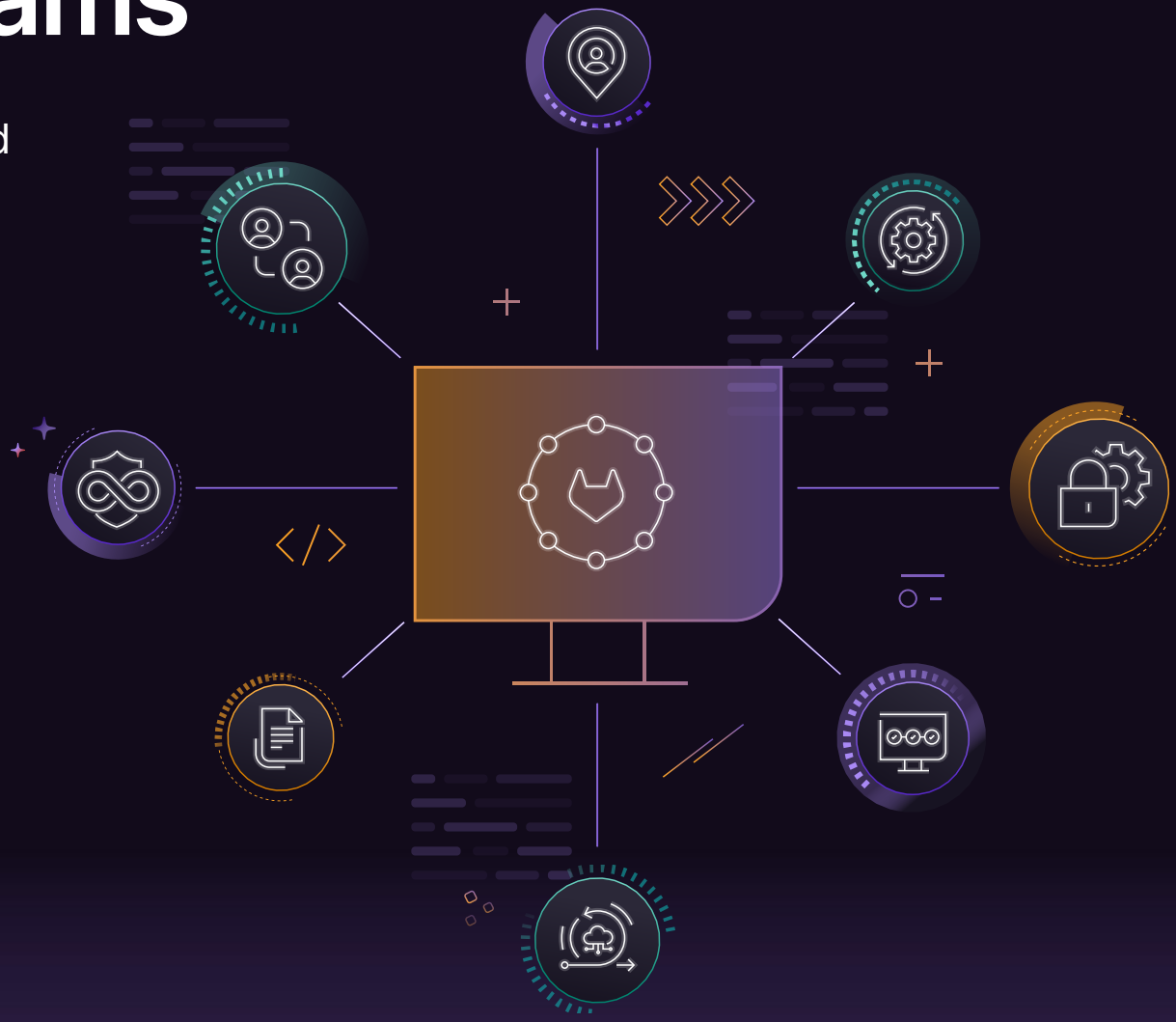
The Ultimate Playbook for High-Performing DevSecOps Teams

8 ways IT leaders can help teams build better, more secure software, faster



GitLab

Table of contents

Introduction

IT leaders may realize that the performance of DevSecOps teams affects how quickly they can produce new software. However, leaders also need to be aware that team performance is integral to how the overall business can take on competitors and ride out changes in a turbulent market.

