The GitLab 2022 Global DevSecOps Survey

Thriving in an insecure world
# What’s inside?

<table>
<thead>
<tr>
<th>Introduction</th>
<th>03</th>
</tr>
</thead>
<tbody>
<tr>
<td>Overview</td>
<td>04</td>
</tr>
<tr>
<td>Developers</td>
<td>14</td>
</tr>
<tr>
<td>Security</td>
<td>19</td>
</tr>
<tr>
<td>Operations</td>
<td>23</td>
</tr>
</tbody>
</table>

## Introduction
- Overview
  - 2022 DevSecOps Survey top findings
  - The starting point
  - Software development today
  - The root causes of release delays
  - The increasing role of AI/ML
  - Of toolchains and popular tools
  - The role of the DevOps platform

## Overview
- Developers top findings
- Devs and DevOps
- Developer daily life
- Security
- Looking to the future

## Developers
- Security top findings
- Security and DevSecOps
- Roles are changing
- Shifting left
- Who’s in charge?
- A look at testing
- Looking to the future

## Security
- Operations top findings
- Operations
- Still so many tools
- Working with development
- Looking to the future

## Operations
- Keeping the DevOps momentum
- 27
For six years now we’ve been asking DevOps teams to share their stories, successes, solutions, and struggles. In May 2022, 5,001 people offered us a snapshot of “their DevOps,” and this time it was set against a backdrop of sweeping socio-economic challenges.

With so many forces out of their control, it’s clear DevOps teams focused on what could be accomplished: from deployment velocity to automation, as well as release speed and adoption of new technologies, the momentum was obvious.

47% of teams have full test automation, nearly double the number in 2021.

70% of teams release code continuously, once a day, or every few days, up 11% from last year.

Nearly three-quarters of DevOps teams are using a DevOps platform or plan to this year.

DevOps roles continue to shift: Developers are taking on ops jobs, ops is cloud or platform-engineering focused, and security pros are “hands on” inside dev teams.

31% of teams are using AI/ML for code review, 16 points higher than last year.

60% of developers are releasing code faster than before.

We also heard about the challenges, including pandemic-based culture changes, hiring and retention struggles, and the level of effort required to integrate complex new technologies like artificial intelligence.

But if there was one overarching concern, it was the very real threat security breaches represent. While security continues to “shift left” in many teams, it also is, perhaps for the first time, a driving force for many decision makers when it comes to choosing a DevOps platform or other technologies. The threat of security breaches is also top of mind for many DevOps teams.

As always, a reminder this is our survey so it’s no surprise some participants use our products. Also, roughly 60% of respondents have been “doing” DevOps for at least three years, so their experiences may feel aspirational for newer, less seasoned teams.

Let’s get started.
Overview

2022 DevSecOps Survey top findings

How does DevOps look today?
Expect to see DevOps platforms, DevSecOps, CI/CD and test automation at work in today’s DevOps teams.

Test automation is (nearly) here
And so is AI/ML for testing, code review, and more.

DevOps works, across the board
DevOps = better code quality, developer productivity, and operational efficiency.

Security at center stage
Getting security right is the number one challenge for DevOps teams and tools that help—like a DevOps platform—are in use and in demand.

Deploy, deploy, and deploy
70% of teams deploy multiple times a day, daily, or every few days, up 11% from 2021.

Too many tools
69% of survey takers want to consolidate their (sometimes sprawling) toolchains because of challenges with monitoring, development delays, and unhappy devs.

