GitLab

How to get started using AI in software development

Integrating AI to boost efficiency, security, and developer collaboration

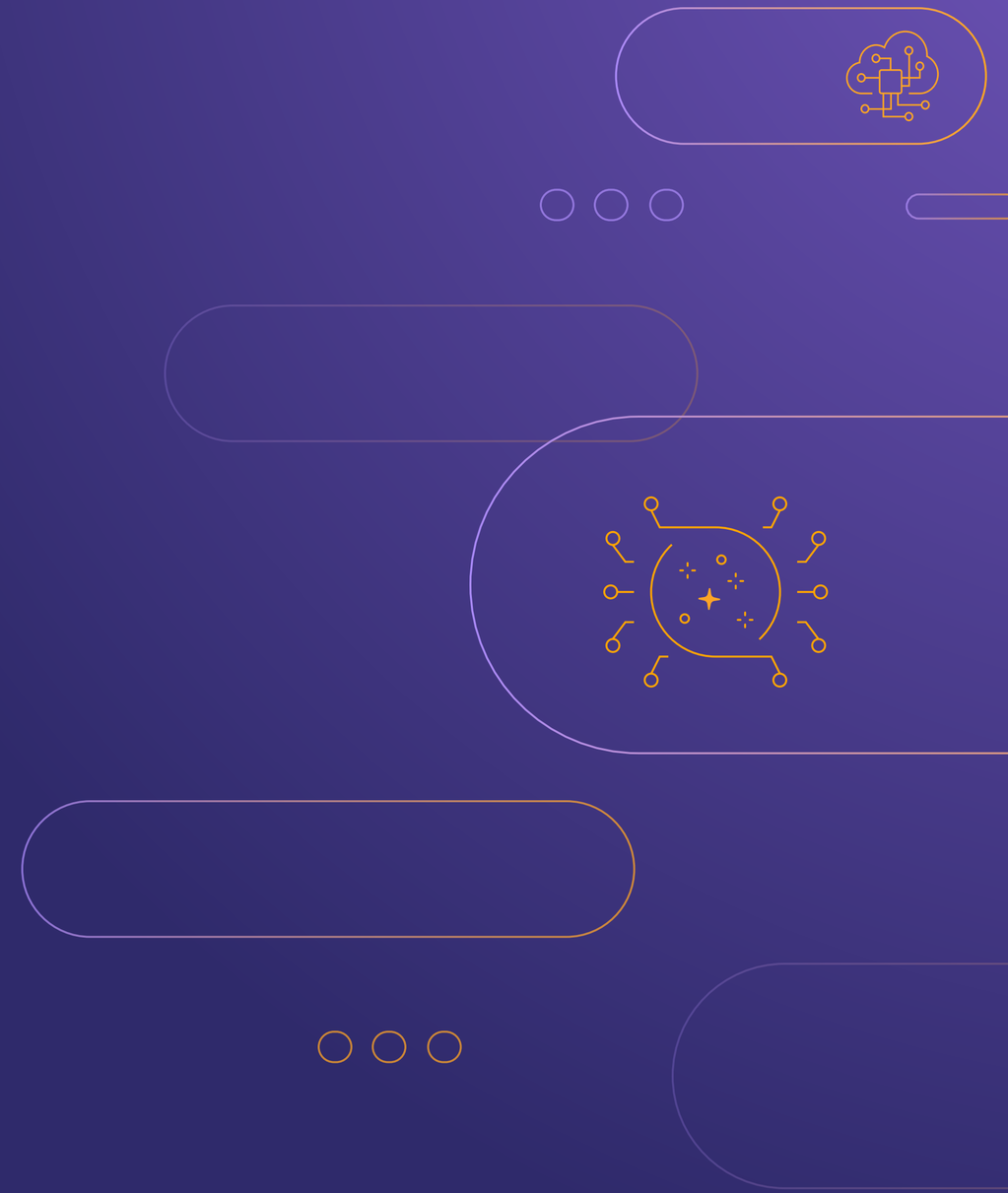


Table of Contents

AI is here. What you need to know:

Artificial intelligence (AI) is no longer just on the way — it's now fundamental to how organizations build applications. Companies are leveraging AI to radically change the way their teams build, secure, and deliver software. According to the GitLab 2024 Global DevSecOps Report, 78% of more than 5,000 respondents are either already using AI or plan to within the next two years — a significant increase from 64% last year.

