GitLab

The Intelligent Software Development Era

How AI will redefine DevSecOps in 2026 and beyond

Global DevSecOps Report

The Harris Poll

Table of Contents

Methodology, Introduction, & Key Takeaways

Methodology

This study was conducted by The Harris Poll on behalf of GitLab from July 31, 2025, to August 15, 2025, among 3,266 DevSecOps professionals. All respondents worked in IT operations, IT security, or software development.

The Harris Poll conducted panel sampling, which reduces bias in the sample. They used proprietary access to lists, panels, and databases to gather quality responses and cleaned the data throughout fielding to ensure data quality.

In this survey, the following definitions were provided:

Artificial intelligence (AI)

The simulation of human intelligence processes by machines, especially computer systems. In software development, AI is embedded into development tools and workflows to assist with coding, testing, and maintenance tasks.

Agentic AI

Refers to AI systems or "agents" that can autonomously plan, execute, and adapt their actions to achieve specific goals with minimal human intervention. Unlike traditional AI tools that respond to prompts, agentic AI can independently manage multi-step workflows.

The software development lifecycle (SDLC)

The process of planning, creating, testing, securing, deploying, monitoring, and maintaining software.

*

Indicates results from the The Economics of Software Innovation research report, based on a study conducted by The Harris Poll on behalf of GitLab from April 25, 2025, to May 19, 2025, among 2,786 C-Suite executives.

Who took the survey?

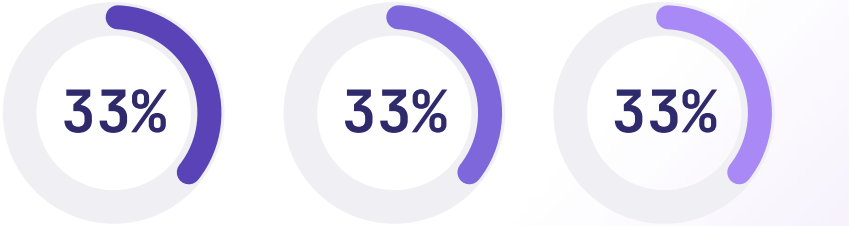
Region	Country	% Total
NAM	US	31%
EUR	UK	8%
EUR	Germany	8%
EUR	France	8%
EUR	Spain	8%
EUR	Italy	8%
AP	Australia	8%
AP	India	8%
AP	Japan	8%
AP	Singapore	8%

Note: Totals may not equal 100% due to round of individual values

Industry	% Total
Financial Services	16%
Automotive	16%
Manufacturing	15%
Telecommunications	15%
Government / Public Sector	14%
Embedded Systems	13%
All others	11%

Who took the survey?

Department



Job role	% Total
Director	42%
Manager	26%
Vice president	21%
Individual contributor	11%

# of employees	% Total
<1,000	37%
1,000-4,999	38%
5,000-9,999	15%
10,000+	10%

Note: Totals may not equal 100% due to round of individual values

The Intelligent Software Development Era

How AI will redefine DevSecOps in 2026 and beyond

Introduction

AI is reshaping the fabric of DevSecOps. Teams are expected to use AI to accelerate development, yet still safeguard the quality and trustworthiness of their software. This balancing act — between speed, security, and new skill sets — is defining a pivotal moment for the next era of DevSecOps.

Key takeaways

Readiness to adopt AI is near universal, but DevSecOps professionals have rising concerns:

97%
of DevSecOps professionals are already using AI for software development or plan to use it in the future

94%
have data privacy concerns about using AI tools

As AI democratizes coding, collaboration is more critical than ever:

76%
of DevSecOps professionals agree that as coding gets easier with AI, there will be more engineers, not fewer

94%
have experienced factors limiting collaboration in the software development lifecycle

DevSecOps teams are looking for deeper AI-human partnerships:

82%
of DevSecOps professionals feel that using agentic AI would make them more satisfied at their job overall

43%
favor a 50/50 split between human and AI contributions in software development

Toolchains continue to expand in the AI era:

60%
of DevSecOps teams use more than 5 tools for software development

49%
use more than 5 AI tools for software development

39%
of DevSecOps professionals use AI tools at work that aren't officially approved by their organization

01

The State of DevSecOps Today

Teams are leveraging AI to accelerate coding, but security, compliance, and administrative tasks continue to create bottlenecks

AI is now an essential part of the SDLC

97%

of DevSecOps professionals say their organizations are using AI now or planning to use it in the future.

Is your organization using or planning to use AI in the SDLC?

Yes (Now / In the future) (Net)	**97%**
Yes, we are currently using AI in the software development lifecycle	63%
Yes (In the future) (Net)	**34%**
Yes, in the next year	17%
Yes, in the next 1-2 years	11%
Yes, in more than 2 years	3%
Yes, but there is no specific timeline	3%
No (No plans / used in past not anymore) (Net)	**3%**
No, my organization has no plans to introduce AI into the SDLC	2%
No, my organization has explicitly prohibited the use of AI in the SDLC	0%
My organization used AI in the SDLC in the past, but not anymore	0%

Q2. Is your organization using or planning to use AI in the software development lifecycle (SDLC)? (Total n=3,266)
Note: Totals may not equal 100% due to round of individual values

DevSecOps professionals only spend fifteen percent of their time writing new code

85% agree

"Agentic AI would allow me to focus on doing the job I was hired to do by handling all the side tasks that pile up (e.g., administrative work, meeting prep, etc.)."

