GitLab

2023 Global DevSecOps Report

The State of AI in Software Development

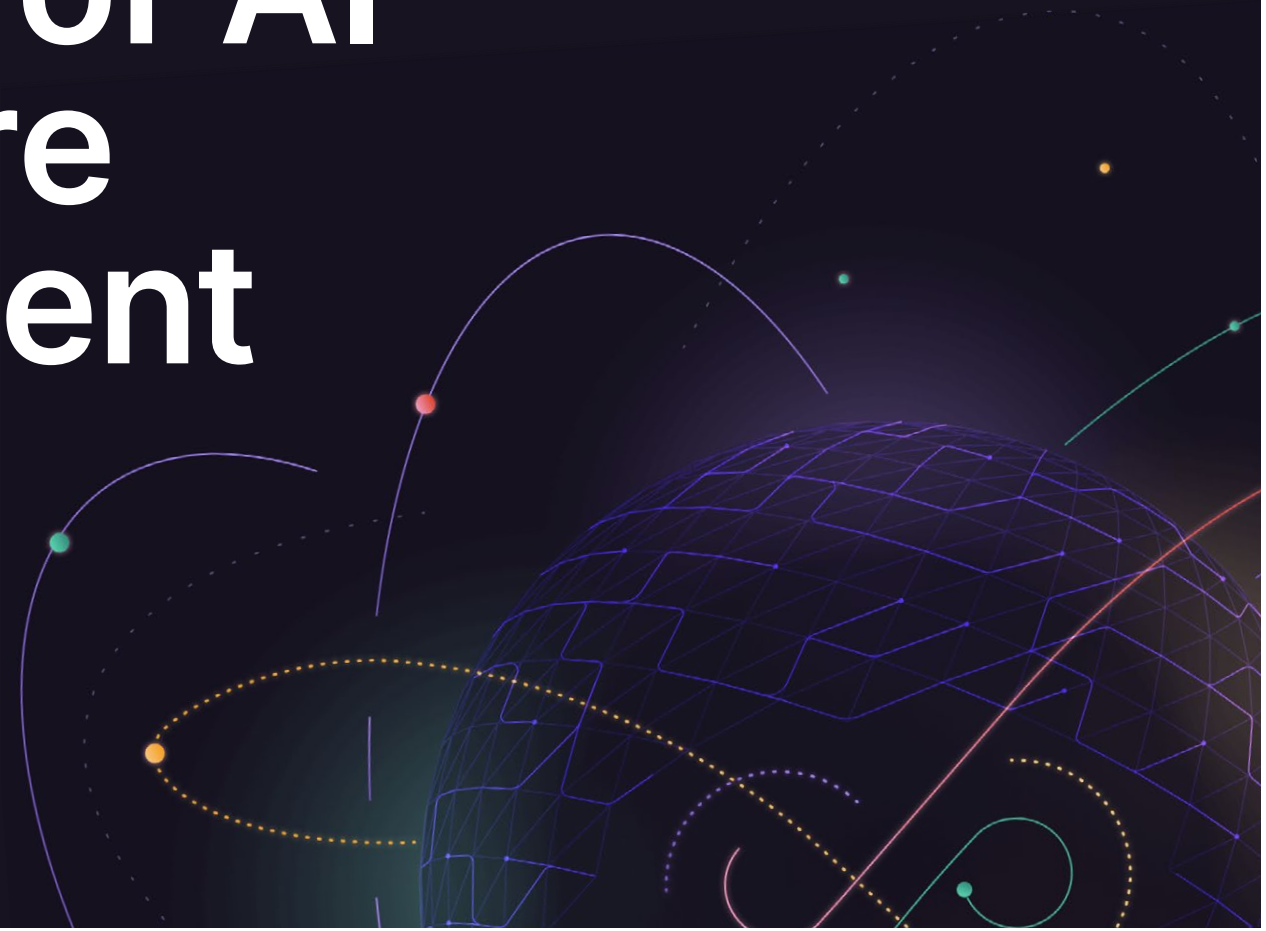
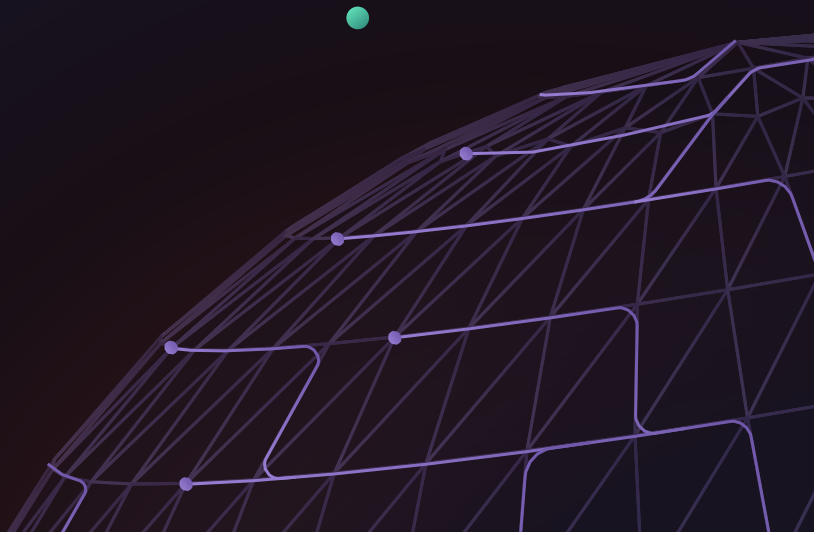


Table of contents



Executive summary

Artificial intelligence (AI) can help development, security, and operations (DevSecOps) teams write code, resolve security vulnerabilities, accelerate code review, and improve collaboration. Our survey suggests DevSecOps teams are feeling optimistic about their adoption of AI and all its potential — but to ensure AI initiatives are successful, organizations will need to examine how AI can support all stages of the software development lifecycle. Respondents also surfaced significant concerns around data privacy, intellectual property, and security.

DevSecOps teams are embracing AI in a big way

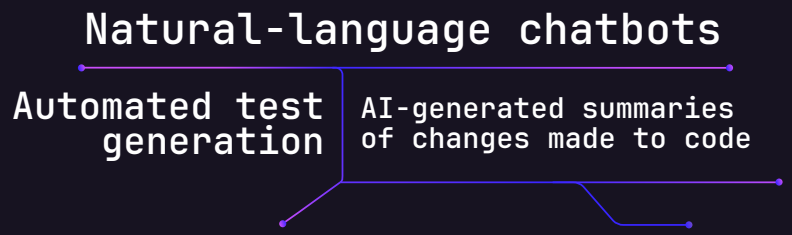
67% of respondents said their organizations are planning to use AI in software development (and 23% are already using it today).

83% of respondents said it is essential to implement AI in their software development processes to avoid falling behind.

AI needs to support the entire software development lifecycle

75% of developers' time is spent on tasks other than code generation — suggesting that code generation is only one area where AI can add value.

Top three use cases for AI in software development, according to respondents



Data privacy, intellectual property, and security are key areas of concern

95% of C-level and VP respondents said privacy and protection of intellectual property are important when evaluating an AI tool or feature.

79% of respondents said they are concerned about AI tools having access to private information or intellectual property.

40% of security professionals were concerned that AI-powered code generation will increase their workload (compared to just 29% of respondents overall).

Teams feel they lack the skills and training necessary to implement AI

81% of respondents said they need more training to use AI in their work.

65% of respondents said their organization has hired or will hire new talent to manage the implementation of AI.

Who took the survey?

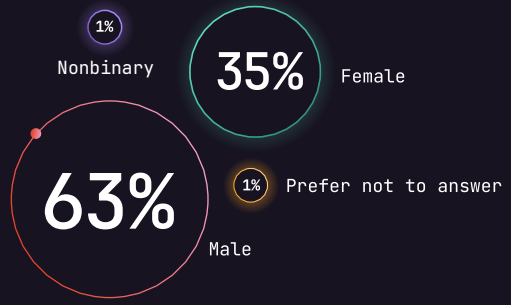
We collected a total of 1,001 survey responses in June 2023 from individual contributors and leaders in development, IT operations, and security across a mix of industries and business sizes worldwide.

We used two sampling methods for the data collection:

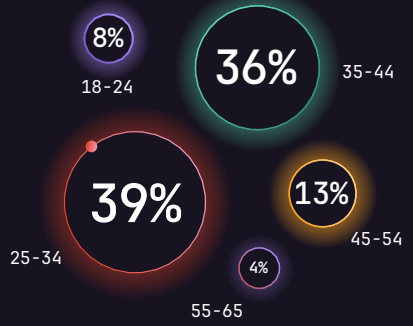
1. We distributed the survey via GitLab's social media channels and email lists.
2. A third-party research partner conducted panel sampling, which reduces bias in the sample. Our research partner used its proprietary access to lists, panels, and databases to gather quality responses and cleaned the data throughout fielding to ensure data quality.

