State of AI and Cybersecurity

Survey Report

Release Date: April 2024

cloud security alliance®

Overview

1. Methodology and Goals for the Survey
2. Key Findings
3. Demographics
4. About the Sponsor

Survey Creation and Methodology

Survey Creation

- Approached by sponsor/member
- Outline overarching questions
- Develop large question pool
- Refine final questionnaire

Data Collection

- Distribute online survey in April 2023
- Received 2486 responses

Analysis and Report

- Research team analyzes data
- Identify 4-7 most interesting or surprising findings
- Write report based on team's analysis

Goals of the Study

The advent of Artificial Intelligence (AI) in cybersecurity marks a transformative era in the realm of digital defense, bringing a blend of promising breakthroughs and intricate challenges. In an age where cyber threats continuously adapt and grow more complex, the role of AI as a vital ally in bolstering security defenses, identifying emerging threats, and facilitating swift responses becomes increasingly critical. However, the journey towards integrating AI into cybersecurity landscapes is fraught with obstacles, including the need to mitigate dual-use concerns, bridge skill gaps, and prevent over-dependence on automated systems. Gaining insights into how industry experts view and prepare for AI's evolving role in cybersecurity is pivotal in navigating this transition and ensuring a resilient, forward-looking digital infrastructure.

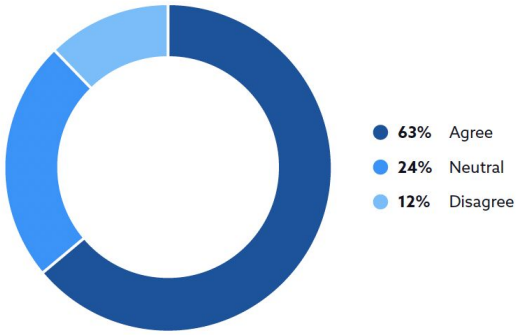
The primary objectives of the survey were to gain a deeper understanding of:

- Current security challenges
- Perceptions of AI in cybersecurity
- Industry familiarity with AI
- Plans for AI use in the industry
- AI impact on staffing and training

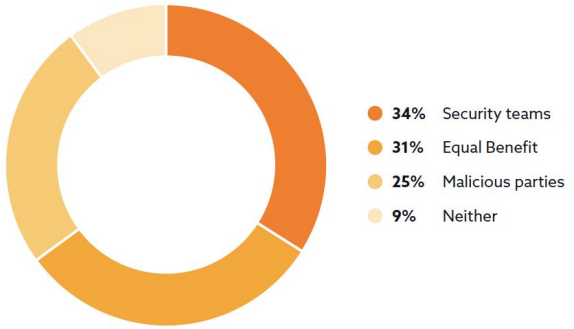
Key Finding 1: Cautious Optimism About AI Among Security Professionals

- Cautious Optimism: 63% of security professionals see AI as a boon for enhancing threat detection and response, expressing cautious optimism about its potential.
- Dual Nature Awareness: There's a split view on AI's benefits—34% believe it favors security teams, while 31% see equal advantages for attackers and defenders. A notable 25% worry AI might favor malicious actors more.
- Top Concerns: Major apprehensions include data quality issues (38%), potentially leading to bias, opacity of AI systems, and gaps in skills/expertise needed to manage complex AI systems.
- Call for Strategy Evolution: Acknowledgment of AI's misuse potential and the necessity for evolving security strategies, rigorous data handling, and enhancing AI system transparency.
- Security Framework Need: Highlighting the importance of developing comprehensive frameworks to secure AI technologies in cybersecurity