Future planning
Security is the number one investment area for 2022, followed closely by cloud computing.
The starting point

In May 2022, 5,001 respondents completed our survey. Here's a closer look at who they are:

**Gender**
- 26% Female
- 72% Male
- 1% Non-binary/third gender
- 1% Prefer not to say
- 0% Prefer to self describe

**Age**
- 56% 18-34
- 36% 35-44
- 7% 45-54
- 2% 55+

**Industry**
- 45% Computer Hardware / Services / Software / SaaS
- 11% Automotive
- 5% Industrial manufacturing
- 5% Telecommunications
- 4% Retail
- 4% Business Services / Consulting
- 3% Energy & utilities
- 3% Media & Entertainment
- 3% Education
- 3% Banking / Financial Services
- 2% Biotech/pharm
- 2% Consumer products mfg
- 2% Insurance
- 2% Healthcare
- 2% Government
- 1% Aerospace & defense
- 1% Other

Prefer not to say
- 0%

Prefer to self describe
- 1%
<table>
<thead>
<tr>
<th>Role</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Software Developer / Software Engineer</td>
<td>15%</td>
</tr>
<tr>
<td>Site Reliability Engineer</td>
<td>9%</td>
</tr>
<tr>
<td>Operations Leadership</td>
<td>8%</td>
</tr>
<tr>
<td>Technology Executive - CIO / CTO / VP</td>
<td>8%</td>
</tr>
<tr>
<td>Project Manager</td>
<td>6%</td>
</tr>
<tr>
<td>Operations Engineer</td>
<td>5%</td>
</tr>
<tr>
<td>DevOps Engineer</td>
<td>4%</td>
</tr>
<tr>
<td>Network Security Specialist</td>
<td>4%</td>
</tr>
<tr>
<td>Security Engineer</td>
<td>4%</td>
</tr>
<tr>
<td>Security Leadership</td>
<td>4%</td>
</tr>
<tr>
<td>Product Manager</td>
<td>4%</td>
</tr>
<tr>
<td>Systems Administrator</td>
<td>4%</td>
</tr>
<tr>
<td>Software Architect</td>
<td>4%</td>
</tr>
<tr>
<td>Development/Engineering Leadership</td>
<td>3%</td>
</tr>
<tr>
<td>DevOps Leadership</td>
<td>3%</td>
</tr>
<tr>
<td>Systems Engineer / Network Engineer</td>
<td>3%</td>
</tr>
<tr>
<td>Release Manager</td>
<td>2%</td>
</tr>
<tr>
<td>App Security Engineer</td>
<td>2%</td>
</tr>
<tr>
<td>Quality Assurance</td>
<td>2%</td>
</tr>
<tr>
<td>Database Engineer</td>
<td>2%</td>
</tr>
<tr>
<td>Network Security Specialist</td>
<td>4%</td>
</tr>
<tr>
<td>Security Engineer</td>
<td>4%</td>
</tr>
<tr>
<td>Product Manager</td>
<td>4%</td>
</tr>
<tr>
<td>Site Availability Engineer</td>
<td>1%</td>
</tr>
<tr>
<td>Technical Writer/in Charge of Documentation</td>
<td>1%</td>
</tr>
<tr>
<td>Other</td>
<td>1%</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Decision maker status</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Primary decision maker</td>
<td>54%</td>
</tr>
<tr>
<td>Not the primary decision maker but on the team that makes the decisions</td>
<td>37%</td>
</tr>
<tr>
<td>Provide decision making input</td>
<td>8%</td>
</tr>
<tr>
<td>Not decision makers</td>
<td>2%</td>
</tr>
</tbody>
</table>
Software development today

In 2022, a majority of respondents (47%) told us DevOps or DevSecOps was their methodology of choice, an 11% increase over 2021. But while that’s substantial progress in DevOps usage, it’s clear respondents, who could “choose all that apply” when it came to software methodologies, are still using a mix-and-match development approach at least some of the time. The percentage of teams using Waterfall was up an astonishing 16% this year over last year, while “Water/Scrum/Fall” practitioners saw a 23% jump from last year.

Dev and ops professionals do have clear favorites, however: 53% of devs use DevOps/DevSecOps (and 50% of ops do as well), while a solid 30% of both groups also use Water/Scrum/Fall.

