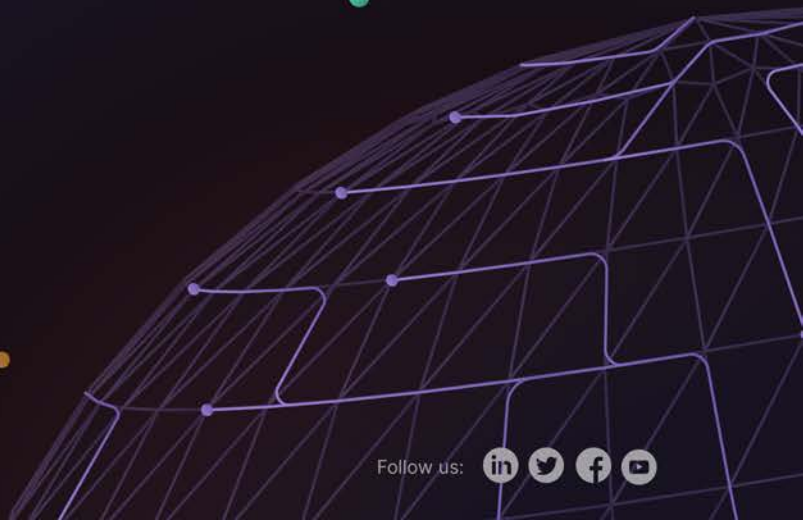
GitLab

2023 Global DevSecOps Report

Security Without Sacrifices

Table of contents



Executive summary

Organizations say they are incorporating security earlier in the software development lifecycle — and we're seeing real results in terms of the number of vulnerabilities discovered by developers and the use of new technologies such as artificial intelligence and machine learning for security testing and code checks. However, friction remains in the form of unclear responsibilities and expanding toolchains.

DevOps and DevSecOps are taking over

56% of respondents reported using DevOps or DevSecOps methodologies, up from 47% in 2022.

The shift left is getting real

74% of security professionals said they have either shifted left or plan to in the next three years.

71% of security professionals said at least a quarter of all security vulnerabilities are being spotted by developers, up from 53% in 2022.

Driving efficiencies with AI

65% of developers said they are using artificial intelligence and machine learning in testing efforts or will be in the next three years.

Too many security tools

57% of security respondents said they use six or more tools, compared to 48% of developers and 50% of operations professionals.

Teams need security *and* efficiency

Better security was one of the top benefits of a DevSecOps platform, according to respondents, along with a more efficient DevOps practice, easier automation, cost and time savings, and better collaboration. We define a DevSecOps platform as a single application with one user interface, a unified data store, and security embedded within the DevOps lifecycle.

Top benefits of a DevSecOps platform

Easier automation

Cost and time savings

Better security

A more efficient DevOps practice

Better collaboration

Who took the survey?

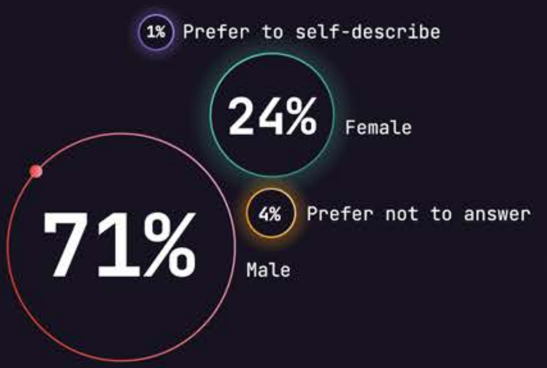
We collected a total of 5,010 survey responses in March 2023 from individual contributors and leaders in development, IT operations, and security across a mix of industries and business sizes worldwide.

We used two sampling methods for the data collection:

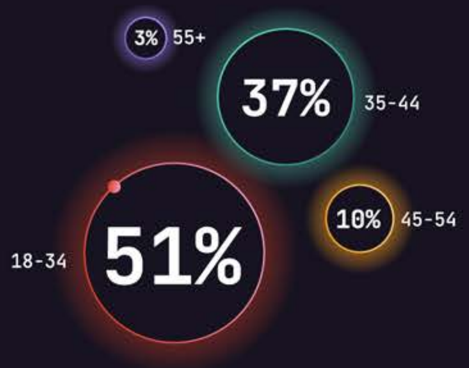
1. We distributed the survey via GitLab's social media channels and email lists.
2. A third-party research partner conducted panel sampling, which reduces bias in the sample. Our research partner used its proprietary access to lists, panels, and databases to gather quality responses and cleaned the data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

Here's a closer look at the survey respondents:

