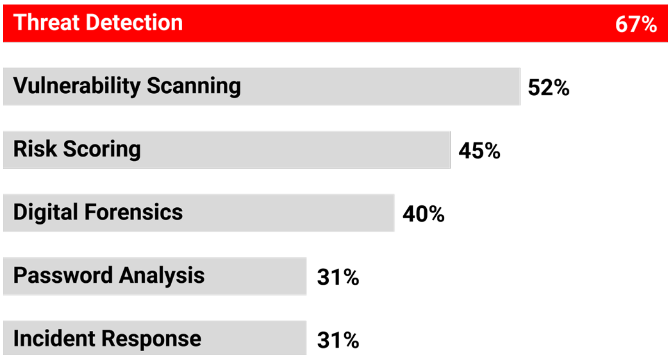
Even so, it's scale which appears to have the most dramatic impact. There's a clear trend to suggest that the smaller the organization (under 100 employees), the less likely they are to encounter challenges either with regularly applying patches and updates, most likely because they have fewer applications and services to protect and administer compared with those employing 100 or more staff. Yet at the other end of the spectrum, it's businesses employing less than 25 (59%) or 26-100 (50%) which have the most trouble identifying new and existing types of cyberattack. This is a finding consistent with organizations having either/both fewer dedicated cybersecurity professionals at their disposal, or having not made the requisite investment in automated cyber defenses.

Where AI can play a positive role

AI has multiple roles to play in cyber protection, but some are more readily identified than others by the survey base. Two thirds of global respondents recognize the technology's potential to help detect threats using advanced pattern recognition to spot common attack methods and anomalies within vast amounts of data for example, which might include subtle signs of malicious activity that human analysts are unable to detect. A slight majority (52%) also highlighted vulnerability scanning which sees AI search large IT environments encompassing hundreds if not thousands of applications, systems, devices, users and networks to find vulnerabilities before they can become an entry point for cyberthreats.

> "
> **Advanced pattern recognition through AI is transforming threat detection for two-thirds of organizations.**

Q2: In which of the following aspects of cyber security provision do you see AI playing a positive role?



These findings are consistent across companies of all sizes bar those employing less than 25 people. These put greater expectation on AI playing a positive role in password analysis (40%), for example by scrutinizing passwords to identify patterns and common mistakes which can make them vulnerable to attack. This group also sees less of a role in risk scoring where AI-enabled automation can help in contract risk analysis, risk management, risk assessment and other processes using natural language processing (NLP) for example. Those employing 26-100 staff are also more likely to identify a positive role for AI in incident response (39%), again reflecting the relative lack of dedicated and/or skilled cyber security practitioners available for this task in-house amongst smaller businesses.

As ever there are significant variations according to region and vertical. Vulnerability scanning appears to be of particular interest to organizations in North America, over 60% of which highlighted the positive role that AI has to play here. The same is true of digital forensics, cited by 46% of NA respondents, and password analysis (37%). Its those working in the financial services sector that identify the most pronounced role for AI in threat detection (75%), though the same is true for vulnerability scanning (59%), digital forensics (46%), and risk scoring (50%) – the latter two findings reflecting the nature of this sector's particular business.

Those working in technology and telecoms are much more likely to see a positive role for AI in incident response (52%) compared to other verticals. This perhaps reflects the position of these businesses in what is often the first line of defense against cyberattacks and being in most need of assistance in improving detection and response times by analyzing large volumes of security data and traffic crossing their networks in real time. Elsewhere password analysis was identified as a defensive task which could be improved using AI by far more respondents in the retail and hospitality, education and training and public sector verticals, most likely due to the large numbers of people they employ and high staff turnover which is characteristic of these industries.