How DevSecOps professionals spend their time

Mean %

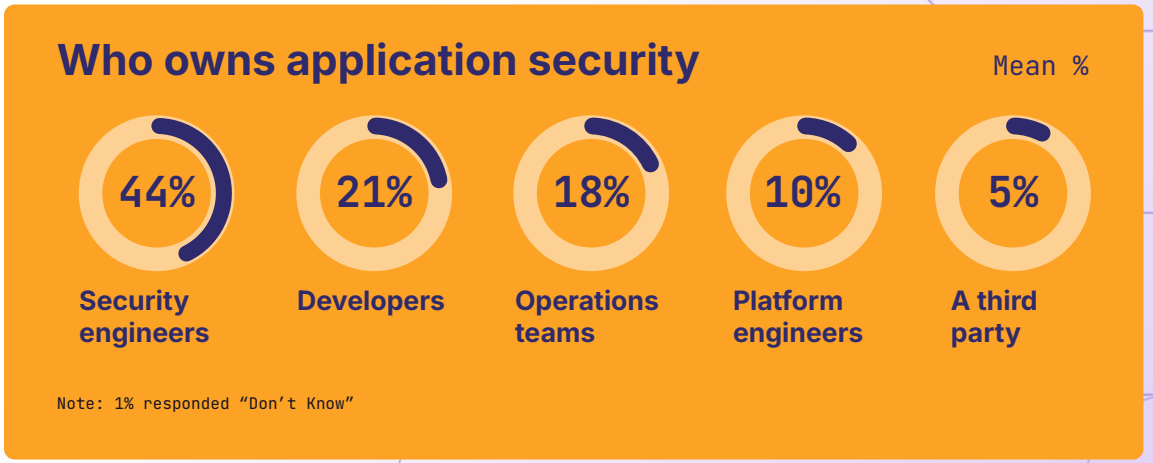
18% Meetings and administrative tasks	12% Testing
15% Writing new code	12% Understanding what code does
14% Identifying and mitigating security vulnerabilities	11% Code maintenance
13% Improving existing code	5% Other

Q1. Approximately what percentage of your time do you spend on each of the following tasks? (Total n=3,266)
Q13. Please indicate how much you agree or disagree with the following statements. (Top 2 Box, Somewhat / Strongly Agree) (Total n=3,266)

Security engineers and developers are largely responsible for application security

85% agree

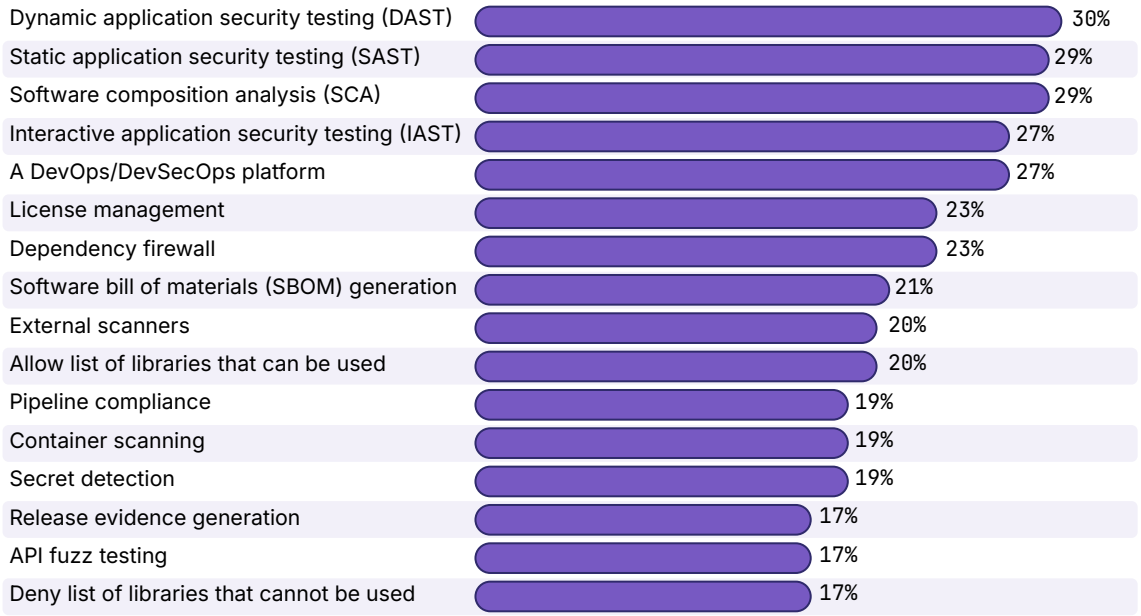
"I feel confident in my organization's approach to application security."



Q26. Who is primarily responsible for application security at your organization? (Total n=3,266)
Q32. Please indicate how much you agree or disagree with the following statements. (Top 2 Box, Somewhat / Strongly Agree) (Total n=3,266)
Note: Totals may not equal 100% due to round of individual values

Organizations are adopting a wide range of tools and practices to embed security in the SDLC

How security is enabled in the SDLC



Note: 3% responded “N/A—my organization does not enable security in the software development lifecycle / I don't know how they enable it”

Q27. How does your organization enable security in the software development lifecycle (SDLC)? (Total n=3,266)

Organizations manage compliance with frameworks like ISO 27001 and GDPR

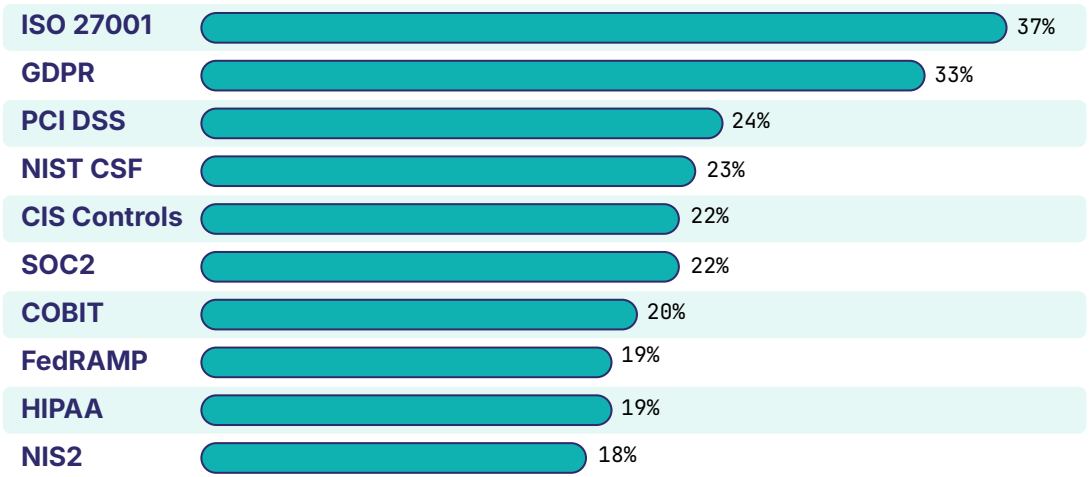
80% agree

"Compliance responsibilities at my organization are largely concentrated within one team."

