2023 Developer Survey

Where are developers spending their time?

qwiet AI

TABLE OF CONTENTS

Executive Summary

Qwiet AI aims to make AppSec (application security) a painless process for developers. The team at Qwiet AI worked with research firm Propeller Insights to conduct a survey of over 1000 developers with the aim of getting to the root of where developers are spending their time and what frustrations they are experiencing with application security. The biggest takeaway from the results is that about a third of developers spend up to half their time fixing bugs instead of writing code. Our research also shows that developers are frustrated by security tools that are too noisy, take too long to scan, and increase tech debt at a time when development teams are already overworked.

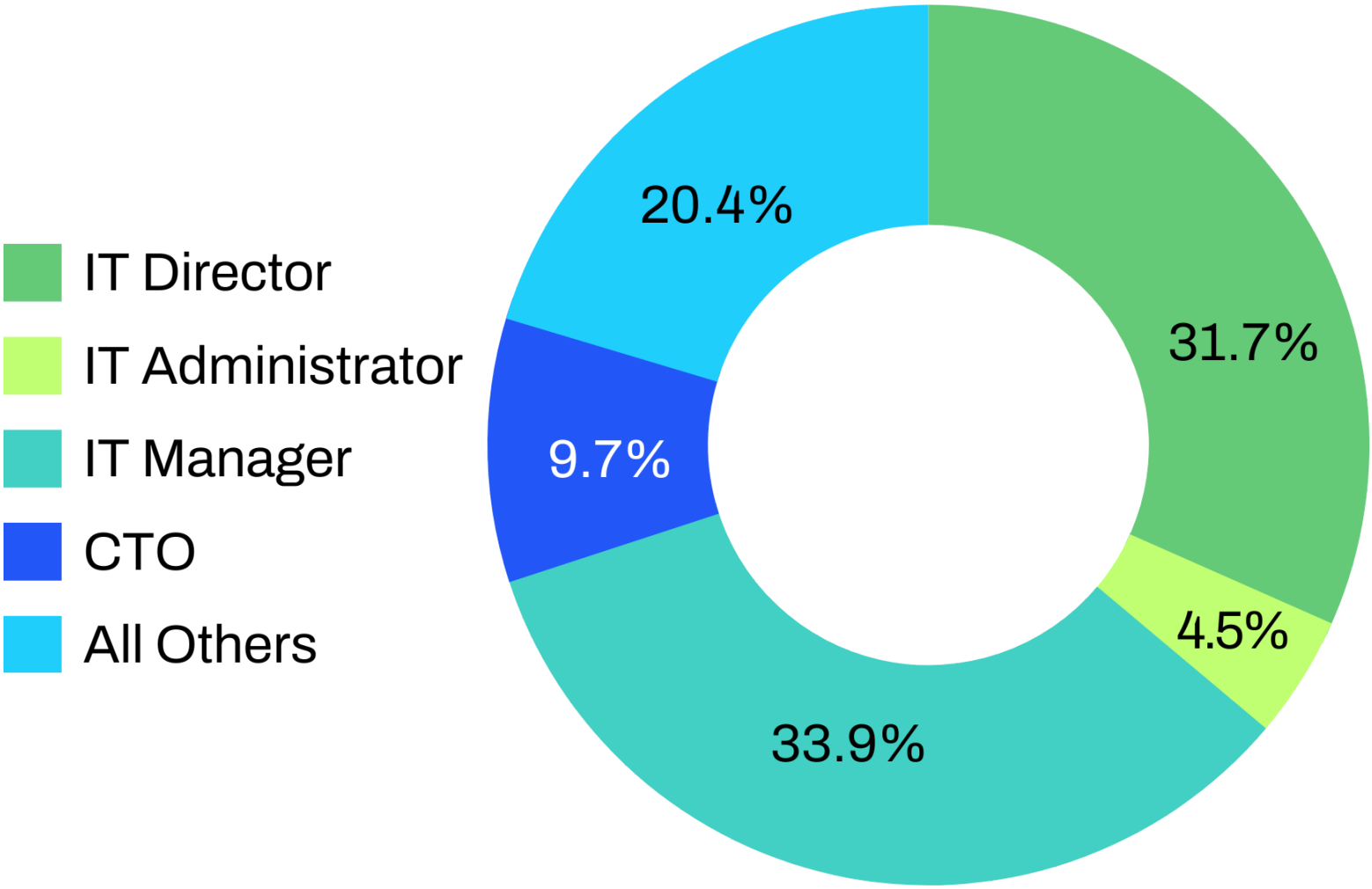
When looking at what developers want from an AppSec tool, the biggest asks were for better prioritization around fixes and real-time updates to the security threats. Developers were also fairly optimistic about the use of AI tools in application security, with 94% saying they feel they will need AI security tools to keep pace with the ever-growing threat landscape.

