DARKTRACE

Executive summary

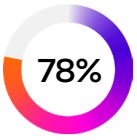
State of AI Cybersecurity 2025

Industry perspectives on the growing role of AI in cybersecurity

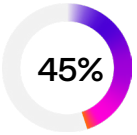
The impact of AI in the cybersecurity field is a double-edged sword: there is an expanding body of evidence showing that it is being harnessed more and more effectively by threat actors, but it is also transforming the defensive arsenals of security teams. We surveyed over 1,500 cybersecurity professionals from around the world to uncover their attitudes, understanding, and priorities when it comes to AI cybersecurity in 2025.

The threat

Cyber-threats are becoming a reality, and organizations are acting now, with many more now saying they feel prepared to defend – but 45% still do not.



Of CISOs now agree
AI-powered cyber-threats are already having a significant impact on their organization. A 5% increase from 2024



Of professionals feel unprepared
to defend against AI-powered cyber-threats.
Down from 60% last year

The confidence gap
62% of CISOs feel prepared vs. 52% in other security roles

Comprehension

Cybersecurity professionals are slowly gaining a better understanding of different AI types and techniques, but there is a long way to go.

42%

Report full confidence
in their understanding of the different AI types used in their security stack.

The knowledge gap
60% of CISOs know exactly what AI types are being used in their stack vs. just 18% in other security roles

AI Security Policy

More talk than action

95%

said their organizations were either discussing a policy on the safe and secure use of AI or had already implemented one, but only a minority (45%) had already established such a policy.

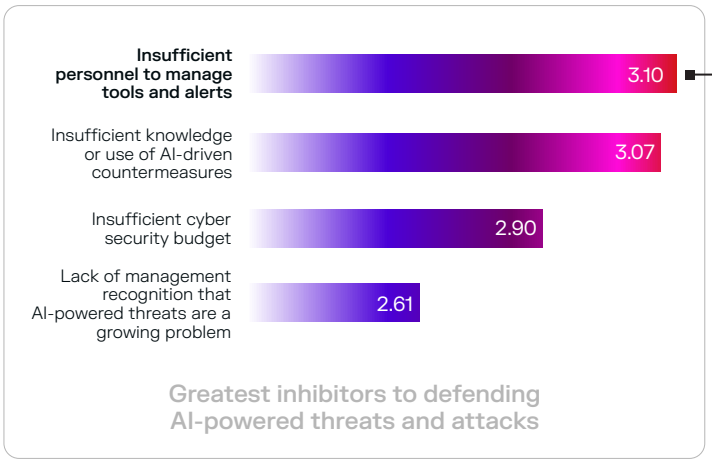
Most common steps taken to reduce risk around AI use:

- Implement security controls to **prevent unwanted exposure** of corporate data when using AI (67%)
- Implement security controls to **protect against other threats/risks** associated with using AI (62%)
- Implement **AI-specific training** for application developers (48%)

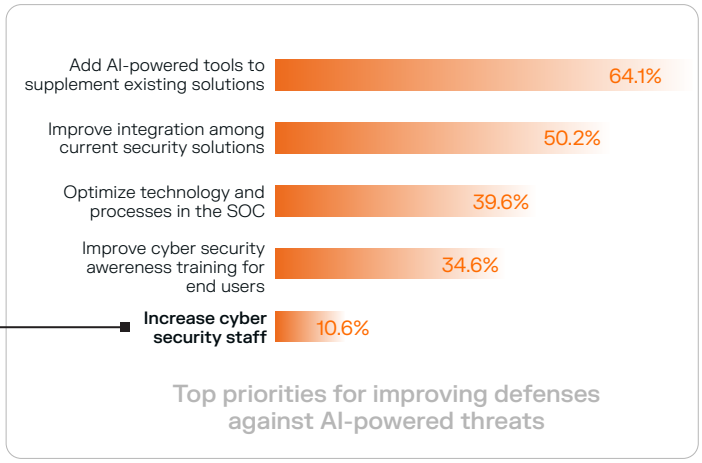
Hiring

Despite 'insufficient personnel' being considered the greatest inhibitor to defending AI-powered threats, increasing cybersecurity staff is at the bottom of the priority list, with 11% (and only 8% of executives) planning to increase cybersecurity staff in 2025 – even less than in 2024.