AI's impact is evident: it drives faster, more secure development processes and offers a competitive edge. This transformation is not optional; 62% of C-level executives recognize AI integration in software development as essential to staying relevant, the report also notes.

If you haven't started using AI in your software development process, now is the time. If you have, it's time to accelerate.

78%

of teams currently using AI in software development or plan to in the next 2 years, up from 64% in 2023.

GitLab 2024 Global DevSecOps Report

IT leaders are perfectly positioned to help their teams not only adopt AI tools but maximize all the benefits that come with using them — adding efficiencies; giving developers more time to be innovative; and fostering, rather than replacing, human-to-human collaboration.

Managers and executives can work with their teams to figure out the pain points in their processes and how AI can help solve those problems. They also can strategize on what AI-powered solutions to start with and how to continue to add capabilities as they progress.

No matter where you are in your journey, there are clear steps you can take to put AI to work for you and your business. This ebook will guide you through how each role in the DevSecOps environment can take advantage of AI, and give you tangible takeaways for creating a strategic AI implementation plan that will ultimately help you create secure software faster.

Let's dive in!

"We, like everybody else, are looking at where AI can help us improve situations across the entire software development life cycle. So if someone is building code, how can it help them? If someone is working on other aspects of the process, how can it help them?"

Guus Houtzager
Engineering Manager at bol

"We want to use all the AI features available so we can make secure software faster. It's important to our business. We need to be fast and efficient to stay competitive in the market."

Mans Booijink
Operations Manager, Cube

Essential insights

This is about empowering, not replacing

Managers need to be clear that using AI isn't about replacing developers, software engineers, or any other members of the software development team. **It's about helping them do their jobs more efficiently, better and faster**. It's about empowerment. AI takes arduous and mundane tasks off people's plates so they have more time to do what they love – create innovative, cutting-edge software that can take on business-critical needs.

Key capabilities of AI in software development

AI capabilities are powered by machine learning algorithms, computer vision, pattern recognition, and natural language processing. These tools — ranging from chatbots to code generation, vulnerability explanation, and anomaly detection — are transforming teams' ability to **uncover valuable insights and automate critical processes**.

Using AI across the entire SDLC

AI's role extends beyond aiding developers to write code — it **enhances every phase of the software development life cycle** (SDLC). From planning and coding to testing and deployment, AI acts as the next generation of automation, supporting developers, security teams, and operations. This holistic approach ensures that every team member benefits from AI's capabilities.

Using AI in a DevSecOps platform

Artificial intelligence capabilities can be used on their own but **it's easier when they're part of a DevSecOps platform**, which weaves security throughout the entire development and operations process. With an AI-driven platform, there's no need to adopt a disparate collection of AI tools because they're all seamlessly integrated in one application. The combination creates a **powerful synergy** that enhances security, automation, and efficiency across the entire development life cycle. In fact, in the 2024 Global DevSecOps report, respondents whose organizations are currently using AI for software development were **much more likely to say they wanted to consolidate their toolchain** than those who aren't using AI.

Using AI to tackle your biggest pain points

Leaders can leverage artificial intelligence to not only automate routine tasks but also to enhance problem-solving, making processes faster and more efficient. If your goal is to streamline operations and boost productivity (and whose isn't?), AI is the solution. Let's take a look at five common problems facing teams and organizations today and see how using AI tools can help overcome them:

The Problem:

Developers are wasting time on manual tasks

Manual, repetitive tasks add up to time-consuming work on efforts ranging from code reviews, to testing, integration, security reviews, and deployment. All of that hands-on work can lead to slow downs, human error, and inconsistencies. And if developers, for example, are spending their time on these arduous tasks, they're not actually focusing on creating innovative software or building the next great feature for a project iteration. According to the 2024 Global DevSecOps Report, respondents say they only spend 21% of their time writing new code and 15% improving existing code — because they are so occupied with other non-code-producing tasks.

