SYNOPSYS®

Global State of DevSecOps 2023

Strategies, Tools, and Practices Impacting Software Security

Overview

About the Synopsys 2023 DevSecOps report

In early 2023, the Synopsys Cybersecurity Research Center (CyRC) and Censuswide, an international market research consultancy, conducted a survey of 1,000 IT professionals who identified security as part of their role or responsibilities. The group includes developers, AppSec professionals, DevOps engineers, CISOs, and experts who work in various roles in technology, cybersecurity, and application/software development. Participants came from the U.S., U.K., France, Finland, Germany, China, Singapore, and Japan.

Respondents from all industries and all company sizes were eligible to participate. One of the challenges faced while developing the survey is that the term "DevSecOps" embraces several disciplines, many of which have unique personas. The goal was to include a broad spectrum of professionals including "hands-on" developers who write the code and people at the CISO level, but targeting those whose work involved some aspect of software security.

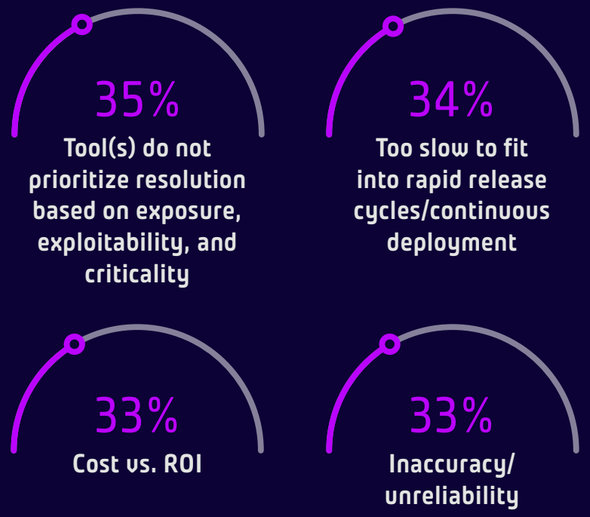
On DevOps and DevSecOps

Achieving the key tenets of DevOps—accelerated development, continuous delivery, pipeline resilience, scalability, and end-to-end transparency—requires a concerted effort from contributors in development, security, and operations.

An extension of the DevOps methodology, DevSecOps is designed to instill a culture of security across teams and address security early and consistently in DevOps environments. By integrating security practices into the software development life cycle (SDLC) and CI pipelines, DevSecOps aims to shift security from a separate, standalone phase to an integral part of the development life cycle.

DevSecOps has gained significant traction in every organization involved with software development. According to the SANS 2023 DevSecOps survey, DevSecOps is now clearly seen as a business-critical practice and a risk management concern. But historically, security and development teams have found themselves at odds when trying to introduce security into their processes, often a consequence of bringing legacy application security testing (AST) into the SDLC. Common complaints include AST tools' complexity and high learning curves, slow performance, and "noisy" results causing DevOps "friction"—that is, anything in the software creation process that prevents developers from easily and quickly building code.

The majority of the respondents cited their general unhappiness with the AST tools they have in use



Benefits of automation

A core tenet of DevOps is to automate manual processes within each stage of the SDLC. Automation is a fundamental requirement before any organization can implement continuous integration or continuous deployment to develop and deliver code faster.

Successful DevSecOps requires the interplay of integration and automation, governed by standards and policies. This allows security teams to trust that security interests are being covered, and allows DevOps teams to keep working and trust that there won't be unpredictable breakdowns in the pipeline.

Unlike manual testing, automated security tests can be executed quickly and consistently, allowing developers to identify issues early in the development process without impacting delivery schedules or productivity.

Consistency

Automated tests ensure that security checks are consistently applied to every build and deployment. Manual testing might lead to variations in testing procedures and coverage.

Scalability

As software grows in complexity, manual testing becomes impractical. Automated tests can easily scale to handle a large number of tests across various components.

Continuous integration and continuous deployment (CI/CD)

Automated testing is crucial in CI/CD pipelines, where rapid and frequent code changes are deployed. Automated tests validate changes quickly and prevent faulty code from reaching production.

Continuous improvement

Automated testing provides data and insights that help teams improve security practices over time. Patterns of vulnerabilities can be analyzed and addressed systematically.

Documentation

Automated tests document the testing process, making it easier to track and audit security measures and compliance requirements.

Reduction of human error

Manual testing can be error-prone due to fatigue or oversight. Automated tests follow predefined scripts, reducing the risk of human error.

Time and cost savings

Identifying and fixing security issues late in the development process or in production can be time-consuming and costly. Automated testing minimizes these expenses.

Improved developer experience

Automated application security testing enhances the developer experience by offering proactive, integrated, and educational solutions to address security concerns. This ultimately leads to more secure software and a more efficient development process.

The growing use of ASOC/ASPM in DevSecOps

This report examines the characteristics of organizations at various stages of DevSecOps maturity and the security tools/practices the organizations employ. Based on the survey results, we offer prescriptive recommendations to those striving to attain a higher level of security maturity.

An interesting data point seen in the findings is the growing use of application security orchestration and correlation (ASOC), now more commonly referred to as application security posture management (ASPM). According to Gartner, ASPM should be a priority for any organization that uses multiple development and security tools.

ASPM solutions continuously manage application risks through the detection, correlation, and prioritization of security issues from development to deployment. ASPM tools ingest data from multiple sources and then correlate and analyze findings for easier interpretation, triage, and remediation.

ASPM also acts as a management and orchestration layer for security tools, enabling controls and the enforcement of security policies. And by providing a consolidated perspective of application security findings, ASPM offers a comprehensive view of security and risk status across an entire application or system.

Given that the majority of the 1,000 survey respondents cited their general unhappiness with the AST tools they have in use—criticisms included that those tools don't prioritize remediation based on business needs (35%) and they can't consolidate/correlate results for issue resolution (29%)—it's little wonder that the use of ASOC/ASPM is growing rapidly.

Key Findings from the Synopsys 2023 DevSecOps Survey

The majority of DevOps teams have adopted some level of DevSecOps

A total of 91% of respondents reported that they incorporate some measure of DevSecOps activities into their software development pipelines. It's safe to say that adoption of the DevSecOps methodology is now an established part of software development.

Organizations with a more mature security program have personnel focused on security

Twenty-nine percent of survey respondents noted that a cross-functional DevSecOps team—a collaborative group from development, security, and operations—was an important factor in a security program's success. Personnel focused on security, working with developers/software engineers and/or QA and testing, are likely to be on the front lines of security testing in organizations with mature security programs.

There are many barriers to effectively implementing DevSecOps

Over 33% of respondents pointed to inadequate security training as a major roadblock. This was closely followed by a shortage of security personnel (31%), lack of transparency into development/operations work (31%), and continuously changing priorities (30%).

Over a third of respondents said that integrating automated security testing into build/deploy workflows was key to a security program's success

Other critical factors included enforcing security/compliance policies through infrastructure-as-code, developing security champions in dev and ops teams, and improving communications across dev, ops, and security teams.

Dealing with critical vulnerabilities late in the SDLC dramatically impacts the bottom line

More than 80% of respondents said that critical vulnerability/security issues in deployed software impacted their delivery schedules in some form during 2022-23.

Twenty-eight percent of respondents said their organizations take as much as three weeks to patch critical security risks/vulnerabilities in deployed applications; another 20% said it can take up to a month

These figures are especially disturbing because vulnerabilities are being exploited faster than ever. The latest studies show that well over half of reported vulnerabilities are exploited within a week of disclosure.

Over 70% said automated scanning of code for vulnerabilities or coding flaws is a useful security measure, with 34% calling automated AST "very useful"

Automated scanning of code for security vulnerabilities and other defects led the "usefulness of tool/processes" category, followed closely by "defining security requirements as part of SDLC requirements stage" and "formal measurement of a software security program through models such as BSIMM and SAMM."

Nearly all respondents agreed that AST tools don't align with their business needs

The majority of the 1,000 respondents cited as major problems a variety of issues with AST tools—including that those tools don't prioritize remediation based on business needs (35%) and they can't consolidate/correlate results for issue resolution (29%).

Fifty-two percent of security professionals are already actively using AI in their DevSecOps practices, but more than three-quarters are concerned about issues with AI use

The survey results indicate that AI, machine learning, natural language processing, and neural networks are in active use by security teams. However, the growing use of generative AI tools such as AI-powered coding suggestions are spawning questions—in some cases, even lawsuits—around IP ownership, copyright, and licensing of the AI-generated code.

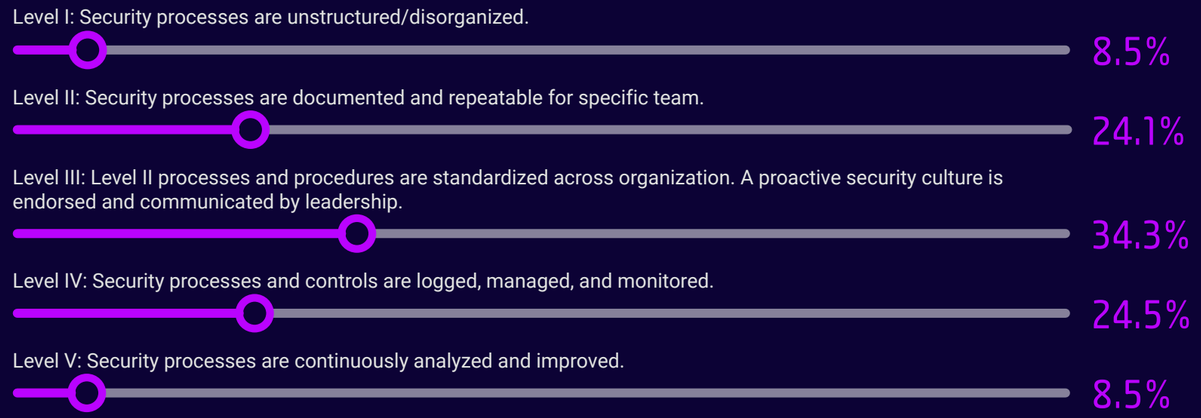
The State of DevSecOps in 2023

DevSecOps adoption

Over a third of the 1,000 respondents characterized their security initiatives at a Level 3 stage of maturity, in which security processes are documented, repeatable, and standardized across the organization. Twenty-five percent felt that they had attained Level 4, with security processes also logged, monitored, and measured.

With a total of 91% of respondents reporting that they have applied some type of DevSecOps activities into their software development pipelines, adoption of DevSecOps appears to have become an established part of DevOps.

Figure A **How would you best describe the maturity of your current software security program/initiative?**



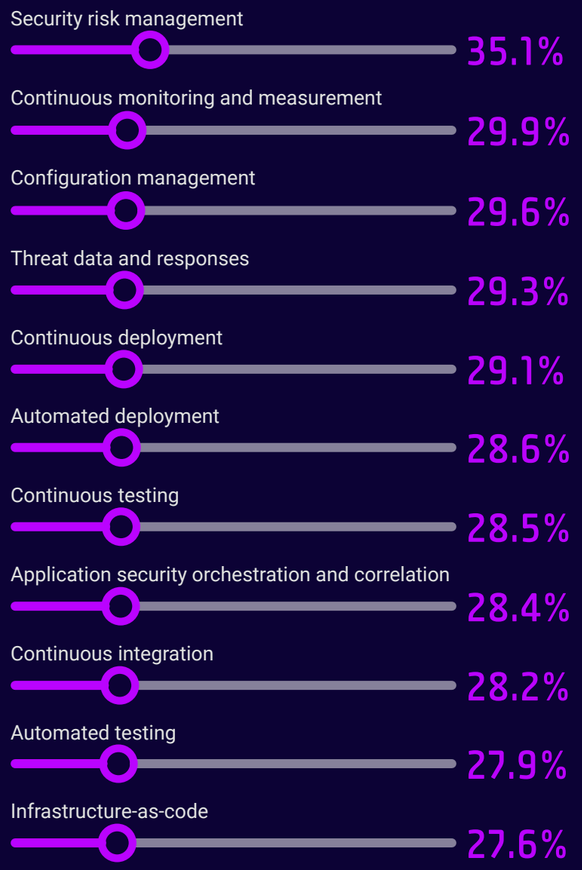
Implementation of security practices indicate a higher level of maturity

Another measurement of DevSecOps maturity can be seen in Figure B, indicative that the respondents have adopted a broad set of security practices, ranging from continuous monitoring and measurement (30%) to automated testing (28%).

