securonix

RESEARCH REPORT / Q4 2026

The Evolution of Cybersecurity Automation

Towards Human-Governed AI Execution

MOMENTUM

AI adoption in cybersecurity is accelerating.

99.6%

have an increased budget for AI in cybersecurity automation.

96%

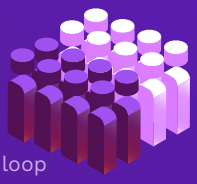
say automation is important.

87%

are using AI to some extent in cybersecurity automation.

EXECUTION BOUNDARY

Humans remain in control.



53%

favor a human-in-the-loop approach to AI cybersecurity strategy.

48% use a human-in-the-loop approach in specific SOC use cases.

32% on average say use cases such as alert triage and incident response will always require a human in the loop.

SEC.03

WORKFORCE DYNAMICS

The SOC workforce is evolving.

35%

are retraining analysts for higher value work.

33%

see new skills and roles emerging around AI governance, validation and oversight.

31%

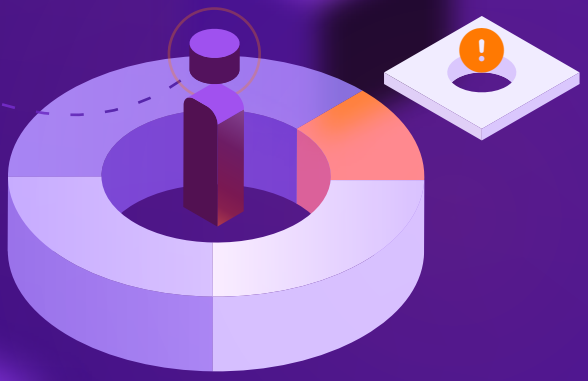
are hiring more specialists as traditional cybersecurity roles evolve.

PROTOCOLS

Governance matters.

42%

have 'defined' or 'managed' AI governance in place.



27%

say AI governance is 'optimized'.

26%

cite ethical issues as a leading concern.

IMPLEMENTATION

Key problems when implementing AI in cybersecurity.

01 Technology issues

02 Management understanding/buy-in

03 Siloed Departments

RISK PROFILING

Leading concerns about AI in cybersecurity.

01 Ethical concerns

02 Understanding the content of third-party tools

03 Dependence on AI or on one AI provider

© Copyright 2026, Securonix, Inc. and ThreatQuotient (Now a Securonix Company).