76% agree

"Currently, more compliance issues are discovered after deployment than during the development process."

Compliance frameworks currently in use

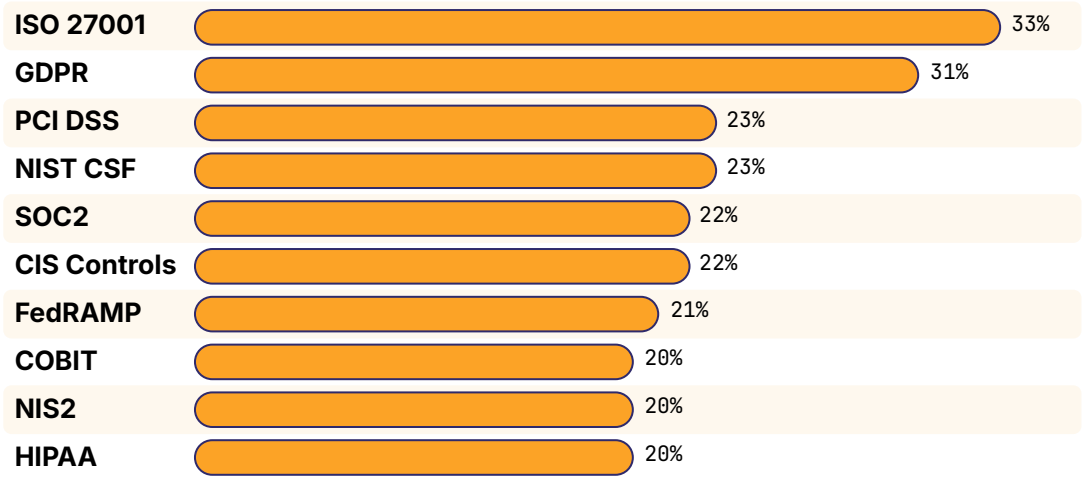


Note: 5% answered "N/A—we do not have to comply with any frameworks"

Q29. With which of the following compliance frameworks does your organization currently need to comply? Please select all that apply. (Total n=3,266)
Q32. Please indicate how much you agree or disagree with the following statements. (Top 2 Box, Somewhat / Strongly Agree) (Total n=3,266)

But DevSecOps professionals also see those frameworks as particularly challenging

Most challenging compliance frameworks in next 18 months



Note: 7% answered “N/A—there aren't any compliance frameworks that are challenging to manage”

Q28. Which compliance frameworks do you anticipate being the most challenging for you to manage over the next 18 months? Please select up to three responses. (Total n=3,266)

Security and compliance continue to demand substantial time and resources

72% agree

"My efforts to quickly fix vulnerabilities are often slowed by red tape at my organization."

Estimated effort for compliance management

Mean/Mean %

- DevSecOps professionals spend **13 hours** per month on compliance-related activities
- They spend **11 hours** per month resolving security issues post-release
- Compliance requirements cause delays in **14%** of DevSecOps professionals' **releases**
- Their teams are directly involved with / responsible for **9 compliance audits** per year

Q29a. Please provide your best estimates of the following (Total n=3,266)
Q32. Please indicate how much you agree or disagree with the following statements. (Top 2 Box, Somewhat / Strongly Agree) (Total n=3,266)

02

The AI-Empowered Software Practitioner

AI is reshaping DevSecOps roles — creating the need for more engineers and more pressure to upskill

DevSecOps teams now trust AI to handle over a third of daily tasks independently

37% Mean %

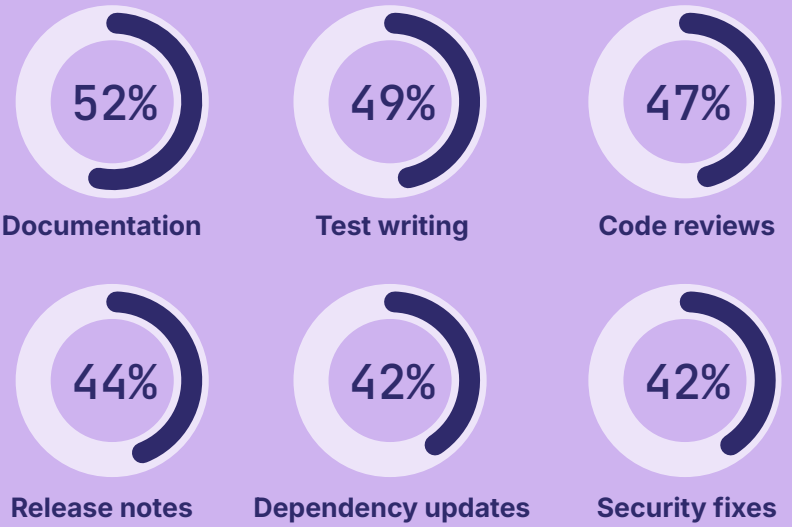
The percentage of daily tasks DevSecOps professionals would trust AI to handle at work **without any human review.**

83% agree

"I would be comfortable with AI agents automatically fixing security vulnerabilities with **human approval workflows**."