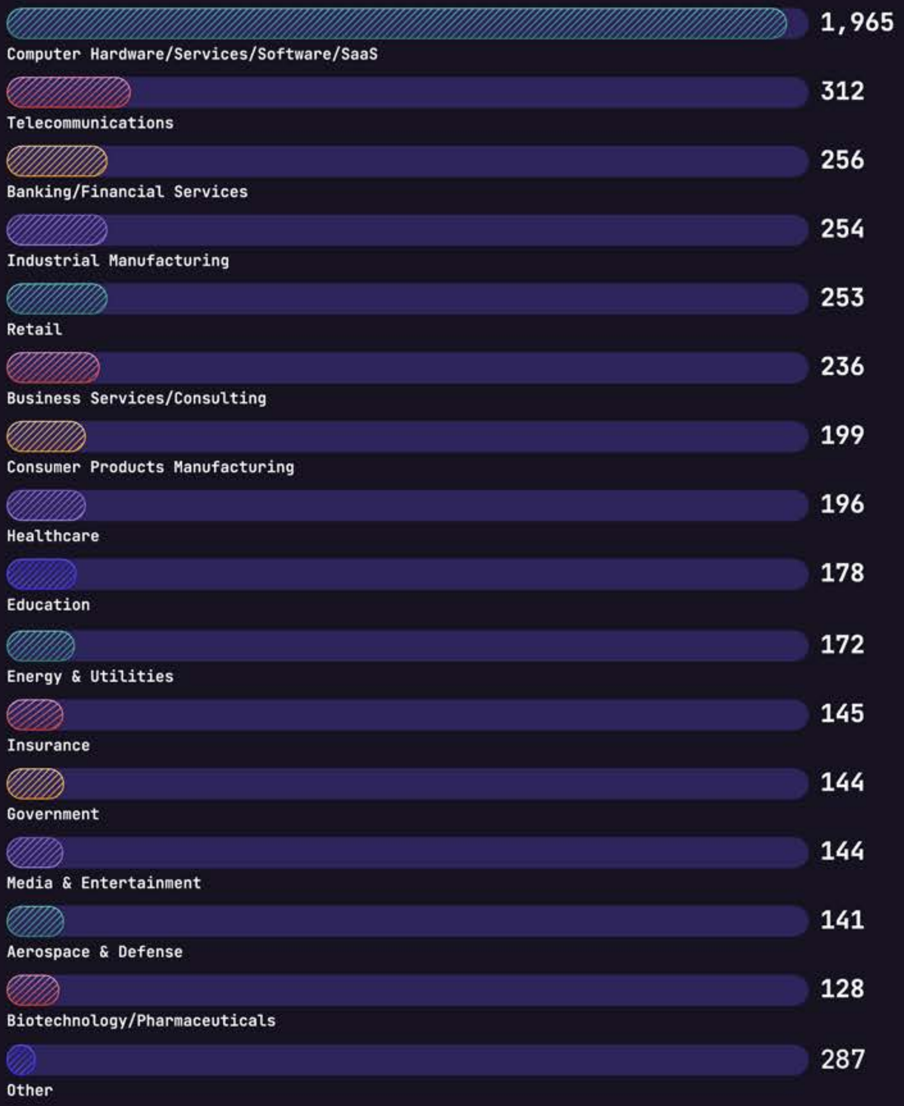
Gender



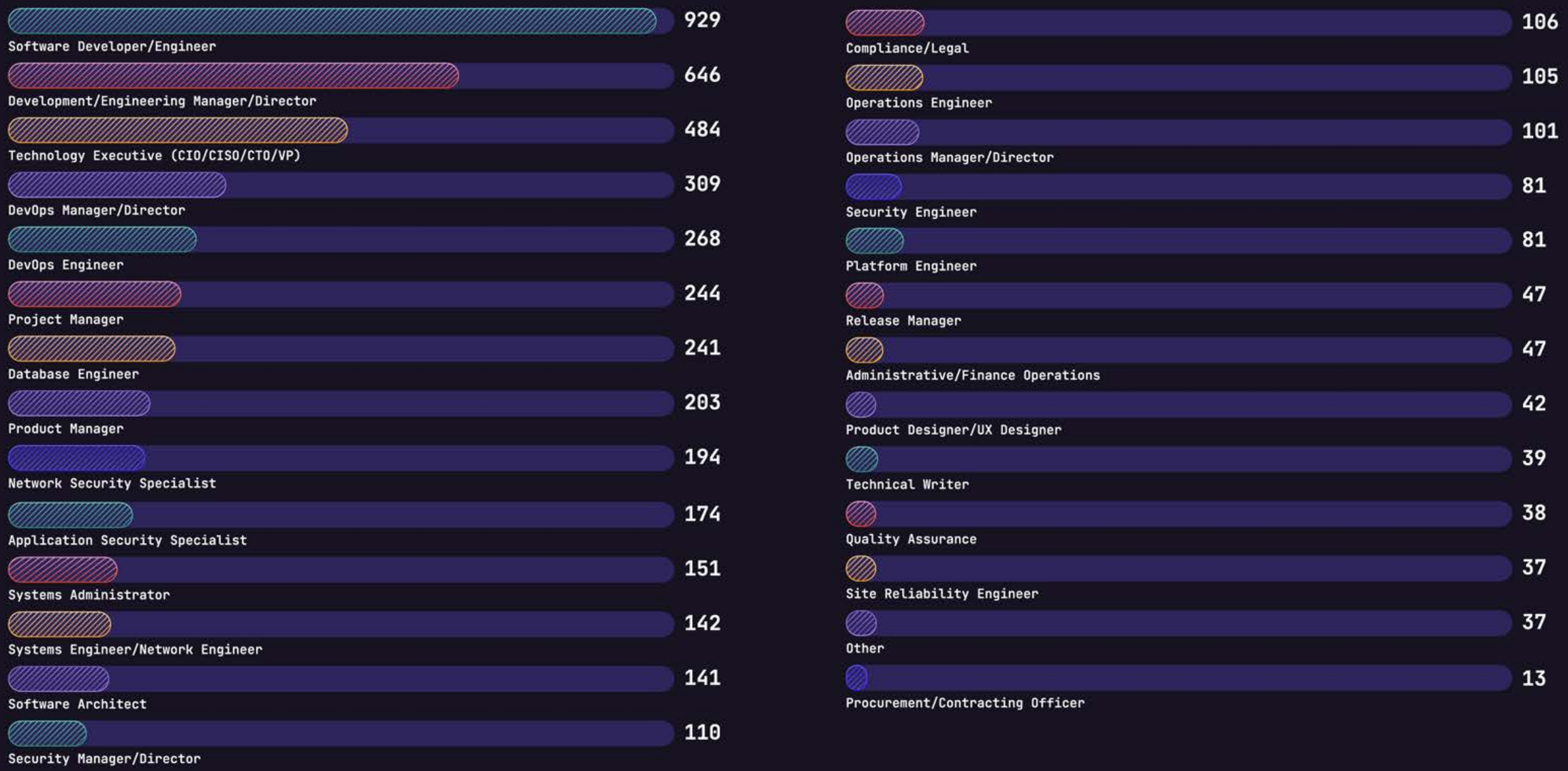
Age



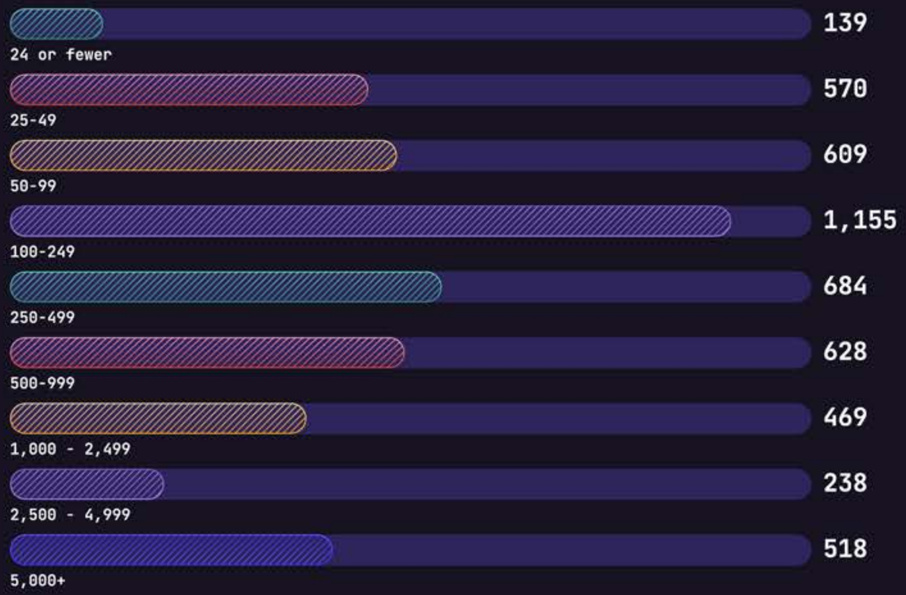
Primary industry



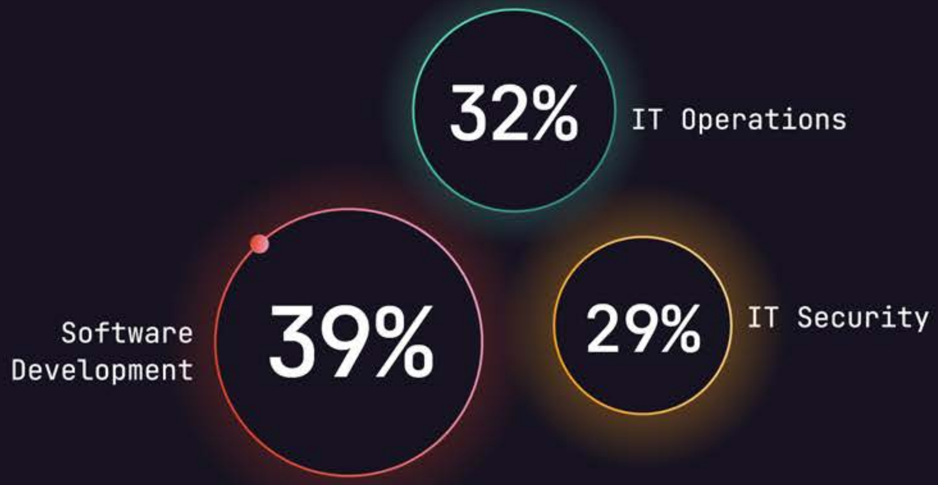
Role within the organization

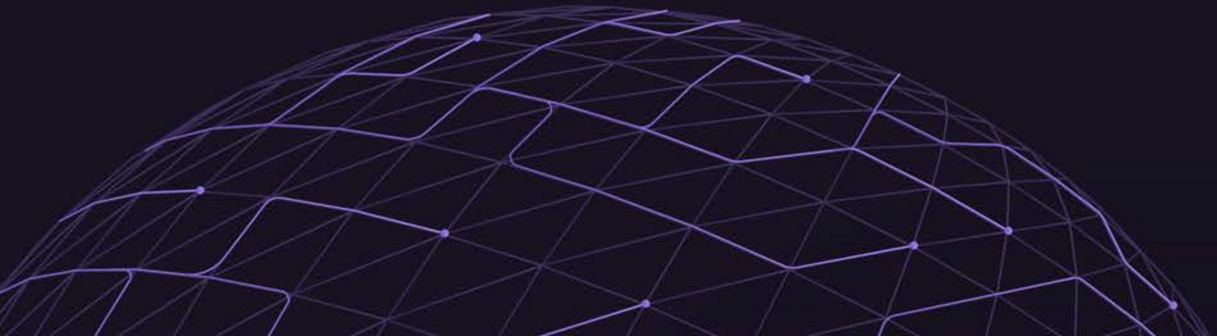


Number of employees

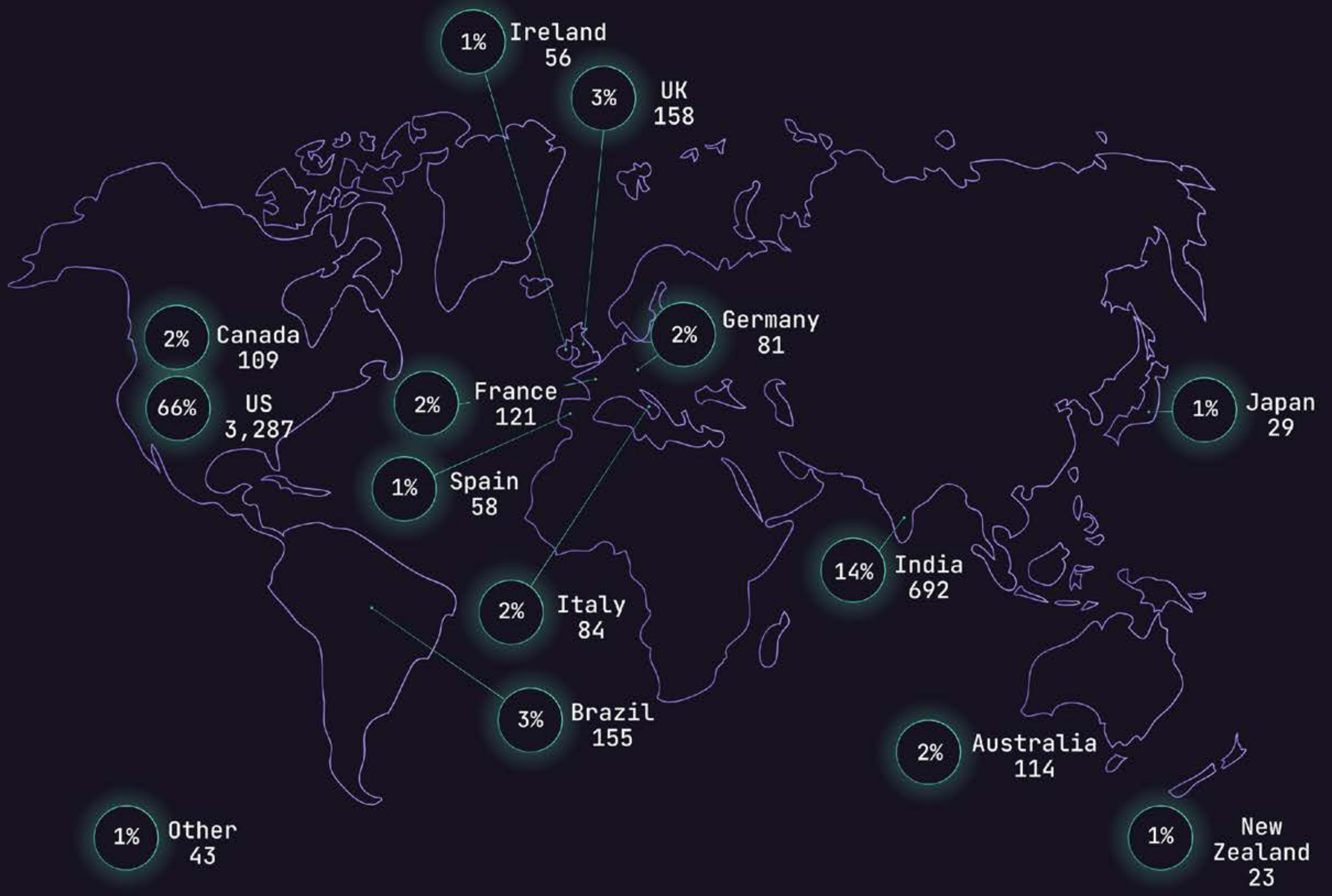


Functional area





Region


1% Ireland 56
3% UK 158
2% Canada 109
66% US 3,287
2% Germany 81
2% France 121
1% Spain 58
1% Japan 29
14% India 692
2% Italy 84
3% Brazil 155
2% Australia 114
1% Other 43
1% New Zealand 23

Introduction

Since our 2019 developer survey, we've been exploring the cross-functional relationships of development, security, and operations teams through the lens of DevSecOps to reveal insights into successful practices, problem areas, and potential solutions.

DevSecOps isn't a new idea, but it continues to evolve as attitudes change and new technologies come to the fore. We believe it is important to keep a pulse on how DevSecOps is changing for two main reasons. First, in order to understand how something is performing, we have to be able to measure it. Our annual survey is an opportunity to see where teams are succeeding with DevSecOps and where they might be struggling. Second, by capturing trends and movement in this market, we hope to give software development teams — from individual contributors to executives — insight into how to get the most out of their DevSecOps investments.