That’s a long way of saying that DevOps shops aren’t necessarily monoliths.

A full 40% of respondents told us their DevOps practices are between three and four years old, very much a “sweet spot” where they’ve known success and are comfortable with the processes and routines. Just a slightly smaller group, 35%, said their teams have been doing DevOps between one and two years, while just 5% have had DevOps implemented for less than a year. About one-fifth of survey takers have had DevOps on board for five or more years.
What do today’s DevOps implementations look like? A DevOps platform was the most likely to be part of the process (44%), followed by DevSecOps (42%), CI/CD and test automation at 34%, and observability/monitoring at 30%. Last year, 11.5% of survey takers used AI/ML; this year the percentage more than doubled to 24%.

For the third year in a row, respondents said devs are the most likely to benefit from a DevOps practice (64%), followed by ops (63%), and security (53%).

The top three reasons to choose DevOps? Better code quality, developer productivity and operational efficiency were called out by 37% of survey takers, followed very closely by better security/more secure applications. Other clear benefits from a DevOps practice included increased time to market, better communication/collaboration, and happier developers/DevOps team members.

An impressive 70% of survey respondents said their teams deploy multiple times a day, once a day, or once every few days, up 11% from 2021. All told 27% deploy continuously (multiple times a day), while 14% deploy once a day, and 29% deploy every few days.

Not surprisingly, the vast majority of survey respondents participate in open source projects – 64% in 2022, down slightly from last year. And 70% of those participants have contributed to GitLab, up an impressive 41% since 2021.
The root causes of release delays

From 2019 through 2021, our survey respondents have consistently pointed to testing as the most likely reason for software release delays. Test is still a bottleneck in 2022 but now it’s one of five equally likely reasons for release delays: code development, code review, security analysis, test data management, and of course testing. A few macro trends may help explain this change:

Testing is becoming increasingly automated, with or without the help of AI, thus it’s (presumably) more efficient and less likely to cause delays.

Test data management is the somewhat ironic outcome of test automation because more tests = more data and, of course, a greater need to communicate and analyze that data. (The “too much information” problem will appear later in this survey.)

Security is increasingly critical for every DevOps team and the shift left is real (both are reflected repeatedly in this survey).

Code development and code review have consistently been the second and third most common reasons for release delays in our last three surveys.
A rise in test automation

This year saw dramatic improvement in test automation: 47% of teams report their testing is fully automated today, up from 25% last year. Another 21% plan to roll out test automation at some point this year, and 15% hope to do so in the next two or more years.

And, there’s just more testing happening all around: 53% of survey takers said testing is happening as code is being written (up 21 points from last year). A full 59% of devs test their own code, up 34% from 2021, and 50% said test and dev work as a team to test code in real time as it’s being written.

The increasing role of AI/ML

Continuing a trend we saw last year, AI/ML may be the test team’s secret weapon. Today, 37% of teams use AI/ML in software testing (up from 25%), and a further 20% plan to introduce it this year. Another 19% plan to roll out AI/ML-powered testing in the next two to three years.

More broadly speaking, artificial intelligence and machine learning are solidly part of many DevOps teams today. Fully 62% of survey takers are practicing ModelOps, while 51% use AI/ML to check (not test) code. Almost 40% of teams said they use “bots” to test their code, up from 15% last year, and 31% of teams are using AI/ML for code review, nearly double what respondents reported last year. Just 5% of teams said they had no plans to incorporate AI/ML into their DevOps practices.
Of toolchains and popular tools

About 44% of DevOps teams use between two and five tools, while 41% use between six and 10 tools. That’s a lot of tools, and 69% of survey takers told us they’d like to consolidate their toolchains. Why would less be more? A full 37% said spending time on toolchain maintenance takes away from time that could be spent on compliance, while 35% said it’s difficult to have consistent monitoring across so many tools and that devs aren’t happy with all of the context-switching. Other concerns included slowed development velocity, cost increases, and difficulty in retaining developers. Clearly, teams are tired of paying the “toolchain tax.”