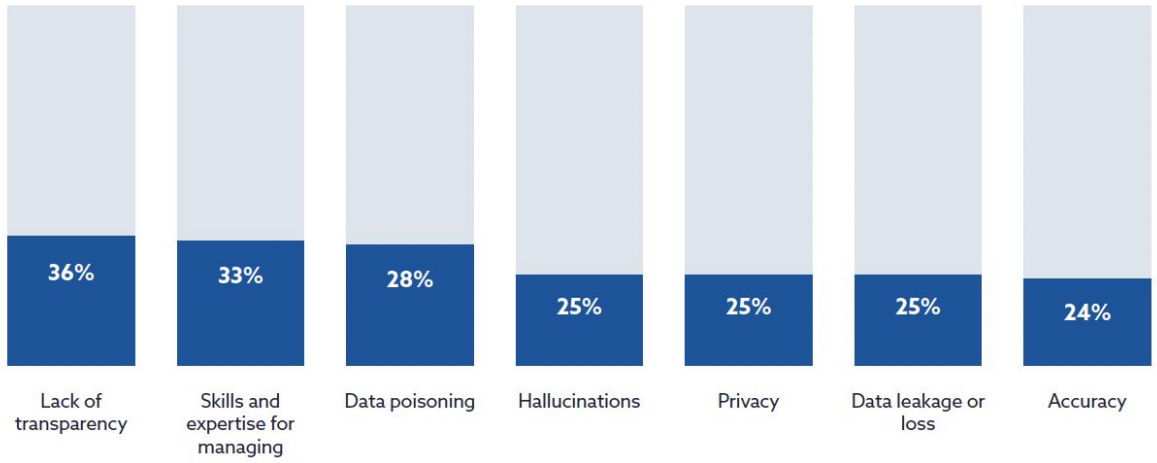
How strongly do you agree or disagree with the following statement: Artificial Intelligence (AI) will improve security within our organization?



In your opinion, would AI be more beneficial to security teams or malicious 3rd parties?



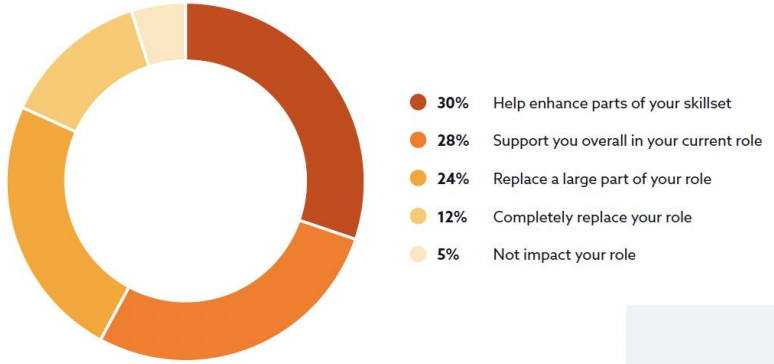
What are your biggest concerns regarding AI in security? (Select up to 3)



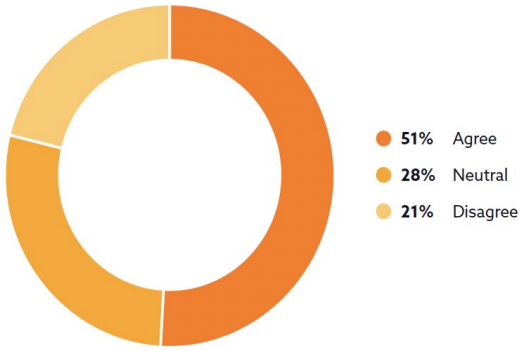
Key Finding 2: AI Will Empower, not Replace, Security Professionals

- AI as an Empowerment Tool: Majority view AI as enhancing their skills (30%), supporting their roles (28%), or automating large parts of their tasks (24%), with only 12% fearing total replacement.
- Role Enhancement through AI: Security professionals see AI as enhancing their skills (30%), supporting their roles (28%), or automating parts of their work (24%), thus freeing them for other tasks
- Discrepancy in Challenges vs. AI Goals: Despite emphasizing AI for skills enhancement, immediate challenges like operational toil and threat detection are ranked higher than talent issues.
- Concerns Over AI Reliance: 50% of respondents worry about overreliance on AI, stressing the importance of balancing AI-driven and human-driven security approaches.

