CISO PERSPECTIVES

Separating the reality of AI from the hype

tines

© TINES / TINES.COM/CISO-AI

tines

2024 Report
CISO perspectives

Separating the reality of AI from the hype

Contents

A word from Eoin Hinchy

CEO and Co-Founder, Tines

The explosion of AI has ignited both excitement and apprehension across various industries. While AI is undeniably having a positive impact on engineering and customer service teams, cybersecurity and IT practitioners remain cautious. Concerns about data privacy, the inflexibility of disparate tools, and the sensitive nature of many mission-critical workflows—which, more often than not, require some level of human oversight—fuel a deep mistrust of LLMs by these teams.

Before starting Tines, I spent 15 years as a security leader at some of the world's most targeted companies. So, I know firsthand just how frustrating and demoralizing it is to be burned by solutions that excel during vendor demonstrations but fall short when faced with real-world problems. Not only were these 'solutions' a complete waste of my budget, time, and mental load, but this post-demo disappointment happened much too often for my liking. That's one of the reasons we took our time to launch AI in Tines - we're evangelical about only shipping products and features that add value for our customers.

We never want to contribute to any sort of hype and ultimately fail to deliver on our mission to power the world's most important workflows. We're very proud of our AI features, and we're just getting started - we have some very exciting launches to come! In the meantime, to better understand the mood around AI's true potential and separate the signal from the noise, we conducted a pulse survey among 53 Chief Information Security Officers (CISOs) from the US, UK, Australia, and the Netherlands between June 27th and July 5th, 2024. Respondents came from Silicon Valley CISO Investments* and Pollfish using organic sampling. This report explores their experiences, concerns, and challenges as they incorporate AI into their scaling security operations.

* Silicon Valley CISO Investments are investors in Tines.

© Tines
tines.com/ciso-ai

Key findings

Here are a few of the insights we learned from the Chief Information Security Officers we surveyed:

#1

94% are concerned about the increased pressure on their security teams due to AI adoption.

#2

66% consider data privacy a challenge to AI adoption.

#3

49% view inflexible technologies as a challenge to AI adoption.

#4

74% believe faster decision-making by AI systems will introduce more benefits to the SOC than risks.

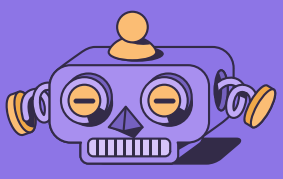
#5

51% say AI will make it easier to hire entry-level employees.

© Tines
tines.com/ciso-ai

Satisfaction with AI adoption

One of the primary objectives of our survey was to gauge CISOs' satisfaction with their teams' progress in adopting AI technologies.



© Tines
tines.com/ciso-ai

An impressive 83% of respondents reported a generally positive outlook on their team's progress in adopting AI with 28% being very satisfied. But there is still a clear desire to tackle the various challenges and concerns associated with AI adoption.

Increasing pressure on security teams

A combined total of 94% of respondents expressed some level of concern the pressure on their security team will increase as AI adoption grows within their organization. Overall, many indicated data privacy concerns (66%) and inflexible technologies (49%) as challenges faced by their teams.

With 63% of analysts reporting burnout in our Voice of the SOC 2023 report, and more pressure on the horizon from AI, these responses highlight the need for additional resources, training, and planning to ensure that security teams are equipped to successfully implement AI technologies and remove bottlenecks.

It's been reported that the immense pressure of the job has led to many CISOs resigning. To alleviate additional burdens, CISOs should involve their teams in decision-making when exploring new technologies.

Misaligned priorities are one of the challenges we'll explore next. A collaborative approach can bridge knowledge gaps and ensure a successful implementation plan.

© Tines
tines.com/ciso-ai

Challenges in AI adoption

Hurdles can hamper progress and create friction within organizations. Despite strong satisfaction rates and a belief in the potential benefits of AI, CISOs need help with its adoption.

© Tines
tines.com/ciso-ai

Five most commonly reported challenges

66%

Data privacy

Data privacy is the most common challenge, with 66% of respondents identifying it as an issue. Integrating AI into cybersecurity raises issues regarding access to sensitive data, compliance with regulations, and the potential for breaches. Organizations must prioritize data privacy in their AI initiatives. AI's ability to rapidly process data is incredibly valuable for cybersecurity but also presents risks to sensitive information.

60%

Insufficient talent and lack of skills

The talent shortage in cybersecurity is a significant challenge, and while AI can address some security issues, it also introduces new ones. Many security teams lack the time and expertize needed to adopt AI technologies effectively, with 60% of CISOs citing insufficient staff and skills as an obstacle. To successfully integrate AI, it's crucial to bridge this skills gap with intuitive solutions.

51%

Misaligned priorities

51% of respondents identified misaligned opinions around priorities and risks as a challenge. This disconnect often stems from a lack of understanding of AI and its implications. Effective AI implementation requires clear communication, collaboration, and educating employees on AI's benefits, and risks, and establishing clear policies.

49%

Inflexible technologies

Almost half of the respondents (49%) find inflexible technologies challenging for AI adoption. Rigid and brittle legacy solutions hinder AI integration into existing and new workflows, as Large Language Models (LLMs) need comprehensive context to perform well. A well-integrated tech stack is essential for accurate AI decision-making, while adaptable workflows are necessary to keep pace with frequent LLM updates, preventing silos and maximizing efficiency.