A quick look at the headlines shows that cybercriminals are not slowing down, and insecure code is ultimately behind the majority of the major attacks. This survey shows the struggle many organizations are having, striking a good balance between getting code out the door quickly and making sure that code is secure. Ultimately, organizations need to find a way to make AppSec less of a burden on developers while still producing high-quality, secure code.

Test Methodology

Propeller Insights (on behalf of Qwiet AI) conducted a nationwide survey of US IT professionals, ages 18 and up, between August 14 and August 29, 2023. All respondents were pre-identified as IT professionals and had to self-identify as such within the survey to qualify.

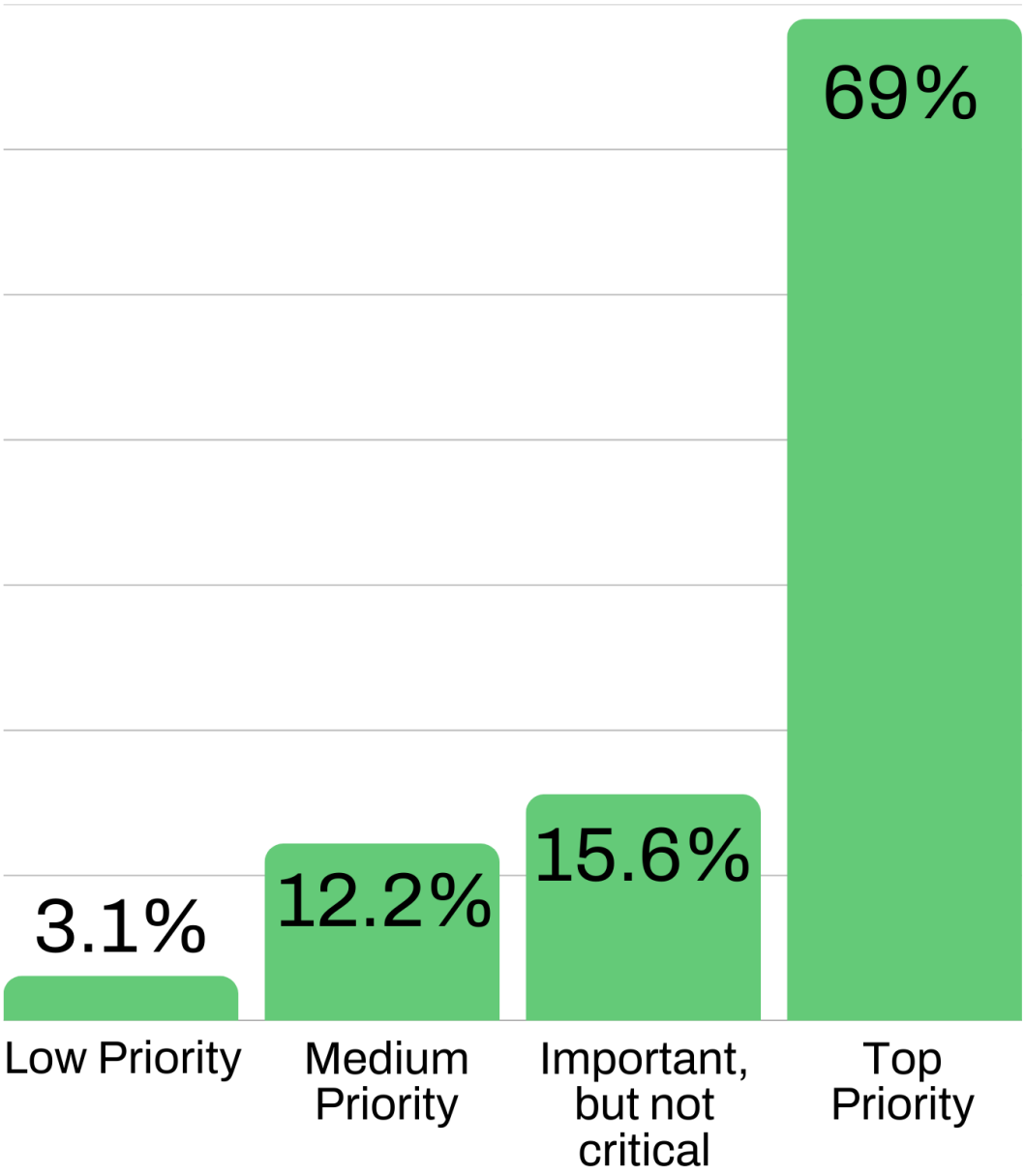
The job titles are broken down as follows:



A View into Process

AppSec programs vary greatly from organization to organization. One of the aims of this survey was to get a better understanding of how many organizations are handling the task of ensuring they release secure code.

Question: How much of a priority is application security at your organization?



With a resounding 69% responding that AppSec is a top priority, the next logical question is how often organizations utilize an AppSec tool to scan for vulnerabilities in their code.

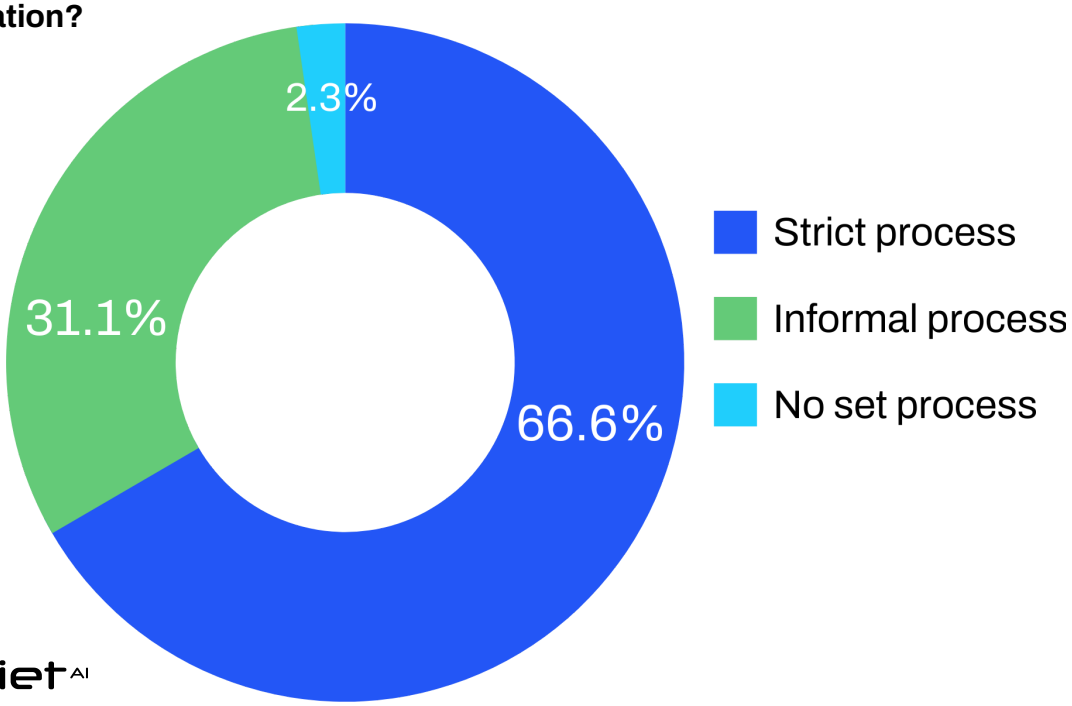
Question: How often do you scan your code for security vulnerabilities?