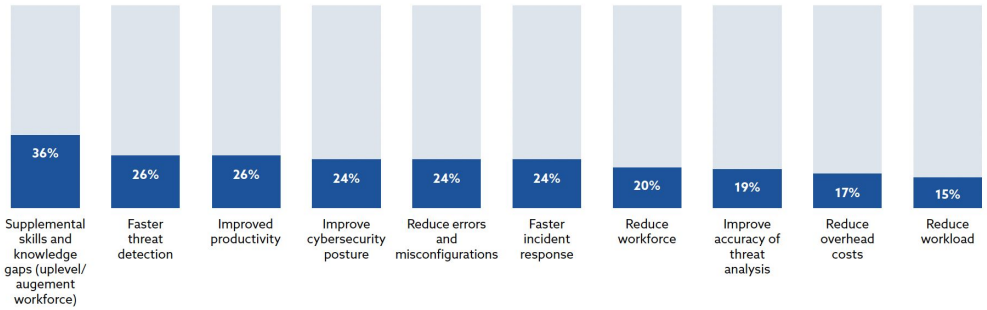
Please select the option that best reflects your opinion about AI's potential impact on your role. Over the next 5 years, AI will...



Are you concerned about the potential risks of over-reliance on AI for cybersecurity?

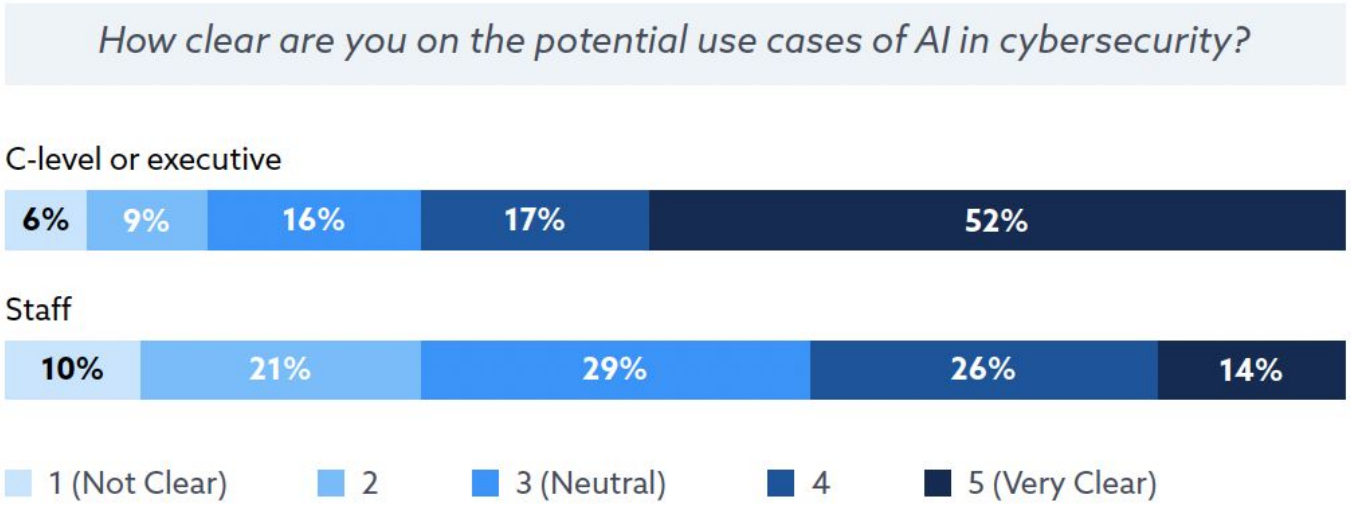


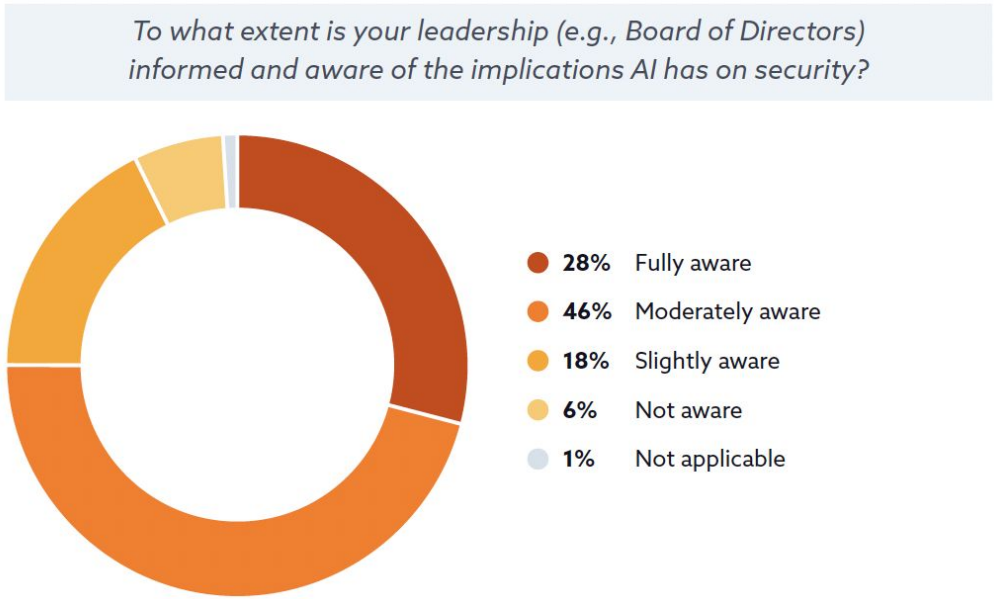
What are your desired outcomes when it comes to implementing AI in your security team?



Key Finding 3: C-Suite Executives Have Different AI Perspectives from Their Staff

- Discrepancy in AI Familiarity: 52% of C-suite executives report being very familiar with AI, versus 11% of staff.
- Understanding of AI Use Cases: 51% of C-levels have a clear understanding, compared to 14% of staff, suggesting a knowledge gap or overestimation of familiarity by executives.
- Leadership Awareness:74% believe their leadership is informed about AI's implications on security.
- AI Adoption Push: 82% note executive leadership and boards are advocating for AI adoption, indicating top-down pressure.
- Need for Enhanced Communication: Highlights the importance of improved education and collaborative approaches to AI implementation in cybersecurity.





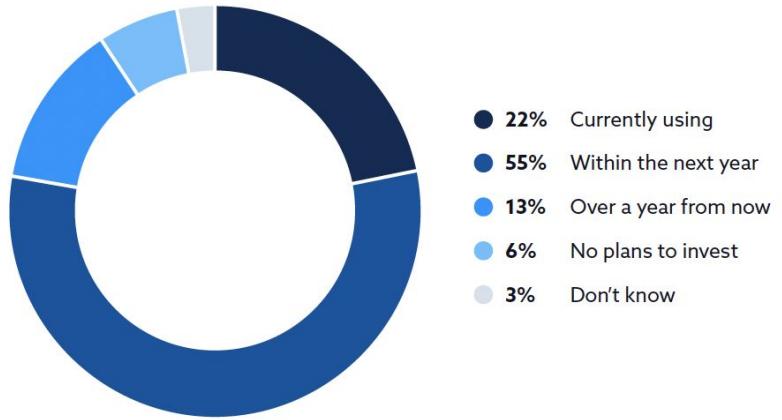