This year's survey respondents offered their views against the backdrop of a growing set of macroeconomic influences. In the face of increasing inflation, a looming economic downturn, and global supply chain challenges, many organizations are bracing for stagnant or shrinking growth. At the same time, organizations are under pressure to undergo digital transformation to stay competitive. As businesses become more digital and accumulate more data — and cyber attackers gain access to more sophisticated techniques and technologies — keeping the software supply chain secure is becoming both more critical and more difficult.

In the first installment of our expanded 2023 Global DevSecOps Report Series, we're looking at where organizations are in their efforts to shift security left — the move to embed security earlier in the software development lifecycle. What's top of mind for development, security, and operations teams when it comes to creating more secure applications? Where are teams seeing the biggest wins, and what work is left to be done?

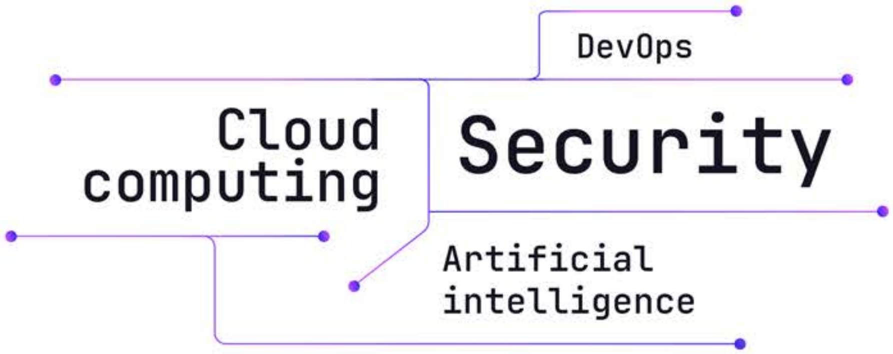
First, we'll check in on what technologies and methodologies organizations are adopting in their efforts to shift security left. We'll also look at changing perceptions around who is responsible for security and where there may be lingering friction between development, security, and operations teams. Then we'll see how DevSecOps teams are using artificial intelligence (AI) and machine learning (ML) to augment security efforts and where teams are concerned about the impacts of AI/ML. Finally, we'll explore how security teams are coming to grips with complicated toolchains, and how they can boost efficiency and productivity without sacrificing security.

Let's get started.