Here's a closer look at the survey respondents:

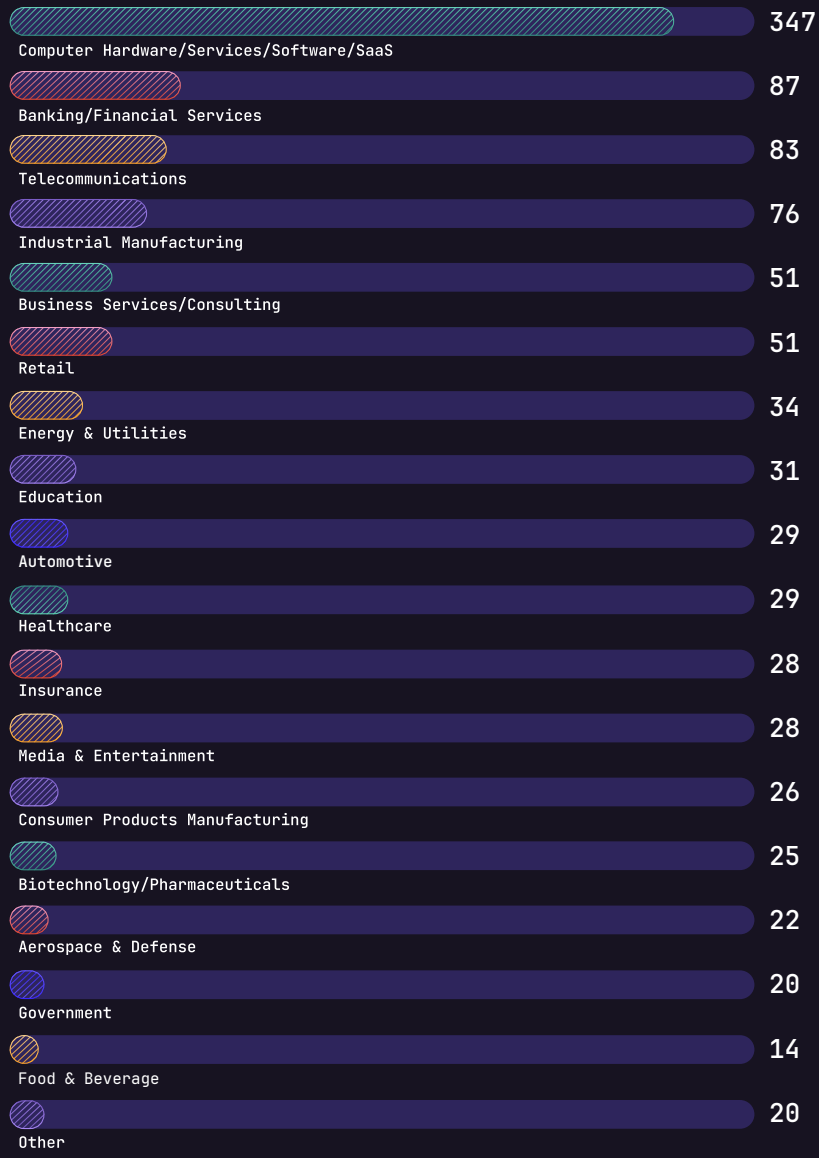
Gender



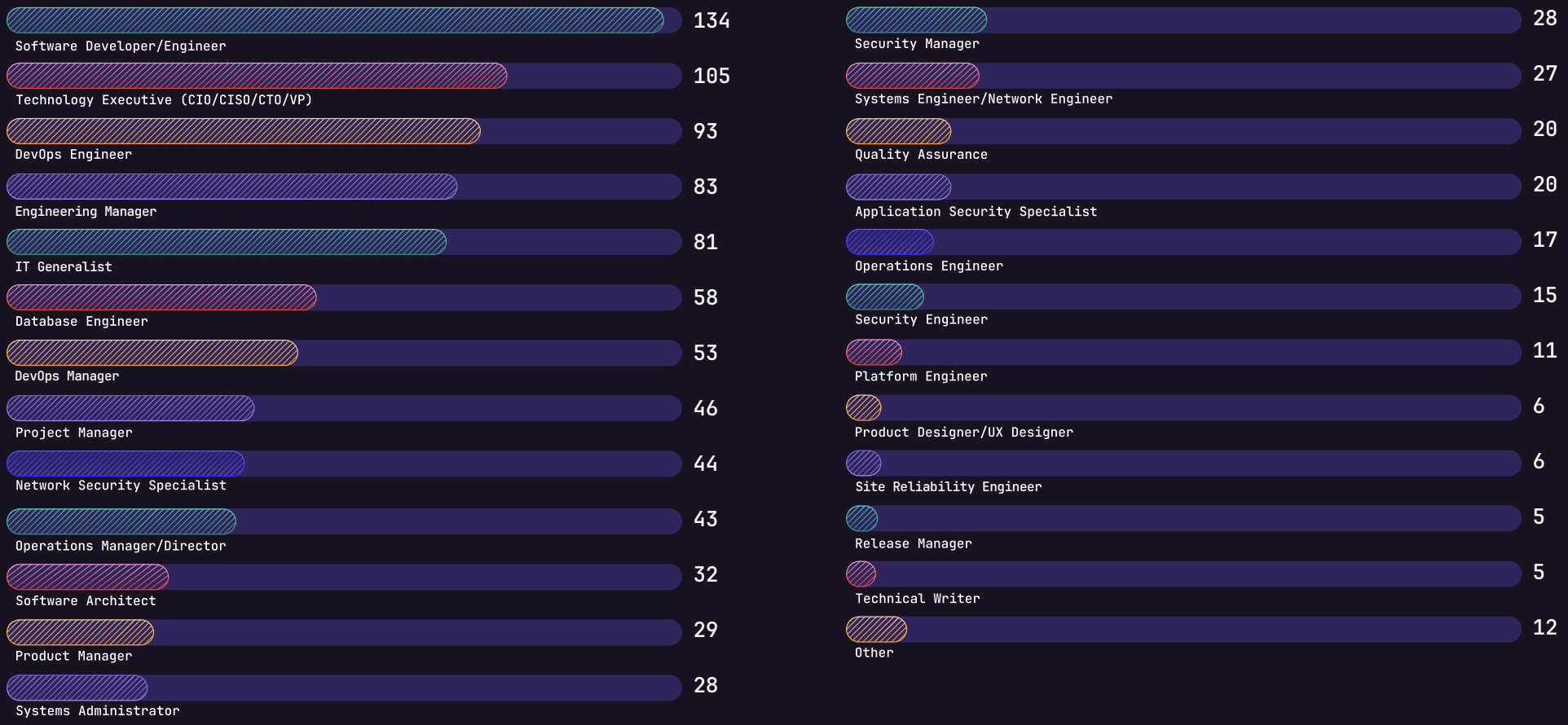
Age



Primary industry

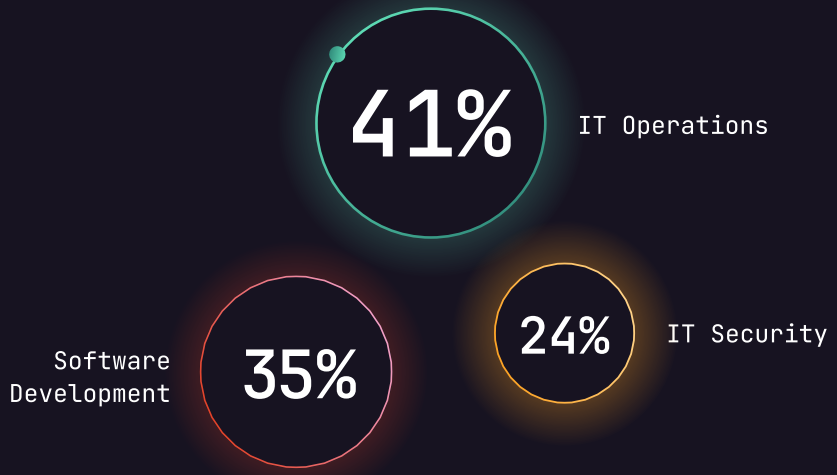


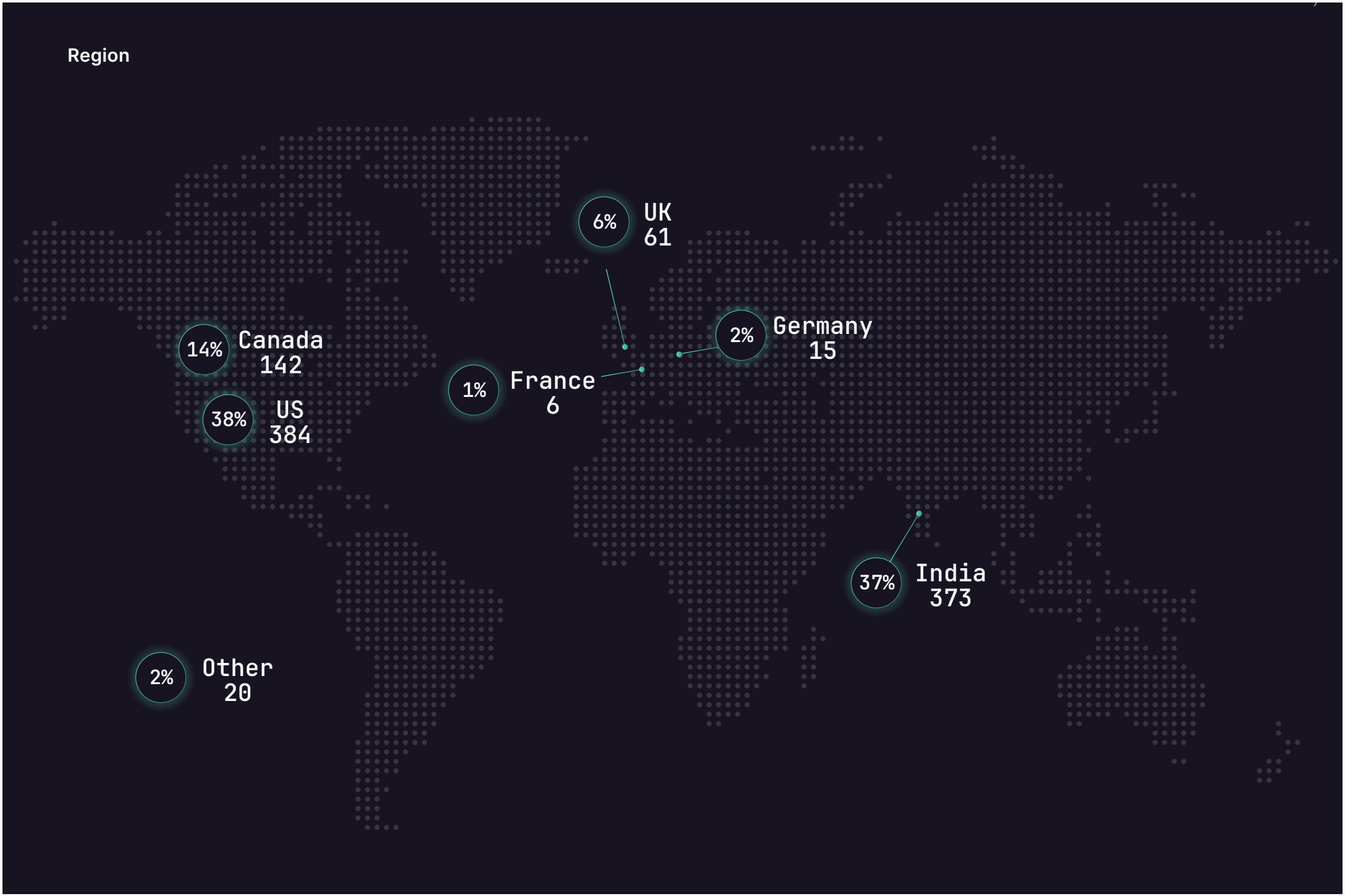
Role within the organization



Number of employees

Functional area




Region
6%
UK
61
2%
Germany
15
14%
Canada
142
1%
France
6
38%
US
384
37%
India
373
2%
Other
20

Introduction

Artificial intelligence (AI) has made incredible technological strides in the past several years. From image and text generation to speech recognition, new developments in AI are poised to have a significant impact on virtually every industry — including software development.

The power of AI to shape how teams plan, build, secure, and deploy software is already being tested in the real world. But is AI living up to its promise? How are DevSecOps teams using AI in software development today, and where do they actually *want* to use it? What are organizations hoping to achieve with AI, and what are the tradeoffs? In this special edition of our 2023 Global DevSecOps Report Series, we seek to answer these questions and understand how AI might be able to introduce new efficiencies and opportunities into the software development lifecycle.

First, we'll look at how many organizations are actually using AI today and the benefits they're hoping to drive. We'll also explore how organizations are using AI across the software development lifecycle, and where there are gaps between DevSecOps teams' interest in and current usage of AI. Then we'll turn to the challenges respondents are facing in implementing AI, focusing primarily on concerns around data privacy, intellectual property, security, and training. We'll conclude with a note on why, despite some fears to the contrary, AI can't replace human experience — and how leveraging the experience of human team members alongside AI can help organizations address the concerns that respondents surfaced in our survey.