The Fix:

A variety of artificial intelligence features, ranging from **AI-powered assistants** to code suggestions, code explanations, code refactoring, test generation and root cause analysis, can save individual contributors time and work by proposing blocks of code, identifying problems, and moving projects forward — enabling team members to focus on bigger picture needs. AI has ushered in a new wave of innovations that are accelerating workflows.

The Outcome:

- Increasing efficiency
- Saved time and money
- Improving the developer experience

"We already are seeing a lot of improvements using code suggestions, test generation and chat for summaries. We're looking to work even more efficiently using AI across the entire SDLC with merge request summaries, vulnerability explanations, and issue summaries."

Mans Booijink
Operations Manager, Cube

The Problem:

It’s taking too long to understand vulnerabilities

When vulnerabilities are found in code, how do you know which ones to address first, or which ones put your applications most at risk? For developers, the answer isn’t necessarily clear. Individual contributors, especially junior members of the team, often spend additional time researching and coordinating with security experts to triage and resolve flagged security issues. This leads to extended periods of open merge requests, slow remediations, and delays in releasing features.

The Fix:

Vulnerability explanation is an AI capability that generates a dedicated summary of security flaws, describes their level of potential impact in detail, and proposes possible mitigation paths. The faster team members can understand the problem, the faster and more efficiently they can fix it.

The Outcome:

- Improved security and efficiency
- Improved developer experience

The Problem:

Vulnerabilities are getting through to production software

If problems in code are slipping past your developers and members of your security team, that can cause problems in your software products. However, it also can cause costly breaches, and harm your reputation and your relationship with partners and customers.

The Fix:

Test generation features can add tests to the source code base to help identify problems. And vulnerability resolution tools evaluate and remediate bugs, keeping them from making it into production software. AI capabilities, which make addressing vulnerabilities more streamlined and proactive, are revolutionizing security in software development and deployment. Embracing AI allows organizations to build secure and resilient software systems, while enabling faster and more efficient development practices.

The Outcome:

- Improved security
- Better customer and partner relations
- Secure brand image

78%

of teams currently using AI, or will in the next two years, in their SDLC.

GitLab 2024 Global DevSecOps Report

The Problem:

Broken CI/CD pipelines causing slowdowns

Broken continuous integration and continuous deployment (CI/CD) pipelines happen when a series of steps fail while developing new features in merge reviews (MRs), delivering new software releases, or doing software maintenance. The breaks can not only halt the workflow, but they also can delay software deployment as teams try to figure out the root cause of the failure.

When this happens, developers have to manually troubleshoot, dig through log files, and often do a lot of trial-and-error development. This can be exceedingly challenging and time-consuming since a typical pipeline fix can consist of several iterations and context switching.

The Fix:

An AI-driven root cause analysis action removes the guesswork by determining the initial cause for a failed CI/CD pipeline and suggesting a fix by analyzing the logs. This can dramatically reduce the time, energy, and mental strain involved in making these critical fixes.

The Outcome:

- Improved developer experience
- Increased velocity

The Problem:

Teams aren't collaborating enough or efficiently

If team members are spending a lot of time — maybe even most of their time — heads down, working on their own, that can be a problem. Operating in silos means they're not sharing knowledge of project backgrounds, work-arounds, and best practices. Without strong collaboration, people might not have an understanding of how their work affects other projects. And it makes for a lack of diverse input, which would have created well-rounded products.

The Fix:

AI summarization and content population tools help with functions such as MRs, MR reviews, discussions, and Issue comments. They drive alignment and action by efficiently communicating the impact of changes, pointing out project needs, and enabling better handoffs between authors and reviewers. These tools create more opportunities for human-to-human collaboration.