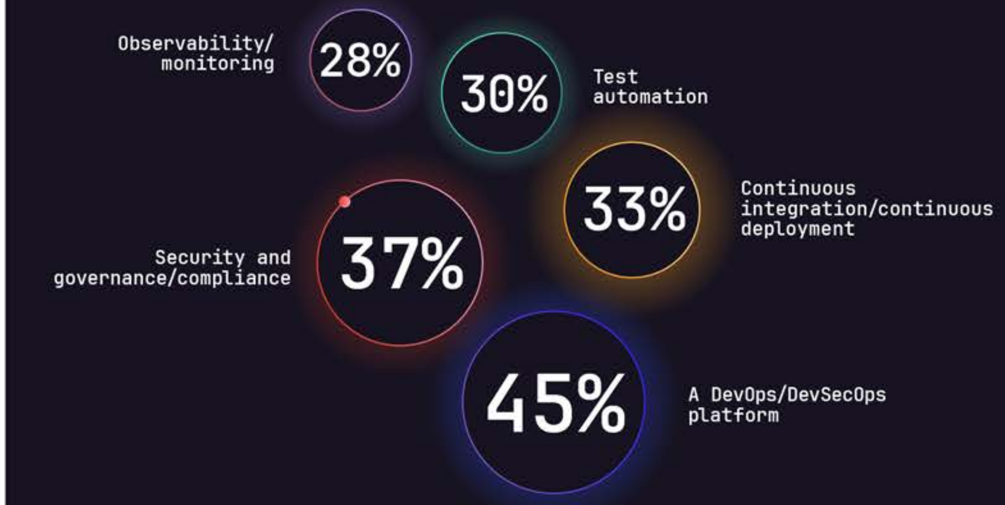
Checking in on the shift left

This year, respondents told us that security's great "shift left" to earlier in the software development lifecycle is well underway. For the past several years, we've consistently observed that security is a top priority for organizations, and that trend continued in 2023. Security ranked a very close second among this year's top investment priorities, after cloud computing. Similarly, "security and governance/compliance" ranked second among what respondents said is included in their DevSecOps implementations.

Top investment priorities for 2023



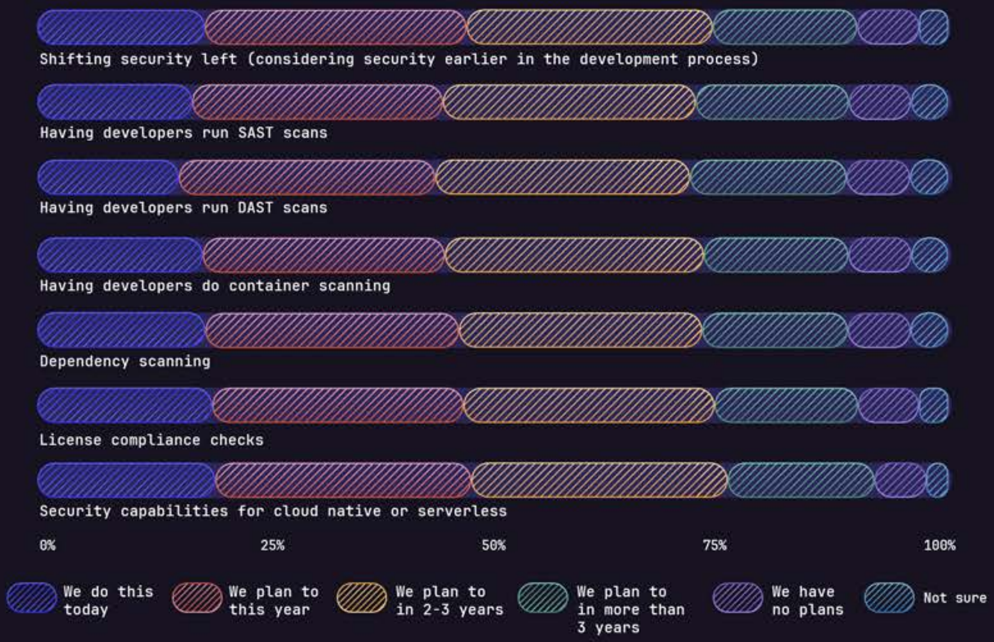
What does your DevSecOps implementation include?



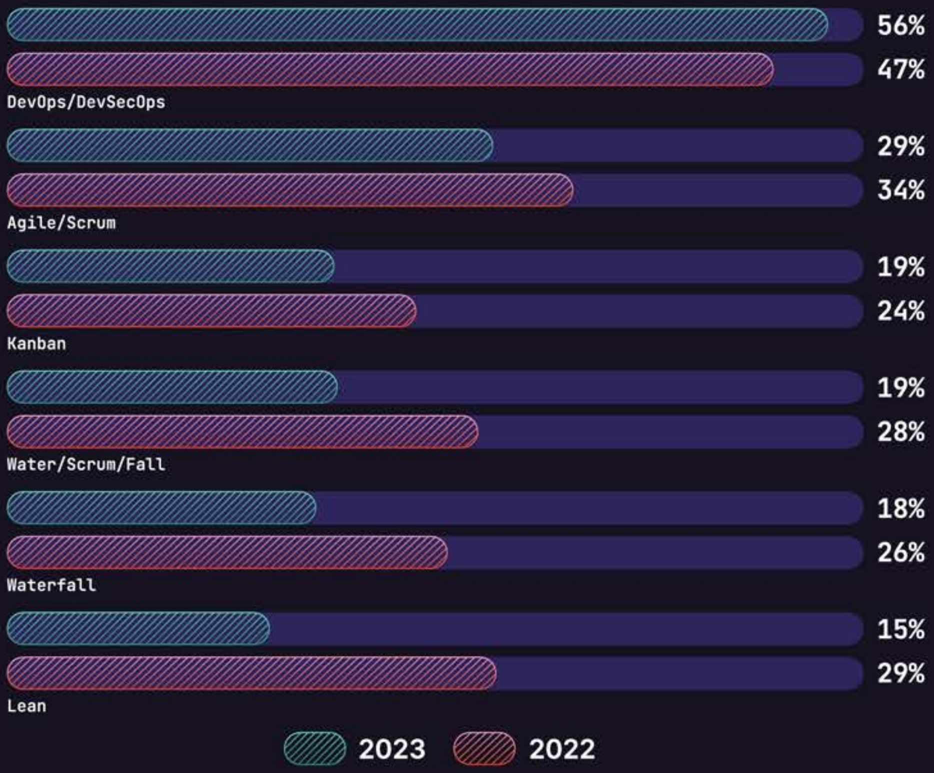
The security professionals we surveyed shared how they currently are enabling security in the software development lifecycle, as well as where they'll be focusing their efforts over the next several years. License compliance checks and security capabilities for cloud native or serverless (both 19%) topped the list of current priorities, while shifting security left (29%) was the top focus for the coming year. Nearly three-quarters (74%) of security professionals said their organizations have either shifted left or plan to in the next three years.

As part of their shift left, organizations are migrating from legacy software development methodologies to DevSecOps. This year, more than half of respondents (56%) reported using DevOps or DevSecOps methodologies, up from 47% in 2022. In fact, DevOps/DevSecOps was the only software development methodology that showed an increase in 2023 — all the others decreased. Lean showed the biggest drop, from 29% in 2022 to just 15% in 2023.

Status of key security initiatives, according to Security

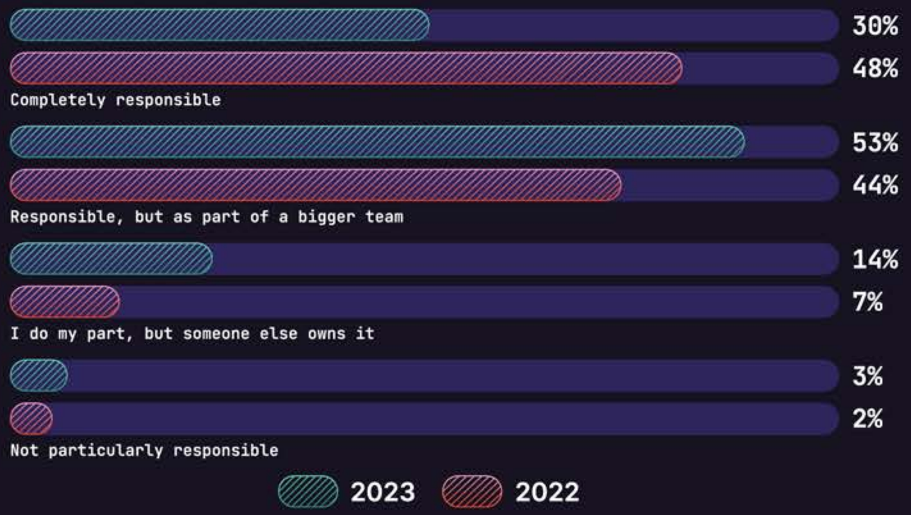


Which software methodologies does your organization use?