But first, a note on terminology.

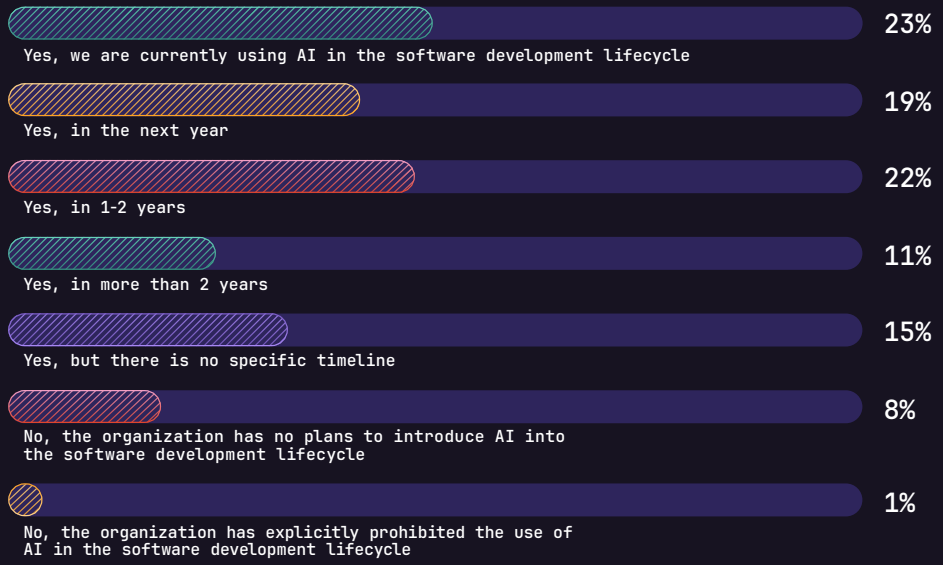
Artificial intelligence is an umbrella term referring to computer software that simulates human capabilities such as logic and problem solving. *Machine learning* (ML), a subset of AI, is the use of complex mathematical models to enable a computer to identify patterns and make predictions based on existing data. There are also a number of other more specific applications of AI, such as *generative AI* (a form of AI that generates new, original content based on patterns in existing data), *deep learning* (a subset of ML that uses complex layers of ML algorithms to carry out sophisticated tasks), and *natural language processing* (a subset of AI that focuses on building systems that can understand language using ML). Throughout this report, we'll use the broadest term, AI, to cover all of these applications.

Now, let's dive in.

AI in the software development lifecycle: Gaining traction

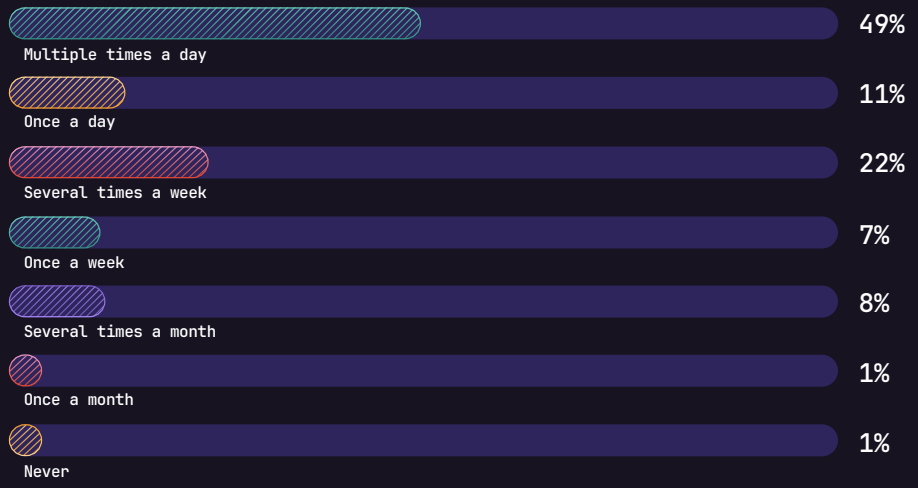
If there was one inescapable takeaway from the survey data, it's that AI in software development is here to stay. The vast majority (83%) of respondents agreed that it is essential to implement AI in their software development processes to avoid falling behind, and this was consistent regardless of respondents' functional area (development, operations, and security), job level, or years of experience. It's not surprising, then, that most organizations have plans to incorporate AI into software development: 23% of respondents said their organizations are currently using AI in the software development lifecycle, and 67% said their organizations are planning to do so.