The Outcome:

- Improved developer experience
- Accelerated time-to-market

Top investment priorities for DevSecOps teams:

1. Security
2. AI

GitLab 2024 Global DevSecOps Report

AI: Empowering every member of your team

Most of the focus on AI in software development and deployment has been almost exclusively on developer productivity when coding. There's no denying it has been a significant advancement for creating software. Less widely understood is what AI-assisted tools can do for the entire software development team, from developers to security, operations, and project managers. It's important to look at the big picture to add layers of efficiency, speed, and security.

As you dive into, or further into, using AI, consider that these tools go well beyond just AI-enabled pair programming. AI can be integrated across the entire software environment to boost every part of development and deployment.

Everyone, regardless of what role they have on the team, can benefit from the power of AI.

This creates a better work experience for team members, while enabling organizations to ship secure software faster.

"When adopting AI into everyone's workflow, it is crucial to identify pain points, and provide users with the confidence that AI will help them get more efficient," says Michael Friedrich, senior developer advocate at GitLab. "For example, a product manager can benefit from long issue discussion summaries. A site reliability engineer (SRE) appreciates a chat prompt to explain source code, and to ask how to troubleshoot specific performance issues with a deployed application. A broken pipeline can slow down everyone's process — and AI can help with that, too."

For Developers:

40%

use code explanation tools

38%

use code change summary tools

47%

use code suggestions/ generation/completion tools

GitLab 2024 Global DevSecOps Report

Take a look at how artificial intelligence capabilities can aid everyone on the team:

For Developers:

- **Code generation and completion** – Provides suggestions, improvements, and potential changes that can substantially improve the programming experience by reducing errors and helping developers write secure and quality code faster and more efficiently.
- **Code explanations** – Analyzes source code and provides detailed descriptions, using natural language, of the code and how it functions.
- **Git suggestions** – Helps developers discover or recall Git commands when and where they need them
- **Suggested reviewers** – Promotes faster and higher-quality analysis by going through MR changes and a project's contribution graph to suggest a list of reviewers with contextual knowledge.
- **Summarize MR changes** – Enables reviewers and authors to spend more time discussing changes and less time scanning byproviding relevant summaries of MRs and their proposed changes. This efficiently and automatically communicates changes' impact.
- **Summarize MR reviews and code review summaries** – Helps developers get their point across, enables better handoffs between authors and reviewers, and helps reviewers efficiently understand merge request suggestions by encapsulating information.

For Security and Operations:

- **Vulnerability explanation and resolution** – Helps developers, particularly junior developers, understand security vulnerabilities, get guidance on how to resolve them, and generate MRs to make the required changes. This helps the team create, evaluate, and fix more secure code, all while increasing their knowledge and skills.
- **Test generation** – Generates code that can be copied into test source code files, relieving people of repetitive and time consuming tasks, while also helping catch bugs early. This enables team members to create tests for merge request changes, helping to reduce the laborious, but important, task of writing tests and increasing test coverage.

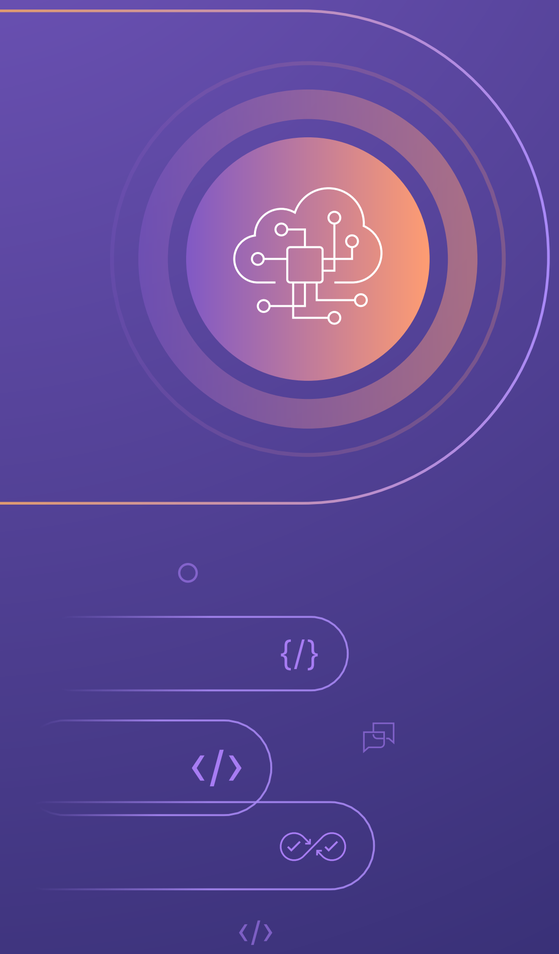
32%

use test generation tools

29%

use vulnerability explanation tools

GitLab 2024 Global DevSecOps Report



For all team members:

- **Issue description generation** – Creates a rundown of important information and tasks in an Issue, sussing what needs to be done and questions waiting to be answered.
- **Issue comment summaries** or discussion summaries – Gets teammates up to speed on lengthy conversations to ensure everyone is on the same page, boosting collaboration without spending time scrolling through lengthy discussions.
- **Code explanation** – Helps contributors understand what the code is doing by explaining it in natural language, saving time and confusion.
- **AI-powered chat assistants** – Offers time-saving assistance for a variety of tasks, such as **answering questions** that range from how to reset passwords to explaining a section of code, and setting up specific security tests. Guidance for technical and non-technical users.
- **Productivity analytics and forecasting** – Assists with predicting productivity metrics, projecting the future behavior of value stream metrics, and identifying anomalies across the software development life cycle by analyzing historical data trends.
- **MR descriptions** – Creates comprehensive descriptions for MRs, and captures the essence of an MR's commit string. Also surfaces missing or incomplete tasks.
- **Vulnerability resolution** – Offers critical information about a vulnerability and where it is in the code. It also can open an automated MR to fix it. Especially helpful to people who aren't on the security team.
- **Root cause analysis** – Determines the reason for pipeline failures and failed CI/CD builds, which can be difficult and time-consuming to troubleshoot. Recommended solutions can be copy and pasted directly back into CI/CD configuration or scripts.

35%

use AI assistants – more than any other AI-powered feature

GitLab 2024 Global DevSecOps Report

Five steps to help your teams become AI pros

Building a strategic approach to using artificial intelligence in software development and deployment should be done intentionally. You need a framework for implementing AI that takes into consideration your team's needs and biggest obstacles, puts data privacy first, gets everyone the training they need, while enforcing best practices and creating space for your AI champions (or even detractors) to have their voices heard.

Let's get started.

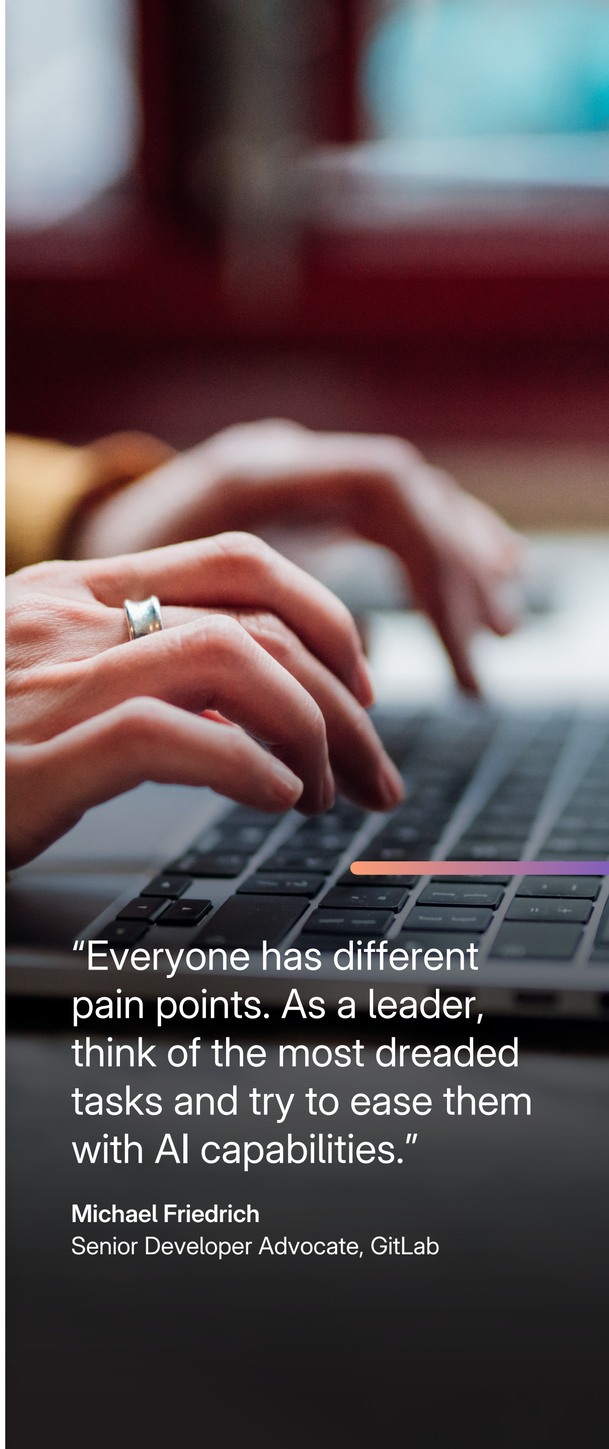
1. Understand needs, and plan around around them