Key Finding 4: 2024 Is the Year for AI Implementation – Get Ready for the Revolution

- Over half (55%) of organizations are planning to implement gen AI solutions in the next year
- A diverse range of use cases are being explored with the top use cases: rule creation (21%), attack simulation (19%), and compliance violation detection (19%)
- Biggest hurdle to AI implementation is the skills gap and staff shortage, as reported by 33% of respondents

How does your organization plan to use Generative AI for cybersecurity? (Select top 3 use cases)

21%	Rule creation	13%	Natural language to search	9%	Forensic analysis
19%	Attack simulation	13%	Threat summarization	9%	Chatbot
19%	Compliance violation monitoring	13%	Data loss prevention, IP protection	8%	Incident summarization
16%	Network detection	11%	User Behavior analysis	8%	Configuration drift
16%	Reduce false positives	10%	Automated report generation	8%	Recommendations for action/ remediation
15%	Training development and support	10%	Endpoint detection	7%	Code analysis
14%	Anomaly classification	9%	Event log summarization		

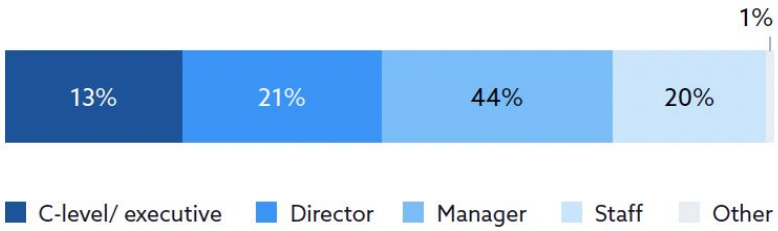
In general, is your organization using or planning to use Generative AI solutions?