Is your organization using or planning to use AI in the software development lifecycle?



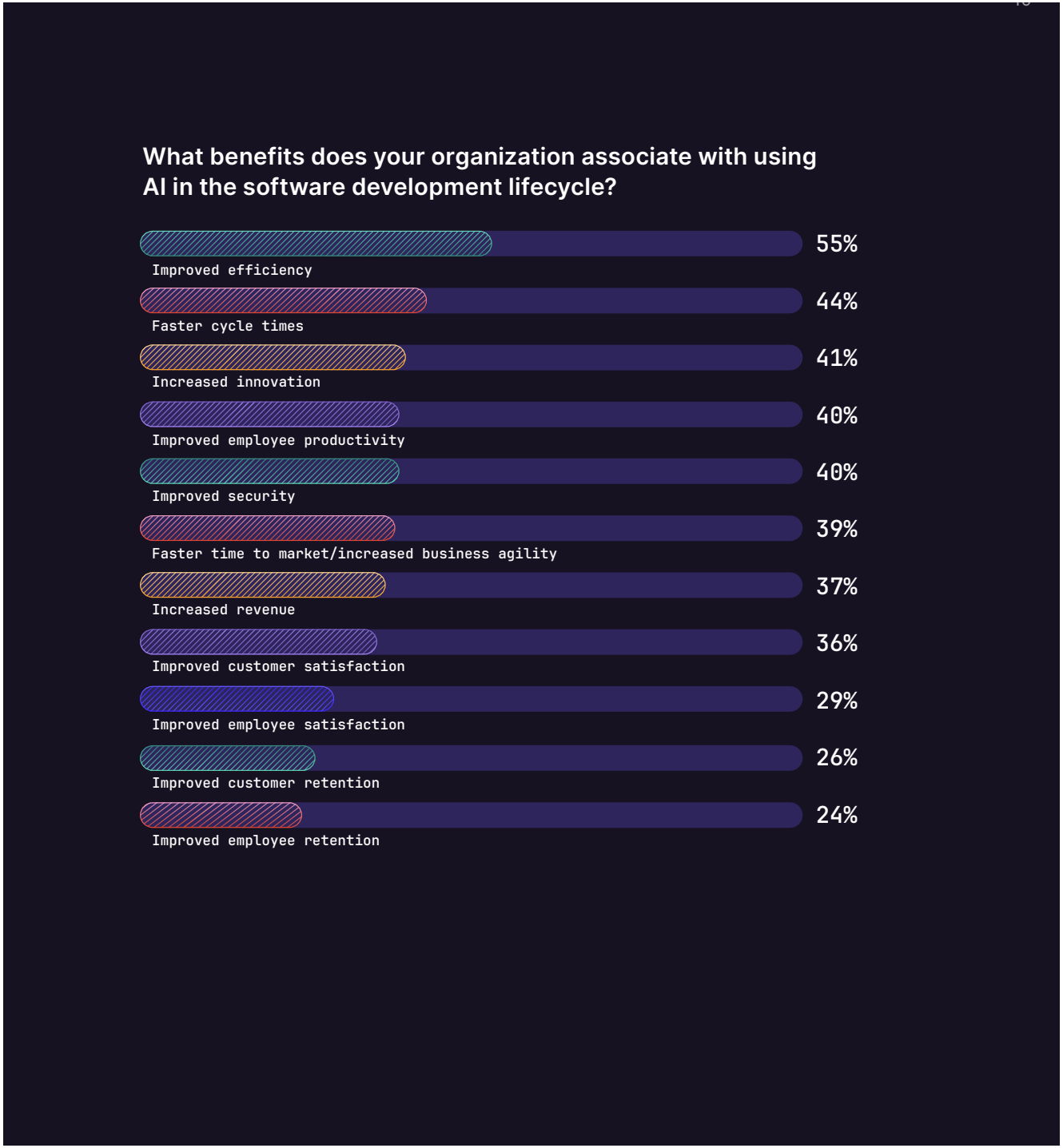
However, AI isn't just another fad — it's seeing real adoption among practitioners. A solid majority (75%) of respondents whose organizations are using AI or planning to use AI for software development said at least a quarter of their DevSecOps team members currently have access to AI tools or functionality. For these teams, AI is becoming embedded in their day-to-day responsibilities: Among respondents whose organizations are using AI in software development today, 60% said they use AI daily, and 22% said they use AI several times a week. This was consistent across development, operations, and security, although respondents with five or fewer years of experience in their functional area were significantly more likely to use AI on a daily basis than more experienced respondents.

Frequency of AI usage, according to respondents whose organizations are using AI in software development today



Promisingly, the vast majority of respondents whose organizations are using AI today (90%) said they feel confident using AI in their daily tasks at work, and more than half (51%) rated their organization's efforts in incorporating AI into the software development lifecycle as "very" or "extremely" successful. In addition, it's clear that organizations as a whole agree that AI is an important investment. Among respondents whose organizations are using AI or plan to in the future, 83% said they have or will have budget specifically allocated to AI for software development.

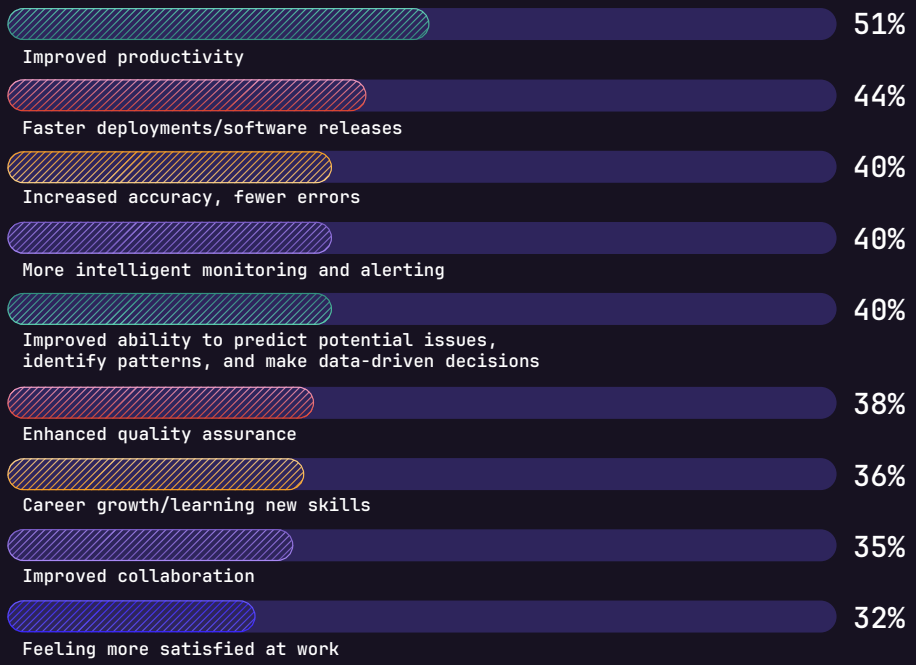
What's driving the widespread adoption of AI? Respondents whose organizations are using AI now or plan to use AI in the future identified improved efficiency (55%), faster cycle times (44%), and increased innovation (41%) as the top organizational benefits of introducing AI into the software development lifecycle.



Different functional areas and job levels identified slightly different benefits from adopting AI. For example, developers (48%) were significantly more likely than security respondents (38%) to identify faster cycle times as a benefit of AI. Similarly, respondents with five or fewer years of experience (50%) were more likely than more experienced respondents (42%) to choose faster cycle times.

Security emerged as a key organizational benefit of AI overall, making the top five, and this was particularly true for managers and executives. Respondents with C-level/VP (46%) or manager titles (43%) were significantly more likely than non-managers (34%) to identify improved security as a benefit.

What benefits have you personally achieved or do you hope to achieve by using AI in the software development lifecycle?



Respondents identified similar benefits when asked what they have personally achieved or hope to achieve by adopting AI in the software development lifecycle, with improved productivity (51%), faster deployments (44%), and increased accuracy (40%) rounding out the top three.

Interestingly, general benefits related to work experience, such as feeling more satisfied at work (32%) and learning new skills (36%), ranked relatively low, although respondents with five or fewer years of experience (41%) were more likely than more experienced respondents (33%) to choose career growth. This suggests that while DevSecOps teams see AI as a utility that assists with their day-to-day work, this doesn't necessarily translate (or isn't expected to translate) into improved work satisfaction for everyone. One explanation is that AI needs to be more uniformly integrated across the entire software development lifecycle — more on that in the next section.