How AI can address cyber security challenges

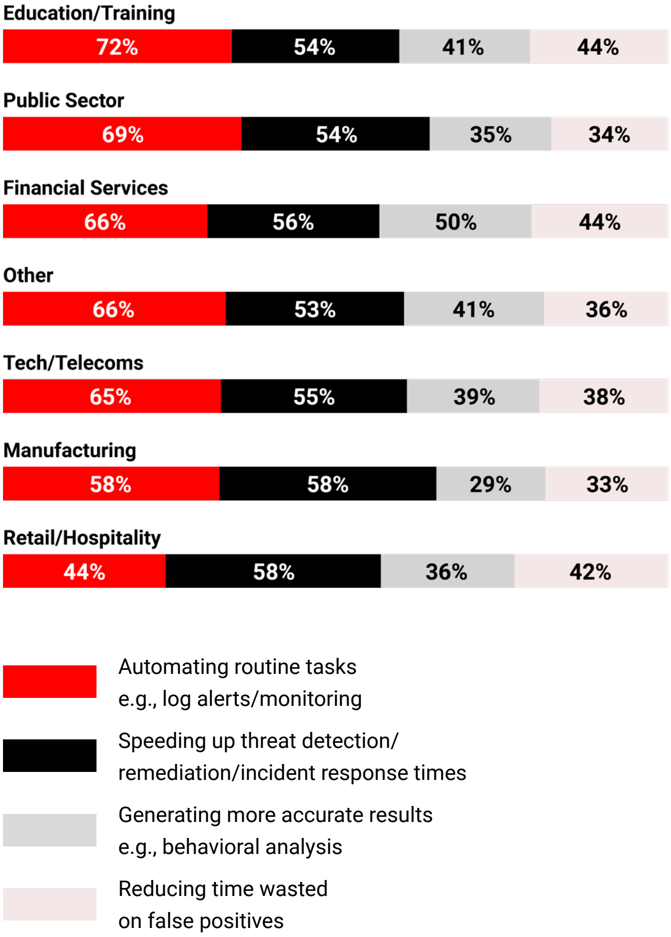
Automation plays a crucial part in the advantages that AI can bring to cyber security defense strategies, and this is not lost on The Register survey base. When asked which challenges they through AI is well suited to help their organization address, almost two thirds (65%) cited the automation of routine tasks such as log alerts or monitoring – ostensibly assuming responsibility for mundane operations which might ordinarily be trusted to a human.

> **Nearly 65% see AI as the key to automating routine security tasks and freeing up human expertise.**

And just as two thirds recognize the value of the technology in helping threat detection (see question 2), the majority (56%) also pointed to AI's ability to help speed up threat detection times, as well as quickening remediation and incident response. The use of behavioral analysis to generate more accurate results (40%) and help reduce time wasted on exploring false positives (ie alerts which ultimately turn out to be inaccurate indicators of cyber threats, 39%) are seen as either less of a challenge and/or processes which AI is not well suited to address by most, however.

This is particularly true in EMEA where only 34% indicated AI could help with false positives, while comparatively fewer organizations in APAC (59%) perceive the technology to be useful in automating routine tasks. The same is true for smaller companies in all three regions employing less than 25 people (60%), probably because they have smaller IT estates and fewer cyber defenses creating those alerts to monitor. Businesses employing between 101 & 1,000 staff indicated a greater appreciation of AI's ability to reduce time wasted on false positives (45%) than their counterparts, while smaller organizations with headcounts in the 26-100 category saw more value in its capacity to address the challenge of speeding up threat detection, remediation and incident response times.

Q3: Which cyber security challenges do you think AI is well suited to help your organization address?



There were marked differences of opinion amongst respondents representing different verticals however. More of those working in education and training (72%) are interested in AI's ability to automate routine tasks for example, with retail and hospitality (44%) and manufacturing (57%) considerably below the average. The manufacturing sector is also less appreciative of AI's ability to help reduce time wasted pursuing false positives (33%) or generate more accurate results from methods such as behavioral analysis (29%), a distinction it shares with the public sector (cited by 34% and 35% respectively).

Can AI supplement scarce human cyber security resources?

Organizations everywhere continue to find it difficult in finding sufficient numbers of skilled cyber security professionals to maintain their defenses. Figures compiled by ISC2 estimated that there were 4.8 million more cybersecurity jobs than there were qualified workers last year, while the Global Cybersecurity Forum's 2024 Cybersecurity Workforce Report found that only 72% of cybersecurity roles were filled.

Those trends are confirmed by the findings of The Register survey, with 41% of respondents reporting that their organization has either a lack (23%) or a serious lack (18%) of skilled security professionals needed to keep it fully protected from cyberattacks. Only a third (34%) said they had enough, with the remaining quarter (26%) non-committal. That skills shortage seems to be slightly more acute in North America, where 44% of organizations seem to be struggling to find expert cyber security staff, and less of a problem in the APAC region where 21% cited a lack and 16% a serious lack of suitable personnel.

Smaller companies appear to be particularly impacted, perhaps unsurprising given their smaller headcounts and more limited recruitment resources. At the other end of the scale, it's the largest organizations employing over 10,000 people which are more confident in existing cyber security expert provision, with over 40% of respondents judging their employers blessed by either more than enough (18%), or enough (22%) skilled professionals.