The leading practice, security risk management, cited by 358 respondents (35.1%), involves integrating security considerations at every stage of the development process to identify, assess, and mitigate potential security risks associated with a software application. Applied within the SDLC, overall security risk management entails

- **Requirement analysis.** Identifying security requirements and constraints early in the SDLC and defining security objectives.
- **Design.** Incorporating security principles into the system architecture and design to ensure an application's design includes appropriate safeguards against common vulnerabilities.
- **Development.** Implementing secure coding practices and adhering to coding standards that address security concerns. Using integrated security testing tools such as static application security testing (SAST) and software composition analysis (SCA) to catch vulnerabilities as code is written and open source or third-party dependencies are brought in.
- **Testing.** Performing various types of security testing, such as SAST, dynamic application security testing (DAST), SCA, and penetration testing to identify vulnerabilities in the application.
- **Deployment.** Securely configuring the environment where the application will run. Implementing access controls, network security, and proper authentication and authorization mechanisms.
- **Monitoring and measurement.** Continuously monitoring the application in production for security incidents and anomalies. Implementing logging and monitoring solutions to detect and respond to potential breaches. This was cited by 30% of survey respondents as a major security practice in their organization.
- **Response and remediation.** Creating an incident response plan to address security incidents quickly and effectively. Remediating risks detected during the testing phase.
- **Transparency and security enablement.** Establishing clear standards, criteria, policies, and reporting of security risks and risk tolerance.
- **Training.** Providing training to development teams on secure coding practices, common vulnerabilities, and security best practices. This empowers developers to proactively address security concerns. Unfortunately, 34% of our survey respondents cited "inadequate/ineffective security training for developers/engineers" as one of the major blocks to implementing DevSecOps effectively at their organization.
- **Continuous improvement.** Regularly reviewing and improving the security processes and practices within the SDLC.

Figure B **What practices does your organization follow? (Select all that apply)**



Measuring a security program

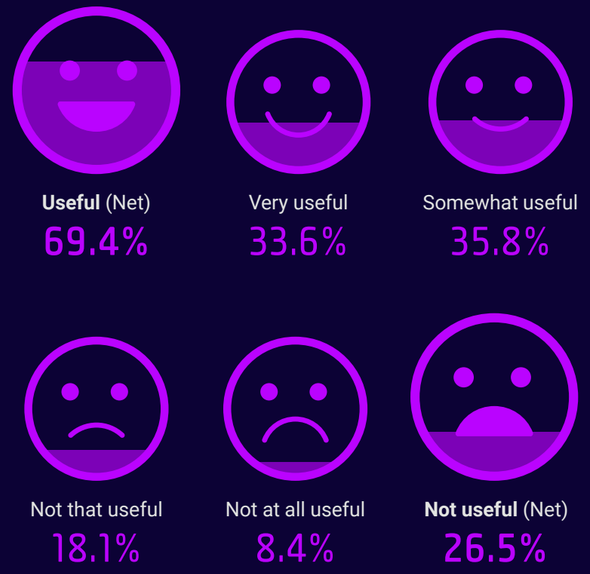
Nearly 70% of respondents said that measuring their security programs through an assessment tool such as Building Security In Maturity Model (BSIMM) was a useful exercise, with over a third calling such assessments "very useful."

An outside assessment of a security posture allows organizations to analyze and benchmark their software security program against other organizations and industry peers. Tools such as BSIMM provide an objective, data-driven analysis on which to base decisions of resources, time, budget, and priorities. Comparing other software security programs with your own can guide the strategy for your efforts, whether you're in the early stages of implementing a security program or want to ensure that your existing program can address changing business and security needs.

If you're in charge of, or beginning to build, a software security program, understanding AppSec trends among your peer organizations can help you plan strategic improvements to your own security efforts. If you're running a security program from the technical side, you can use the information garnered by a BSIMM or Software Assurance Maturity Model (SAMM) assessment to define tactical improvements for people and processes—for example, by building a Security Champions program.

In fact, according to the BSIMM report, one of the first initiatives that many software security groups undertake is identifying people who are a driving force in software security but not directly connected to a software security group. Collectively referred to as "software security champions," these people can enable and emphasize software security efforts. Security champions in engineering teams, for instance, can encourage engineers to own the security of their software deliverables. Developing a Security Champions program was cited by 33% of survey respondents as a key factor to a security program's success.

Figure C **Usefulness of formal measurement of your software security through models such as BSIMM, SAMM, etc.**



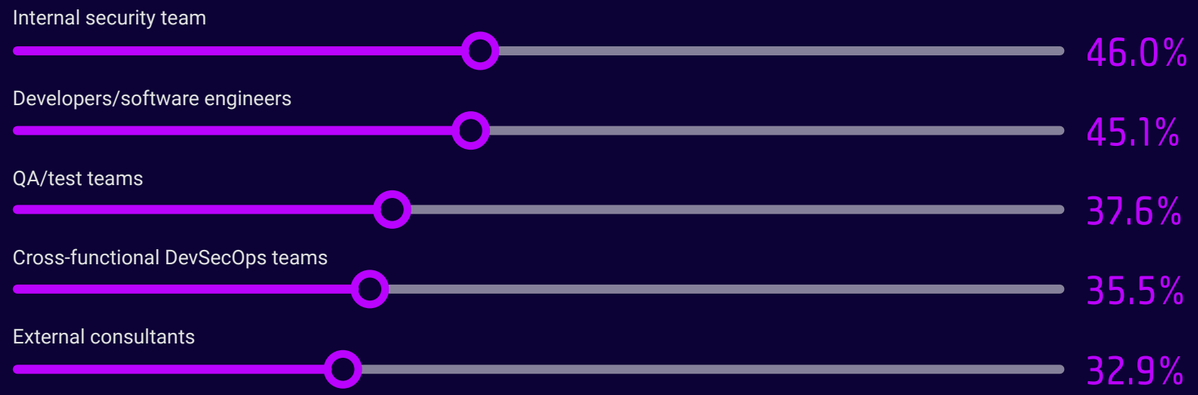
The importance of cross-functional teams for DevSecOps success

Twenty-nine percent of survey respondents noted that a cross-functional DevSecOps team—a collaborative group from development, security, and operations—was an important key to a security program's success (see Appendix Q16). Personnel with a focus on security, working with developers/software engineers and/or QA and testing teams (whether formally in DevSecOps groups or otherwise) are likely to be on the front lines of security testing in organizations in more mature security programs.

Monolithic, stove-piped security teams that stepped in to test shortly before or after deployment have gone the way of the dodo. In today's software development environment, security testing is the responsibility of the entire engineering team, including QA, dev, and ops, and most will have had a hand in building security into their software at different stages of the SDLC.

Thirty-three percent of respondents mentioned that external consultants also conducted security tests for their organizations. Best practices advise that organizations should conduct security audits regularly. It can be invaluable to contract third-party auditors or penetration testers to conduct such tests in order to gain an unbiased view of an organization's security posture.

Figure D Who is responsible for conducting security testing in your organization? (Select all that apply)

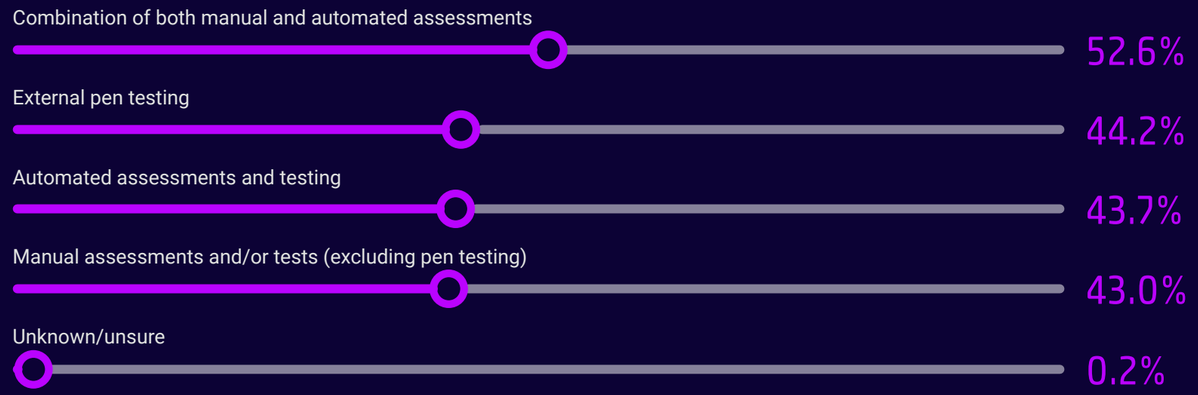


Combining manual and automated testing for the best results

The survey results indicate that the majority of respondents feel combining manual and automated security testing provides a more comprehensive approach to assessing the security of business-critical applications. As important as automated testing is for consistency, scalability, and time and cost-savings, the human factor adds a layer of insight and adaptability essential for identifying complex and subtle security issues. For example, the very nature of DAST as "black box" testing (that is, without knowledge of an application's internal structure) requires developer and security experts to verify and triage findings.

Similarly, the fact that 44% of respondents include external pen testing as a key element of their security testing demonstrates the value of penetration testing as a complement to internal testing. Often required to comply with industry regulations and standards, external pen testing brings added benefits such as an unbiased viewpoint of your security posture, as well as accurate simulation of potential threats and vulnerabilities that external adversaries might exploit.