Tasks DevSecOps professionals would trust AI to handle solo

Note: 3% responded "N/A—I wouldn't be comfortable letting AI agents work autonomously on any of these tasks"



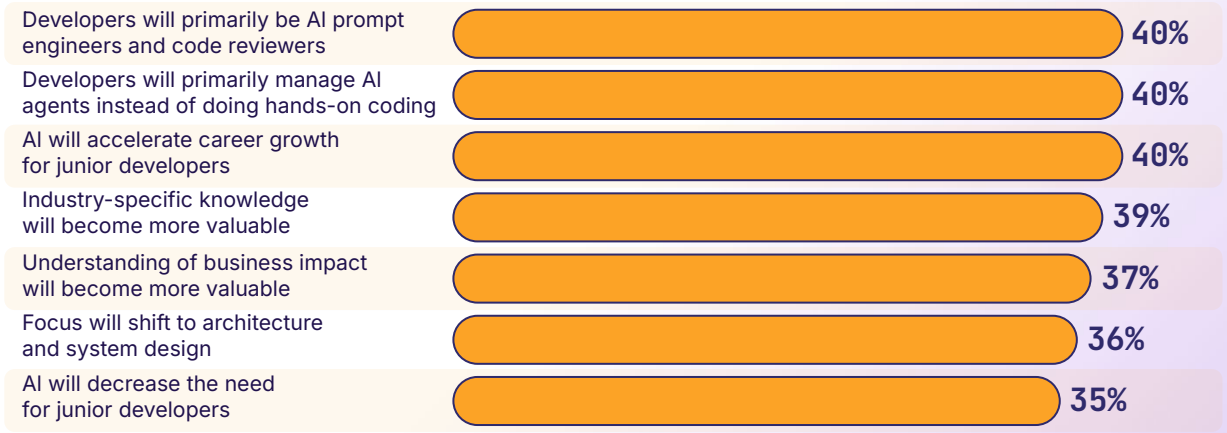
Q8. Regardless of whether you use AI in software development, what percentage of your daily tasks at work would you trust an AI agent to handle without human review? Your best estimate is fine. (Total n=3,266)
Q11. For which of the following tasks would you be comfortable letting AI agents handle without human review? Please select all that apply. (Total n=3,266)
Q13. Please indicate how much you agree or disagree with the following statements. (Top 2 Box, Somewhat / Strongly Agree) (Total n=3,266)

DevSecOps professionals expect AI to change their day-to-day and overall role

83% agree
"AI will significantly change my role within the next five years."

76% agree
"As coding gets easier with AI, I think there will be more engineers."

How DevSecOps professionals expect their role to evolve throughout 2026



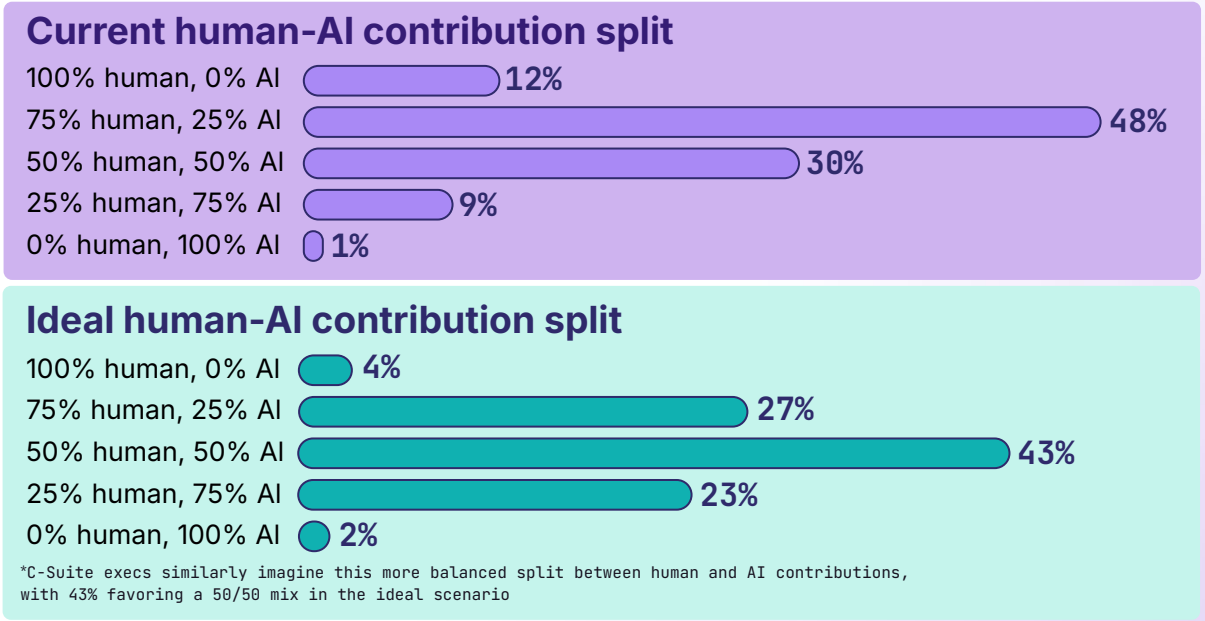
Note: 3% responded "N/A-developers will continue working much the same way they do today"

Q13. Please indicate how much you agree or disagree with the following statements. (Top 2 Box, Somewhat / Strongly Agree) (Total n=3,266)
Q18. How do you expect the developer role to evolve throughout 2026? Please select all that apply. (Total n=3,266)
Q19. Please indicate how much you agree or disagree with the following statements. (Top 2 Box, Somewhat / Strongly Agree) (Total n=3,266)

Teams see a future where AI is an equal partner in software development

82% agree

"Using agentic AI would make me more satisfied at my job overall."