Taxed or not, tools are popular with DevOps teams. Here’s a look at what’s in use:

- **This year 30% of survey respondents** said they used Git for source control, while 24% used Team Foundation Server and 13% used CVS (Concurrent Versions System). GitLab is the Git solution for 48% of survey takers, followed by GitHub (31%) and BitBucket (17%).

- **GitLab is also the tool of choice** for CI/builds (43%), with GitHub Actions at 29%, Azure DevOps at 28%, and BitBucket at 20%.

- Slightly more than one-third of survey takers (36%) use microservices today while another 28% plan to at some point this year. A further 29% see microservices in their future over the next two to three years.

- **Kubernetes is in use by 33% of teams right now**, and another 25% plan to roll it out at some point this year. Another 29% of teams said they plan to implement K8s in the next two to three years.

- **Low code/no code development tools** may be finally having their day in the DevOps world: 66% of survey takers told us they are now using a low code/no code tool in their DevOps practice, up a remarkable 25% from last year.
The role of the DevOps platform

Three-quarters of respondents told us their teams use a DevOps platform or plan to use one this year. Another 21% said they are considering a DevOps platform in the next two to three years. What advantages does a DevOps platform offer? The top choice was improved security, followed closely by cost and time savings, improved DevOps, and easier automation. Other benefits included improved monitoring, observability, and metrics.

Although a majority of dev, sec, and ops respondents agreed that better security is the key advantage with a DevOps platform, each group saw other “specific-to-their-roles” perks. Devs said a DevOps platform gave them cost and time savings and a more streamlined DevOps practice. Ops told us they liked the cost and time savings too, but also appreciated better monitoring and metrics as well as easier compliance. And sec pros called out easier automation and more streamlined deployments.

The group most likely to use a DevOps platform is devs, but 38% said the entire DevOps team uses their platform, while 37% said security and 36% said operations. Other roles taking advantage of a DevOps platform included product manager, designers, the business side, and SREs.

Has your organization adopted microservices?

Yes we use this today 36%
We plan to this year 28%
We plan to in 2-3 years 29%
We have no plans to use them 2%

Does your organization use Kubernetes?

Yes we use this today 33%
We plan to this year 25%
We plan to in 2-3 years 29%
We have no plans to use it 4%

Does your organization use a low code or no code tool?

Yes 66%
No 28%
Developers

Development top findings

 Releases are faster
And devs say the number one reason is a DevOps platform.

 The challenges are real
Developers acknowledge that Covid-19, hiring, security threats, culture changes, and complex tech learning curves added more real-world difficulties to their roles than ever before.

 More, more, more
Code review, automated testing, and planning are the top three areas devs would like to spend more time on.

 All in a day's work
Devs continue to take on more ops and sec responsibilities.

 For the future
Devs think advanced programming languages and soft skills will be key to their future careers.
It’s easy to think software developers are insulated from real-world fluctuations; after all, every company is a software company today and demand for DevOps talent seems insatiable.

But in 2022, it’s clear reality has crept in.

We asked developers to tell us the most challenging parts of their role, and their answers were far less likely to be about learning a new programming language than dealing with big picture trends, including security/hackers, the economy, Covid-19, an insufficient labor force, and more. There was a strong sense of culture change and dread of looming, complicated technologies, with a clear undercurrent of “we may not be ready for this.”