Figure E How do you assess or test the security of your business-critical applications? (Select all that apply)



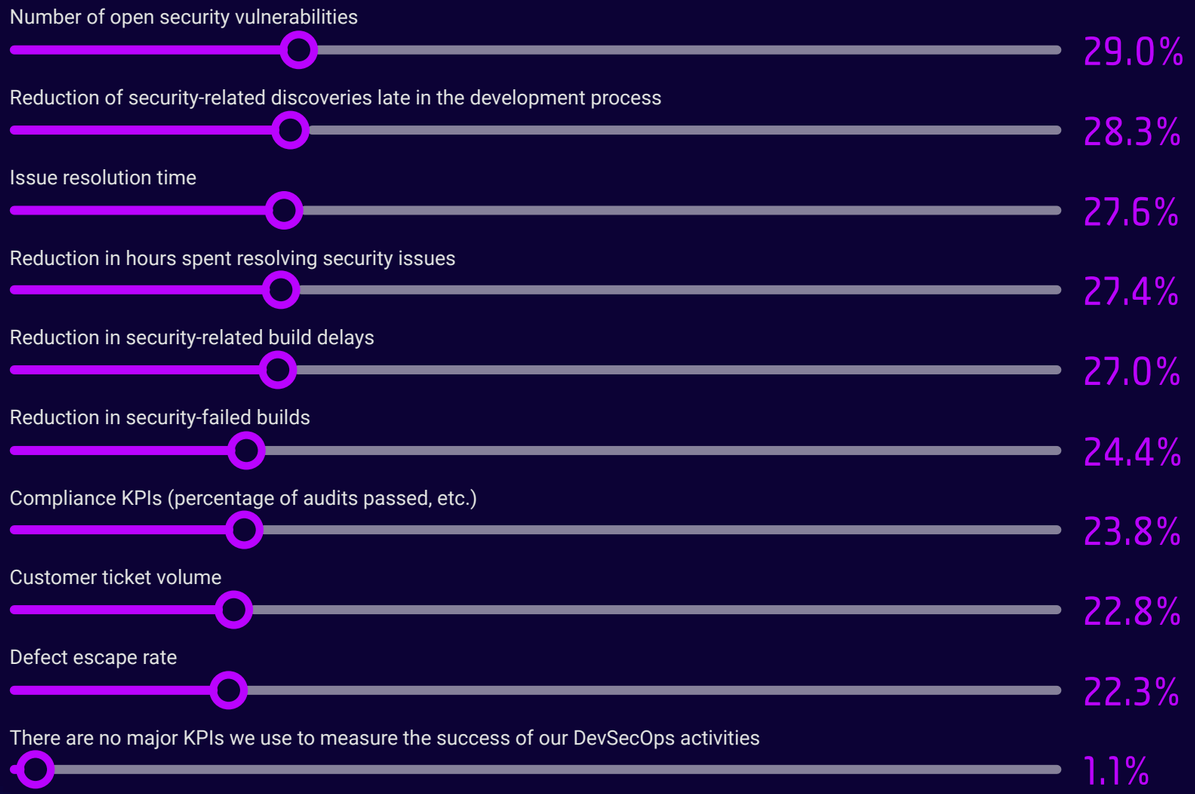
Key performance indicators

Respondents were asked to pick the top three key performance indicators (KPIs) used to measure the success of their DevSecOps program. Overall reduction of open security vulnerabilities was cited by 295 respondents (29%), closely followed by the 28% (288 respondents) who referenced a reduction of security-related discoveries late in the SDLC as a crucial KPI. Rounding out the top three KPIs was issue resolution time, noted by 28% (281 respondents).

As the survey results demonstrate, time, productivity, and costs are the three commonalities among the top KPIs and the challenges organizations face in implementing a secure SDLC. Or, in other words, the three major questions those involved with DevSecOps face are

- *How can we reduce the number of vulnerabilities/ issues we encounter?*
- *What can we do to move vulnerability discovery earlier in the SDLC?*
- *How can we reduce the time it takes to resolve issues to both reduce build delays and improve developer productivity?*

Figure F What are the major KPIs you use to measure the success of your DevSecOps activities? (Select up to 3)



Which AST tools are in use? How useful are they?

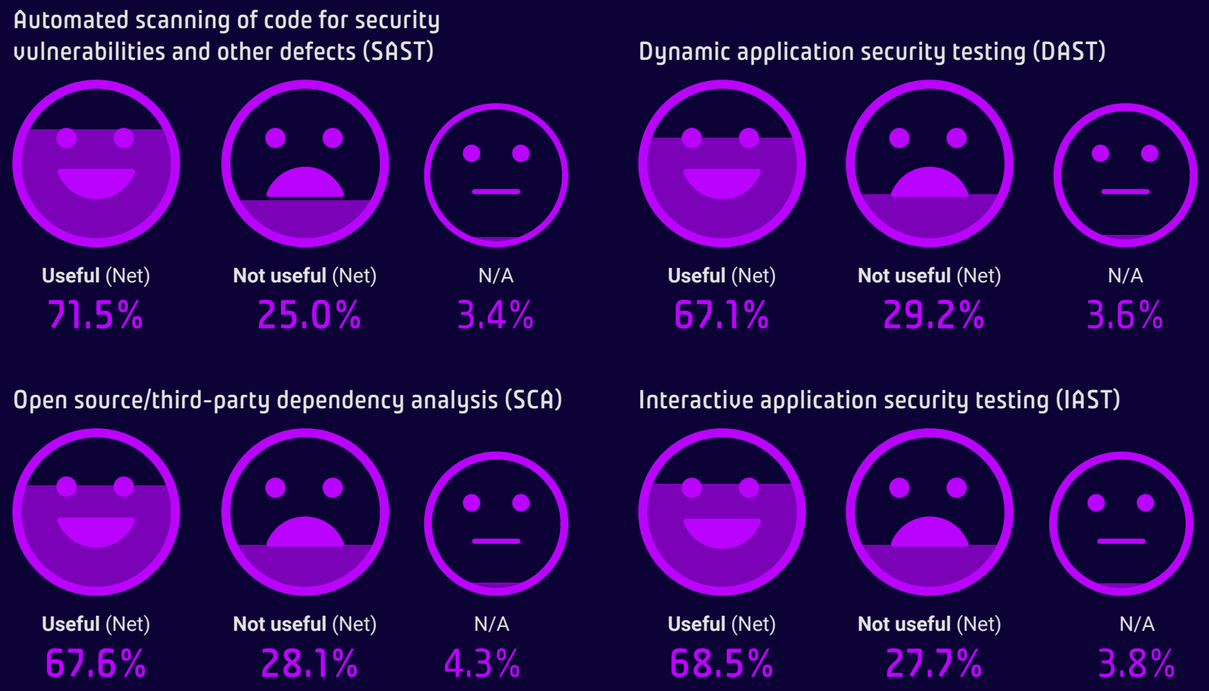
The survey results show that successful DevSecOps strategies use a full security toolset—including dynamic application security testing (DAST), interactive application security testing (IAST), static application security testing (SAST), and software composition analysis (SCA) tools—to address code quality and security flaws throughout the software development life cycle.

SAST was found to be the leading AST tool used by respondents, with 72% finding it useful. It was closely followed by IAST (69%), SCA (68%), and DAST (67%).

SAST and DAST use different testing approaches that work most effectively in different phases of the SDLC. SAST is critical for uncovering and eliminating vulnerabilities in proprietary software early in the SDLC, before the application is deployed. DAST, on the other hand, is used after deployment to spot issues that manifest at runtime, such as authentication and network configuration flaws. Combining some of the features of both SAST and DAST, IAST is used to detect critical security flaws that may not be identified by other types of tests.

SCA is used to identify and manage open source security and license risk, a critical need in modern software development, especially considering that over three-quarters of the code in any given application is likely to be open source. And since many organizations use packaged software procured from independent software vendors, as well as Internet of Things (IoT) devices and embedded firmware, many will also need some form of SCA binary analysis in their AST toolbox.

Figure 6 How useful, if at all, are the following application security tools used in your organization?



When to test? When to patch? What's the impact on our schedules?

The frequency of application security testing depends on several factors, including the business criticality of the application, the industry, and the threat landscape. For highly critical applications, assessments should be performed regularly, as reflected in our survey results (Figure H). Most respondent organizations run vulnerability scans on business-critical applications an average of two to three days a week.

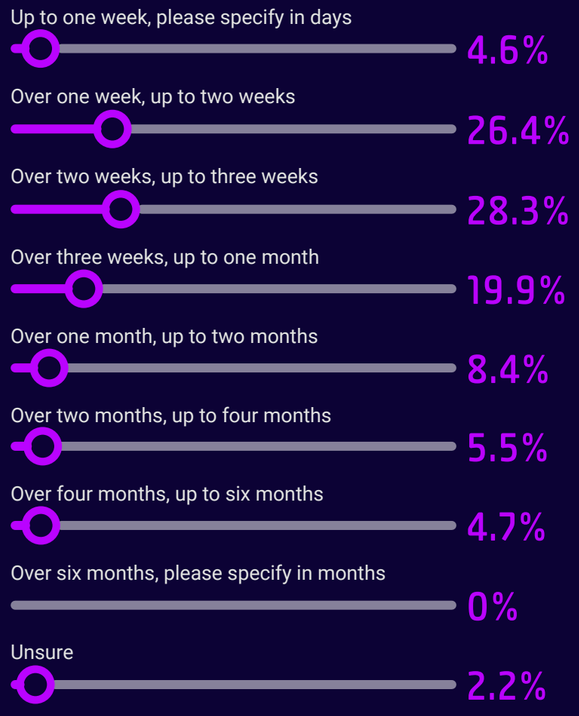
On first blush, the survey results showing that 28% of organizations take up to three weeks to patch critical vulnerabilities (Figure I) may seem concerning, but there are other factors to consider. There is a myth that the proverbial developer can fix each and every vulnerability, but no one can rationally expect developers to dig into vulnerabilities that haven't been prioritized for resolution.

It's worth noting that 31% of respondents cited "lack of transparency into development/operations work," while another 29% identified "organizational silos between development, operations, security" as major barriers in implementing DevSecOps (Figure K). Both are indicative of issues with the communication of risk from security to development and the need for rapid alerting and automation with security policies.

In any case, patch priorities need to align with the business importance of the asset being patched, the criticality of the asset, and the risk of exploitation. That last is of high importance. Studies show that well over half of reported vulnerabilities are exploited within a week of disclosure.

Figure H On average, how often, if at all, do you assess or test the security of your business-critical applications?

Figure I On average, how long does it take for your organization to patch/resolve critical security risks/ vulnerabilities for applications already deployed/in use?



With that in mind, organizations need to prioritize their efforts based on Common Vulnerability Scoring System (CVSS) scores and Common Weakness Enumeration (CWE) information, as well as the availability of exploits, not only on "day zero" of a vulnerability disclosure but over the life cycle of the application.

CVSS scores are an industry standard for assessing the severity of a vulnerability. Vulnerabilities in the National Vulnerability Database (NVD) have a base score that aids in calculating severity and can be used as a factor for prioritizing remediation. The CVSS score provides an overall base score that takes both exploitability and impact into account.

Temporal scores consider metrics that change over time owing to events that are external to the vulnerability. Remediation levels (Is there an official fix available?) and report confidence (Is the report confirmed?) can help temper the overall CVSS score to an appropriate level of risk.

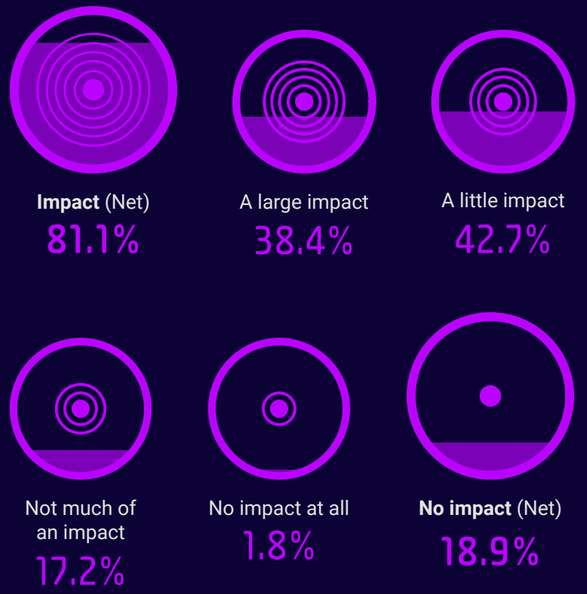
CWE information lists software or hardware weaknesses that have security ramifications. A CWE tells developers which weakness could be exploited if an exploit is available. This information can help security and development teams understand where to focus developer security training, which additional security controls to implement across the SDLC and into production, and adds one more mechanism for assessing risk severity. For example, a development team may prioritize a SQL injection differently than a buffer overflow or denial of service, given the context of the data the application touches, where it is deployed, and other environmental and security factors.