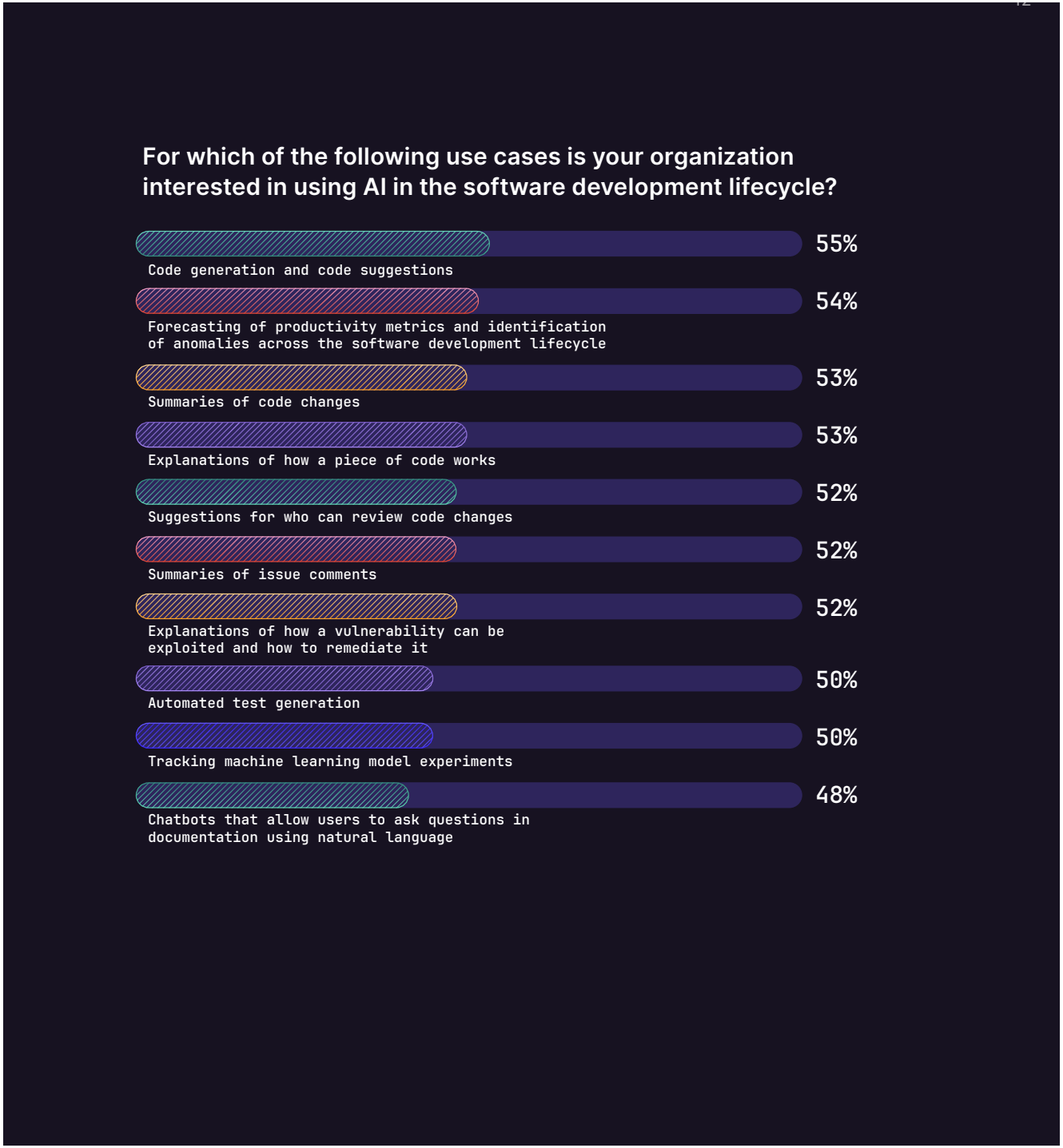
Next, let's explore where respondents are using AI today, where they're interested in using AI, and where in the software development lifecycle AI has the potential to have the biggest impact.

> "The role of software developers is evolving because of AI. It can help them with their code, but we're years away from AI being able to write code completely on its own or replace developers."
>
> ***– Executive in the computer/SaaS industry***

Code generation — the start of a larger shift

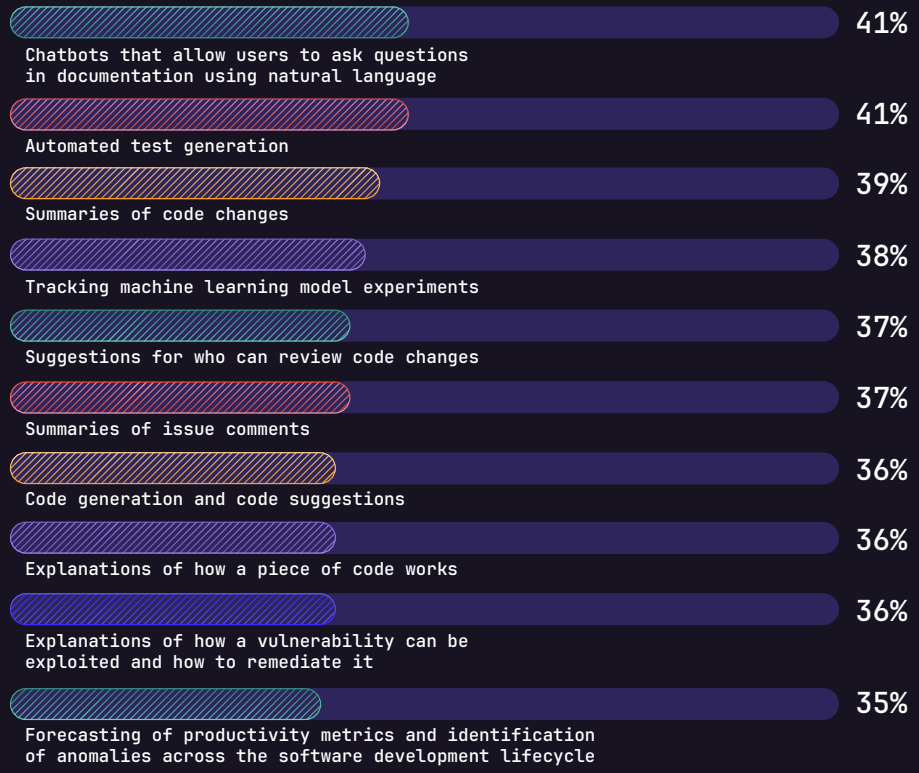
Generative AI has important applications in software development. By using AI to suggest common lines of code or generate logic for function declarations, developers can boost their accuracy, efficiency, and productivity.

Given that generative AI has been in the spotlight for much of this year, it's no surprise that DevSecOps teams are curious about how it might be able to help them accelerate code creation. In fact, code generation and code suggestions (55%) topped the list of software development use cases where respondents were interested in applying AI, closely followed by forecasting of productivity metrics and identification of anomalies (54%), summaries of code changes (53%), and explanations of how a piece of code works (53%).



However, when we look at how respondents said they're using AI today, we get a slightly different picture. The top ways respondents said they are currently using AI for software development were natural-language chatbots in documentation (41%), automated test generation (41%), and summaries of code changes (39%).

For which of the following use cases is your organization currently using AI in the software development lifecycle?



Our survey findings suggest that although code generation is important, it's only one area where AI can potentially add value. Developers reported spending only 25% of their total work time writing code, with the rest spent improving existing code (17%), understanding code (14%), testing (11%), maintaining code (9%), and identifying and mitigating security vulnerabilities (7%). That's nearly 60% of developers' day-to-day where AI — in the form of vulnerability explanations, code change summaries, automated tests, and more — can introduce efficiencies and boost productivity and collaboration.

Amount of time developers report spending on daily tasks

Respondents also identified several concerns around generative AI in the context of code creation. More than half (57%) of respondents said they think AI will replace their role within the next five years. In addition, among the 32% of respondents who expressed concern about introducing AI into the software development lifecycle, two of the top three specific concerns were related to code generation: code generated using AI may not be subject to the same copyright protection as human-generated code (48%) and code generated using AI may introduce security vulnerabilities (39%).