Leaders should stay current with what AI features are available, and work with their teams to figure out what workflows to simplify first. Ask users where they spend the most time. What is their most inefficient, time-consuming, or tedious task? Team members will have great ideas about what they need and where to start. Once managers have identified the top pain points, they can look at the entire SDLC from a high level and then choose which AI-powered tools to use first to ensure everyone benefits from the adoption journey.

Initially integrate AI capabilities in specific areas where they can provide the most benefit, and then gradually expand adoption as teams learn more about their effectiveness and limitations. Moving gradually through a laid out roadmap also helps to keep team members from being overwhelmed.

Note that conversations shouldn't stop just because AI adoption has begun.

Managers could think about checking in — even using surveys — to keep tabs on what is going well, what challenges are popping up, and what tools teams want to start using next. If contributors didn't fully adopt a code explanation tool, for example, find out why and then go back and help them make it work.



"Everyone has different pain points. As a leader, think of the most dreaded tasks and try to ease them with AI capabilities."

Michael Friedrich
Senior Developer Advocate, GitLab

2. Make sure sensitive company data is protected

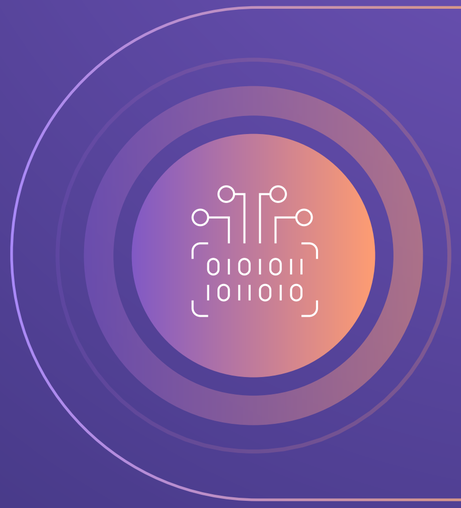
Since AI is moving so quickly, naturally, it raises a lot of concerns — mainly about privacy and data security. While AI brings many potential security benefits, it also can create security risks if not deployed strategically.

According to the GitLab 2024 Global DevSecOps Report, 34% of respondents note that concerns around privacy and security are the top obstacle around using AI.

To deal with this, managers need to understand what data AI tools use and how they use that information. They also need to know who owns the intellectual property and any other rights to the data.