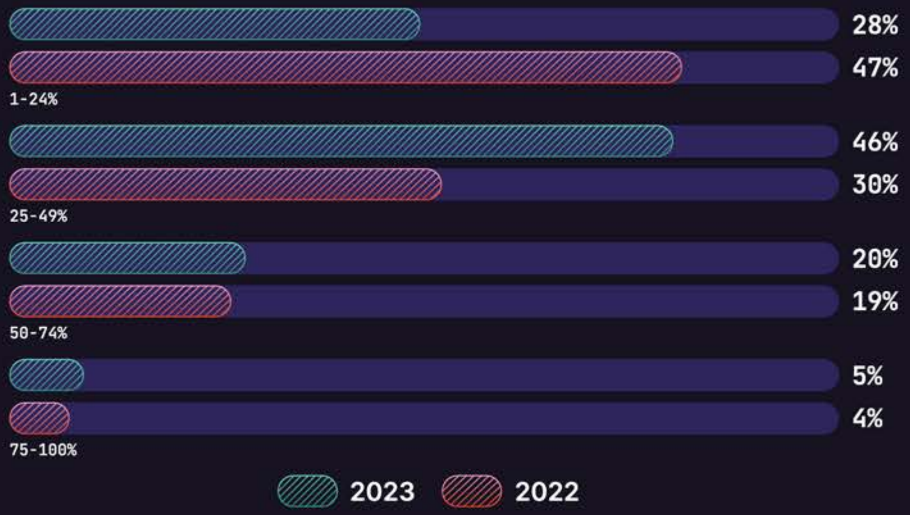
The shift left is driving a number of benefits across the software development lifecycle — most notably, development, security, and operations teams are coming together instead of working in silos. Increasingly, no single group feels like they're on their own when it comes to application security. This year, less than a third of survey respondents (30%) said they are "completely" responsible for application security (down from 48% last year). The majority of respondents (53%) said they are responsible for application security as part of a larger team — up from 44% last year.

How responsible do you feel for application security in your organization?



Similarly, 38% of security professionals told us they are increasingly part of a cross-functional team focused on security, up from 29% last year. These changes are having a real impact on how teams work together. More than 70% of the security professionals we surveyed said a quarter or more of all security vulnerabilities are being spotted by developers, up from 53% of security professionals last year.

Percentage of vulnerabilities spotted by developers, according to Security



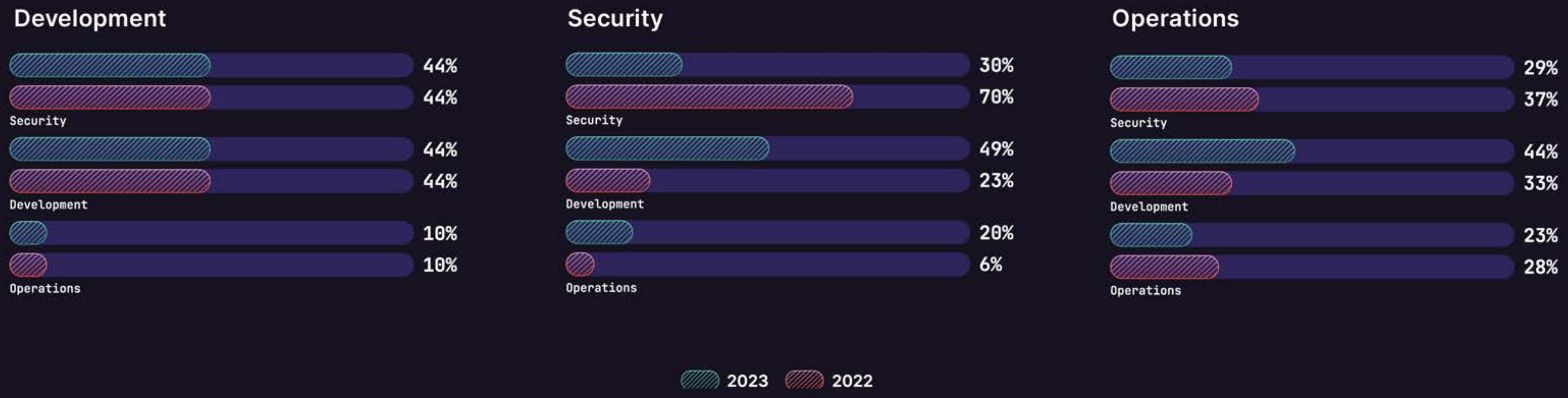
Although organizations are making progress, a number of opportunities remain. Organizations will need to follow through on their shift left by bringing security testing as close as possible to the developer — empowering teams to find vulnerabilities earlier and lowering the cost of remediation. In addition, as AI and ML become a more integral part of the software development lifecycle, organizations will need to ensure security teams are equipped with the right skills and tools to take full advantage of AI/ML. And finally — as we've observed in our past several surveys — toolchains remain a pain point for DevSecOps teams as the number of point solutions continues to outpace efforts to consolidate.

Let's dive into what this year's survey tells us about these gaps and what teams need to take into account in 2023.

The shift left isn't one and done

Although the number of respondents who feel they are completely responsible for application security dropped in 2023, those who said they aren't completely responsible had different takes on where the bulk of responsibility for application security does fall. Developers were split equally between saying Security is primarily responsible and Development is primarily responsible. But developers were more likely than security or operations professionals to say Security is primarily responsible, while security professionals were more likely than developers or operations professionals to say Development is primarily responsible. Operations professionals were more likely than developers and about equally likely as security professionals to say Operations is primarily responsible.

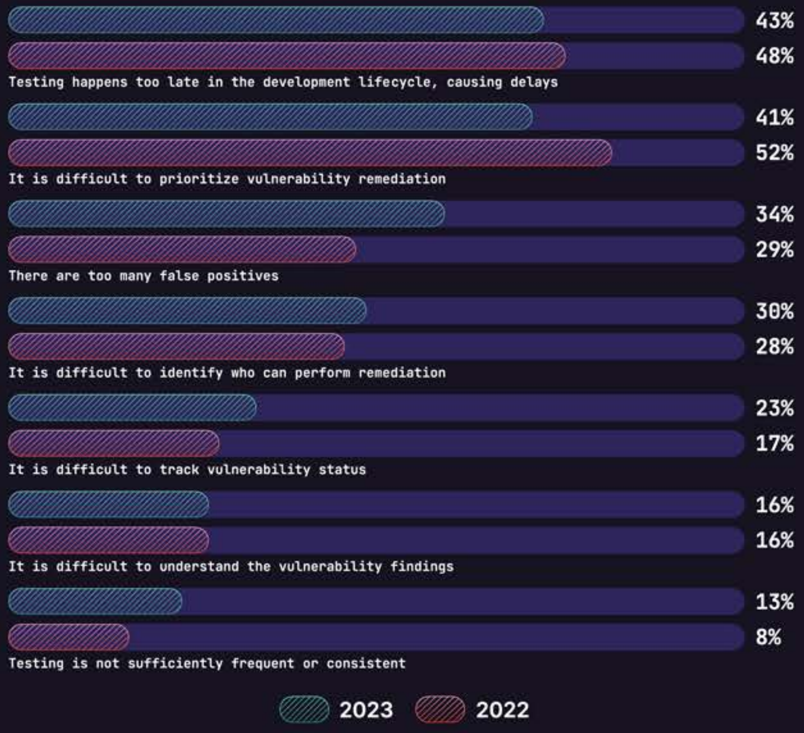
Who's primarily responsible for application security, according to...