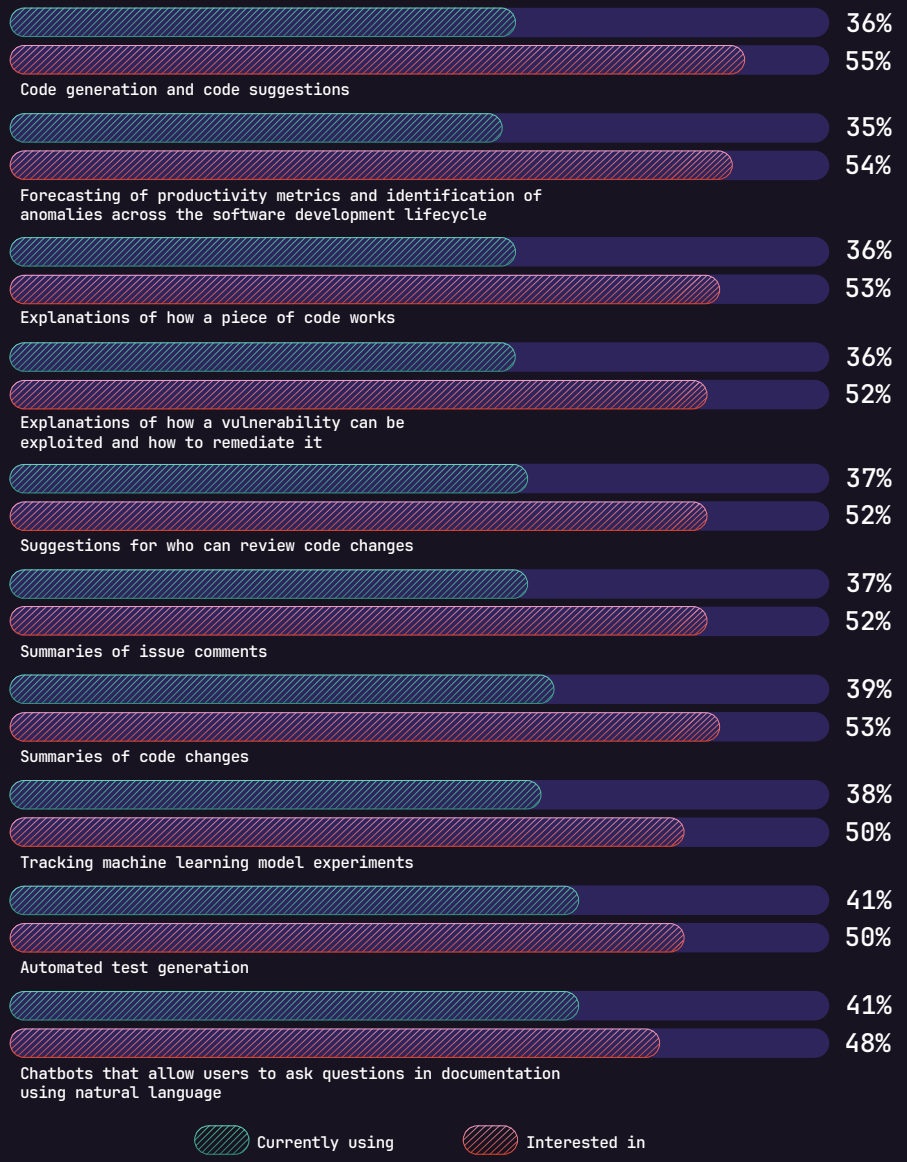
It's apparent that DevSecOps teams see the bigger picture: From test generation to vulnerability analysis to summaries of issue comments, 50% or more of respondents expressed interest in a number of AI-powered use cases beyond code generation. In other words, there's a strong appetite for more — and more integrated — AI spanning the breadth of the software development lifecycle.

Looking at the gaps between respondents' interests and current usage helps us see exactly how much opportunity there is for AI across the software development lifecycle. After code generation, forecasting productivity metrics and anomalies represents the next biggest area of demand, with 54% of respondents saying they are interested, but only 35% saying they are doing it today.

As DevSecOps teams capitalize on these opportunities and AI becomes more embedded in software development workflows, where are they expecting challenges? Next, we'll dive deeper into where respondents expressed concerns about incorporating AI into the software development lifecycle, and what we can learn from the common themes that emerge.

> "Testing and quality assurance can benefit the most from AI, as intelligent algorithms can spot bugs and errors that humans might miss."
>
> ***– Software engineer in the industrial manufacturing industry***

For which of the following use cases is your organization currently using or interested in using AI in the software development lifecycle?

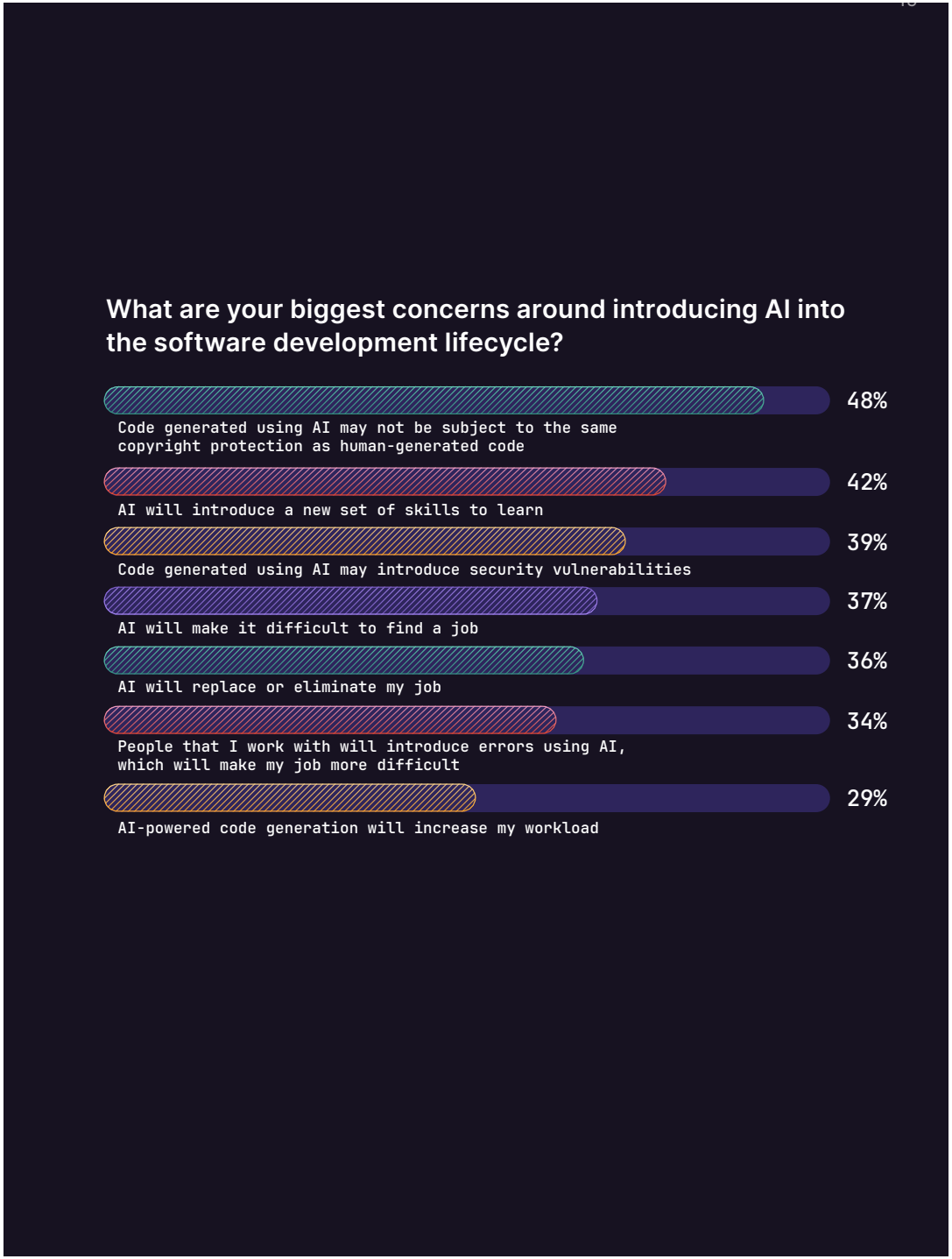


The stumbling blocks: Security, privacy, and IP

As we've seen, respondents expressed mostly positive sentiments about AI and their organizations' use of AI in software development; however, concerns around privacy, intellectual property, and security emerged repeatedly, suggesting that organizations should seriously consider these areas when implementing AI initiatives.

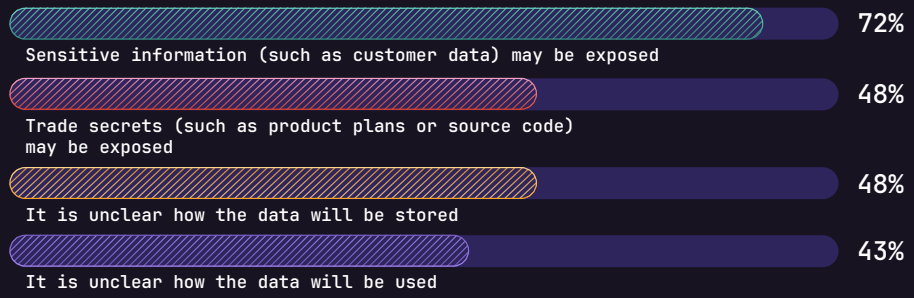
Overall, nearly a third (32%) of respondents said they were "very" or "extremely" concerned about AI being introduced into the software development lifecycle, while 23% were "not very" or "not at all" concerned. As mentioned above, when asked to identify specific areas of concern, respondents pointed to ambiguities in copyright protection (48%) and the potential to introduce security vulnerabilities (39%) as two of the top concerns.