The existence of an exploit will raise the risk score and help teams prioritize the highest-risk vulnerabilities for remediation. Understanding whether there is an existing patch, mitigating factor, or compensating controls is another key piece of information to examine once you have assessed the overall risk. If you have two medium-risk vulnerabilities without exploits available, for example, the final determination of which to fix first might come down to whether either has a patch or workaround available.

Critical security or vulnerability issues in deployed applications tend to cascade downhill, not only through their potential of disrupting an organization's (or its customers') business operations, but also their impact on the entire SDLC, as shown in Figure J.

Issues that might have been minor fixes if they had been caught early in development could mutate into "all hands on deck" firedrills in deployed applications. Automated security testing tools, integrated into IDEs and CI pipelines, can identify vulnerabilities and weaknesses in the code as soon as—or even before—it's committed, enabling developers to address issues before they propagate downstream.

Figure J **How much of an impact, if at all, has addressing a critical security/vulnerability issue had on your organization's software delivery schedule within the past year (2022-2023)?**



Challenges to effective DevSecOps

The shortage of cybersecurity personnel is a significant challenge for DevSecOps, with many organizations unable to fill critical cybersecurity positions, as reflected in Figure K. According to some studies, there are 3.5 million unfilled cybersecurity jobs around the world. As the demand for trained cybersecurity professionals grows, the scarcity of supply is driving up wages for skilled practitioners, pricing out many government entities and SMBs. But, as the top response indicates, inadequate security training for developers/engineers remains the biggest challenge.

One strategy that has shown to be effective to address these issues is the development of a Security Champions program, a collection of people across the organization who show an above-average level of security interest or skill and who are already contributing software security expertise to development, QA, and operations teams. Security champions can act as a sounding board for new projects, and in new or fast-moving technology areas, help combine software security skills with domain knowledge that might be under-represented in security or engineering teams. Agile coaches, scrum masters, and DevOps engineers can make particularly useful security champions, especially for detecting and removing process friction.

Figure K What are the challenges/barriers in implementing DevSecOps at your organization? (Select all that apply)

As noted earlier in this report, AST tools such as SAST, DAST, IAST, and SCA are all widely used by respondents, but effectively aligning those tools to business needs remains a challenge (Figure L).

Many respondents complained that the security testing tools they use do not prioritize resolution based on such factors as exposure, exploitability, and criticality; are too slow to fit into continuous deployment release cycles; and are inaccurate and unreliable.

With no way to consolidate or correlate results from different security tests, security and DevOps teams spend too much time determining what needs to be fixed first—probably one of the reasons why nearly three-quarters of respondents noted that their organizations can take anywhere from two weeks to a month to patch known critical vulnerabilities (Figure I).

Failure to patch quickly affects the bottom line. More than 80% of respondents said that dealing with critical vulnerabilities or related security issues of deployed software impacted their delivery schedules during 2022-23 (Figure J).

The problems of fragmented AST tools and slow remediation are precisely what application security orchestration and correlation (ASOC) and application security posture management (ASPM) are designed to address. Gartner notes that ASOC/ASPM acts as a management layer to orchestrate multiple AST tools, automatically correlating and contextualizing findings to accelerate and focus remediation.

By ingesting results from diverse sources and providing a unified view of risk across the application landscape, ASOC/ASPM enables data-driven prioritization based on business context like criticality and facilitates faster patching of the highest-risk vulnerabilities. By providing visibility into production environments, ASOC/ASPM closes the gap between lengthy remediation times for deployed applications and the reality that most exploits appear within days.

Figure L **What are the major issues with the application security testing tools used in your organization? (Select up to 3)**

Promises and pitfalls of AI

These survey results demonstrate that AI use is already deeply embedded in many organizations' software security initiatives, with over 50% of respondents indicating that they are actively using AI in their DevSecOps practices. Fifty-four percent expect AI to improve the efficiency and accuracy of their security measures. Forty-eight percent hope that AI will help reduce manual review of security testing.

This makes sense when you consider the major advantages AI could potentially provide for DevSecOps. AppSec teams are constantly caught between the need to perform complete and consistent security testing and the need to keep pace with development teams using DevOps methodologies and CI pipelines. When deadlines are tight, it's easy for developers to skip key security risk–assessment procedures.

Survey respondents cited "improve accuracy and efficiency of security measures" (54%) and "reduce the need for manual review and analysis of security data" (48%) as two major benefits they anticipate from introducing AI into the secure SDLC.

Note that respondents also said, however, that they expected AI to "increase the complexity and technical requirements of software security," perhaps anticipating that at some future point, the only entities capable of adequately reviewing AI-generated code may be AI itself.

Figure M **Are you currently using any AI tools to enhance your software security measures?**

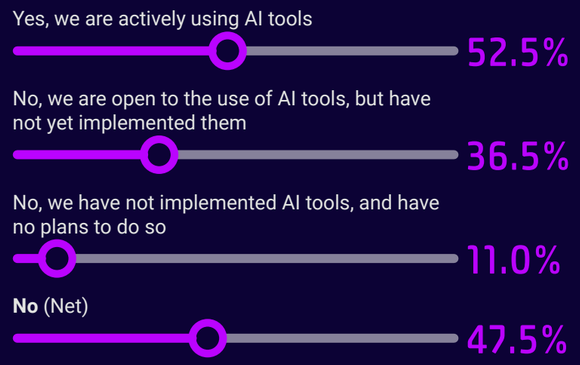
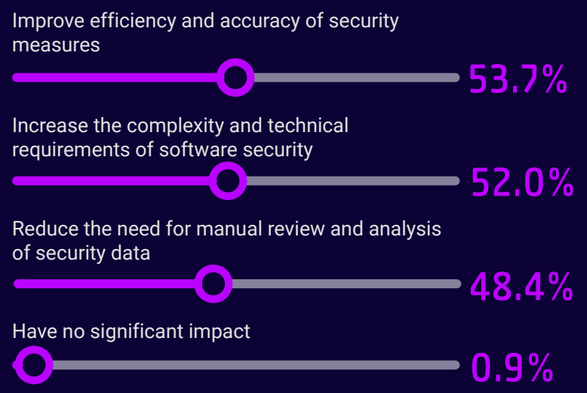


Figure N **How do you expect the use of AI tools to impact your DevSecOps processes and workflows? (Select all that apply)**

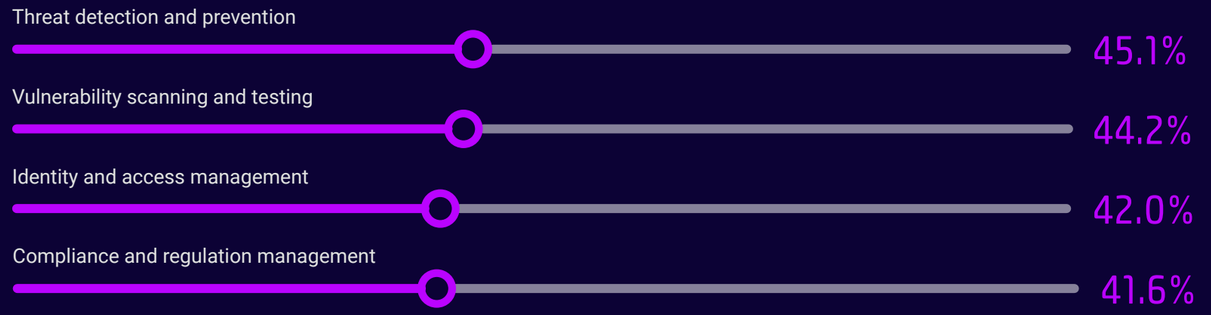


Implementing AI in DevSecOps comes with additional challenges, such as ensuring data quality and addressing security and privacy concerns. As AI tools are more integrated into the DevOps pipeline, they will almost certainly become key targets for security threats. The handling of sensitive data used for AI training can raise privacy issues as well.

One scenario that illustrates potential risks of AI in action is the use of AI-assisted coding, which is generating questions around ownership, copyright, and licensing of the AI-created code.

In late 2022, a class-action lawsuit was filed against GitHub, Microsoft, and OpenAI, claiming that GitHub Copilot—a cloud-based AI tool that offers developers autocomplete-style suggestions as they code—violates both copyright law and software licensing requirements, as well as the rights of the developers whose open source code the Copilot service is trained on. The lawsuit further claims that the code suggested by Copilot uses licensed materials without attribution, copyright notice, or adherence to the original licensing terms.

Figure 0 **What specific areas of software security do you believe AI tools could be most effective in enhancing?**

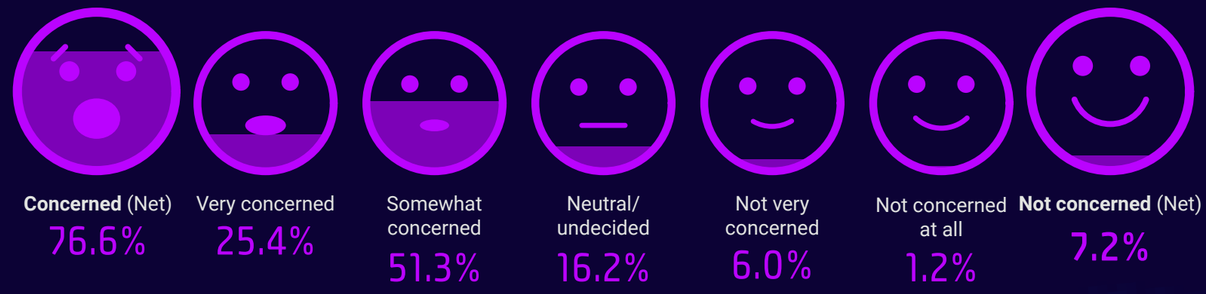


Large language model–based generative AI chatbots such as ChatGPT and Google Bard also have the problem of randomly producing "hallucinations," false responses that may seem credible and confident but are not true—in lay terms, a "lie."

AI hallucinations are a clear danger to software supply chain security. Researchers have found that ChatGPT may recommend a hallucinatory nonexistent code library or package. A malicious actor could create a package with the same name, fill it with malicious code, and then distribute it to unsuspecting developers who follow the AI's recommendations. This could be a game-changer for cybercriminals, allowing them to sidestep more traditional and easily detectable techniques such as typosquatting or masquerading. In fact, the researchers discovered malicious packages created through ChatGPT's hallucinatory recommendations already on popular package installers like PyPI and npm.

That threat isn't theoretical; it's real and happening right now. Whether defending against supply chain attacks originating from AI hallucinations or malicious actors, it's crucial to know your code's origin, authenticate developers and maintainers, and only download from reliable vendors or sources.

Figure P **How concerned, if at all, are you about potential bias or errors in AI-based security solutions?**



Lessons Learned

While most organizations have largely adopted some level of DevSecOps practices, they continue to face barriers to its effective implementation. Two major problem areas emerged from the survey.

- Integrating and aligning the results of multiple application security testing (AST) tools to meet business priorities
- Reducing the time needed to resolve critical vulnerabilities

Twenty-eight percent of respondents said their organizations take as much as three weeks to patch critical security risks/vulnerabilities in deployed applications. Another 20% said it can take up to a month, even as most exploits appear within days. Respondents cited an inability to prioritize vulnerability resolution based on business need as a top complaint they have with AST tools.

As mentioned in the introduction to this report, one of the challenges of developing the survey questions was that term "DevSecOps" embraces several different disciplines, many of which have unique personas. When it comes to "business priorities," the term can mean different things to different personas.