In their own words:

“Security, security, security”...offered by more than one thousand respondents
“Limited potential for young developers”
“To keep it secure and keep it updated”
“Keeping up with the latest tools and security for optimal performance and privacy”
“Trying to build applications that are secure and stable”
“Cyber security attacks are the biggest challenge facing us today”
“The biggest challenge is finding sufficient coding staff”
“Data security, data security, I repeat, data security”
“Keeping pace with innovation, cultural changes, data privacy”
“The biggest challenge is to find people to fill the jobs”

“We have experienced significant difficulty in finding and retaining qualified staff”
“4G, 5G, AI, Metaverse, virtual space—developers have to support all of this”
“The ‘Covid effect’”
“Too many software frameworks”
“QA, undefined quality standards”
“Technology is rapidly changing” (mentioned very frequently)

Shared thoughts:

Supply chain issues (a common response)
Personnel turnover
The economy
Covid (hundreds of comments)
AI (mentioned frequently)

Two respondents summed it up well:

“We have a development capacity challenge, a recruiting challenge and a knowledge-sharing challenge.”

“For me, these are the 8 biggest challenges we are facing as software developers:
1) Keeping pace with innovation 5) Cybersecurity
2) Cultural change 6) AI and automation
3) Customer experience 7) Data literacy
4) Data privacy 8) Cross-platform functionality”
Devs and DevOps

Fear about the future aside, nearly 60% of devs told us they’re releasing code faster than before, continuing a release pace trajectory that’s done nothing but increase over the past few years. A full 35% said they’re releasing code twice as fast, while 15% are releasing code between three and five times faster, and 8% said the code is flying out the door more than five times faster.

To find out why code is being released more quickly we asked developers what’s changed in their process. A majority said use of a DevOps platform was the number one reason for the increased pace of code release, followed by automated testing, source code management, planning tools, and observability.

What do devs wish they could do more of? Their answers directly addressed those areas most likely to cause delays: more and better code review, automated testing, and better planning (all at 31%). Coming in as a strong second was AI/ML for code writing and review (27%) followed by code reuse (26%). These responses don’t represent any significant deviation from what developers said last year, perhaps underscoring how difficult it is to make systemic process and technology changes.

The growing adoption of DevOps has also meant teams are broadening their technical reach. What did DevOps teams add to their tech stack in 2022? Automated testing, source code management (SCM), and continuous delivery were the most popular additions; in 2021, SCM was the most added process, and automated testing was fourth. But teams didn’t just add in old favorites like SCM and CD: cutting-edge technologies, including observability, AI, and ModelOps also made the list.
All that automation has translated into a huge list of things devs told us they no longer have to do, including:

“I’m no longer testing my code. I ask my peer to review the code.”

“Less infrastructure handholding”

“I don’t need a proofreader for my code and the collaboration has calmed down.”

The code once written will not be tested again and again.

“Planning and architecture...our tickets have all the necessary steps already outlined”

“Develop some functionality from scratch where there’s already library/functionality available”

“I am no longer in charge of tasks like running integration tests as there is a dedicated QA team for that now”

“Planning docs - at this point it’s open up the IDE and hit the ground running”

“Design and design documentation are no longer part of the software development process”

“We use cucumber coding so more code is reused and less time is spent writing it”

“We no longer manually review code”

“Write a detailed plan before you develop the code”

Input, processing, testing and analyzing code

“We are no longer writing messy code and ignoring code quality”

Shared thoughts:

Testing

Manual testing

Code review

Documenting

Deploy to production

Maintaining other peoples’ code

Commented out code

Hard coding

Debugging

Manual drafting

Developer daily life

In a trend that we saw beginning in 2020, developer roles continue to shift, taking on more responsibility for what were traditionally ops roles. Fully 38% said they instrument the code they’ve written for production monitoring (up from 26% in 2021 and just 18% in 2020), while 36% define and/or create the infrastructure their app runs on, roughly the same as in 2021. But 38% now monitor and respond to that infrastructure (up 25% in just one year) and 36% say they’re on call for app-in-production alerts. Devs also said they’re writing the runbooks for apps in production, and that they’re now serving as an escalation point when incidents occur.

This year, the largest percentage of devs (27%) said they review code weekly, while 21% either review it with every commit or daily. A full 76% of developers said code reviews are “very valuable” while the remainder said they were “somewhat valuable.”