So, while organizations' efforts to shift security left have succeeded in making DevSecOps teams more broadly aware of security as a shared responsibility, there remains confusion around which discipline should take the lead, with developers and security professionals pointing at each other.

In addition, frustrations persist around security testing in particular, although there are signs that things are improving. This year, 43% of security professionals said testing happening too late in the development cycle is a major source of frustration (ranked 1 or 2 on a scale of 1-7, 1 being the most frustrating), down from 48% last year. Forty-one percent of security professionals said difficulty prioritizing vulnerability remediation is most frustrating, down from 52% last year. Meanwhile, frustrations around false positives, identifying who can perform remediation, and tracking vulnerability status showed slight increases over last year, suggesting that integrating security testing into DevSecOps team workflows should be a continued focus for organizations as part of their efforts to shift security left.

Biggest frustrations with security testing, according to Security



What are the biggest challenges in software development in 2023?

We asked respondents to share, in their own words, their opinions on the biggest challenges in software development this year. Not surprisingly, security was a major theme. Here's what a few of the respondents had to say:

> "**Security, security, security, and more security**... not only is this now an absolute MUST, we owe it to our customers, our organizations, our colleagues, ourselves, future DevOps Engineers, and humanity at large to do everything we can to create a safe, secure, compliant, and scalable future for our industry."
>
> **– *DevOps Engineer, Healthcare***
>
> "There's too much focus from Product on pushing out new features without taking the time to keep an eye on **security, code quality, and code rot.**"
>
> **– *Site Reliability Engineer, Media & Entertainment***

"**Security is becoming more important** and quickly shows the gaps between traditional development methodologies such as waterfall and newer, product-based organizations. In some ways, I see the gap between mature, capable teams and less mature teams as growing rather than closing."

– DevOps Leader, Business Services/Consulting

"How to make AI models better to meet the needs of customers and meet the **ever-changing security challenges of globalization.**"

– Software Developer, Government

"Ensuring software is designed to be compliant with **emerging security standards.**"

– Operations Engineer, Computer Hardware/Services/ Software/SaaS

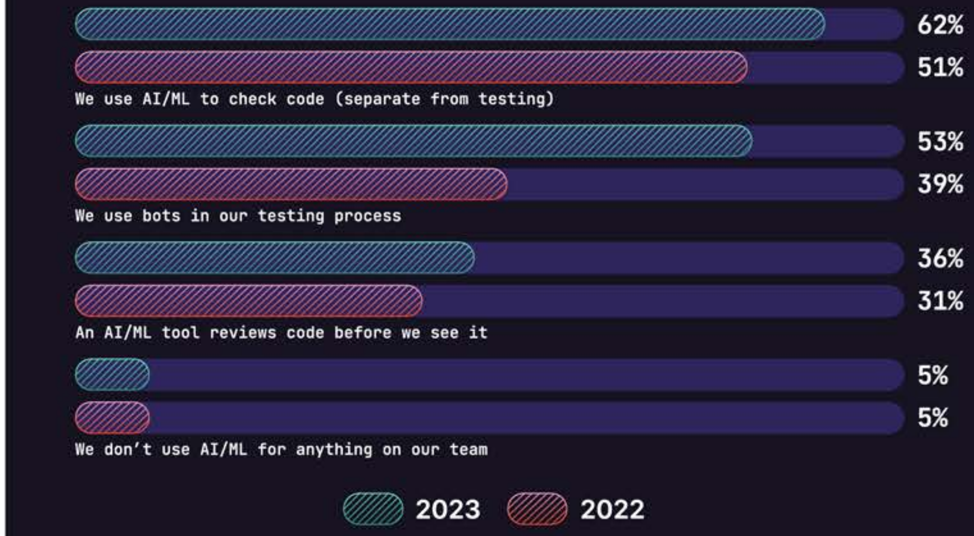
"There are an **overwhelming amount of vulnerabilities** to triage and resolve."

– Security Engineer, Computer Hardware/Services/ Software/SaaS

Driving efficiencies with AI

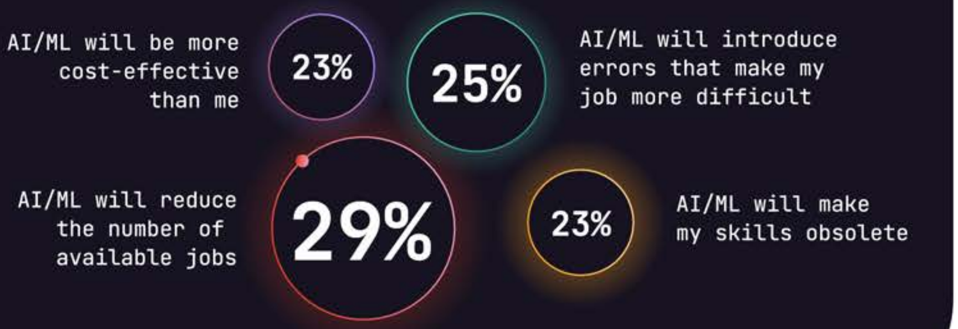
AI and ML are becoming well established in software development workflows, including for security testing and code checks. This year, more than half (65%) of developers said they are using AI/ML in testing efforts or will be in the next three years. Among developers who are using AI/ML today, 62% said they use AI/ML to check code, up from 51% last year; 53% use bots for testing (up from 39% last year); and 36% use AI/ML for code review (up from 31% last year).

Top uses for AI/ML, according to Development



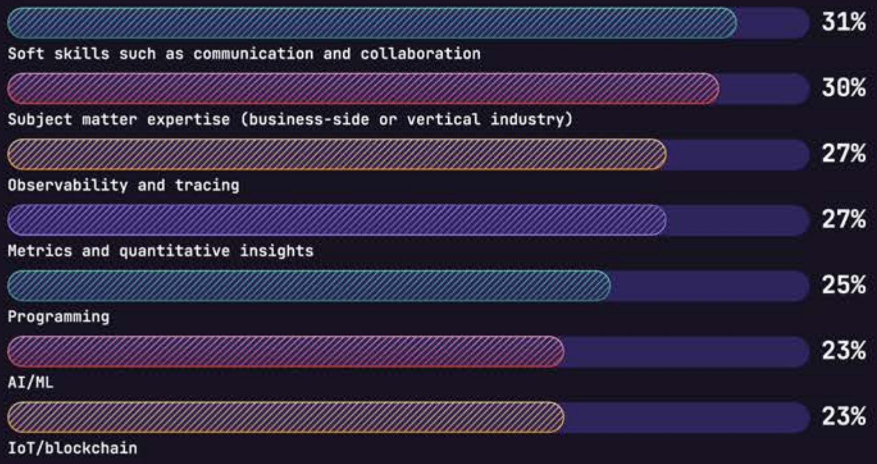
The rise of AI/ML isn't all smooth sailing: A solid majority (67%) of security respondents said they are concerned about the impact of AI/ML capabilities on their job, and 28% of them said they are "very" or "extremely" concerned. Of those respondents who expressed concern, 25% said they are worried about the potential for AI/ML to introduce errors that will make their job more difficult.

Top concerns related to AI/ML, according to Security



Despite its rising prevalence on the development side, AI/ML is competing with other high-impact areas as security professionals shuffle their professional goals and priorities. Last year, security professionals identified AI/ML as the most important skill for furthering their careers, and security professionals were significantly more likely than either developers or operations professionals to choose AI/ML. This year, while nearly a quarter (23%) of security professionals chose AI/ML, they placed more importance on skills such as soft skills (31%), subject matter expertise (30%), and metrics and quantitative insights (27%).