Q10. How would you rate the balance between human input and AI automation in your current software development projects vs. your ideal balance? (Total n=3,266)
Q13. Please indicate how much you agree or disagree with the following statements. (Top 2 Box, Somewhat / Strongly Agree) (Total n=3,266)
*Q21. How would you rate the balance between human input and AI automation in your current software development projects vs. your ideal balance?
(GitLab Economics of Software Innovation C-Suite Survey, Those in the C-suite, n=2,786)
Note: Totals may not equal 100% due to round of individual values

Adopting AI across the SDLC will unlock long-term benefits

86% agree

"Systematic AI adoption will generate more long-term returns than using AI for tactical quick fixes."

*91% of C-Suite execs agree

Where AI tools have created the most efficiency

- 43% Automating repetitive tasks
- 41% Testing / quality assurance
- 37% Generating code
- 37% Detecting errors / bugs
- 32% Updating documentation
- 32% Updating documentation
- 32% Vulnerability detection / remediation
- 25% Prototyping product concepts
- 24% Refactoring code

Note: 1% responded "N/A-working alongside Al tools has not created efficiencies for me"

Q6. Where have AI tools created the most efficiencies for you? (Currently using AI tools, n=2,988)
Q13. Please indicate how much you agree or disagree with the following statements. (Top 2 Box, Somewhat / Strongly Agree) (Total n=3,266)
*Q19. Please indicate how much you agree or disagree with the following statements. (Top 2 Box, Somewhat / Strongly Agree) (GitLab Economics of Software Innovation C-Suite Survey, Those in the C-suite, n=2,786)

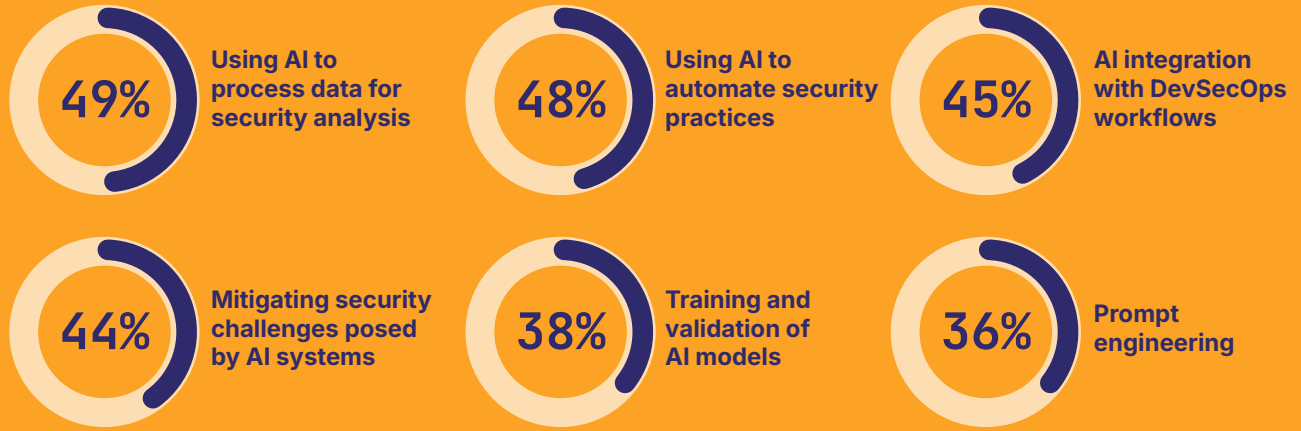
AI and security skills will be essential for career advancement in 2026 and beyond

87% agree

"Software engineers who adopt AI are future-proofing their careers."

AI skills needed for the next 18 months

Note: 2% responded "N/A—I don't believe DevSecOps professionals need to develop AI skills"



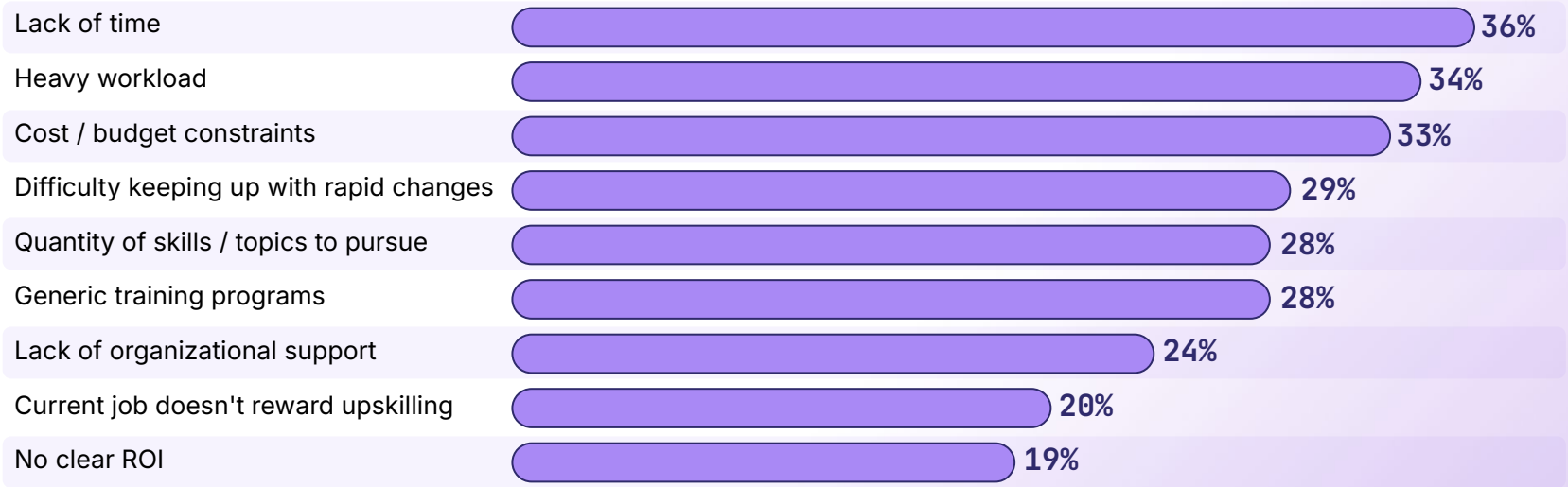
Q6. Where have AI tools created the most efficiencies for you? (Currently using AI tools, n=2,988)
Q13. Please indicate how much you agree or disagree with the following statements. (Top 2 Box, Somewhat / Strongly Agree) (Total n=3,266)
*Q19. Please indicate how much you agree or disagree with the following statements. (Top 2 Box, Somewhat / Strongly Agree) (GitLab Economics of Software Innovation C-Suite Survey, Those in the C-suite, n=2,786)