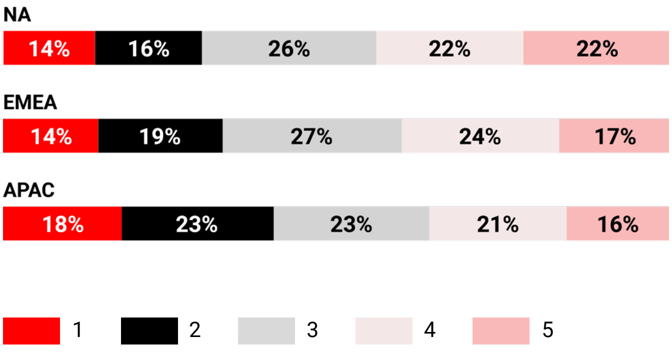
4 in 10

organizations admit they lack the skilled security professionals needed to protect against cyberattacks.

There's considerable variation here between different verticals. A worrying 20% of organizations in the retail/hospitality (28%), education and training (22%) and public sector (20%) all reported a serious lack of skilled cyber security professionals available to help protect them from cyberattacks for example. The shortfall doesn't appear quite as acute in the financial servicesa and technology and telecoms industries but exists nevertheless, with the manufacturing sector demonstrating the most confidence in existing staffing levels (40% reported having either enough or more than enough skilled cybersecurity professionals at their disposal).

Q4: Does your organization currently have enough skilled security professionals to keep it fully protected from cyberattacks?

Rate on a scale of 1 to 5 where 1 = more than enough and 5 = a serious lack.

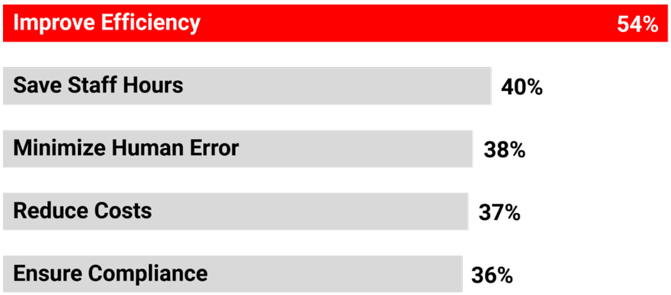


Automation provides the key

AI's ability to automate routine cybersecurity maintenance and management tasks is widely understood to have the residual effect of improving the productivity of highly skilled and well-paid human professionals – essentially freeing up workers' time to tackle more difficult problems. This perception is reflected in responses to question 5, which asked participants to identify which benefits their organizations were most likely to prioritize when implementing AI-enabled cyber security tools, almost 40% of which cited saving staff hours. Other widely cited priorities included minimizing human error (37%) and ensuring compliance (36%).

But perhaps the biggest surprise is that more respondents felt the single biggest priority for AI lies in improving efficiency (cited by 54% or respondents), over and above reducing costs (37%).

Q6: Which of the following benefits is your organization most likely to prioritize when implementing AI enabled cyber security tools?



These findings were mostly consistent across geographies. The exception is organizations in North America which seem markedly more interested in using AI-enabled security tools to ensure compliance compared to their counterparts in Europe and APAC, possibly because the volume and scope of legislation is heavier in those territories. Conversely, US and Canadian respondents were less motivated by any need to save staff hours. This is perhaps because (as evidenced by their responses to question 4) they feel the cybersecurity skills shortage more acutely and have a greater need to recruit extra heads anyway.

There's a clear correlation between saving staff hours and company size. Organizations employing over 10,000 people (42%) and between 1,001 and 10,000 people (43%) with larger IT estates are more likely to have higher complements of existing cyber security professionals and are therefore in greater need of time saving assistance. The opposite is true for those employing less than 25 people (35%). The Register Survey also indicates that any imperative to harness AI in pursuit of cost reduction is also proportionately more acute in larger compared to smaller companies. Elsewhere it's mid-sized companies - those employing 26-100 (59%) and 101-1,000 (60%) - which are more interested in using AI-enabled cyber security tools to improve efficiency. We can surmise that this is because they are also those that judge themselves as having the fewest number of skilled security professionals to maintain their defenses.

> "
>
> **Efficiency trumps cost savings: 54% prioritize AI for improving security operations versus 37% for cutting costs.**

Saving staff hours is more of a priority for organizations in education and training (49%) and public sector (44%) compared to other verticals. Improving efficiency is valued more highly by those in technology and telecoms (60.1%), manufacturing (55%) and financial services (55%). The latter are also the most likely to prioritize ensuring compliance (41%) and minimizing human error (43%), findings which reflect the generally stricter regulatory and numbers-based commercial environments they inhabit.