Continuing the security theme, concern that the use of AI will increase professionals' workload was particularly prevalent among security professionals: 40% of security professionals said they were concerned that AI-powered code generation will add more to their plate, compared to just 29% of respondents overall.



In addition, the vast majority of respondents (79%) said they are concerned about AI tools having access to private information or intellectual property. Among these respondents, the top reason for concern was, by far, that sensitive information such as customer data may be exposed (72%).

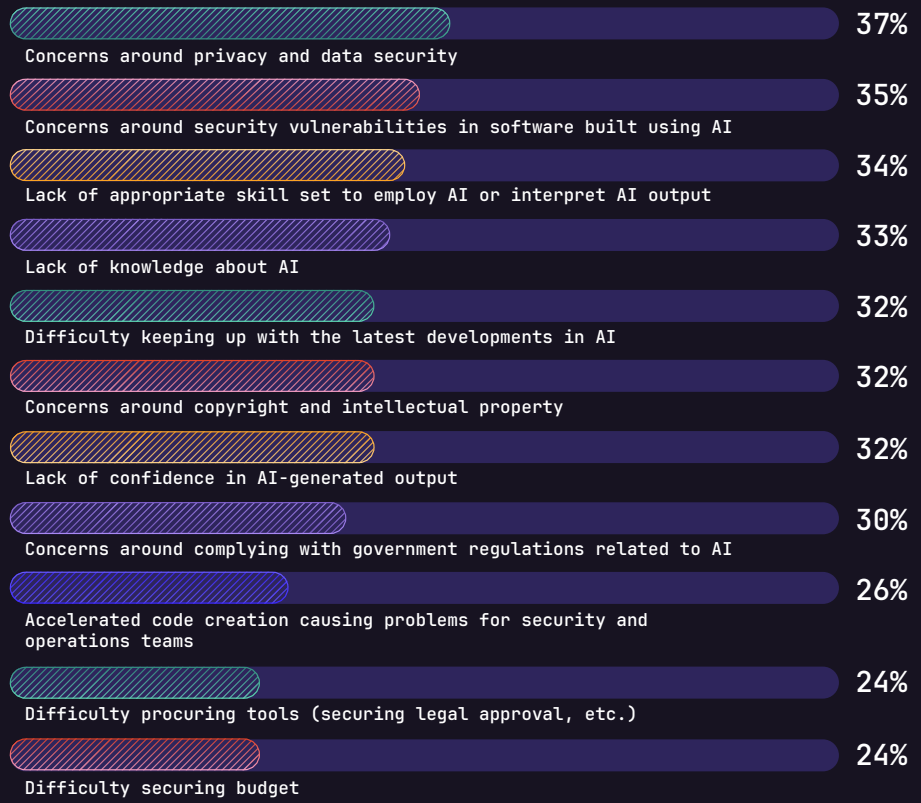
Why are you concerned about AI tools having access to private information?



Privacy, security, and intellectual property also emerged as common themes in the obstacles respondents said they have encountered or expect to encounter while implementing AI in the software development lifecycle. Concern around privacy and data security (37%) was the top obstacle identified by respondents, followed by security vulnerabilities in software built using AI (35%). Nearly a third (32%) of respondents pointed to copyright and intellectual property.

> "AI will have the biggest impact on overall planning and monitoring/ prioritizing the software development cycle. It's pretty harmless to have AI help to keep things on track, but I personally wouldn't trust it to write code due to the risk of bugs or fundamental flaws in logic.
>
> ***– Software engineer in the computer/SaaS industry***

What obstacles has your organization encountered or do you expect will encounter regarding the use of AI in the software development lifecycle?

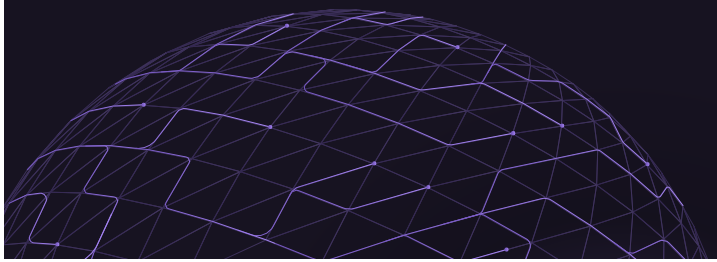


Given these concerns, it's not surprising that an overwhelming 90% of respondents said that privacy and protection of intellectual property are important to them when evaluating an AI tool or feature for use in the software development lifecycle. This was particularly true for executives: 95% of C-level and VP respondents said they prioritize privacy and protection of intellectual property when selecting an AI tool.

Bridging the skills gap

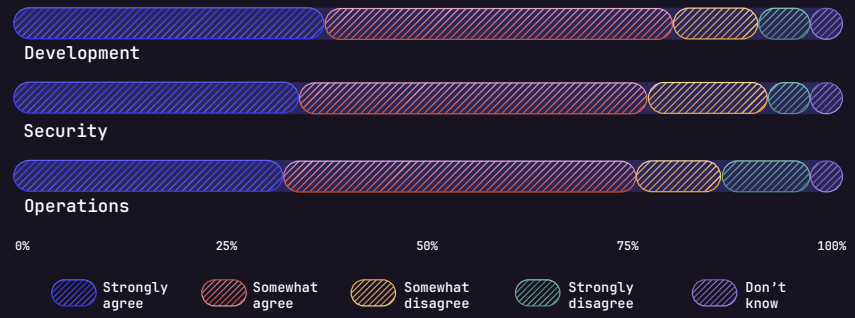
Training and skills also emerged as a common theme in the obstacles and concerns identified by respondents: A lack of the appropriate skill set to use AI or interpret AI output was one of the top obstacles (34%) and AI introducing a new set of skills to learn was one of respondents' top areas of concern (42%). Clearly, despite overall optimism about AI in software development, DevSecOps professionals feel a pressing need to grow and maintain their skills to stay ahead.

An overwhelming 81% of respondents agreed that they need more training to use AI at work, and 87% said organizations will need to re-skill employees to adapt to the changes AI will bring. This was largely consistent across functional areas, job levels, and organization sizes, although operations respondents (91%) were significantly more likely to agree that organizations will need to re-skill employees than either developers (85%) or security respondents (83%)

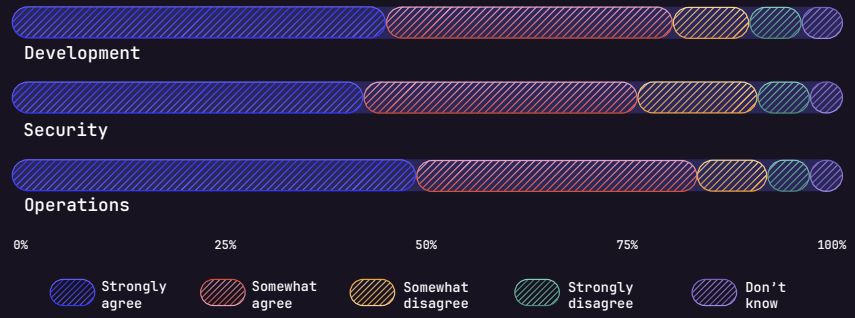


Percentage of respondents in Development, Security, and Operations who agreed with the following statements:

I feel I need more training to use AI at work



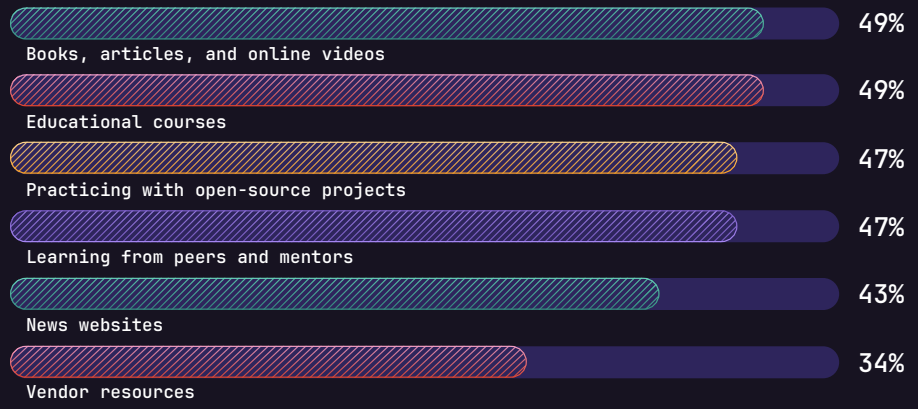
Organizations will need to re-skill employees to adapt to the changes AI will bring



To address the lack of in-house skills, 65% of respondents said their organization has hired or will hire new talent to manage the implementation of AI in the software development lifecycle.