Every time I upload new changes	59.9%
Once a day	25.5%
Once a week	9.5%
At the end of the project, right before launch	5.1%

Question: How satisfied are you with your process for fixing bugs and vulnerabilities?

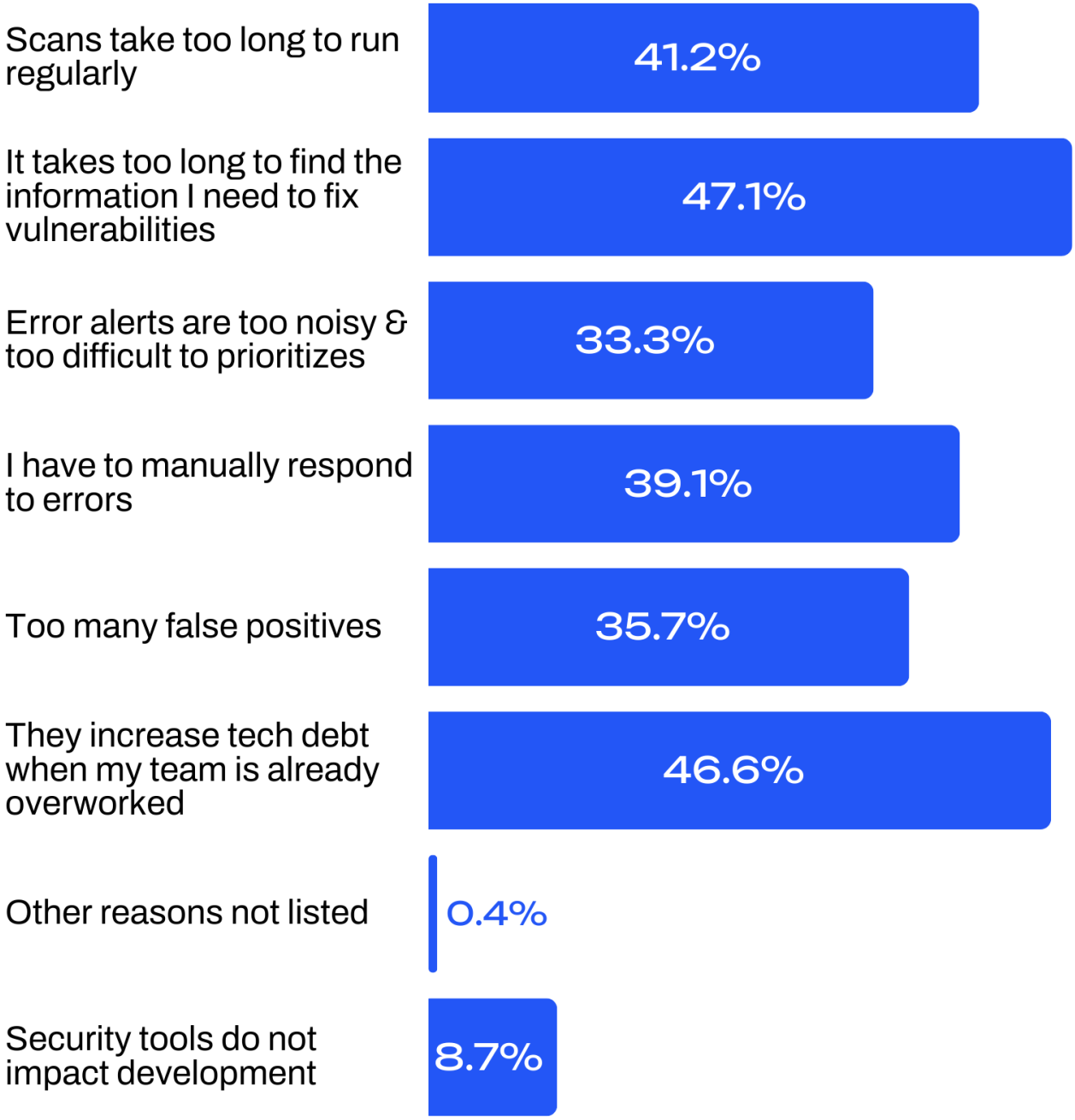
Not at all satisfied	0.3%
Not very satisfied	3.1%
Somewhat satisfied	31.2%
Very satisfied	64.9%

Question: Is there a set process for handling code security vulnerabilities at your organization?