77%

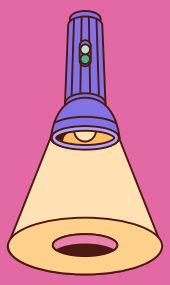
Policies and perceptions

77% of respondents have introduced policies for AI usage, indicating CISOs are taking a proactive approach to managing AI integration. But with 51% of respondents citing misaligned opinions around priorities and risks as a challenge, creating a policy is only the first step. To counteract shadow AI, organizations need to educate employees and introduce technologies that enable them to leverage AI securely and compliantly.

© Tines
tines.com/ciso-ai

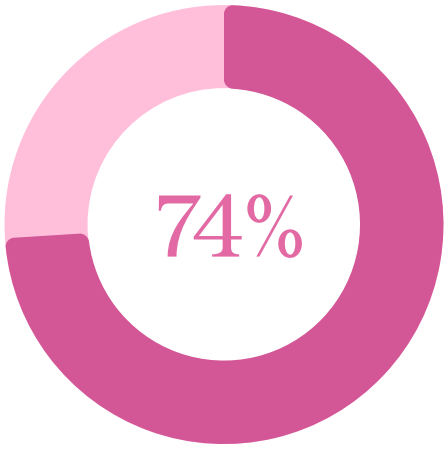
Opportunities in AI adoption

Despite the challenges they encounter, CISOs remain optimistic about AI's potential to enhance security operations.

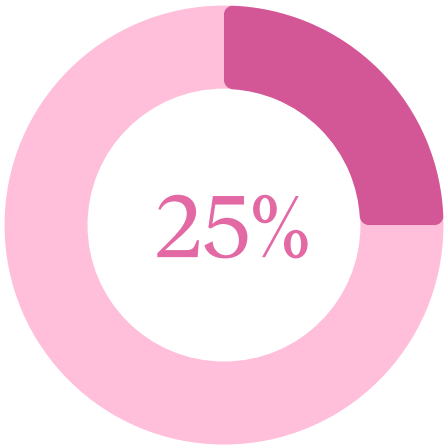


© Tines
tines.com/ciso-ai

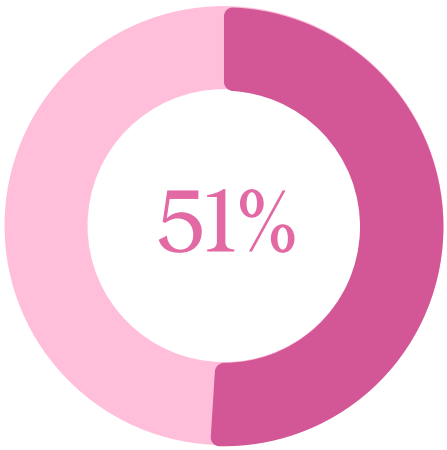
Despite the concerns and challenges, there is a general sense of optimism about AI. **A significant 74% of respondents believe that the benefits of faster decision-making by AI systems outweigh the risks.**



Just 25% of respondents are worried that incorrect decisions made by AI could slow down threat detection or containment of benign activities. This highlights the necessity for humans to maintain full control over AI systems through diligent oversight and continuous monitoring to ensure their reliability and accuracy.



While the talent shortage remains a challenge, 51% of CISOs surveyed think AI will make it easier for their organization to hire entry-level employees. AI-enhanced workflows will allow new hires to concentrate on more strategic activities, accelerating their professional growth.



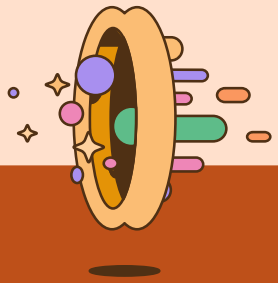
© Tines
tines.com/ciso-ai

Summary

The survey results paint a nuanced picture of AI adoption in cybersecurity. While there is significant satisfaction with the progress made so far, many concerns and challenges still need to be addressed.

Feedback from respondents highlights a spectrum of sentiments, ranging from anticipation to skepticism. For instance, some respondents are "looking forward to adoption" and remain "excited about AI usage to augment security operations, if clear value can be shown." These comments suggest a strong belief in AI's potential to enhance security operations. On the other hand, insights such as the "lack of enterprise assigned owner/decision-makers" indicate the importance of cross-functional coordination, visibility between stakeholders, and shared responsibility for implementing AI effectively. AI fatigue is evident in comments like "I'm tired of it, already," reflecting a growing weariness among some leaders. These insights reveal the complexity of AI adoption in cybersecurity, emphasizing the optimism for its potential and the necessity for incremental implementation.

Despite these revelations and challenges, the excitement around the potential benefits of AI—such as faster decision-making—is clear. Ensuring that these benefits are realized requires a strategic approach that includes flexible, intuitive AI-enhanced workflow solutions, clear AI policies, continuous skill development, and alignment of organizational priorities.



How Tines can help

Despite the advancements in AI, its practical relevance to businesses is limited. While LLMs can describe complex topics well, they can't yet provide real-time information or integrate with real-world business workflows.

This is where Tines comes into play. AI in Tines is secure and private by design, enabling your security team to securely integrate and control LLMs and AI in your workflows. Tines automates and orchestrates powerful workflows, letting you choose when to call an AI—whether for real-time data analysis, vulnerability assessments, or incident response.

There's no public networking, training, storage, or query/output logging. With Tines, your security team can build, run, and monitor repetitive workflows so they can focus on more impactful work, detecting and responding to incidents faster and more accurately.

To learn more, explore AI in Tines.

© Tines
tines.com/ciso-ai