High-performing DevSecOps teams are directly tied to creating a stronger business. And IT leaders — from managers to directors and executives — play a critical role in exactly how effectively and efficiently those teams function and are able to bolster the company's brand, customer loyalty, partner relationships, and ultimately the bottom line.

"It's not just up to team members to make sure they're running at top performance, creating software efficiently, at speed, and securely," says **Fatima Sarah Khalid**, developer evangelist at GitLab. "IT leaders have a shared responsibility in ensuring their teams have a strong vision, resources, and a culture of learning, collaboration, and development. It would be difficult for any team to be successful without strong leadership."

If your organization already has an AI-powered **DevSecOps platform**, that's a great start because it eliminates the complexity, mounting costs, and **headaches that go along with a toolchain**. But there's a chasm of

How IT leaders can support their teams:

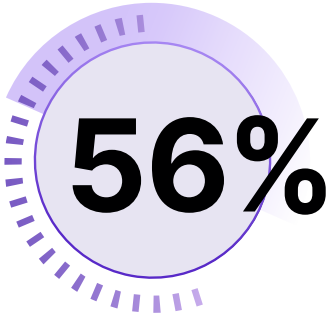
- Invest in training for team members
- Stay current with new technologies, like AI
- Connect with business leaders to better align DevOps efforts with company goals
- Make sure team members are using automation
- Embed security team members in with developers and operations
- Ensure security is a shared responsibility
- Foster a culture of collaboration

difference between elite teams and everyone else, affecting how resilient, secure, and reliable your team is able to be.

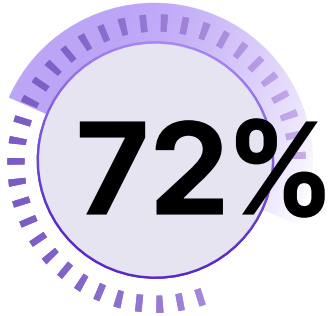
If teams are falling somewhere below a top performance level, they're not taking full advantage of all the features and processes that could be powering software deployment and securing your products.

Take advantage of a shifting market

In 2023, industry analyst firm Gartner® Inc. recognized "DevOps Platforms" as a market category by making it the focus of one of its **Magic Quadrant™ research reports**[1] for the first time. We believe this move is a strong indicator of the market's shift from point solutions to platforms and validates the importance of DevOps platforms.



Survey respondents who reported using DevOps or DevSecOps methodologies, up from 47% in 2022



Survey respondents who said they are using a DevSecOps platform or are considering adopting one in the next year

Source: GitLab's 2023 Global DevSecOps report

DevSecOps: Understand the terms

DevOps: A set of practices and methodology that bring together development and operations to increase the efficiency, speed, and security of software development and delivery compared to traditional processes

DevSecOps: An evolution to DevOps, it's an approach to software development that integrates security throughout the development lifecycle

DevOps toolchains: Multiple stitched-together tools and point solutions

DevSecOps platform: A single-application approach to DevSecOps that allows teams to have visibility throughout and control over all stages of the software development lifecycle

That means DevOps, and by extension its evolution into DevSecOps, has reached a **whole new level of maturity**. So it's time to up your game or risk being left behind.

Why performance matters to your business

High performance translates to higher deployment frequency, faster time to market, improved security, and better quality — all of which **directly correlate to cost savings** and the company's ability to quickly pivot to meet volatile and changing markets. And creating secure software means protecting the company's data and brand, avoiding embarrassing headlines, and ensuring customer and partner trust isn't lost.