However, professionals need more time and support to build new skills

Q19. Please indicate how much you agree or disagree with the following statements. (Top 2 Box, Somewhat / Strongly Agree) (Total n=3,266)

In addition, heavy workloads and time pressures are creating barriers to upskilling

What are the biggest barriers you encounter in pursuing upskilling opportunities at work?



Note: 4% responded “N/A—I don't encounter barriers in pursuing upskilling opportunities”

Q17. What are the biggest barriers you encounter in pursuing upskilling opportunities at work? Please select up to three responses. (Total n=3,266)

Despite the significant changes coming to their roles, professionals agree that AI can't fully replace humans

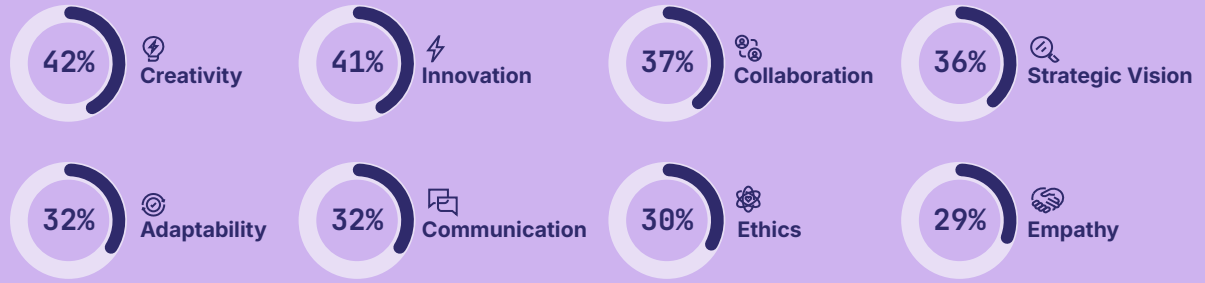
88%

of DevSecOps professionals agree

"There are essential human qualities that agentic AI will never fully replace."

*89% C-Suite execs agree

Most valuable human contributions to software development



*C-Suite execs are valuing similar human contributions to software development, seeing creativity (39%), strategic vision (39%), collaboration (37%), and innovation (37%) as the most valuable.

Q13. Please indicate how much you agree or disagree with the following statements. (Top 2 Box, Somewhat / Strongly Agree) (Total n=3,266)
Q19. Please indicate how much you agree or disagree with the following statements. (Top 2 Box, Somewhat / Strongly Agree) (Total n=3,266)
*Q31. Please indicate how much you agree or disagree with the following statements. (Top 2 Box, Somewhat / Strongly Agree) (GitLab Economics of Software Innovation C-Suite Survey, Those in the C-suite, n=2,786)
Q9. What aspects of the human element do you find most valuable in software development? (Total n=3,266)
*Q27. What aspects of the human element do you find most valuable in software development? (GitLab Economics of Software Innovation C-Suite Survey, Those in the C-suite, n=2,786)

03

New Challenges in AI-Driven Development

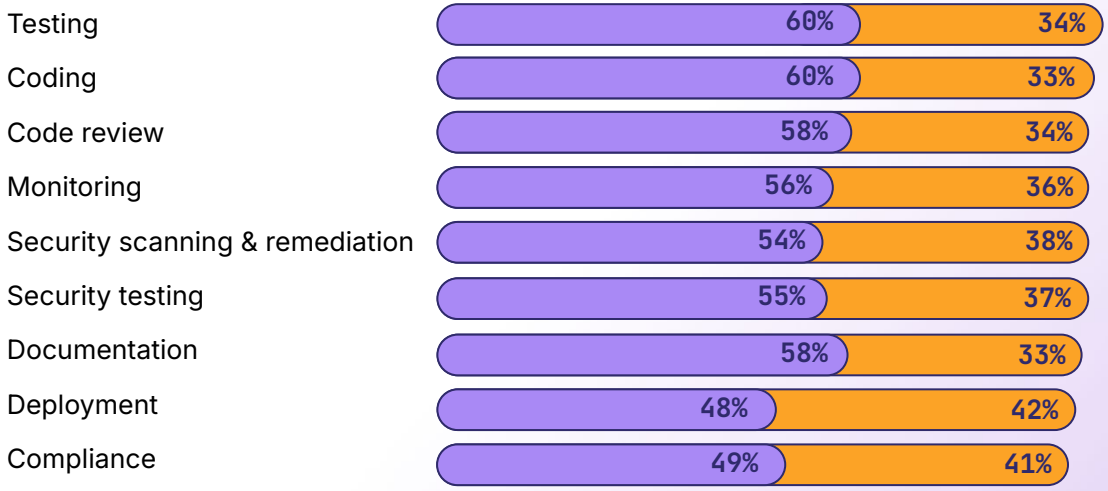
As roles transform and AI capabilities expand, teams face new challenges around security, compliance, and maintaining quality standards