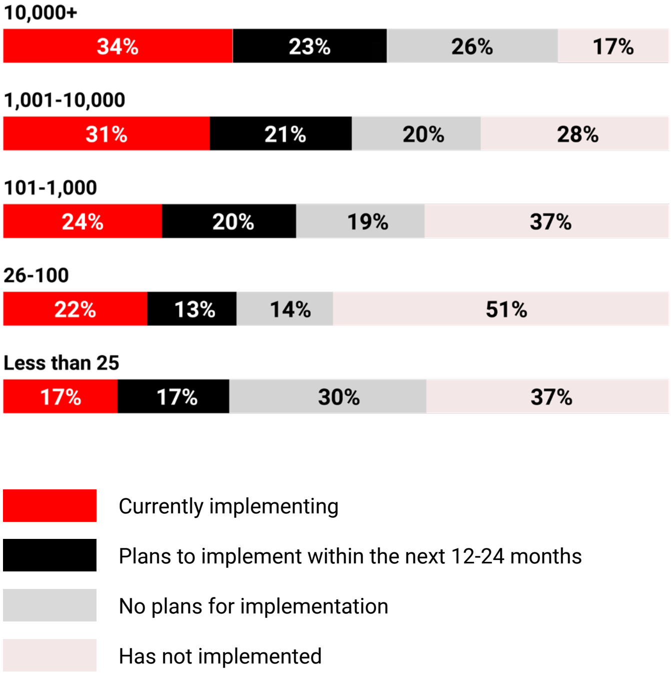
Implementation plans

The majority of organizations worldwide do appear to see the potential for AI-enabled security tools to improve their cyber defense capabilities, even where they are not currently in operation. Less than a quarter of those taking part in The Register survey (23%) reported their employers had no plans to implement them, although another 32% haven't done so to date. Another quarter (26%) are in the process of adding AI-enabled security tools to their cyber security infrastructure right now, with 19% planning to do so within the next 12-24 months.

Those in the EMEA region are little further behind in those plans compared to their counterparts in North America and APAC, with 24% currently implementing and 19% scheduling rollouts over the next couple of years. More EMEA organizations (35%) have also not implemented to date. But it's a large percentage of those in North America (27%) which have no plans for implementation at all.

There's a clear correlation between implementation plans and company size which suggests that, for the moment at least, AI-enabled security tools are more the preserve of larger organizations. Over a third (34%) of those employing over 10,000 people are currently upgrading for example, with another quarter (23%) planning to do so within 12-24 months. These figures shrink progressively with company size, with only 17% of businesses with headcounts less than 25 currently engaged in an implementation, and 17% planning one.

Q5: What best describes your organization's current implementation of AI enabled cyber security tools?



The financial services sector leads from an industry vertical perspective. Almost 60% of respondents here reported that employers are either currently putting in AI-enabled cyber security tools (31%) or are planning to do so (30%). Only 17% said they have not implemented and a further 22% have no plans to do so. The opposite is true for education and training, where a smaller percentage (41%) are either currently putting tools in (23%) or are planning upgrades over the next two years (17%). More activity is seen in the technology and telecoms sector, where exactly a third (33%) are busy putting in appropriate AI-enabled cyber defenses.

Key findings:

- Large numbers of organizations say they don't have enough skilled security professional to keep them protected from cyberattacks, and see AI-enabled cyber security tools as a way to supplement human expertise and improve defenses.
- Automating routine cyber security administration and configuration tasks and speeding up threat detection/remediation/response times are judged as the top challenges AI can help address.
- Improving efficiency is more of a priority than reducing costs when it comes to implementing AI-enabled security tools. The larger the company however, the keener they are on harnessing AI to trim expenditure.
- Using AI to ensure compliance with data protection regulation and industry frameworks is more of a priority for organizations in North America and the financial services industry.
- The majority of organizations expect AI to play a positive role in threat detection and vulnerability scanning.
- For the moment, it's bigger companies which are more likely to be using AI-enabled security tools or planning their implementation.

Achieving an optimal defensive balance

While The Register survey found significant variations in knowledge of, and expectations for, AI-enabled cyber tools across different regions, verticals and company sizes, it's clear that interest in using AI to combat cyber threats, accelerate incident responses and supplement scarce human expertise is gathering momentum. That's important, with the UK National Cyber Security Centre (NCSC) amongst others having predicted that, although the impact will be uneven, AI will almost certainly increase the volume and severity of cyberattacks over the next two years.

All types of cyber threat actor – including state, non-state, skilled and less skilled – are already using AI to varying degrees, and the threat to 2025 is likely to come from a scaling up of existing tactics, techniques and procedures to simultaneously target more victims while also making attacks more effective and harder to detect.

Our survey indicates that the most pressing challenge now is for all types of enterprise – from SMB to large corporates and public sector organizations – to quickly establish an optimal balance of in-house expertise and their own AI-enabled automation to best defend themselves against those threats.