Devs are also spending more time than ever before on maintaining or integrating toolchains. Nearly 40% said they spend between one-quarter and one-half of their time on these tasks (more than double the 2021 percentage), while 33% are spending at least half their time and as much as all of their time on toolchain integration and maintenance.

Who sets devs’ priorities? In 2022, 44% of devs said product managers while 41% said devs set their own priorities. When prioritizing work and features, cost of development is the most important priority to developers (32%), followed by ROI, developer workload, and the product roadmap timeline.
Developers and security

This year, 53% of developers told us they are “fully responsible” for security in their organizations, a 14% increase over 2021, and perhaps yet another sign of security shifting left. Another 39% said they feel responsible for security but as part of a larger team, while 7% said they do their part but others on the team were more responsible. Developers continue to be very upbeat about their team’s security posture: 87% said their organizations make it possible for them to avoid breaches, a substantial increase from 75% in 2021.

Looking to the future

What will matter most for a developer’s future career seems to change every year. In 2021, devs said AI/ML would be most important, while in 2020 it was soft skills like communication and collaboration. This year devs were split between soft skills and advanced programming languages, followed by subject matter expertise; AI/ML was at the bottom of the list.

But, by a single percentage point, devs were the most optimistic about the future of their careers, despite ongoing changes and shifts. Just over three-quarters (76%) said they feel “somewhat” or “very” prepared for the future; in fact, 43% of devs said they feel very prepared, strikingly higher percentages than either ops (37%) or security (30%).
DevSecOps = in the thick of it
Sec pros are increasingly involved in daily tasks and doing “hands on” work with team members in dev and ops.

The shift left continues
DevSecOps teams are running more scans, but results delivery continues to lag.

Closing the gap
It’s complicated, but relations between sec and dev are improving...slowly.

Not as optimistic
Concern about security has never been higher, so perhaps it’s not surprising 43% of sec pros feel “somewhat” or “very” unprepared for the future.
Security and DevSecOps

For the second year in a row, a large majority of security pros (71%) rated their organization's security efforts as either "good" or "excellent." This was nearly identical to last year's assessment and certainly reflects the increasing focus on security we've seen throughout the survey.

Roles are changing

As we saw starting last year, security roles are evolving. Nearly 29% of sec pros said they're now part of a cross-functional team (identical to 2021's findings), while 28% are now more focused on compliance and 35% are more involved in daily tasks/more hands-on, an 11-point jump from last year. About 48% of survey takers said their roles aren't changing, but 10% said they have more budget, and 7% have more influence over engineering decisions.

Shifting left

The great shift left continues: 57% of sec team members said their orgs have either shifted security left or are planning to this year. One-third of teams, though, aren't thinking about a shift left until at least two years from now.

Scanning has certainly increased: Today 53% of developers run static application security testing (SAST) scans (a dramatic jump from last year, which was less than 40%) and 55% employ dynamic application security testing (DAST) scans (up 11 points from last year). Nearly 60% of security pros report their devs scan containers today (up 10% from 2021), while 56% take advantage of dependency scans, and 61% do license compliance checks.

But all that scanning hasn't translated into devs having more data in their workflows, which is an ongoing problem we've seen over the past few years. In fact, just 30% of teams put SAST lite scanners in a web IDE, and only 29% pull scan results into a web pipeline report for devs. Nearly 30% of DAST and dependency scans are easily available to devs and 30% do the same for container scans. Scan availability has improved about 10% on average since 2021, but there clearly is substantial room for improvement.
And, while it may be a bit simplistic to suggest sec and dev really don’t get along, year after year the data continues to support that they at least don’t always see eye to eye. For the third year in a row, the largest percentage of sec pros (47%) said devs find 24% or less of the available bugs that could be found in existing code...to put it another way, 75% of the bugs were left for sec to find. Less than 20% of security team members said devs found between half and three-quarters of the bugs.