Things to consider to limit risk:

- Make sure AI companies don't use customer data to train their models, which could cause security and privacy risks. Also monitor AI uses and look for vendors that have a privacy-first mindset.
- Ensure there is publicly available documentation on data usage, and read and understand how customer data is utilized.
- Consider the data any AI tool is interacting with and set up guardrails around your information to mitigate risk and meet compliance regulations.
- Also set up guardrails that control which users, projects, and groups can use AI-driven capabilities.
- Connect your organization's legal, compliance, and software development teams to think through risks and **ask tough questions** of any AI providers.
- Streamline the number of separate AI tools that teams are using throughout the SDLC and across the organization. The more tools used, the more complexity grows, potentially causing operational issues, oversight challenges, and security risks. Consider tools that are seamlessly integrated with your existing DevSecOps solutions.
- If using a DevSecOps platform, verify that it has transparency and a privacy-first approach to building AI features to help protect customers' intellectual property.



55%

say introducing AI into the software development life cycle is risky

GitLab 2024 Global DevSecOps Report

3. Ease fears and empower AI champions

It's important for leaders to communicate to their teams that AI is meant to enhance their work and give them more time to spend on innovation, not replace them. Take the time to talk — and listen: Discuss obstacles hindering different teams and explore together how AI tools can ease them, keeping the focus on saving time and mental energy, and providing more opportunities to do the work they actually enjoy. Walk through your team's feedback, including their concerns and requests.

"There is a component of psychological safety and team culture that impacts how people feel about AI," says Rachel Stephens, senior analyst at industry analyst firm RedMonk.

"Individuals may be concerned about the security or privacy implications of AI, but their sense of unpreparedness may also stem from a feeling that AI has personal risk to their livelihoods."

Feeling involved in the adoption process can ease the transition into new AI tools. Identify and enable key members on different teams who are excited about using AI. They will naturally act as champions and liaisons, encouraging others who might be more hesitant to begin using new capabilities and lending them a hand getting started.

4. Get teams the training they need

Getting people the tools they need is just one step in the process. They also need the knowledge to use those tools well. Simply telling someone to use a new feature without any training could lead to frustration and pushback, instead of happy, productive users. And keep in mind that just because using AI is gaining a lot of steam, skill gaps still exist. Now is the time to ensure that teams get the education and support that they need so they can move faster later.

Training is key.

Leaders should keep in mind that they sometimes assume teams need less training than team members want or need. For instance, only 15% of executive-level respondents in the GitLab 2024 Global DevSecOps Report, say their organizations do not provide adequate training and resources for using AI.

However, 25% of individual contributors say they're not receiving enough training and resources.

It's managers' job to ensure people are receiving the right instruction for the tools they're expected to use, so they can employ them efficiently and with confidence. If managers are trying to convince a contributor to use AI, providing tutorials, best practices, and guidance are important steps to take to make AI adoption easier and less stressful.

5. Set up and enforce best practices

Managers and executives need to make sure that every team — and all the members of those teams — understand the best, and safest, ways to use AI capabilities. AI guidance and best practices should be documented, widely shared, easy to understand, and enforceable.

25%

of individual contributors say their organizations do not provide adequate training and resources for using AI

Lack of appropriate skills and a lack of knowledge about AI are cited as two of the top three obstacles to using AI

GitLab 2024 Global DevSecOps Report

Guidance should encompass:

- What people, projects, and teams are allowed to use AI tools.
- What data can be used in AI features.
- Periodic performance evaluations and dashboards to measure improvements, ensuring the tools are providing intended benefits.
- Roadmaps for getting started, and milestones they should try to hit with each tool.
- Clear lines of responsibility and oversight for AI-driven processes to maintain trust and confidence in the system.
- Data governance policies and secure data storage solutions to ensure the information being used is high quality and safe.
- Human oversight to ensure tools are making intelligent decisions and processes are working optimally.
- Documentation for use cases, user experiences, lessons learned, benefits, and challenges.