AI is transforming every aspect of software development

81% agree

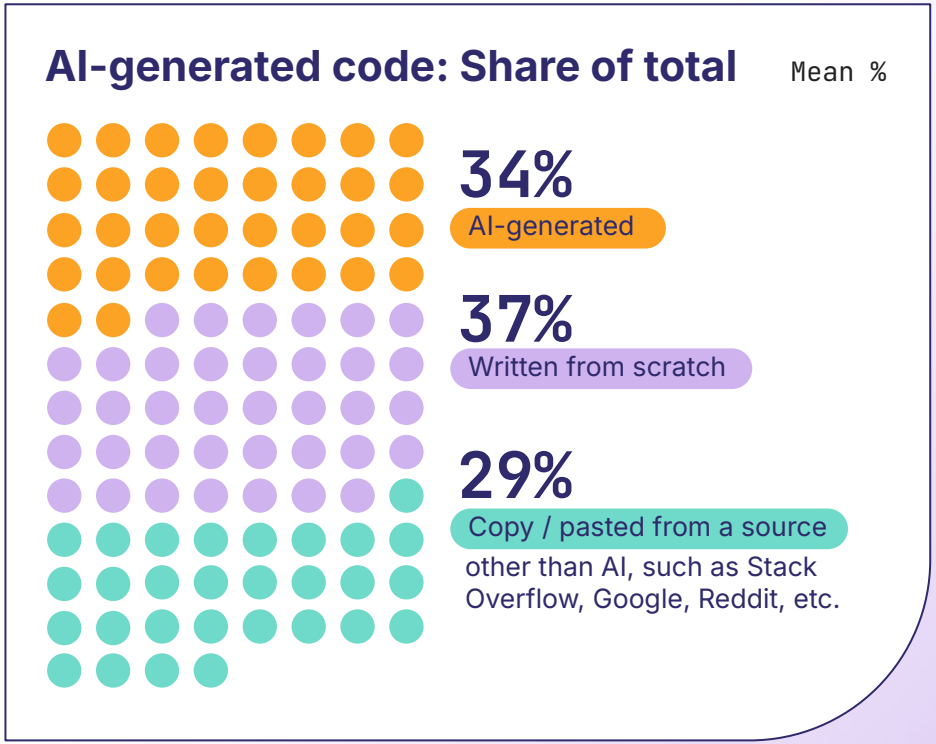
"The integration of AI into the software development life cycle is moving faster than expected at my organization."

AI use cases across the SDLC



Q3. For which aspects of software development does your team currently use or plan to use AI tools? (Those whose organization is using or planning to use AI in SDLC, n=3,173)
Q13. Please indicate how much you agree or disagree with the following statements. (Top 2 Box, Somewhat / Strongly Agree) (Total n=3,266)

AI-generated code is here to stay, approaching the same share as code written from scratch



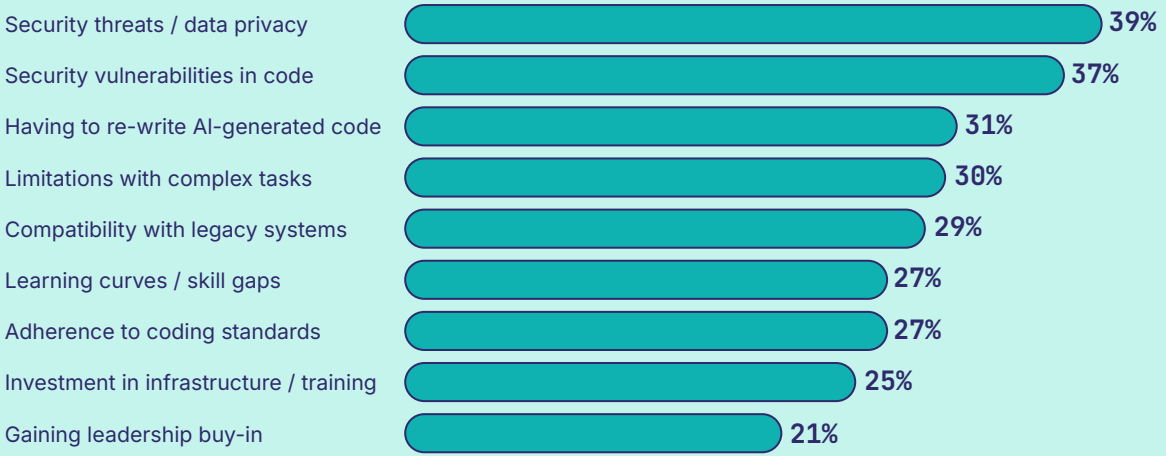
Q4. What percentage of the code you work on is now AI-generated versus other sources? Your best estimate is fine. (Currently using AI tools, n=2,988)

But this AI-generated code is introducing new challenges for development teams

73% agree

"**I have experienced problems with code that was created with 'vibe coding'** *(i.e., using natural language prompts to generate functional code without having to fully understand how the code works).*"

Top challenges in using AI to generate code



Note: 3% responded "N/A—there haven't been challenges so far in working alongside AI tools"

Q5. What have been the biggest challenges so far in using AI to generate code? (Currently using AI tools, n=2,988)
Q13. Please indicate how much you agree or disagree with the following statements. (Top 2 Box, Somewhat / Strongly Agree) (Total n=3,266)

DevSecOps professionals worry most about data storage, exposure, and compliance when using AI

Top data privacy concerns with AI use

49%
Data may be stored or logged by AI service providers without clear retention policies

48%
Sensitive information might be inadvertently included in model outputs for other users

45%
Difficulty ensuring compliance with data protection regulations (e.g., GDPR, CCPA, etc.)