While a strong percentage of respondents said they were very satisfied with the overall process of fixing bugs and vulnerabilities, only 9% responded that security tools did not impact their development process.

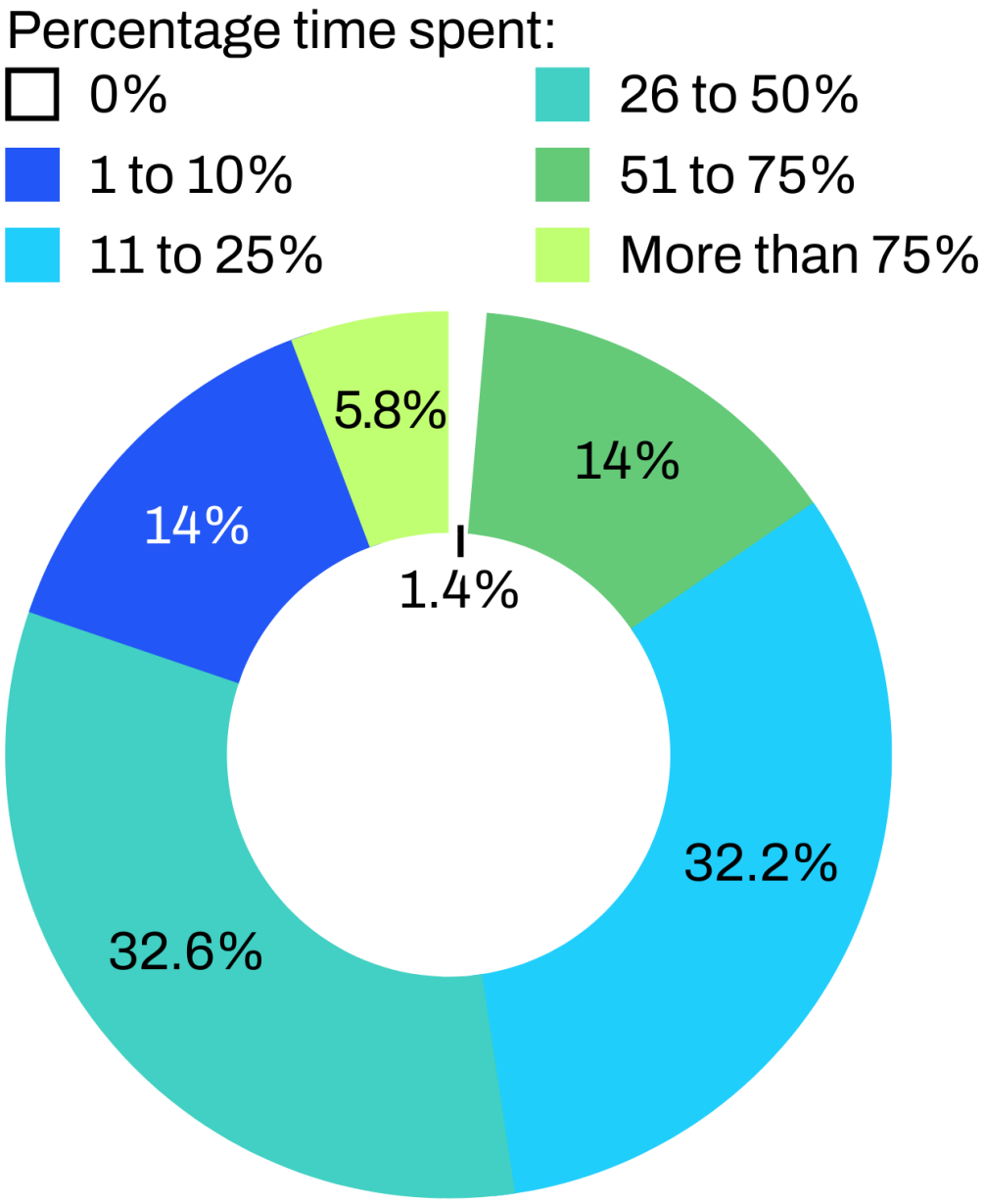
In which of the following ways, if any, do security tools impact your development process? (Multiple answers possible)



Getting to the Fix

Of course, finding the vulnerabilities is just the first step. Survey respondents also spent more time than they would have liked fixing bugs. 33% of the survey group found they spent 33% of their time fixing bugs instead of writing code. 39% also found that at least 1 hour of every day was spent searching for ways to fix issues.