Being more efficient and having teams develop and deploy faster and more securely means the business can respond to whatever comes at it. Also delivering a lot of value to customers means increasing brand loyalty since users won't be so easily enticed to switch to one of your competitors who beat you to the market with a tempting new feature.

Do you have high performers?

So how well are your DevSecOps teams operating? Here are several questions you can ask yourself as you think about team performance:

- How quickly and efficiently are your teams deploying software?
- What's their change failure rate?
- What's their lead time for changes?
- Are they reliable, meaning can they deliver on promises made?
- Is their time to restore service solid?
- Is your organization struggling to release software fast enough to meet customer needs?
- Are releases slower, or not as smooth, as they used to be?
- Are security vulnerabilities consistently, or increasingly, popping up in your software?
- Do different parts of your DevSecOps teams know what the others are working on?
- Does pushing new features into production often cause issues or slowdowns?
- Are team members showing signs of burnout?

> **If teams are having trouble with any of these areas, they may need a little extra support.**

Getting started

In this ebook, we'll not only help you understand what helps DevSecOps teams become high performers, but how IT leaders can help them achieve that level of success. We'll look at keeping software teams' focus on users, the importance of team-wide collaboration, sharing security responsibilities, and combining the cloud with a flexible infrastructure.

Whether your DevSecOps teams are struggling to up their game or could simply add to what they're already doing right, remember that becoming a highly successful team of DevSecOps professionals is an attainable goal.

Let's dive in

8 steps to building top-performing DevSecOps teams

1. Create a culture of collaboration

At its core, DevSecOps is about collaboration. It's a team sport that relies on cooperation and joint responsibility. It's simple: Better cooperation leads to more, and more efficient, continuous, iterative development and feature deployment. Cooperation makes a DevSecOps team more agile so it can adapt to changes in projects and workloads. It also can mean less worker burnout and turnover.

Making this cultural shift means more diverse input, which leads to more well-rounded products and software. Imagine everyone having visibility into a project so when someone sees a bottleneck, they can jump in and offer, "Hey, I can show you how to fix that."

Fueling a culture of communication and cooperation isn't just for DevSecOps team members. A truly collaborative culture also should include colleagues in different parts of the company—from finance to marketing, customer relations, and the C-suite. And that all-inclusive, collaborative culture gives software development teams the boost they need to be more productive, more efficient, and create more well-rounded products.

Action item:
Curate the culture

Culture streams down from the top. It's the responsibility of leadership to establish a positive culture. That means making sure teams are set up with people who have the right skills and ongoing training. Teams also need to be aligned with business goals and customer needs so they are working toward the right set of objectives.

2. Focus on users

It's critical to stay focused on your users and what they need — before they go looking for it from one of your competitors. When teams are focused on user needs, they're building the right new features, fixing bugs, and creating new software that will keep customers happy and sticking with your brand.

User focus is a real differentiator for high-performing teams. It's not just about shipping software. It's about understanding how that software is being used. If you're shipping lots of new features really fast but no one wants to use them, you're not delivering much value. Listening to users has to be a key part of the DevSecOps process.

Action item:
Maintain a user focus

IT leaders should ensure they are involved in meetings with business teams, including customer service, marketing, and strategic planning. They also need to set up continuous processes to monitor and collect user feedback and insights on how customers are interacting with your products and then guide iterations to make sure customers are getting what they need and the business is reaching its goals.

40% Increase in organizational performance from teams with strong user focus.

20% Increased job satisfaction when teams focus on the user.

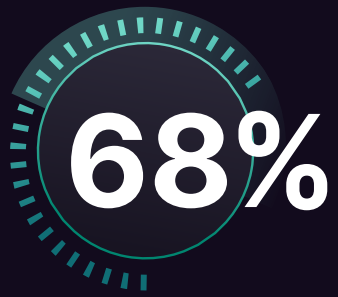
Source: 2023 Accelerate State of DevOps Report

3. Automate tasks

Want to help your software development teams work faster, more easily, and more securely? Want to decrease the possibility of human error? **Automation is a big part of the answer.**

While it doesn't remove humans from the equation, automation provides consistency and minimizes the need for a lot of hands-on and time-consuming work, like tasks involved in backup, installation, and maintenance. It also can be used for testing, configurations, integrations, and alerts for everything from compliance to security and continuous integration and delivery.