For example, a priority to business leaders is the need to understand how effective their AppSec tools are, and they want complete visibility into process and performance across teams. Development and operations teams want a centralized view of all issues so they can identify the security activities that have the most impact. Those whose focus is on security want to cut through the noise to prioritize critical issues quickly.

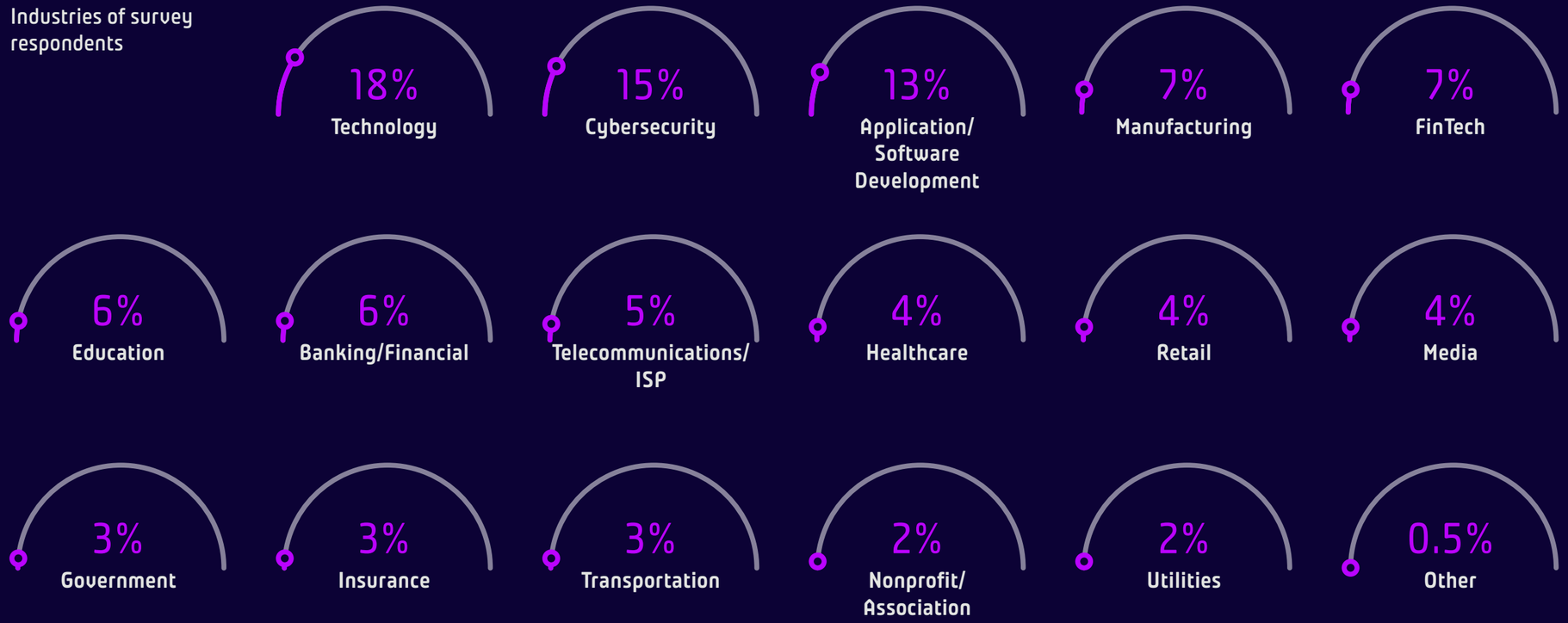
For organizations struggling to gain cohesion across siloed security tools while keeping pace with business demands, application security posture management (ASPM) can provide a needed force multiplier. Automating coordination, context, and prioritization, ASPM allows organizations to focus efforts on the application security business priorities that matter most to them.

- By integrating with development and security testing tools and operations monitoring tools, ASPM offers a single, consolidated view of security-related information from different parts of the organization.
- By correlating and grouping data from different tools analyzing specific applications and vulnerabilities, ASPM can deliver a comprehensive view of the application's overall security stance. DevSecOps groups can produce data relevant to their roles and responsibilities, and ASPM makes it possible to view that data in a way that makes sense to line-of-business managers and others who require a broader perspective.
- ASPM enables the creation and enforcement of security policies for specific applications and the specific risks a vulnerability may pose. When integrated with development or operational infrastructure, ASPM also enables the identification of security issues that require remediation as early in the process as possible.

Using data from 2021, Gartner noted that about 5% of its surveyed organizations had adopted ASPM or the application security orchestration and correlation (ASOC) tools from which they evolved. Gartner expects the pace of adoption to accelerate rapidly, a prediction reflected in these 2023 survey results, which show 28% of respondents using ASOC/ASPM. As Gartner also notes, the early adopters tend to be groups with mature DevSecOps programs and those using multiple security tools, both characteristic of our DevSecOps survey respondents.

The survey explored in this report makes a compelling case that fragmented results from security tools, overloaded teams, and slow vulnerability resolution represent fundamental challenges to successful DevSecOps. For those organizations with diverse DevSecOps teams using multiple application security testing tools, ASPM could be the key to effectively addressing those challenges.

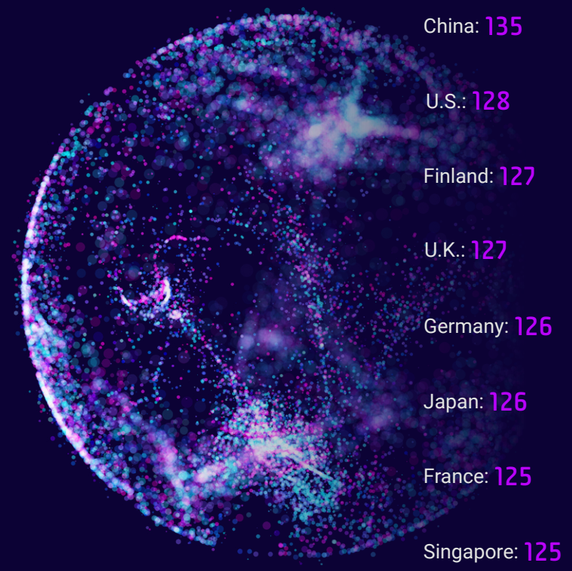
Industries of survey respondents



Job role(s) of respondents

Application Security Architect | Application Security Manager | CISO | Developer | DevOps Engineer | Director, Application Security | Director, Cybersecurity | Director, IT Risk Management | Director, IT Shared Services | Director, Product Security | Director, Security Assurance | Executive Director, Product Security | Incident and Security Manager | Information Assurance Director | Manager, Software Security Engineering | Operations Engineer | Product Security, AppSec | Programmer | QA/Tester/Test Manager | Release Engineer/Manager | Security Administrator/Security Analyst | Security Architect | Security Director | Security Engineering Manager | Senior Director, Product Security | SVP, Product Security and Technology | Technical Lead | VP, Product and Application Security | VP, Security Architecture | VP, Security Compliance

Countries/Number of Respondents



China: 135

U.S.: 128

Finland: 127

U.K.: 127

Germany: 126

Japan: 126

France: 125

Singapore: 125

Software/Apps That the Organization Creates/Manages

Application Software	46%
System Software	44%
Web Applications	42%
Product Software	38%
Artificial Intelligence Software	37%
Engineering/Scientific Software	35%
Embedded Software	31%

Security Practices Followed

Security Risk Management	35%
Continuous Monitoring and Measurement	30%
Configuration Management	30%
Threat Data & Responses	30%
Continuous Deployment	29%
Automated Deployment	29%
Continuous Testing	28%
Application Security Orchestration and Correlation	28%
Continuous Integration	28%
Automated Testing	28%
Infrastructure-as-Code	28%

Organization Size (Employee/Contractor Headcount)

1% More than 100,000	4% 50,001–100,000	7% 15,001–50,000	8% 10,001–15,000	13% 5,001–10,000
12% 2,001–5,000	19% 1,001–2,000	19% 501–1,000	15% 100–500	2% Fewer than 100

Q1. What is your organization's primary industry?

	Global	U.K.	U.S.	France	Finland	Germany	China	Singapore	Japan
Technology	**18.45%**	10.24%	34.38%	14.40%	12.60%	9.52%	42.96%	12.00%	9.52%
Cybersecurity	**14.52%**	17.32%	13.28%	20.00%	14.96%	10.32%	7.41%	18.40%	15.08%
Application/software development	**12.66%**	4.72%	7.03%	20.00%	14.17%	1.59%	26.67%	5.60%	20.63%
Manufacturing	**7.26%**	3.94%	3.13%	4.00%	5.51%	9.52%	13.33%	8.80%	9.52%
Fintech	**6.87%**	6.30%	7.03%	4.80%	10.24%	11.11%	2.22%	8.80%	4.76%
Education	**5.59%**	6.30%	5.47%	7.20%	6.30%	3.97%	0.00%	9.60%	6.35%
Banking/financial	**5.50%**	7.09%	3.91%	5.60%	4.72%	11.11%	0.74%	4.00%	7.14%
Telecommunications/ISP	**5.10%**	5.51%	3.13%	6.40%	8.66%	7.14%	2.22%	3.20%	4.76%
Healthcare	**4.12%**	6.30%	7.03%	4.00%	3.94%	3.17%	1.48%	4.00%	3.17%
Retail	**4.02%**	7.09%	5.47%	4.00%	3.94%	5.56%	0.00%	3.20%	3.17%
Media	**3.63%**	3.15%	2.34%	0.80%	3.94%	5.56%	0.74%	4.80%	7.94%
Government	**3.14%**	5.51%	3.13%	2.40%	3.15%	4.76%	0.74%	4.00%	1.59%
Insurance	**2.85%**	5.51%	3.13%	1.60%	3.15%	4.76%	0.00%	3.20%	1.59%
Transportation	**2.55%**	3.94%	0.00%	3.20%	1.57%	6.35%	0.74%	3.20%	1.59%
Nonprofit/association	**1.67%**	3.94%	0.78%	0.80%	1.57%	3.17%	0.00%	2.40%	0.79%
Utilities	**1.57%**	2.36%	0.78%	0.00%	0.79%	2.38%	0.74%	4.00%	1.59%
Other (Please specify)	**0.49%**	0.79%	0.00%	0.80%	0.79%	0.00%	0.00%	0.80%	0.79%

Q2. How large is your organization, including both employee and contractor staff?