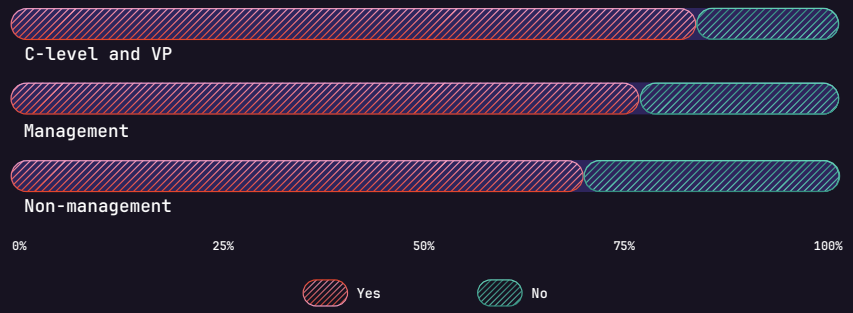
When we asked respondents what types of resources they are using to build their skills in AI, the top responses were books, articles, and online videos (49%), educational courses (49%), practicing with open-source projects (47%), and learning from peers and mentors (47%).

What types of resources do you use to learn about AI?



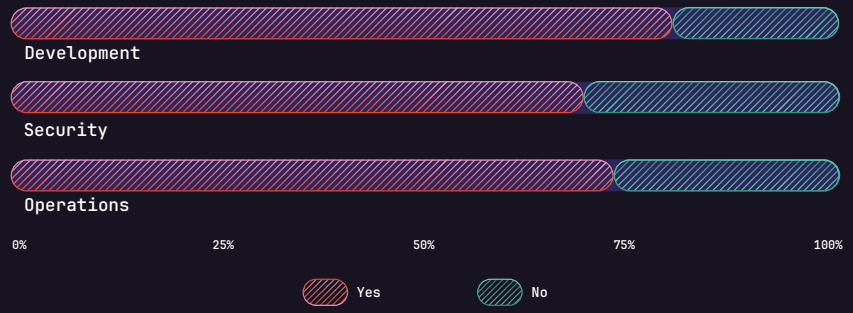
The vast majority of respondents (75%) told us their organization provides training and resources for using AI — but C-level respondents (85%) and respondents with manager titles (78%) were significantly more likely than non-managers (69%) to say their organization provides training and resources for using AI. This suggests that although organizations are making a top-down attempt to make AI resources available to employees, those resources may not be adequate, or some employees may not be aware of them.

Does your organization provide training and resources for using AI?



Interestingly, despite three-quarters of respondents saying their organization provides training and resources for using AI, a roughly equal proportion also said they are finding resources on their own, further suggesting that the currently available resources and training may be insufficient. Developers (82%) were significantly more likely than either security (69%) or operations respondents (74%) to report finding AI resources on their own.

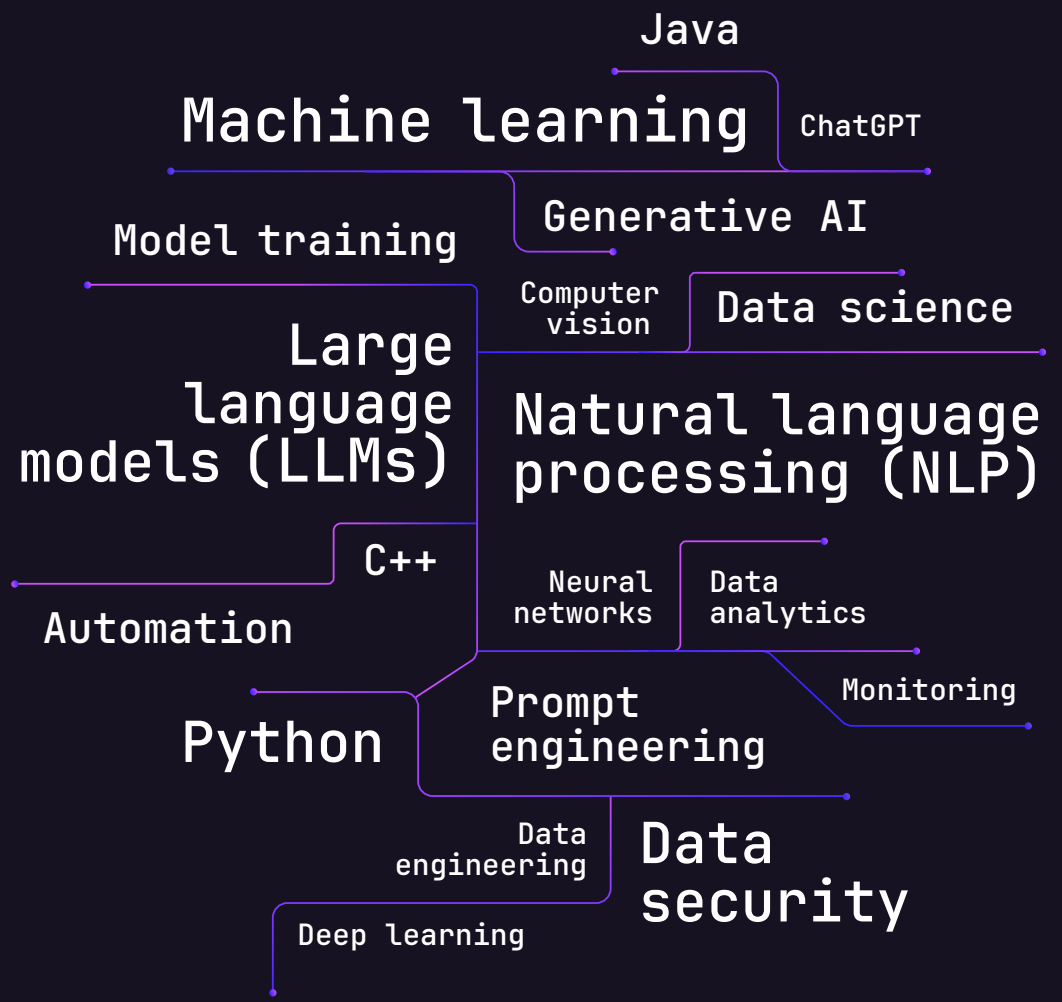
Are you finding training and resources on your own for using AI?



This makes sense, as developers are likely to be more hands-on with generative AI use cases that require training to use effectively. Developers were also significantly more likely to lack confidence in AI-generated output than either security or operations respondents (38% versus 28% and 28%, respectively). While organizations should focus on providing AI training and resources to all job roles and functional areas that will be using AI, it may be especially important to ensure that the resources for development teams are relevant, up to date, and cover the latest AI technologies and applications.

What AI-related skills would you like to learn as part of your career development?

We asked respondents to share, in their own words, how they'd like to build their AI skills. Here are a few of the most common responses:



AI can’t replace human experience

DevSecOps professionals are in agreement that AI has the power to boost their teams’ productivity and efficiency, and that it will be essential for them to build and maintain AI skills to stay competitive as individuals. At the same time, they acknowledge the inherent limitations of AI — such as the potential to introduce security risks — and the need for human review of AI-generated output.

One respondent, a DevOps engineer in the financial services industry, summed up DevSecOps teams’ cautious optimism towards AI: “Given current levels of AI, I would argue that simple, repeatable tasks are the best way forward. Everything else requires human interaction and review. I think AI can help speed up some tasks, but the humans involved have to be aware and responsible for what the AI is generating.” Another respondent, a quality assurance associate in the software industry, wrote: “I think AI could be beneficial in many areas, but it’s important to not lose a personal touch and connection.”

As organizations work to embed AI more deeply into their workflows, a tension is emerging between promises and reality — with human expertise as the inflection point. In our survey, more experienced respondents were less likely to associate AI with value drivers such as productivity gains and faster cycle times. One explanation is that more experienced DevSecOps professionals accept AI as a supportive tool for skill development, but don’t think it can completely replace the expertise, knowledge, and problem-solving of seasoned professionals like themselves. Conversely, DevSecOps professionals who are newer to the field may have more confidence in AI, perhaps because of their exposure to the technology through their schooling or on-the-job training.

Ultimately, however, it comes down to more than simply human versus machine. Leveraging the experience of human team members alongside AI is the best — and perhaps only — way organizations can fully address the concerns around security and intellectual property that emerged repeatedly in our survey data. AI may be able to generate code more quickly than a human developer, but a human team member needs to verify that the AI-generated code is free of errors, security vulnerabilities, or copyright issues before it goes to production. As AI comes to the forefront of software development, organizations should focus on optimizing this balance between driving efficiency with AI and ensuring integrity through human review.

GitLab