> **"Stress Testing is a great example of an activity that should be automated because, if it's done manually, it could require hundreds or even thousands of user hours to manage it."**
>
> **— Darva Satcher, Director of Engineering, GitLab**



Percentage of surveyed developers using a DevSecOps platform who have implemented test automation or plan to in the next year.

Percentage of time developers spend actually writing code, as opposed to testing and understanding code, and IDing vulnerabilities.

Source: GitLab's 2023 Global DevSecOps report

With automation, every task is performed identically and with reliability and accuracy. This promotes speed and increases deliveries, while decreasing infrastructure hand-holding.

Darva Satcher, director of engineering at GitLab, notes that executives should consider how much work can get done by using automation, which unlike humans, never has off hours.

“Stress Testing is a great example of an activity that should be automated because, if it’s done manually, it could require hundreds or even thousands of user hours to manage it,” she added. “This is easily handled with automation whereas having so many testers running the same simulation would be ridiculously expensive and highly inefficient.”

Automation lets developers focus on what matters most instead of wasting time on repetitive tasks that don’t let them use their expertise. With automation, team members can focus on big, creative new projects, propelling the company’s software forward.

Action item: Prioritize automation

For their part, executives need to ensure their teams have access to the automation built into a DevSecOps platform. Then they should help prioritize which processes are automated first by weighing needs in security, compliance, and speed.

4. Share security responsibility

Integrating security throughout the software development lifecycle enables DevSecOps teams to identify issues that could ultimately hurt the company's finances and brand, and break customer and partner trust. Catching and fixing security vulnerabilities also reduces legal liability connected to breaches.

That means working security into every phase of software development is critical for every business.

However, despite so much concern and talk about security, it can still be more of an afterthought than a full-cycle focus in the software development process. Instead of catching and dealing with vulnerabilities as they're created along the way, many teams are still waiting until right before deployment to check for problems. And at that point, it's going to be more difficult and time consuming to go back, find the issue, and fix it.

The best DevSecOps teams know that high delivery and operational performance are directly linked to integrating security practices throughout their development process. Security reviews must be integrated into every phase and applied to all major features, while security professionals must

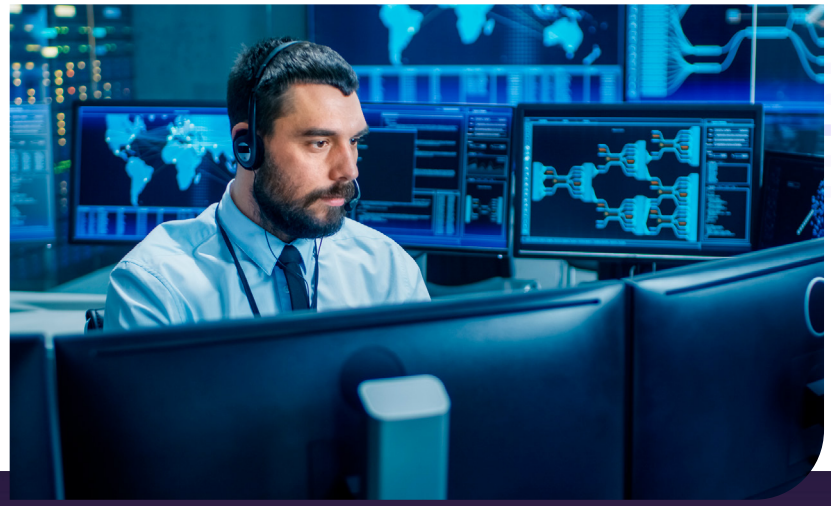
Security professionals surveyed who said a quarter or more of all security vulnerabilities are being spotted by developers, up from 53% of security professionals last year

Security professionals using a DevSecOps platform who rated their organization's security efforts as "good" or "excellent"

Source: GitLab's 2023 Global DevSecOps report

be included in planning and development, and security testing should be automated. All of that can be done in an end-to-end DevSecOps platform.