It's not the budget or the lack of awareness ...it's the headcount

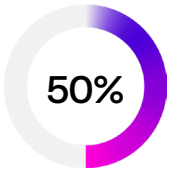


... but very few are prioritizing hiring this year

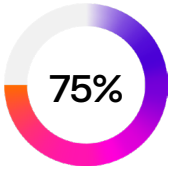


AI Cybersecurity Solutions

Confidence in defensive AI is growing ...

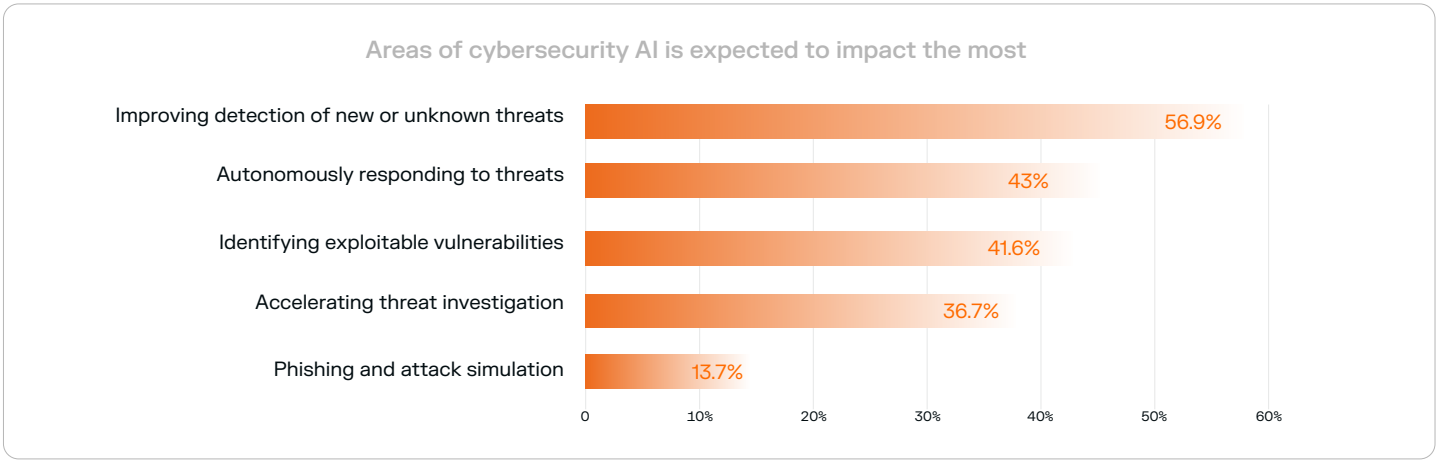


- **Strongly agree** that AI-powered security solutions **significantly improve the speed and efficiency** of their ability to prevent, detect, respond to and recover from cyber-threats



- **Are confident** that AI security solutions can **better defend against AI-powered threats** than traditional tools

.... and the area AI is expected to have the MOST impact is the detection of new / unknown threats



Priorities

Decision-makers expressed a preference for broader platforms over point products and solutions that don't require their data to be shared externally. The vast majority have confidence in AI's ability to help them become more proactive.

Proactive

88%

agree the use of AI within the security stack is critical to freeing up time for the security team to become more **proactive**

Platform

87%

prefer a **platform approach** to defense over implementing a collection of point solutions

Privacy

84%

prefer solutions that do **not require their data to be shared externally** for model training and other purposes

Download the report

for the full findings, trends, and analysis

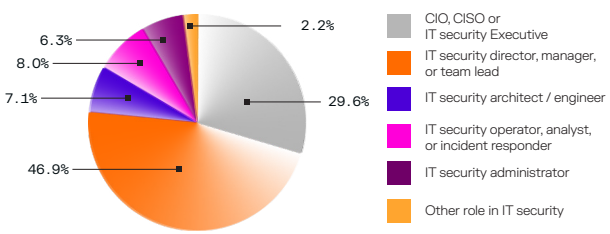
Uncover the complete findings from the 23-question survey. See how these results break down by org size, job title, industry, and region, and get practical advice on dealing with the reality of cybersecurity in the era of AI.

State of AI Cybersecurity 2025 →

Survey Methodology

Our survey was conducted online in September 2024. Respondents held a variety of positions within information security. Roughly 30% were CIOs, CISOs, or other senior leaders. Survey participants came from 14 different countries in four different regions, including North and Latin America, Europe, and the Asia-Pacific region. Their organizations ranged in size from 500 employees to more than 25,000, with most (59%) working for organizations with more than 1,000 and less than 10,000 employees.

Survey participants by role



Survey participants by size of organization