A full 57% of survey takers agreed security is a performance metric for developers in their organization but 56% said it was difficult to get devs to actually prioritize fixing code vulnerabilities. In the end, 59% said security vulnerabilities were most likely to be found by the security team after the code is merged in a test environment. These aren’t new opinions—we’ve heard them since 2020, but this year the percentage of security pros “complaining” was down dramatically from last year’s 80%+ view, perhaps a sign of improving relations.

**Who's in Charge?**

While dev and ops are taking on a larger share of security ownership, it’s not so straightforward on the sec team. In 2020 and 2021, the percentage of security pros who said they were fully responsible for security was roughly the same as those who said **everyone** was responsible. This year the picture has changed dramatically: 43% of sec team members admitted to full ownership of security (a 12% jump from last year) but a resounding majority (53%) said everyone was responsible, a 25% increase from 2021.
A look at testing

Security testing is, not surprisingly, a continuing bump in the road for DevOps teams. We asked sec pros to rank their challenges by most to least frustrating, and they didn’t hold back. In the last several years security team members have complained the most about test timing (it’s always too late in the process). But this year, sec pros said the biggest challenge was prioritizing vulnerability remediation, followed by tardy testing, and the incredible difficulty in finding someone to actually fix the problems. Other concerns included the volume of false positives, how hard it is to track vulnerability status and the difficulty in unpacking the test findings.

When bugs are found, severity level is most important, followed by time elapsed since found, mean time to resolution (MTTR), and number of vulnerabilities spotted.

Microservices and containers continue to gain traction in DevOps teams, but security processes to monitor them continue to lag. Just 65% of sec pros said they had a security plan for microservices and just 64% said they had one for containers. The security outlook is a bit brighter when it comes to cloud native and serverless, however. Last year 60% of respondents said their organizations had nothing in place to secure cloud native and serverless, but this year 53% of teams have built it in.

Looking to the future

When it comes to what will help them most in their future careers, a majority of security pros (54%) said AI/ML, followed by communication and collaboration (33%), and advanced programming (32%). Since our 2020 survey, security pros have been consistent about the critical importance of soft skills, but the interest in AI/ML jumped 33% from 2021 to 2022.

But security pros don’t share the confidence their ops and dev colleagues do about the future: Just 56% said they feel “somewhat” or “very prepared” for the future (almost 20 points lower than the average dev and ops response), while 43% feel “somewhat” or “very” unprepared.
Operations top findings

All. The. Hats.
From DevOps coach to platform engineer and cloud administrator, operations includes more roles than ever.

Too much is really too much
Ops is suffering from data overload with over one-third saying it’s difficult to find and access needed information.

Automation gets real
Almost one-quarter of ops teams report full automation, while 44% are “mostly” automated, both big jumps from 2021.

Moving forward
Ops pros continue to think programming and soft skills will be the most important skills they can have.
Operations

At the nexus of every single change that happens in DevOps, operations pros need to be prepared for anything, particularly shifting roles and responsibilities. We asked them to describe their primary job responsibilities in 2022.

And that’s just the beginning. When asked what DevOps has added to ops roles that didn’t exist before, options were nearly evenly divided among the seven choices. Managing the cloud was the top response, but managing hardware/infrastructure, maintaining the toolchain, DevOps coaching, responsibility for automation, overseeing all compliance, and platform engineering were almost equally mentioned.

Of all of those newer tasks, managing audit and compliance requirements is becoming increasingly critical. The majority of respondents said they spend between one-quarter and half their time on audit and compliance, a 15% increase from 2021. Almost one-quarter of ops pros said they spend between half and three-quarters of their time dealing with audit and compliance.

54% are managing hardware infrastructure all or most of the time

32% manage hardware infrastructure “sometimes”

52% manage cloud services all or most of the time

31% manage cloud services “sometimes”
Still so many tools

And of course there are always lots of tools for ops to manage. Roughly 49% of ops pros said their teams use between two and five monitoring tools (unchanged from 2021) and one-third use between six and 10. All told, 63% of ops teams use a DevOps platform to feed real-time data back to developers (a 23% increase from last year).