Ayoub Fandi, staff field security engineer at GitLab, points out that developers should rarely have to reach out to the security team because they should already be involved. “Often companies adopt a platform and have the developers using it but they keep security people off to the side,” he says. “Executives need to draw the security team in and fully take advantage of the power of that integration. It will change everything.”



Action item: Foster team connections

IT leaders play a significant role in ensuring not only that DevSecOps teams are using automated security and compliance testing and alerts, but that there’s a high-level of communication and collaboration between security professionals and the rest of the team.

To get there, executives should be creating a collaborative, inclusive culture where people from every team — and even across corporate departments — work together on security, and understand that it’s a shared responsibility. Set up casual in-person or Zoom meetings between different team members. Invite security teams to product planning meetings. Invite developers to threat-modeling sessions.

5. Enable platform engineering

Action item: Make use of platform engineering

First of all, if teams aren't already employing platform engineers, IT leaders should explore the idea. They also should be meeting with their cloud and DevSecOps teams to find out where they're hitting slow-downs and priorities for building efficiencies into their systems. And adopting a DevSecOps platform will help as new processes and efficiencies can be built on a single, well-tested application.

Setting up a DevSecOps team's work environment to make their jobs easier only makes sense. That's where platform engineering comes into play.

Platform engineering is an approach to designing and building workflows that gives developers and operations team members more self-service capabilities and accelerates application delivery. To do that, platform engineers optimize the DevSecOps platform and infrastructure with automation, repository configurations, template installation, and monitoring tools. That paves the way for greater efficiency, compliance, and consistency for the development and deployment teams. It doesn't replace DevSecOps. It's a natural part of it, with the focus on minimizing human errors, and planning, designing, and managing the developer experience.

"Platform engineering is about building the internal tools and systems that empower developers," says Fandi. "It's having a specific team doing custom work on the platform to tailor the system for your organization and your particular goals. It's literally having a team dedicated to making developers' jobs easier."

For instance, if an organization has a complex way of handling secrets, a platform engineer might build a way to manage them in the platform by creating a specific workflow or process. Existing tools can be part of the solution but the engineer can make sure they're being used and used consistently. "It's about finding the right feature and unveiling it," adds Fandi.

Since platform engineering makes it easier for people across the breadth of the DevSecOps team to work more efficiently, it will increase everyone's performance, enabling them to work faster and focus on productivity, rather than tedious tasks.

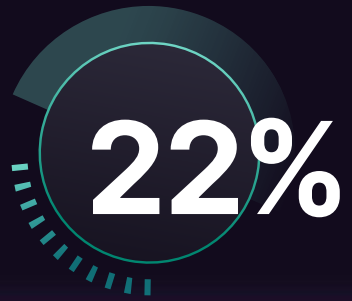
6. Combine cloud with flexible infrastructure

For a long time, word was that companies needed to take advantage of the cloud to be successful. While that still is true, it's not the whole story.

According to the **2023 Accelerate State of DevOps Report from DORA**, the DevOps Research and Assessment team at Google, using the cloud doesn't automatically produce benefits. Actually, the report notes that simply "lifting and shifting," or moving data workloads from a data center to the cloud, is not as helpful as executives might expect and actually can be detrimental.

It's really about how companies implement the cloud. And it's specifically about taking advantage of the flexible infrastructure the cloud enables.

"Creating a flexible infrastructure is how cloud computing differentiates itself," the DORA report concludes. "Flexible infrastructure is a predictor of team, organizational, operational and software delivery performance."