Most important skills for the future, according to Security



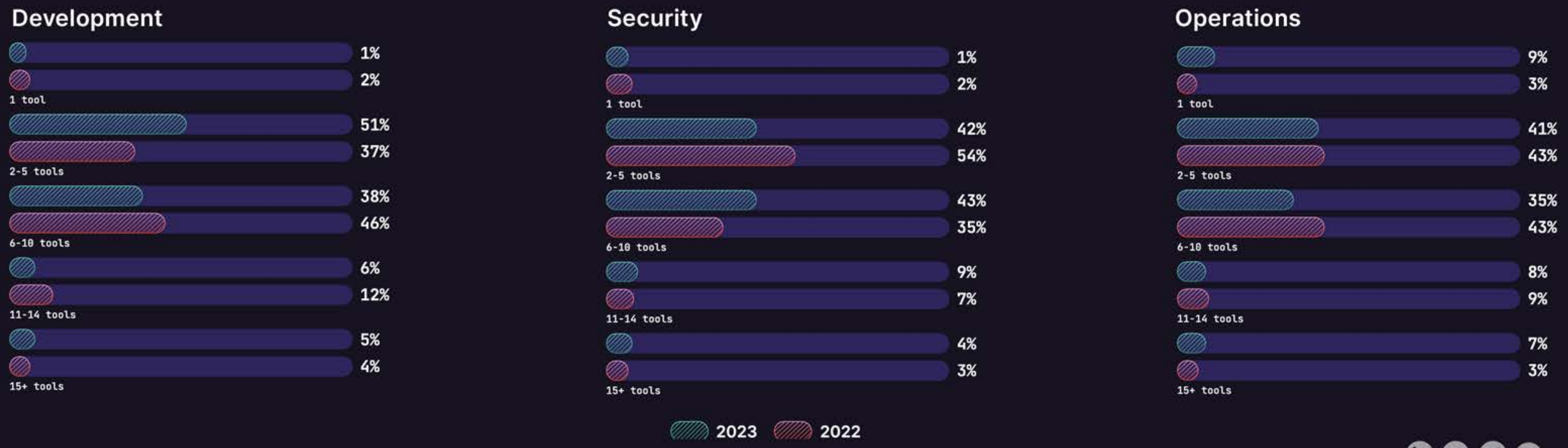
Too many security tools

Toolchain management continues to be an area where DevSecOps teams are feeling the pressure. This year, 66% of survey respondents (and 69% of security respondents) told us they want to consolidate their toolchains. Security professionals in particular reported using a lot of tools — 57% of security respondents said they use six or more tools, compared to 48% of developers and 50% of operations professionals. What's more, security teams appear to be shifting toward using more tools than before: This year there was a significant drop (from 54% to 42%) in the number of security respondents who said they use 2-5 tools, and a corresponding increase (from 35% to 43%) in the number of security respondents who said they use 6-10 tools.

When we asked how having too many tools negatively impacts their software development practice, the largest group of security respondents (28%) said spending time maintaining toolchains makes it difficult to stay on top of compliance; 27% said it is difficult to have consistent monitoring across many different tools; and 26% said it is difficult to draw insights across all the tools.

Despite these challenges, the ability to "bring your own tools" to the job remains attractive: 68% of survey respondents (and 67% of security respondents) said they brought at least one preferred development tool to their current job.

The number of tools teams use for software development, according to...

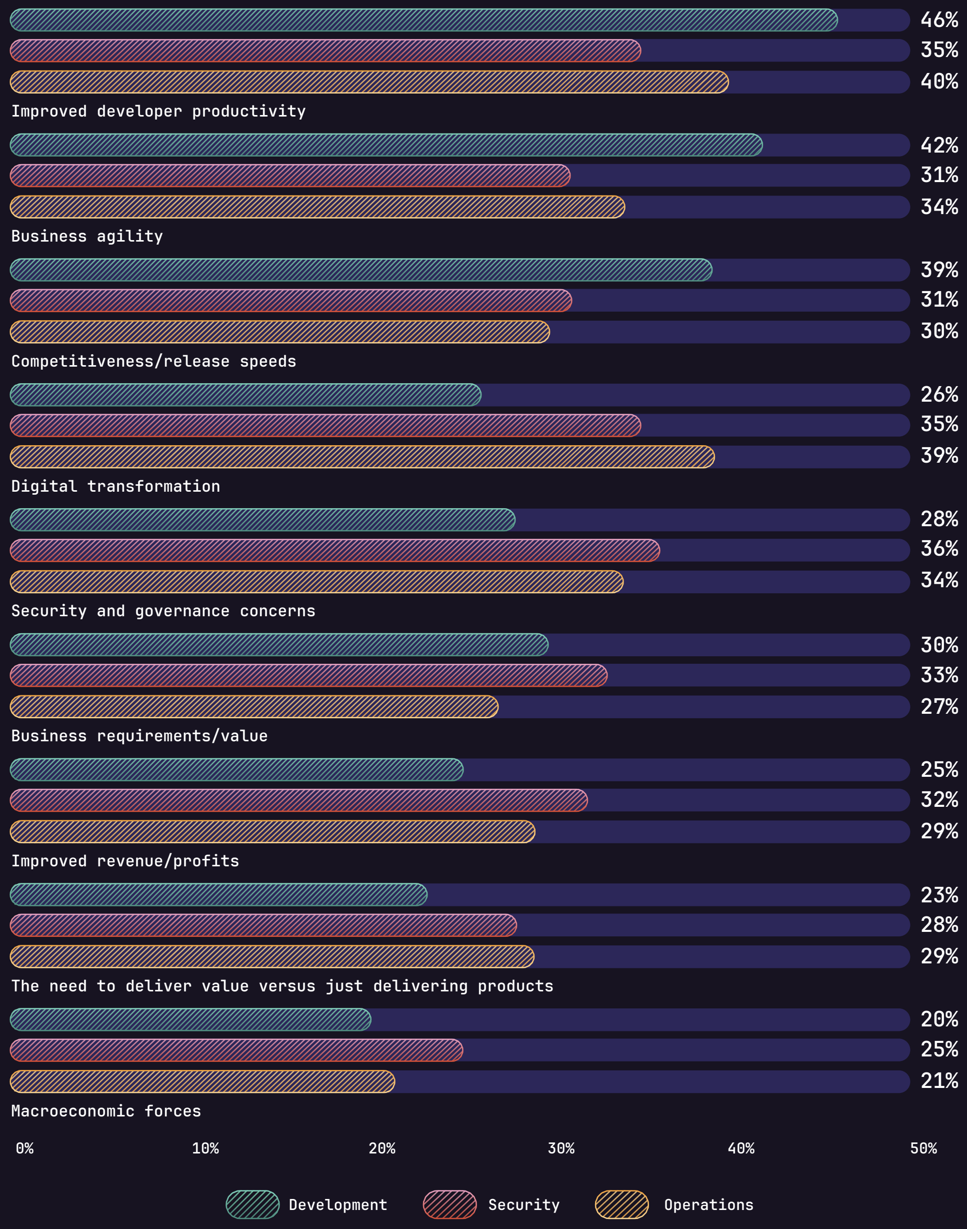


Follow us:

The rise of the DevSecOps platform

In today's uncertain macroeconomic environment, organizations of all sizes are facing slower growth and tighter budgets. Security teams may be feeling the headwinds more acutely — only 15% of security respondents told us they have more budget this year than they did in 2022, and security professionals were also more likely than both developers and operations professionals to cite macroeconomic forces as a primary factor driving DevSecOps practices to scale at their organizations.

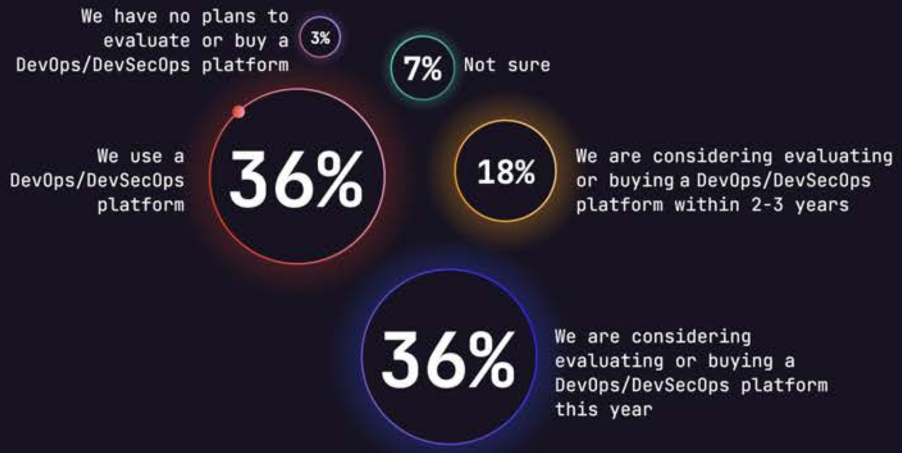
Factors driving DevSecOps to scale, according to...