Secure, innovate, and accelerate with AI

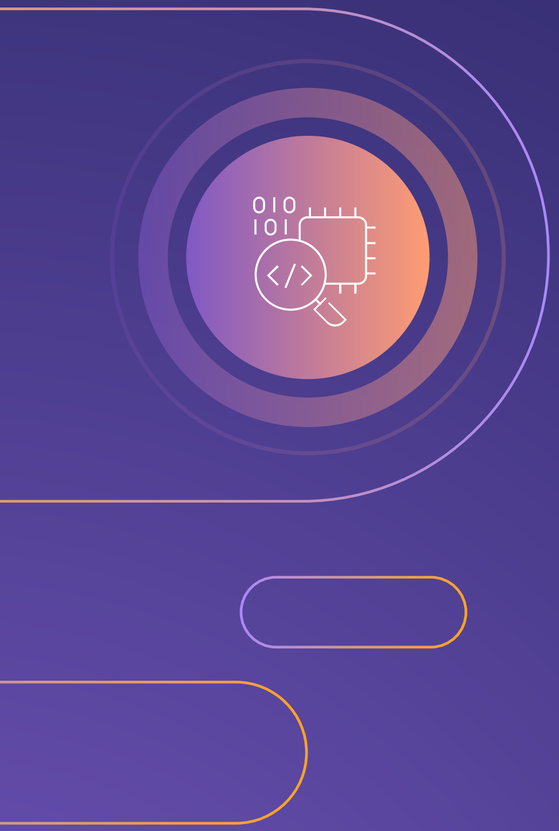
AI is transforming software development. Companies with a clear AI vision and strategy have a critical advantage in creating and deploying secure products and increasing software quality. With AI helping you stay secure and reducing mundane repetitive tasks, your software team is able to adjust to changing customer needs faster so you can stay ahead of your competitors.

Whether you have already adopted some AI into your software development lifecycle or not, this is the time to consider the role AI should play within your entire organization.

Leaders are perfectly positioned to help their teams begin to use AI or to expand their current work with it, enabling them to harness this powerful technology.

Seven AI takeaways

- **Help the entire team:** There are AI capabilities that can help everyone on your team — from developers to members of the security, operations, and platform engineering teams.
- **Support the whole SDLC:** The entire software development lifecycle can benefit from using AI.
- **Reduce manual tasks:** The true value of AI allows you to take on time-consuming and costly challenges, like being mired in manual tasks, losing sight of the power of collaboration, and being slowed down trying to understand vulnerabilities or broken pipelines.
- **Increase innovation:** Using AI isn't about replacing anyone on your team. It's about enabling them to work faster, more efficiently, and giving them more time to be innovative.
- **Tackle vulnerabilities:** AI can help teams find, understand, and fix vulnerabilities more easily and sooner in the development process. It's about security without sacrificing speed.
- **Increase speed:** Optimize workflows to improve velocity and business results.
- **Improve team member experience:** Ease team members' jobs and give them more time to be innovative.



What's next for your AI journey

And while AI can help teams deliver effective, high-performing software faster, its impact extends far deeper, affecting every phase of your business. According to the 2024 Global DevSecOps Report, AI not only drives operational efficiency but also significantly enhances customer and employee experiences, ultimately fueling the company's bottom line.

Tangible benefits of AI for your business:

Protect customer relationships

By identifying problems in soft-ware code sooner and under-standing those issues more easily, it reduces the potential risk of brand-damaging and costly data breaches that grab headlines and hurt customer and partner connections.

Benefit from innovative software

Spending less time on manual, repetitive tasks, leaves teams with more time to build creative products.

Outperform competitors

Increase productivity, leading to faster time-to-market, getting updates and new products to customers faster and more reliably, which gives your business a competitive edge.

AI capabilities are transformative

Take the next step to fully harness their potential for your organization.

Unlock AI across the SDLC with a free trial of GitLab Duo.

Learn more

About GitLab

GitLab is the most comprehensive AI-powered DevSecOps Platform for software innovation. GitLab provides one interface, one data store, one permissions model, one value stream, one set of reports, one spot to secure your code, one location to deploy to any cloud, and one place for everyone to contribute. The platform is the only true cloud-agnostic end-to-end DevSecOps platform that brings together all DevSecOps capabilities in one place.

With GitLab, organizations can create, deliver, and manage code quickly and continuously to translate business vision into reality. GitLab empowers customers and users to innovate faster, scale more easily, and serve and retain customers more effectively. Built on open source, GitLab works alongside its growing community, which is composed of thousands of developers and millions of users, to continuously deliver new innovations.