DARKTRACE

Executive Summary

THE STATE OF AI CYBERSECURITY 2026

How the industry is responding to the shifting role of AI in cyber defense

With AI adoption in the enterprise now widespread, cybersecurity leaders are being challenged to protect a rapidly expanding attack surface while managing never-before-seen risks. Securing AI is a growing challenge for enterprises, and the stakes are high. We surveyed over 1,500 cybersecurity professionals from around the world to uncover their attitudes, understanding, and priorities when it comes to AI threats, agents, tools, and operations in 2026.

The AI attack surface

Nearly half (44%) of security professionals are “extremely” or “very” concerned about the security implications of employee use of generative AI tools like Copilot or ChatGPT.

Top concerns with the increasing use of AI in the enterprise:

61%
Exposure of sensitive data

56%
Violating data and privacy regulations

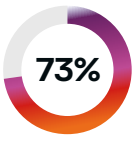
51%
Abuse of AI tools

37% 45%

Fewer organizations have a formal policy in place for the safe and secure use of AI than this time last year.
Last year 45% of survey respondents said they had a formal policy in place, this year it dropped to 37%.

Evolving threats

There is still a strong consensus that threat actors are using AI to augment their operations.



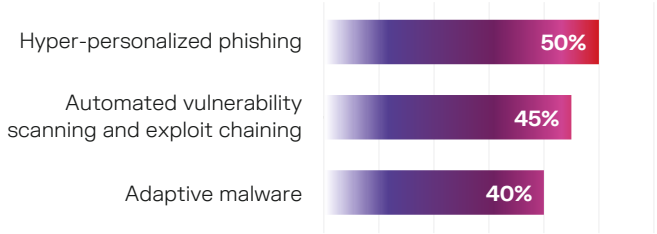
- say AI-powered threats are already having a significant impact

- say these threats are forcing them to significantly upgrade defenses

68% 78%

The perception gap:
78% of CISOs are feeling the impact of AI threats, compared to 68% of SecOps roles.

AI techniques posing the greatest threat:



Nearly half (46%) don’t feel confident in their ability to defend against AI-powered attacks (*up* from last year), with hyper-personalized phishing topping the list of concerns.

Shifting workflows

Familiarity with types of AI is growing, but trust in AI is lagging behind.

77% Generative AI is now playing a role in 77% of security stacks.

Still, the majority (74%) limit the autonomy of AI taking action in the SOC. Only 14% allow it to act independently, without a human in the loop.

Outsourcing security vs managing in-house

85%

of security professionals prefer to obtain new SOC capabilities in the form of a managed service (as opposed to a product managed in-house).

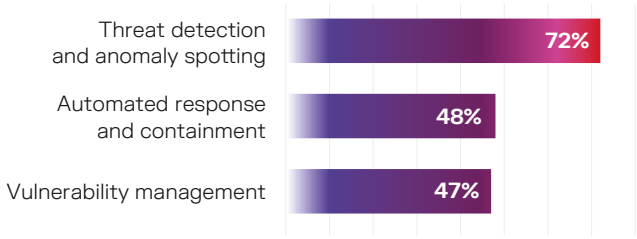
AI capabilities

There's a consensus on the necessity of defensive AI.

- of cybersecurity professionals agree that AI can significantly improve the speed and efficiency with which they work

- prefer solutions that are part of a platform over individual point products. Up 5% on last year.

These are the areas defensive AI is expected to have the greatest impact:



Security priorities

Top 3 priorities for the next 12 months:

65% adding AI-powered tools to the stack

57% improving integration among current solutions

56% improving cyber readiness for potential incidents

Access the report for the full findings, trends, and analysis

Uncover the full survey findings, and see how the results break down by org size, job title, industry, and country.

State of AI Cybersecurity 2026 →

Survey methodology

Darktrace surveyed 1,540 cybersecurity leaders and practitioners from 14 different countries including the U.S., U.K., France, and Germany. The survey was fielded online between October and November 2025. The majority of participants hold leadership roles such as CIO, CISO, IT security executive, director, manager, or team lead, while a significant minority have hands-on experience in security operations, engineering, or administration.