Increase in infrastructure flexibility for respondents using a public cloud compared to not using the cloud

Source: GitLab's 2023 Global DevSecOps report

Higher organizational performance from using flexible infrastructures

Source: GitLab's 2023 Global DevSecOps report

Organizations with more than a quarter of their apps in the cloud are 2.2x more likely to release software faster than they did a year ago

Source: GitLab 2023 Global DevSecOps Report

Cloud computing in itself is important because it enables that flexible infrastructure.

So what is flexible infrastructure?

It means the system architecture is set up to be easily and quickly adaptable so it can scale up or down on demand. It delivers agility, and offers reliable application performance. It also speeds application development and deployment, which essentially should be plug and play.

“Flexibility and elasticity are top benefits of the cloud,” says Fandi. “It would be difficult to be a top-performing DevSecOps team without using the cloud and creating a flexible infrastructure. If you have this setup, you can spin up resources as you need them. Everything just flows more easily.”

Action item: Ensure flexibility

To create this cloud and flexible infrastructure combination, IT leaders need to work with business executives to make the case not only for using the cloud but to have the resources needed to focus on building in the necessary flexibility. They also have to give teams the time and resources they need to properly configure both systems.

“You can’t just throw what you’ve had on premises into the cloud,” says Fandi. “To build actual business value, you have to rethink how you set up that cloud experience. You have to map out your infrastructure so you take advantage of all the benefits available.”

7. Prioritize documentation

Quality documentation is foundational to every software development effort.

There's a direct correlation between creating documents — everything from manuals to code comments, bottleneck fixes, and code quality metrics — and creating usable best practices. Solid documentation is accurate, up to date, comprehensive, searchable, well-organized, and clear. It shouldn't be left to the end of a project or foisted on one person to manage.

When a DevSecOps team has this repository of information, it affects team performance, productivity, and even job satisfaction and employee retention. That's because team members aren't spending their time solving problems that have been solved before or trying to figure out best practices.

With one search, all of that information is at their fingertips. That drives the implementation of technical capabilities and amplifies the impact of DevSecOps on the overall business, according to the DORA report.

The problem can be that documentation often is seen as something that forces people to stop creating to "take notes." Developers and security team members would generally rather be working on big projects than maintaining a knowledge stockpile.

Better continuous integration from using high-quality documentation

Source: GitLab 2023 Global DevSecOps Report

Action item: Make documentation a priority

To make sure documentation is thorough and up to date, managers need to make sure that problems, fixes, and best practices are recorded throughout the development and deployment process. They also have to ensure that all DevSecOps team members are working on it, instead of making one individual responsible for it at the end of a project, or even worse, at the end of a quarter when a lot of knowledge will have been forgotten.

Leaders have to guide team members to always document in the same, easily accessible platform, set documentation requirements, automate documentation when possible, and make sure people from every part of the team—development, production, security, and monitoring—all are adding to documentation.

But that is missing the point, because documentation is a fundamental part of big projects, as well as day-to-day operations. Building and maintaining strong documentation strengthens every aspect of the software delivery lifecycle.

“Whether there’s a new developer onboarding to a team, someone is transferring from another team, or a key player leaves the company, documentation will help get people up to speed and make sure there’s no knowledge lost,” says John Coghlan, director of Developer Relations at GitLab. “It also enables self service. People won’t need to go ask a team lead questions about, say, a specific API call. They can just read the documentation and find the answer. It’s important for collaboration and efficiency.”

> **“Documentation will help get people up to speed and make sure there’s no knowledge lost.”**
>
> **— John Coghlan, Director of Developer Relations, GitLab**

8. Look toward AI benefits

Since every team is looking to gain operational efficiencies and increased velocity, all eyes right now are on artificial intelligence (AI) and machine learning (ML). Generative AI, whether in the form of vulnerability explainers, code suggestions, or code completion, has the ability to dramatically affect workflows across the entire software development lifecycle. Leveraging AI tools built into a platform can increase security, monitoring, and scalability, while decreasing time spent on code reviews and application development.