Question: What percentage of your time do you spend fixing bugs instead of writing new code?



Question: How much time do you typically spend searching for answers or solutions to bug fixes?

Over 2 hours a day	6.5%
1 - 2 hours a day	21.5%
30 - 60 minutes a day	38.5%
15 - 30 minutes a day	25.6%
Less than 15 minutes a day	7.9%

AI in the Mix

Given the huge influx of AI into so many aspects of our lives, it's not surprising to see AI tools taking a bigger role in application development and security. We probed our respondents to see how they felt about current and future use of AI.

Question: Do you feel AI tools help code development?

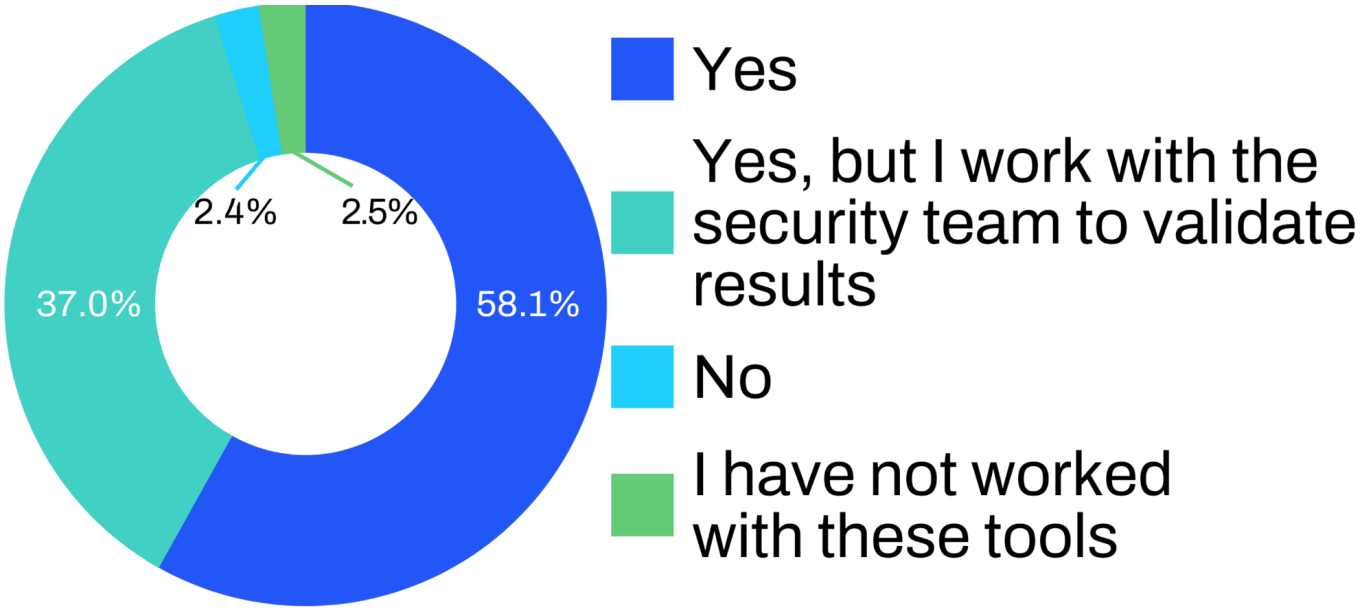
Skeptical	11%
Could help	23.3%
I have started experimenting with these tools	20.3%
These tools have helped	27.9%
These tools have been a game-changer	17.5%

Moving from code development, we wanted to see how developers viewed tools (like Qwiet AI) that utilize AI for finding vulnerabilities in their code.