	Global	U.K.	U.S.	France	Finland	Germany	China	Singapore	Japan
Fewer than 100, please specify	**1.57%**	1.57%	0.00%	2.40%	0.00%	0.00%	3.70%	1.60%	3.17%
100–500	**15.11%**	11.02%	16.41%	20.80%	12.60%	19.05%	14.81%	6.40%	19.84%
501–1,000	**19.04%**	14.96%	23.44%	23.20%	14.96%	21.43%	8.89%	16.00%	30.16%
1,001–2,000	**18.65%**	15.75%	17.19%	15.20%	19.69%	15.87%	37.78%	16.00%	10.32%
2,001–5,000	**12.37%**	22.83%	10.94%	16.00%	18.11%	7.14%	5.93%	8.80%	9.52%
5,001–10,000	**13.05%**	18.11%	11.72%	7.20%	15.75%	6.35%	20.00%	17.60%	7.14%
10,001–15,000	**8.44%**	10.24%	9.38%	3.20%	8.66%	5.56%	2.96%	16.80%	11.11%
15,001–50,000	**6.67%**	3.94%	4.69%	4.00%	6.30%	17.46%	0.74%	10.40%	6.35%
50,001–100,000	**4.42%**	1.57%	5.47%	4.00%	3.15%	7.14%	5.19%	6.40%	2.38%
More than 100,000, please specify	**0.69%**	0.00%	0.78%	4.00%	0.79%	0.00%	0.00%	0.00%	0.00%

Q3. What types of software/applications does your organization create or manage? (Select all that apply)

	Global	U.K.	U.S.	France	Finland	Germany	China	Singapore	Japan
Application software	**46.03%**	40.94%	61.72%	48.00%	37.01%	34.13%	70.37%	36.80%	37.30%
System software	**44.06%**	42.52%	54.69%	40.00%	30.71%	34.92%	67.41%	39.20%	41.27%
Web applications	**41.71%**	27.56%	45.31%	40.80%	44.09%	37.30%	68.89%	39.20%	28.57%
Product software	**38.27%**	29.13%	47.66%	28.80%	39.37%	30.16%	65.19%	30.40%	33.33%
Artificial intelligence software	**36.60%**	30.71%	41.41%	32.00%	32.28%	33.33%	57.04%	35.20%	29.37%
Engineering/scientific software	**35.23%**	25.20%	39.84%	27.20%	31.50%	38.89%	57.04%	30.40%	30.16%
Embedded software	**30.91%**	29.13%	34.38%	20.80%	29.92%	30.16%	42.22%	29.60%	30.16%
Other, please specify	**0.20%**	0.79%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.79%

Q4. What practices does your organization follow? (Select all that apply)

	Global	U.K.	U.S.	France	Finland	Germany	China	Singapore	Japan
Security risk management	**35.13%**	35.43%	40.63%	33.60%	32.28%	19.84%	56.30%	32.80%	28.57%
Continuous monitoring and measurement	**29.93%**	25.20%	34.38%	29.60%	32.28%	22.22%	44.44%	25.60%	24.60%
Configuration management	**29.64%**	19.69%	31.25%	24.80%	23.62%	23.02%	49.63%	30.40%	33.33%
Threat data & responses	**29.34%**	22.83%	39.84%	31.20%	28.35%	19.84%	41.48%	27.20%	23.02%
Continuous deployment	**29.05%**	27.56%	35.16%	21.60%	29.13%	28.57%	41.48%	20.80%	26.98%
Automated deployment	**28.56%**	18.90%	28.91%	32.80%	28.35%	23.81%	48.15%	24.80%	21.43%
Continuous testing	**28.46%**	22.05%	32.03%	24.80%	30.71%	23.02%	48.15%	17.60%	27.78%
Application security orchestration and correlation	**28.36%**	29.13%	39.84%	20.00%	19.69%	18.25%	51.85%	28.00%	18.25%
Continuous integration	**28.16%**	23.62%	30.47%	24.80%	25.98%	19.84%	47.41%	28.00%	23.81%
Automated testing	**27.87%**	19.69%	33.59%	28.00%	24.41%	15.08%	48.15%	20.00%	32.54%
Infrastructure-as-code	**27.58%**	23.62%	41.41%	22.40%	20.47%	22.22%	48.15%	25.60%	15.08%
Other (Please specify)	**0.10%**	0.00%	0.00%	0.00%	0.79%	0.00%	0.00%	0.00%	0.00%

Q5. How useful, if at all, are the following application security tools, practices, or techniques that you use in your organization?

Defining security requirements as part of SDLC requirements stage	Global	U.K.	U.S.	France	Finland	Germany	China	Singapore	Japan
Useful (Net)	**71.25%**	**66.93%**	**78.91%**	**73.60%**	**81.10%**	**62.70%**	**97.04%**	**55.20%**	**52.38%**
Very useful	**32.09%**	25.20%	46.88%	32.00%	35.43%	24.60%	54.07%	17.60%	19.05%
Somewhat useful	**39.16%**	41.73%	32.03%	41.60%	45.67%	38.10%	42.96%	37.60%	33.33%
Not that useful	**16.78%**	15.75%	12.50%	16.80%	13.39%	20.63%	2.96%	26.40%	26.98%
Not at all useful	**7.56%**	11.02%	3.13%	8.00%	3.15%	11.90%	0.00%	14.40%	9.52%
Not useful (Net)	**24.34%**	**26.77%**	**15.63%**	**24.80%**	**16.54%**	**32.54%**	**2.96%**	**40.80%**	**36.51%**
N/A	**4.42%**	6.30%	5.47%	1.60%	2.36%	4.76%	0.00%	4.00%	11.11%

Formal measurement of your software security through models such as BSIMM, SAMM, etc.	Global	U.K.	U.S.	France	Finland	Germany	China	Singapore	Japan
Useful (Net)	**69.38%**	**55.91%**	**79.69%**	**71.20%**	**70.87%**	**57.94%**	**94.81%**	**67.20%**	**55.56%**
Very useful	**33.56%**	24.41%	47.66%	25.60%	30.71%	26.98%	57.04%	28.80%	25.40%
Somewhat useful	**35.82%**	31.50%	32.03%	45.60%	40.16%	30.95%	37.78%	38.40%	30.16%
Not that useful	**18.06%**	25.20%	10.94%	17.60%	25.20%	23.02%	3.70%	16.80%	23.02%
Not at all useful	**8.44%**	11.81%	7.03%	8.80%	2.36%	16.67%	0.74%	10.40%	10.32%
Not useful (Net)	**26.50%**	**37.01%**	**17.97%**	**26.40%**	**27.56%**	**39.68%**	**4.44%**	**27.20%**	**33.33%**
N/A	**4.12%**	7.09%	2.34%	2.40%	1.57%	2.38%	0.74%	5.60%	11.11%

Automated scanning of code for security vulnerabilities and other defects (e.g., static application security testing (SAST)	Global	U.K.	U.S.	France	Finland	Germany	China	Singapore	Japan
Useful (Net)	**71.54%**	**62.20%**	**76.56%**	**76.00%**	**78.74%**	**65.87%**	**94.07%**	**54.40%**	**62.70%**
Very useful	**34.35%**	29.13%	46.09%	33.60%	38.58%	27.78%	54.07%	21.60%	22.22%
Somewhat useful	**37.19%**	33.07%	30.47%	42.40%	40.16%	38.10%	40.00%	32.80%	40.48%
Not that useful	**17.37%**	22.05%	10.94%	16.80%	18.11%	17.46%	5.93%	29.60%	19.05%
Not at all useful	**7.65%**	13.39%	8.59%	5.60%	2.36%	11.90%	0.00%	12.80%	7.14%
Not useful (Net)	**25.02%**	**35.43%**	**19.53%**	**22.40%**	**20.47%**	**29.37%**	**5.93%**	**42.40%**	**26.19%**
N/A	**3.43%**	2.36%	3.91%	1.60%	0.79%	4.76%	0.00%	3.20%	11.11%

Open source/third-party dependency analysis (SCA)	Global	U.K.	U.S.	France	Finland	Germany	China	Singapore	Japan
Useful (Net)	**67.62%**	**50.39%**	**75.00%**	**73.60%**	**74.80%**	**61.11%**	**94.81%**	**53.60%**	**55.56%**
Very useful	**30.32%**	22.05%	33.59%	32.00%	30.71%	23.81%	60.74%	20.00%	17.46%
Somewhat useful	**37.29%**	28.35%	41.41%	41.60%	44.09%	37.30%	34.07%	33.60%	38.10%
Not that useful	**19.73%**	25.98%	16.41%	18.40%	22.05%	22.22%	5.19%	27.20%	21.43%
Not at all useful	**8.34%**	14.17%	5.47%	6.40%	1.57%	11.90%	0.00%	12.80%	15.08%
Not useful (Net)	**28.07%**	**40.16%**	**21.88%**	**24.80%**	**23.62%**	**34.13%**	**5.19%**	**40.00%**	**36.51%**
N/A	**4.32%**	9.45%	3.13%	1.60%	1.57%	4.76%	0.00%	6.40%	7.94%

Internal or third-party penetration testing	Global	U.K.	U.S.	France	Finland	Germany	China	Singapore	Japan
Useful (Net)	**67.91%**	**53.54%**	**71.88%**	**72.00%**	**80.31%**	**56.35%**	**96.30%**	**54.40%**	**56.35%**
Very useful	**30.23%**	18.11%	37.50%	35.20%	43.31%	23.02%	48.89%	17.60%	16.67%
Somewhat useful	**37.68%**	35.43%	34.38%	36.80%	37.01%	33.33%	47.41%	36.80%	39.68%
Not that useful	**19.33%**	29.13%	19.53%	16.80%	16.54%	20.63%	3.70%	24.80%	24.60%
Not at all useful	**8.64%**	10.24%	7.03%	7.20%	3.15%	17.46%	0.00%	15.20%	9.52%
Not useful (Net)	**27.97%**	**39.37%**	**26.56%**	**24.00%**	**19.69%**	**38.10%**	**3.70%**	**40.00%**	**34.13%**
N/A	**4.12%**	7.09%	1.56%	4.00%	0.00%	5.56%	0.00%	5.60%	9.52%

Fuzz testing	Global	U.K.	U.S.	France	Finland	Germany	China	Singapore	Japan
Useful (Net)	**62.32%**	**50.39%**	**75.00%**	**58.40%**	**68.50%**	**53.97%**	**88.15%**	**55.20%**	**46.83%**
Very useful	**25.02%**	19.69%	35.94%	17.60%	23.62%	27.78%	42.96%	18.40%	12.70%
Somewhat useful	**37.29%**	30.71%	39.06%	40.80%	44.88%	26.19%	45.19%	36.80%	34.13%
Not that useful	**19.73%**	18.90%	12.50%	22.40%	18.90%	23.02%	10.37%	25.60%	26.98%
Not at all useful	**9.52%**	14.96%	4.69%	4.80%	9.45%	18.25%	0.74%	12.00%	11.90%
Not useful (Net)	**29.24%**	**33.86%**	**17.19%**	**27.20%**	**28.35%**	**41.27%**	**11.11%**	**37.60%**	**38.89%**
N/A	**8.44%**	15.75%	7.81%	14.40%	3.15%	4.76%	0.74%	7.20%	14.29%

Q6. How useful, if at all, are the following application security tools, practices, or techniques that you use in your organization?