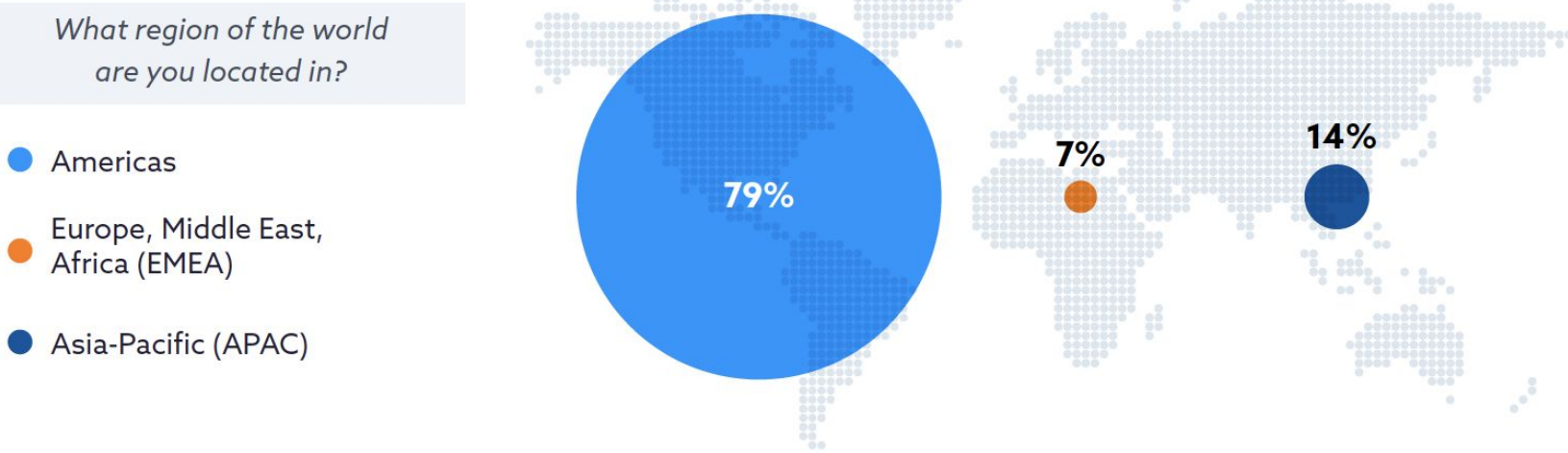
Demographics

Total of 2,468 responses

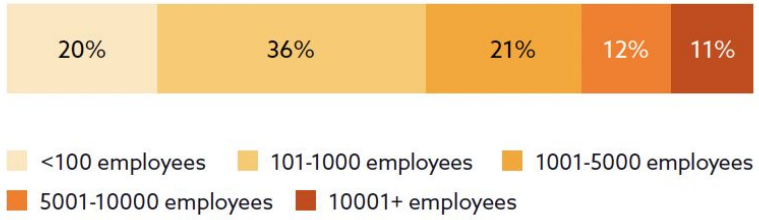
What is your position within your organization?



What region of the world are you located in?



What is the size of your organization?



Which of the following best describes the principal industry of your organization?

About the Sponsor

Google Cloud is the new way to the cloud, providing AI, infrastructure, developer, data, security, and collaboration tools built for today and tomorrow. Google Cloud offers a powerful, fully integrated and optimized AI stack with its own planet-scale infrastructure, custom-built chips, generative AI models and development platform, as well as AI-powered applications, to help organizations transform. Customers in more than 200 countries and territories turn to Google Cloud as their trusted technology partner. For more information, please visit https://cloud.google.com/ https://cloud.google.com/security/ai