The AI transformation is just beginning, with many teams only starting to see the impact of these tools. The DORA report notes that AI's biggest impact on team performance levels will be in coming years. Building a foundation today is critical. Khalid notes that an AI-powered evolution is coming quickly.

"In two to five years, teams regularly will be using generative AI to support code creation, automated testing, and fixing security flaws," Satcher says. "The importance of AI will just continue to grow. Teams need to use it now to familiarize themselves with the technology and figure out what it can do for them."

She puts even more emphasis on the need for companies to begin using,

Action item: Focus on training, priorities

IT leaders need to make sure they stay current with what AI features are available and then talk with their teams about prioritizing what areas of their workflows they would like to first make more efficient and faster. Once they have buy-in from their teams, give everyone from developers to security and operations the time and resources to begin working AI into their jobs.

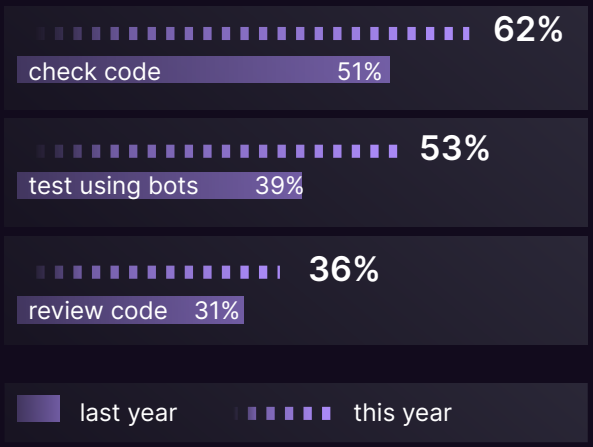
Khalid notes it's always critical for executives to make training available to team members but with something as new as AI, it should be a special consideration.

"It would be difficult for a team to succeed without strong leadership who have a vision for what is coming," she says. "Leadership has to support training to continuously equip the team with the knowledge they need of DevSecOps processes and practices and new technologies, like AI."

or at least testing the waters, with AI features in their DevSecOps platform. “If you’re not infusing AI into your process, you might be out of the picture someday because your competition will have left you in the dust,” she says. “You have to stay up to date with this because AI makes everything faster. Everywhere we’ve used it, it’s increased productivity. If people can find a place in their cycle to squeeze it in, they should get that boost.”

> **“Some people might say they don't see the need to use AI because they're doing fine without it. Well, you can do better.”**
>
> **— Darva Satcher, Director of Engineering, GitLab**

How developers are using AI/ML today



65%

Developers who said they’re using AI/ML in testing efforts or will be in the next three years

Source: GitLab’s 2023 Global DevSecOps report

83%

Respondents who said it is essential to implement AI in their software development processes to avoid falling behind

81%

Respondents who said they need more training to use AI in their work

IT leaders support DevSecOps success

While individual contributors obviously greatly add to the success of their DevSecOps teams, IT leaders share that responsibility. Performance and culture flow down from the top, as teams tend to adopt the mindset mirrored to them.

That means leaders need to ensure their teams:

- Are able to use an end-to-end DevSecOps platform, which has necessary security, communication, and automation features built in
- Are using the features available to them
- Have goals aligned with business needs
- Share responsibility for incorporating security into the entire lifecycle
- Foster a culture of collaboration
- Understand new, helpful technologies coming down the road

To help your team reach their full potential, you must ensure they aren't struggling under the weight of dealing with context switching and the pressure of integrating and updating a multitude of tools. **Using an AI-powered, end-to-end DevSecOps platform will streamline workflows, speed production, and increase security for the software, their customers, and the overall business.**

Have your team try out this **free trial** of the GitLab DevSecOps Platform. Also feel free to **reach out to a DevSecOps expert** who can answer any questions you may have.

[1] Gartner, Magic Quadrant for DevOps Platforms, Manjunath Bhat, Thomas Murphy, et al., 05 June 2023


GitLab
Software.
Faster.