Dynamic application security testing (DAST)	Global	U.K.	U.S.	France	Finland	Germany	China	Singapore	Japan
Useful (Net)	**67.12%**	48.82%	74.22%	76.80%	74.80%	62.70%	91.11%	49.60%	57.14%
Very useful	**29.44%**	16.54%	38.28%	36.80%	29.92%	27.78%	46.67%	20.00%	18.25%
Somewhat useful	**37.68%**	32.28%	35.94%	40.00%	44.88%	34.92%	44.44%	29.60%	38.89%
Not that useful	**19.63%**	32.28%	16.41%	16.80%	17.32%	20.63%	7.41%	28.80%	18.25%
Not at all useful	**9.62%**	12.60%	6.25%	5.60%	6.30%	12.70%	0.74%	18.40%	15.08%
Not useful (Net)	**29.24%**	44.88%	22.66%	22.40%	23.62%	33.33%	8.15%	47.20%	33.33%
N/A	**3.63%**	6.30%	3.13%	0.80%	1.57%	3.97%	0.74%	3.20%	9.52%

Interactive application security testing (IAST)	Global	U.K.	U.S.	France	Finland	Germany	China	Singapore	Japan
Useful (Net)	**68.50%**	60.63%	72.66%	75.20%	77.17%	53.97%	96.30%	53.60%	56.35%
Very useful	**31.11%**	22.05%	35.16%	34.40%	37.01%	18.25%	54.07%	24.00%	22.22%
Somewhat useful	**37.39%**	38.58%	37.50%	40.80%	40.16%	35.71%	42.22%	29.60%	34.13%
Not that useful	**18.06%**	18.11%	20.31%	15.20%	18.11%	21.43%	3.70%	24.80%	23.81%
Not at all useful	**9.62%**	14.17%	6.25%	9.60%	3.15%	18.25%	0.00%	14.40%	11.90%
Not useful (Net)	**27.67%**	32.28%	26.56%	24.80%	21.26%	39.68%	3.70%	39.20%	35.71%
N/A	**3.83%**	7.09%	0.78%	0.00%	1.57%	6.35%	0.00%	7.20%	7.94%

Web application firewall (WAF)	Global	U.K.	U.S.	France	Finland	Germany	China	Singapore	Japan
Useful (Net)	**68.99%**	62.99%	78.13%	66.40%	78.74%	55.56%	97.78%	51.20%	58.73%
Very useful	**33.17%**	33.86%	39.84%	32.00%	36.22%	21.43%	52.59%	21.60%	26.19%
Somewhat useful	**35.82%**	29.13%	38.28%	34.40%	42.52%	34.13%	45.19%	29.60%	32.54%
Not that useful	**18.25%**	19.69%	14.84%	20.00%	15.75%	23.02%	2.22%	32.80%	19.05%
Not at all useful	**8.73%**	11.02%	6.25%	10.40%	3.94%	14.29%	0.00%	12.80%	11.90%
Not useful (Net)	**26.99%**	30.71%	21.09%	30.40%	19.69%	37.30%	2.22%	45.60%	30.95%
N/A	**4.02%**	6.30%	0.78%	3.20%	1.57%	7.14%	0.00%	3.20%	10.32%

Container security testing	Global	U.K.	U.S.	France	Finland	Germany	China	Singapore	Japan
Useful (Net)	**66.93%**	48.82%	79.69%	73.60%	74.80%	57.94%	91.11%	57.60%	50.00%
Very useful	**29.93%**	20.47%	38.28%	29.60%	39.37%	24.60%	49.63%	21.60%	14.29%
Somewhat useful	**37.00%**	28.35%	41.41%	44.00%	35.43%	33.33%	41.48%	36.00%	35.71%
Not that useful	**18.65%**	29.13%	13.28%	14.40%	17.32%	19.84%	6.67%	24.00%	25.40%
Not at all useful	**9.42%**	14.96%	3.91%	8.80%	6.30%	18.25%	1.48%	12.80%	9.52%
Not useful (Net)	**28.07%**	44.09%	17.19%	23.20%	23.62%	38.10%	8.15%	36.80%	34.92%
N/A	**5.00%**	7.09%	3.13%	3.20%	1.57%	3.97%	0.74%	5.60%	15.08%

Use of vulnerability/risk management tool (e.g., XDR, SRM, etc.)	Global	U.K.	U.S.	France	Finland	Germany	China	Singapore	Japan
Useful (Net)	**69.77%**	58.27%	82.81%	74.40%	74.02%	57.14%	97.78%	53.60%	57.94%
Very useful	**32.58%**	24.41%	47.66%	35.20%	41.73%	22.22%	50.37%	20.00%	17.46%
Somewhat useful	**37.19%**	33.86%	35.16%	39.20%	32.28%	34.92%	47.41%	33.60%	40.48%
Not that useful	**17.86%**	21.26%	8.59%	19.20%	22.05%	19.05%	1.48%	27.20%	25.40%
Not at all useful	**9.62%**	16.54%	7.03%	5.60%	1.57%	20.63%	0.74%	16.00%	9.52%
Not useful (Net)	**27.48%**	37.80%	15.63%	24.80%	23.62%	39.68%	2.22%	43.20%	34.92%
N/A	**2.75%**	3.94%	1.56%	0.80%	2.36%	3.17%	0.00%	3.20%	7.14%

Remediation prioritization	Global	U.K.	U.S.	France	Finland	Germany	China	Singapore	Japan
Useful (Net)	**67.12%**	53.54%	82.81%	67.20%	71.65%	53.97%	96.30%	56.80%	52.38%
Very useful	**29.83%**	21.26%	40.63%	24.80%	36.22%	21.43%	54.07%	21.60%	16.67%
Somewhat useful	**37.29%**	32.28%	42.19%	42.40%	35.43%	32.54%	42.22%	35.20%	35.71%
Not that useful	**18.45%**	28.35%	7.81%	19.20%	22.05%	19.84%	3.70%	24.00%	23.81%
Not at all useful	**9.91%**	9.45%	7.03%	10.40%	5.51%	17.46%	0.00%	12.00%	18.25%
Not useful (Net)	**28.36%**	37.80%	14.84%	29.60%	27.56%	37.30%	3.70%	36.00%	42.06%
N/A	**4.51%**	8.66%	2.34%	3.20%	0.79%	8.73%	0.00%	7.20%	5.56%

Software supply chain management/monitoring	Global	U.K.	U.S.	France	Finland	Germany	China	Singapore	Japan
Useful (Net)	**69.28%**	59.84%	72.66%	71.20%	77.95%	58.73%	95.56%	56.00%	60.32%
Very useful	**32.29%**	24.41%	36.72%	33.60%	32.28%	25.40%	57.04%	19.20%	27.78%
Somewhat useful	**37.00%**	35.43%	35.94%	37.60%	45.67%	33.33%	38.52%	36.80%	32.54%
Not that useful	**18.84%**	22.83%	17.19%	17.60%	18.11%	23.81%	3.70%	31.20%	17.46%
Not at all useful	**8.34%**	11.81%	7.81%	10.40%	1.57%	10.32%	0.74%	11.20%	13.49%
Not useful (Net)	**27.18%**	34.65%	25.00%	28.00%	19.69%	34.13%	4.44%	42.40%	30.95%
N/A	**3.53%**	5.51%	2.34%	0.80%	2.36%	7.14%	0.00%	1.60%	8.73%

Q7. How would you best describe the maturity of your current software security program/initiative?

	Global	U.K.	U.S.	France	Finland	Germany	China	Singapore	Japan
Level I: Unstructured/disorganized.	**8.54%**	11.02%	3.91%	4.80%	11.02%	12.70%	2.22%	10.40%	12.70%
Level II: Security processes are documented and repeatable for specific team.	**24.14%**	28.35%	23.44%	16.00%	29.13%	26.19%	9.63%	34.40%	26.98%
Level III: Level II processes and procedures are standardized across organization. A proactive security culture is endorsed and communicated by leadership.	**34.25%**	33.07%	38.28%	40.00%	35.43%	36.51%	21.48%	33.60%	36.51%
Level IV: Security processes and controls are logged, managed, and monitored.	**24.53%**	22.05%	20.31%	28.00%	14.96%	21.43%	48.89%	20.00%	19.05%
Level V: Security processes are continuously analyzed and improved.	**8.54%**	5.51%	14.06%	11.20%	9.45%	3.17%	17.78%	1.60%	4.76%
Other (Please specify)	**0.00%**	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%

Q8. On average, how often, if at all, do you assess or test the security of your business-critical applications?

	Global	U.K.	U.S.	France	Finland	Germany	China	Singapore	Japan
Every day	**7.07%**	3.94%	8.59%	19.20%	4.72%	3.17%	3.70%	2.40%	11.11%
4-6 days a week	**17.17%**	15.75%	16.41%	15.20%	11.81%	11.11%	37.04%	11.20%	17.46%
2-3 days a week	**20.41%**	18.90%	21.09%	28.00%	14.96%	20.63%	27.41%	14.40%	17.46%
Once a week	**16.98%**	16.54%	15.63%	14.40%	18.11%	16.67%	17.78%	19.20%	17.46%
Once every 2 to 3 weeks	**11.09%**	11.02%	12.50%	5.60%	18.11%	12.70%	5.19%	14.40%	9.52%
Once a month	**7.16%**	6.30%	4.69%	5.60%	12.60%	7.94%	5.19%	5.60%	9.52%
Once every 2 months	**7.46%**	7.87%	7.81%	3.20%	11.02%	3.97%	2.22%	18.40%	5.56%
Once every 3 to 5 months	**6.38%**	7.87%	10.16%	5.60%	3.15%	7.14%	1.48%	7.20%	8.73%
Once every 6 to 11 months	**4.42%**	7.87%	2.34%	1.60%	4.72%	10.32%	0.00%	6.40%	2.38%
Once a year	**1.67%**	2.36%	0.78%	1.60%	0.79%	6.35%	0.00%	0.80%	0.79%
Less than once a year, please specify	**0.00%**	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%
Never	**0.20%**	1.57%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%

Q9. How do you assess or test the security of your business-critical applications? (Select all that apply)

	Global	U.K.	U.S.	France	Finland	Germany	China	Singapore	Japan
Combination of both manual and automated assessments	**52.61%**	50.40%	65.63%	44.80%	50.39%	51.59%	68.89%	47.20%	40.48%
External pen testing	**44.15%**	37.60%	39.06%	40.00%	43.31%	47.62%	63.70%	45.60%	34.92%
Automated assessments and testing	**43.66%**	40.00%	46.88%	39.20%	42.52%	45.24%	68.15%	29.60%	35.71%
Manual assessments and/or tests (excluding pen testing)	**43.07%**	36.00%	46.88%	37.60%	46.46%	44.44%	58.52%	33.60%	39.68%
Unknown/Unsure	**0.20%**	0.00%	0.00%	0.80%	0.79%	0.00%	0.00%	0.00%	0.00%
Other (Please specify)	**0.00%**	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%

Q10. How much of an impact, if at all, has addressing a critical security/vulnerability issue had on your organization's software delivery schedule within the past year (2022-2023)?

	Global	U.K.	U.S.	France	Finland	Germany	China	Singapore	Japan
Impact (Net)	**81.06%**	**72.44%**	**86.72%**	**80.00%**	**92.91%**	**89.68%**	**79.26%**	**80.80%**	**66.67%**
A large impact	**38.37%**	24.41%	41.41%	33.60%	33.86%	54.76%	60.74%	24.80%	31.75%
A little impact	**42.69%**	48.03%	45.31%	46.40%	59.06%	34.92%	18.52%	56.00%	34.92%
Not much of an impact	**17.17%**	25.20%	12.50%	17.60%	7.09%	7.94%	20.00%	18.40%	28.57%
No impact at all	**1.77%**	2.36%	0.78%	2.40%	0.00%	2.38%	0.74%	0.80%	4.76%
No impact (Net)	**18.94%**	**27.56%**	**13.28%**	**20.00%**	**7.09%**	**10.32%**	**20.74%**	**19.20%**	**33.33%**

Q11. Who is responsible for conducting security testing in your organization? (Select all that apply)

	Global	U.K.	U.S.	France	Finland	Germany	China	Singapore	Japan
Internal security team	**46.03%**	39.37%	50.00%	36.80%	41.73%	38.89%	67.41%	46.40%	46.03%
Developers/software engineers	**45.14%**	34.65%	53.13%	33.60%	44.88%	42.86%	63.70%	44.00%	42.86%
QA/test teams	**37.59%**	41.73%	35.94%	32.80%	33.86%	38.89%	51.11%	34.40%	30.95%
Cross-functional DevSecOps teams	**35.53%**	31.50%	44.53%	28.80%	39.37%	30.95%	48.15%	32.00%	27.78%
External consultants	**32.88%**	29.92%	46.09%	28.00%	28.35%	38.10%	32.59%	31.20%	28.57%
Unsure	**0.10%**	0.00%	0.00%	0.00%	0.00%	0.79%	0.00%	0.00%	0.00%
Other (Please specify)	**0.00%**	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%

Q12. On average, how long does it take for your organization to patch/resolve critical security risks/vulnerabilities for applications already deployed/in use?