Security continues to be a non-negotiable priority for organizations. At the same time, as AI evolves from a "nice-to-have" into a "must-have" and the number of disparate tools security teams are using continues to expand, organizations will need to find ways to be efficient without sacrificing security.

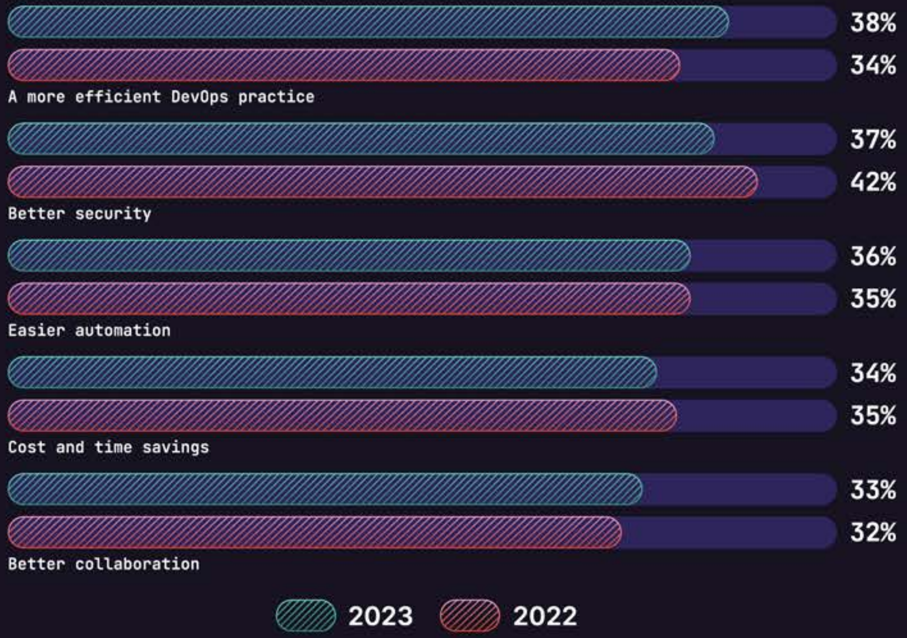
Against this background, it's not surprising to see DevSecOps platforms continue to gain traction (in the survey, we defined a DevSecOps platform as a single application with one user interface, a unified data store, and security embedded within the DevOps lifecycle). This year, 72% of survey respondents (73% of security respondents) said they are using a DevSecOps platform or are considering adopting one in the next year. Of the survey respondents who reported using a DevSecOps platform, 46% said the entire DevOps team is using the platform, up from 43% last year.

Which of the following best describes your team's current situation regarding a DevOps/DevSecOps platform?



Security remains important as a major benefit of a DevSecOps platform, and efficiency is emerging as equally important. Last year's respondents identified "better security" as the top benefit of a DevSecOps platform; this year security came second, after "a more efficient DevOps practice."

Top benefits of a DevSecOps platform



By improving both security and efficiency, DevSecOps platform usage accelerates organizations' shift left: Security professionals who use a DevOps/DevSecOps platform were significantly more likely than those who don't use a platform to say they have shifted left already or are planning to shift left this year. Security respondents who use a platform also said developers catch more security vulnerabilities and had a higher opinion of their organization's security efforts. In contrast, security respondents who don't use a DevSecOps platform were more likely to struggle to identify who can perform remediation and find it difficult to understand vulnerability findings.

Of security professionals using a DevSecOps platform...

62% have shifted left or are planning to shift left this year.

78% rate their organization's security efforts as "good" or "excellent."

Meanwhile, developers who use a DevOps/DevSecOps platform were significantly more likely than those who don't use a platform to say they feel their organization makes it possible for them to identify and mitigate security vulnerabilities, and they were more likely to have implemented automation and AI/ML for testing.

Of developers using a DevSecOps platform...

90% feel their organization makes it possible for them to identify and mitigate security vulnerabilities.

68% have implemented test automation or plan to in the next year.

54% have implemented AI/ML for testing or plan to in the next year.

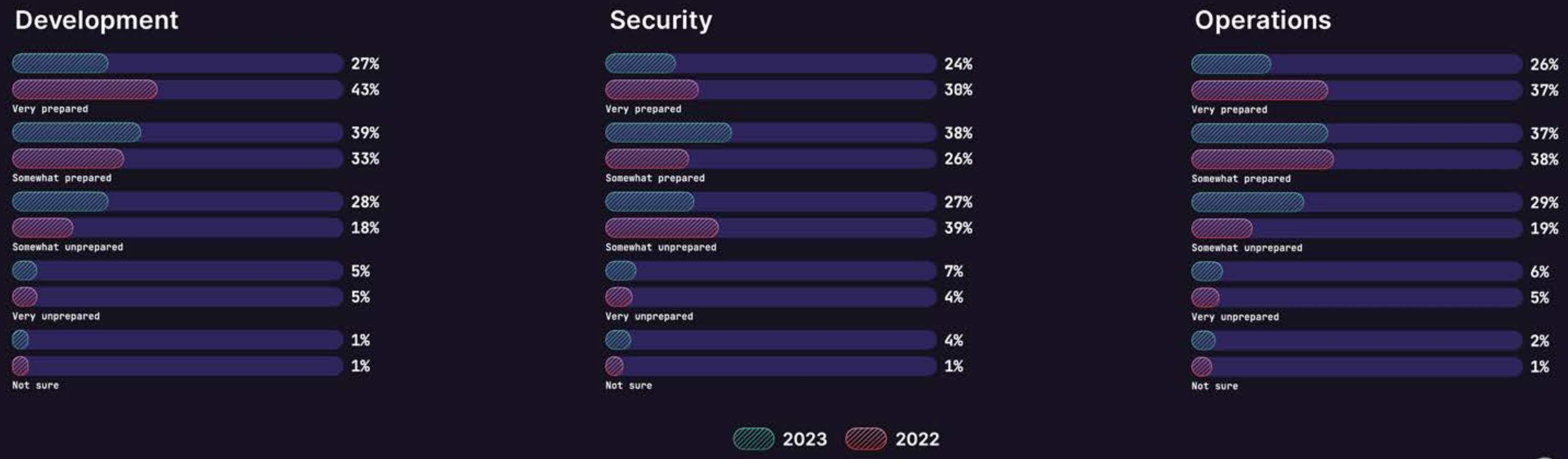
Looking to the future

Given all the uncertainties in today's environment, it's not surprising that DevSecOps teams might feel less optimistic this year than in past years. Overall, 64% of this year's survey respondents said they feel "very" or "somewhat" prepared for the future, down from 69% last year. Interestingly, while this trend held for developers and operations professionals, security professionals showed the opposite: 62% of security respondents this year said they feel "very" or "somewhat" prepared for the future, up from 56% in 2022.

New programs that aim to address threats to the software development lifecycle — in response to headline-grabbing software security incidents from the last several years — could be one explanation for this change in attitude among security teams. In other words, the security professionals we surveyed may feel better prepared because their security and development programs are now dedicating cycles to mitigate software and application risks.

Although security teams are facing new and unpredictable hardships in the form of economic uncertainty, increasing cyber attacks, and organizational challenges, teams also have many reasons to be optimistic about what's to come. Evolving mindsets around who is responsible for security, new technologies like AI/ML, and tools that consolidate complicated security toolchains are all giving teams new ways to build secure software faster and more efficiently.

How prepared do you feel for the future, considering how your job function or industry is changing?



GitLab