42%
Lack of transparency about how input data is processed and protected

42%
Proprietary code could be exposed to competitors through shared training data

Note: 6% responded “N/A—we haven't identified data privacy challenges that arise when using AI tools”

Q30. What specific data privacy concerns do you have about using AI tools, especially when proprietary code or sensitive information is used as input for AI models? (Total n=3,266)

When it comes to AI agents, professionals have similar concerns

Top concerns around AI agent adoption

- 43% Privacy / data security
- 42% Security risks
- 36% Quality control
- 32% Regulatory compliance
- 31% AI agents being given too much autonomy
- 28% Complexity of integration
- 26% Lack of transparency in decision-making
- 20% Debugging

Note: 4% responded “N/A—I don't have concerns about adopting AI agents in software development”

Q12. Thinking about the next 18 months, what are your biggest concerns about adopting AI agents in software development? Please select up to three responses. (Total n=3,266)

AI is reshaping security and compliance challenges and building a new future

As AI adoption grows, DevSecOps professionals face increasing compliance complexity today but foresee a shift **from manual oversight to compliance-as-code by 2027.**

Current / emerging pressures

76% agree
"Agentic AI will create **unprecedented security challenges** for our organization to navigate."

70% agree
"AI is making **compliance management more challenging** for my organization."

Manual burden today

86% agree
"My company still requires **heavy human oversight** for more complex compliance tasks."

79% agree
"My organization uses **manual compliance solutions** for development."

Future state

82% agree
"By 2027, compliance will be built into code and **automatically applied."**

Q32. Please indicate how much you agree or disagree with the following statements. (Top 2 Box, Somewhat / Strongly Agree) (Total n=3,266)

04

The AI Efficiency Paradox

AI is empowering teams to move faster, but toolchain sprawl and inefficient processes continue to slow down collaboration

Fast, frequent deployment is now the norm

83%

of organizations who **deploy multiple times a day** are **currently using AI in the SDLC**.

How often organizations deploy to production

Daily / Multiple times a day (Net)	**36%**
Multiple times a day (continuous deployment)	20%
Once a day	15%
Once every few days / Once a week (Net)	**46%**
Once every few days	26%
Once a week	20%
Once a month / Every few months (Net)	**17%**
Once a month	12%
Every few months	5%
Don't know	2%

Q2. Is your organization using or planning to use AI in the software development lifecycle (SDLC)? (Total n=3,266)
Q21. How often does your organization deploy to production? (Total n=3,266)
Note: Totals may not equal 100% due to round of individual values

At the same time, most teams continue to deal with sprawling software development toolchains

49%
of DevSecOps teams are using more than **5 AI tools.**

53%
of DevSecOps teams are using more than **5 security tools.**

Number of tools used for software development

1	4%
2-5	33%
6-10	36%
11-14	18%
15+	7%
Don't know	3%

Q20. How many tools in the following categories does your team use for software development? (Total n=3,266)
Note: Totals may not equal 100% due to round of individual values

As AI usage ramps up, many organizations lack formal protocols for AI tool usage

39%
of DevSecOps professionals are using unofficial AI tools at work to some degree.

Are you using AI tools that are approved by your organization?

Yes, only approved tools	61%
Mostly approved with some personal / unofficial tools	24%
Mix of approved and personal / unofficial tools	14%
Primarily personal / unofficial tools	1%

Q20. How many tools in the following categories does your team use for software development? (Total n=3,266)
Note: Totals may not equal 100% due to round of individual values

Disconnected tools and a lack of communication are hindering collaboration

7 hours

Amount of time per week DevSecOps professionals report losing due to inefficient processes.

Collaboration barriers in the software development lifecycle

- 32% Lack of cross-functional communication
- 31% Lack of knowledge sharing
- 30% Different tools used across teams
- 28% Inefficient / unclear work processes
- 27% Organizational silos
- 27% Outdated documentation
- 26% Too many tools used
- 24% Different locations / time zones
- 19% Linguistic / cultural barriers

Note: 6% responded “N/A—there aren't factors limiting collaboration in the software development lifecycle”

Q22. What factors are limiting collaboration in the software development lifecycle (SDLC) at your organization? Please select up to three responses. (Total n=3,266)
Q25. Please read each statement below, and provide your best estimates, in hours per week. (Total n=3,266)

Platform engineering, which focuses on self-service workflows, can enhance performance and productivity

85% agree

"Agentic AI will be most successful when implemented in a platform engineering approach."

Observed benefits of platform engineering

Note: 4% responded "N/A—I haven't noticed any benefits of platform engineering / We do not use platform engineering at our organization"

Q13. Please indicate how much you agree or disagree with the following statements. (Top 2 Box, Somewhat / Strongly Agree) (Total n=3,266)
Q23. Which of the following benefits of platform engineering have you noticed at your organization, if any? Please select all that apply. (Total n=3,266)

Professionals know that to keep up with these speed and security demands, AI skills are essential to the growth and redefinition of their careers in 2026 and beyond

Skills needed to advance career on DevSecOps team

Note: 2% responded “N/A—I don't feel I need any additional skills to advance my career”

Q14. As part of a DevOps/DevSecOps team, what skills do you feel you currently need to advance your career? Please select all that apply. (Total n=3,266)

Are you ready to balance AI productivity with security and governance?

The challenge ahead

While AI coding assistants help developers write code faster, teams still struggle to evolve how they collaborate across the entire software lifecycle. Developers must balance quality, security, and delivery speed — and today's ways of working haven't caught up to that reality.

Reach out to GitLab to learn how we can help your team navigate the intelligent software development era.

Contact us

Explore GitLab Duo Agent Platform

GitLab can help you navigate the increasingly complex demands of DevSecOps

AI that goes beyond coding

Bring automation and intelligence to every stage of the SDLC with agents that handle repetitive work and keep humans focused on what matters most: creativity, strategy, and innovation.

Platform consolidation that scales

Replace fragmented toolchains with a single platform that encompasses planning, coding, security, and compliance — reducing the time teams lose to inefficient processes.

Security and compliance at speed

Move at the speed of innovation without compromising security or compliance. Automate scanning, apply consistent policies across environments, and adapt frameworks to fit your organization's needs.

Unified AI with built-in governance

Reduce shadow AI usage and data privacy risks with centralized controls, hybrid model configurations, and enterprise-grade security built into your development platform.

GitLab

Global DevSecOps Report