	Global	U.K.	U.S.	France	Finland	Germany	China	Singapore	Japan
Up to one week, please specify in days	**4.61%**	0.00%	7.81%	11.20%	5.51%	0.00%	6.67%	3.20%	2.38%
Over one week, up to two weeks	**26.40%**	14.96%	21.88%	40.80%	25.98%	14.29%	57.04%	10.40%	23.81%
Over two weeks, up to three weeks	**28.26%**	33.86%	28.91%	24.80%	26.77%	23.02%	29.63%	28.00%	30.95%
Over three weeks, up to one month	**19.92%**	22.83%	19.53%	16.00%	21.26%	32.54%	4.44%	26.40%	17.46%
Over one month, up to two months	**8.44%**	9.45%	5.47%	3.20%	11.81%	11.90%	1.48%	14.40%	10.32%
Over two months, up to four months	**5.50%**	3.94%	5.47%	3.20%	4.72%	11.11%	0.74%	8.80%	6.35%
Over four months, up to six months	**4.71%**	9.45%	10.16%	0.80%	1.57%	4.76%	0.00%	8.00%	3.17%
Over six months, please specify in months	**0.00%**	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%
Unsure	**2.16%**	5.51%	0.78%	0.00%	2.36%	2.38%	0.00%	0.80%	5.56%

Q13. What are the major KPIs you use to measure the success of your DevSecOps activities? (Select up to 3)

	Global	U.K.	U.S.	France	Finland	Germany	China	Singapore	Japan
Number of open security vulnerabilities	**28.95%**	27.56%	32.81%	28.80%	27.56%	24.60%	40.00%	26.40%	23.02%
Reduction of security-related discoveries late in the development process	**28.26%**	33.07%	33.59%	24.00%	24.41%	29.37%	30.37%	30.40%	20.63%
Issue resolution time	**27.58%**	24.41%	30.47%	28.00%	24.41%	23.02%	31.11%	25.60%	33.33%
Reduction in hours spent resolving security issues	**27.38%**	27.56%	30.47%	24.00%	21.26%	34.13%	32.59%	24.80%	23.81%
Reduction in security-related build delays	**26.50%**	25.98%	28.91%	28.80%	26.77%	19.84%	27.41%	26.40%	27.78%
Reduction in security-failed builds	**24.44%**	22.05%	24.22%	21.60%	25.20%	27.78%	25.93%	25.60%	23.02%
Compliance KPIs (percentage of audits passed, etc.)	**23.75%**	30.71%	28.91%	17.60%	22.83%	26.98%	24.44%	23.20%	15.08%
Customer ticket volume	**22.77%**	29.13%	28.91%	25.60%	21.26%	22.22%	15.56%	25.60%	14.29%
Defect Escape Rate	**22.28%**	22.83%	17.19%	16.00%	30.71%	23.81%	28.15%	17.60%	21.43%
There are no major KPIs we use to measure the success of our DevSecOps activities	**1.08%**	0.00%	0.00%	0.00%	1.57%	0.00%	0.00%	0.80%	6.35%
Other, please specify	**0.00%**	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%

Q14. What are the challenges/barriers in implementing DevSecOps at your organization, if any? (Select all that apply)

	Global	U.K.	U.S.	France	Finland	Germany	China	Singapore	Japan
Inadequate/ineffective security training for developers/engineers	**33.86%**	33.07%	42.97%	27.20%	31.50%	35.71%	32.59%	35.20%	32.54%
Shortage of application security personnel/skills	**31.40%**	25.98%	29.69%	28.80%	23.62%	31.75%	46.67%	32.80%	30.95%
Lack of transparency into development/operations work	**31.31%**	27.56%	37.50%	28.80%	35.43%	29.37%	36.30%	28.00%	26.98%
Continuously changing requirements and priorities	**30.42%**	25.20%	30.47%	27.20%	29.13%	27.78%	43.70%	32.80%	26.19%
Insufficient budget/funding for security programs and tools	**29.44%**	30.71%	39.06%	32.80%	37.01%	23.02%	22.96%	21.60%	28.57%
Organizational silos between development, operations, security	**29.05%**	31.50%	42.19%	24.80%	28.35%	29.37%	29.63%	22.40%	23.81%
Lack of coding skills in security teams	**28.95%**	24.41%	30.47%	26.40%	31.50%	30.95%	28.89%	29.60%	29.37%
There are no challenges/barriers	**2.06%**	4.72%	3.13%	1.60%	2.36%	0.79%	1.48%	0.00%	2.38%
Other, please specify	**0.00%**	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%

Q15. What are the major issues with the application security testing tools used in your organization? (Select up to 3)

	Global	U.K.	U.S.	France	Finland	Germany	China	Singapore	Japan
Tool(s) do not prioritize resolution based on exposure, exploitability, and criticality	**34.74%**	35.43%	41.41%	40.00%	37.01%	34.13%	35.56%	22.40%	31.75%
Too slow to fit into rapid release cycles/continuous deployment	**34.15%**	26.77%	42.97%	33.60%	28.35%	30.16%	47.41%	40.00%	23.02%
Cost vs. ROI	**33.46%**	29.92%	34.38%	32.00%	38.58%	34.92%	33.33%	30.40%	34.13%
Inaccuracy/unreliability	**33.07%**	25.20%	39.84%	28.80%	36.22%	33.33%	31.85%	32.00%	37.30%
High number of false positives	**32.19%**	38.58%	39.06%	21.60%	31.50%	35.71%	29.63%	36.00%	25.40%
No way to consolidate/correlate results from different tools	**28.95%**	23.62%	28.91%	22.40%	26.77%	30.95%	34.07%	28.00%	36.51%
There are no major issues	**3.14%**	6.30%	3.13%	4.00%	2.36%	0.00%	5.19%	0.00%	3.97%
Other (Please specify)	**0.00%**	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%

Q16. What do you consider to be the top factors that have contributed to a security program's success? (Select up to 3)

	Global	U.K.	U.S.	France	Finland	Germany	China	Singapore	Japan
Enforcing security/compliance policies through infrastructure-as-code	**33.56%**	36.22%	37.50%	39.20%	26.77%	26.98%	40.74%	29.60%	30.95%
Developing security champions in Dev and Ops teams	**32.58%**	22.05%	39.06%	32.80%	28.35%	38.89%	28.15%	40.00%	31.75%
Improving communications across Dev, Ops, and Security teams	**32.48%**	34.65%	42.97%	27.20%	31.50%	34.13%	32.59%	34.40%	22.22%
Integrating automated security testing into build/deploy workflows	**32.29%**	28.35%	36.72%	32.00%	36.22%	33.33%	32.59%	28.00%	30.95%
Minimizing time/cost to fix vulnerabilities through automation	**30.03%**	32.28%	31.25%	31.20%	23.62%	27.78%	40.74%	27.20%	25.40%
Creating cross-functional DevSecOps teams	**28.95%**	29.92%	32.03%	21.60%	37.01%	28.57%	35.56%	26.40%	19.84%
Training developers/engineers in secure coding	**27.58%**	25.20%	28.91%	20.80%	35.43%	26.98%	33.33%	21.60%	27.78%
I don't consider there to be any top factors	**0.79%**	2.36%	0.00%	0.80%	0.00%	0.79%	0.74%	0.00%	1.59%
Other (Please specify)	**0.00%**	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%

Q17. Are you currently using any AI tools to enhance your software security measures?

	Global	U.K.	U.S.	France	Finland	Germany	China	Singapore	Japan
Yes, we are actively using AI tools	**52.50%**	38.58%	64.06%	47.20%	47.24%	69.84%	57.04%	47.20%	48.41%
No, we are open to the use of AI tools, but have not yet implemented them	**36.51%**	39.37%	23.44%	42.40%	47.24%	22.22%	40.00%	35.20%	42.06%
No, we have not implemented AI tools, and have no plans to do so	**10.99%**	22.05%	12.50%	10.40%	5.51%	7.94%	2.96%	17.60%	9.52%
No (Net)	**47.50%**	**61.42%**	**35.94%**	**52.80%**	**52.76%**	**30.16%**	**42.96%**	**52.80%**	**51.59%**

Q18. How do you expect the use of AI tools to impact your DevSecOps processes and workflows? (Select all that apply)

	Global	U.K.	U.S.	France	Finland	Germany	China	Singapore	Japan
Improve efficiency and accuracy of security measures	**53.69%**	51.52%	58.93%	49.11%	44.17%	43.97%	68.70%	57.28%	54.39%
Increase the complexity and technical requirements of software security	**52.04%**	51.52%	64.29%	42.86%	50.83%	54.31%	61.83%	47.57%	41.23%
Reduce the need for manual review and analysis of security data	**48.40%**	50.51%	45.54%	42.86%	50.83%	45.69%	64.12%	42.72%	42.11%
Have no significant impact	**0.88%**	0.00%	0.00%	0.89%	0.83%	2.59%	0.00%	0.00%	2.63%
Other (please specify)	**0.00%**	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%

Q19. What specific areas of software security do you believe AI tools could be most effective in enhancing?

	Global	U.K.	U.S.	France	Finland	Germany	China	Singapore	Japan
Threat detection and prevention	**45.09%**	42.42%	50.00%	46.43%	46.67%	41.38%	44.27%	46.60%	42.98%
Vulnerability scanning and testing	**44.21%**	39.39%	46.43%	45.54%	46.67%	37.07%	52.67%	42.72%	41.23%
Identity and access management	**42.01%**	43.43%	50.00%	44.64%	38.33%	37.93%	54.20%	33.98%	31.58%
Compliance and regulation management	**41.57%**	47.47%	46.43%	31.25%	42.50%	36.21%	45.04%	37.86%	45.61%
Other (please specify)	**0.00%**	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%

Q20. How concerned, if at all, are you about potential bias or errors in AI-based security solutions?

	Global	U.K.	U.S.	France	Finland	Germany	China	Singapore	Japan
Concerned (Net)	**76.63%**	**76.77%**	**83.93%**	**74.11%**	**77.50%**	**84.48%**	**55.73%**	**82.52%**	**81.58%**
Very concerned	**25.36%**	27.27%	33.04%	16.96%	15.83%	50.00%	7.63%	28.16%	27.19%
Somewhat concerned	**51.27%**	49.49%	50.89%	57.14%	61.67%	34.48%	48.09%	54.37%	54.39%
Neutral/undecided	**16.21%**	15.15%	10.71%	22.32%	18.33%	8.62%	28.24%	12.62%	11.40%
Not very concerned	**5.95%**	6.06%	4.46%	2.68%	3.33%	6.03%	13.74%	3.88%	6.14%
Not concerned at all	**1.21%**	2.02%	0.89%	0.89%	0.83%	0.86%	2.29%	0.97%	0.88%
Not concerned (Net)	**7.17%**	**8.08%**	**5.36%**	**3.57%**	**4.17%**	**6.90%**	**16.03%**	**4.85%**	**7.02%**

The Synopsys difference

Synopsys provides integrated solutions that transform the way you build and deliver software, accelerating innovation while addressing business risk. With Synopsys, your developers can secure code as fast as they write it. Your development and DevSecOps teams can automate testing within development pipelines without compromising velocity. And your security teams can proactively manage risk and focus remediation efforts on what matters most to your organization. Our unmatched expertise helps you plan and execute any security initiative. Only Synopsys offers everything you need to build trust in your software.

For more information about the Synopsys Software Integrity Group, visit us online at www.synopsys.com/software.