Metrics is the most important monitoring category followed by logging.

The top choice for capturing and viewing logs is Datadog (47%), followed by LogDNA (43%), and Splunk (41%). Datadog was also the first choice for tracking traces, followed by AppDynamics and Dynatrace. And Datadog was also the tool of choice for capturing time-series metrics, followed by Solar Winds.

A majority of ops teams (58%) use Google Cloud Platform, up 35% from 2021, followed by Azure and AWS. Just 4% of respondents currently don’t use a cloud provider or don’t know which one it is, down 9 points from last year.

Working with development

A full 68% of ops teams told us their software development lifecycle was either completely or mostly automated, a 13% increase from 2021. And 29% said it was somewhat automated. To look at it another way, 24% of teams told us they were fully automated—that’s up from 19% last year and just 8% in 2020, meaning dramatic progress in just a few short years.

Ops continues to value visibility into what devs are doing, with 86% of ops pros reporting it was moderately, very, or extremely important to them to have visibility into development, up 15 points over 2021.

But that visibility brings information and it’s increasingly clear ops is struggling with true information overload: 39% of ops respondents said the DevOps data they need exists but accessing and managing it is difficult, while 27% went further and acknowledged being “overwhelmed” by the amount and scope of data available. Another 14% either don’t know what data is available or say their organization doesn’t track what they need. Just 18% report they have all the data they need and find it easy to access.

In a continuing sign of shifting roles, nearly 77% of ops pros said their devs are able to provision testing environments, which is an 8% increase from last year. And there is more actual DevSecOps happening: Just over 76% of ops teams agree at some level that devs are able to receive and address security issues during the development process (that’s a 10% jump from last year).

There’s no question that ops pros are experiencing an increasing sense of urgency and ownership around security. An impressive 48% of operations team members said they were solely responsible (up from 28% last year), while 40% believe they are responsible but as part of a bigger team, a 6% increase since 2021.
Looking to the future

Like their dev and sec colleagues, ops pros are fairly consistent in what they believe will be most important in their future careers. In 2021 they told us programming and soft skills would matter most and the same was true this year (46% for each). Other key skills mentioned included subject matter expertise and IoT/blockchain.

And ops pros feel optimistic about the future, in spite of the ways DevOps continue to evolve. Three-quarters of ops team members told us they feel “somewhat” or “very” prepared for the future, while just 24% feel “somewhat” or “very” unprepared.
Keeping the DevOps momentum

With all the changes—in the world, the technology, and in DevOps roles—dev, sec, and ops pros are unanimous in their desire to keep themselves and their careers moving forward. One obvious example: 81% of survey takers said certifications were either somewhat or very important to their future careers.

More globally, dev, sec, and ops agreed that their top area of investment in 2022 would be security. A close second priority will be cloud computing (21%), followed by DevOps, AI, and blockchain (all 20%). Combine AI with its technology cousin machine learning/MLOps and that was the clear investment winner at 30%.

Priorities varied depending on where in the DevOps team respondents were. Ops pros plan to double down on cloud computing (24%), followed by security at 23% and DevOps (21%). Interestingly a full 24% of devs want to put their focus on DevOps this year, followed by AI (22%), and cloud computing and a DevOps platform (21% each). The security team is primarily interested in blockchain (36%) followed by security (25%) and cloud computing and AI (both 17%).

Management’s top areas of investment were blockchain (23%), security (22%), and cloud computing (21%).

Today’s teams are clearly doing the planning, thinking, and work to move DevOps and software development forward, even during stressful world events. Use this survey and see how your team compares, and then share with colleagues also on the DevOps journey. DevOps isn’t a destination, it’s a process.

🔥GitLab