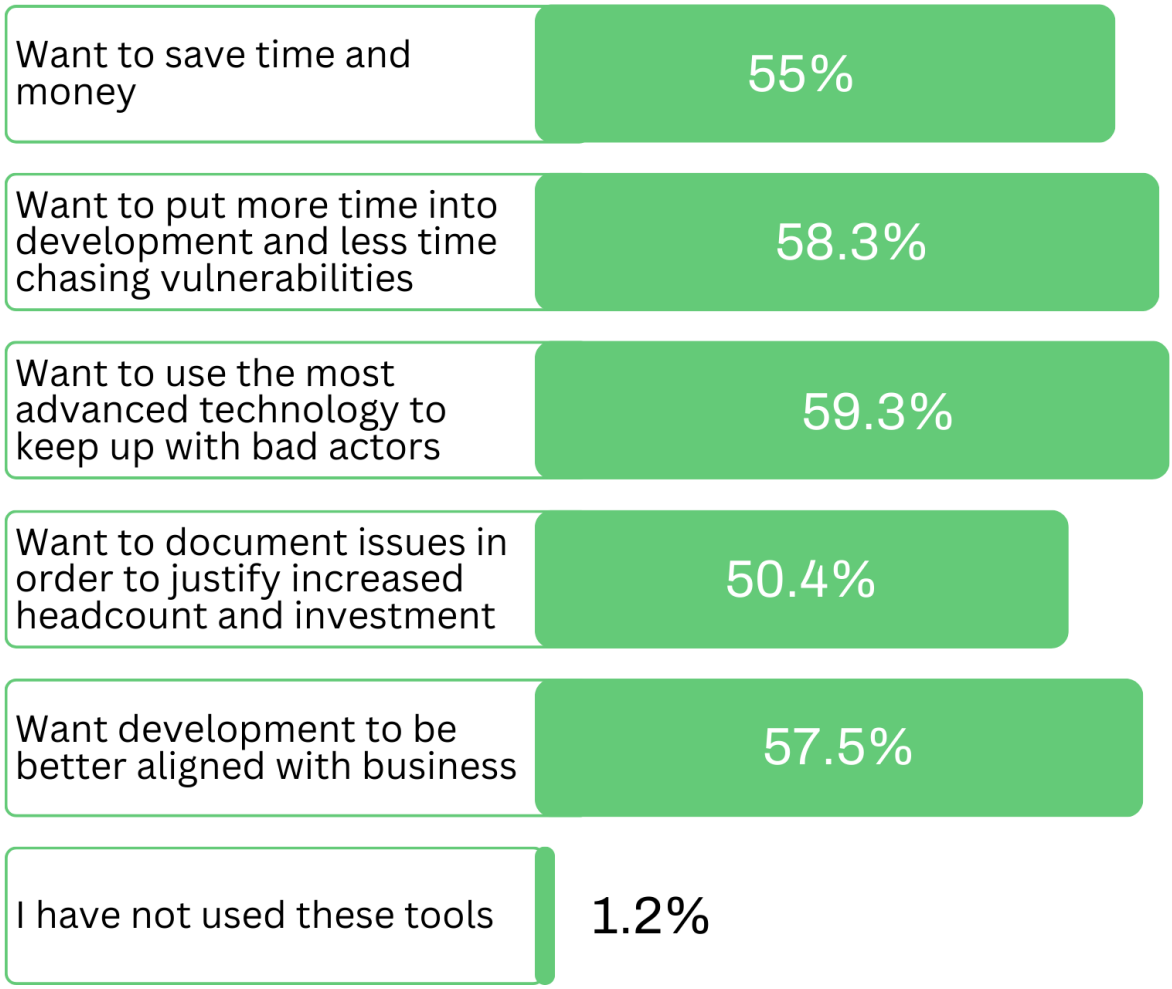
Question: Do you think new AI-based AppSec tools can help you find vulnerabilities?

I don't think they are helpful	2.4%
I've heard mixed things	19.6%
I have started experimenting with these tools	22.5%
They have helped, but still need to mature	26.7%
These tools have been a game-changer	28.8%

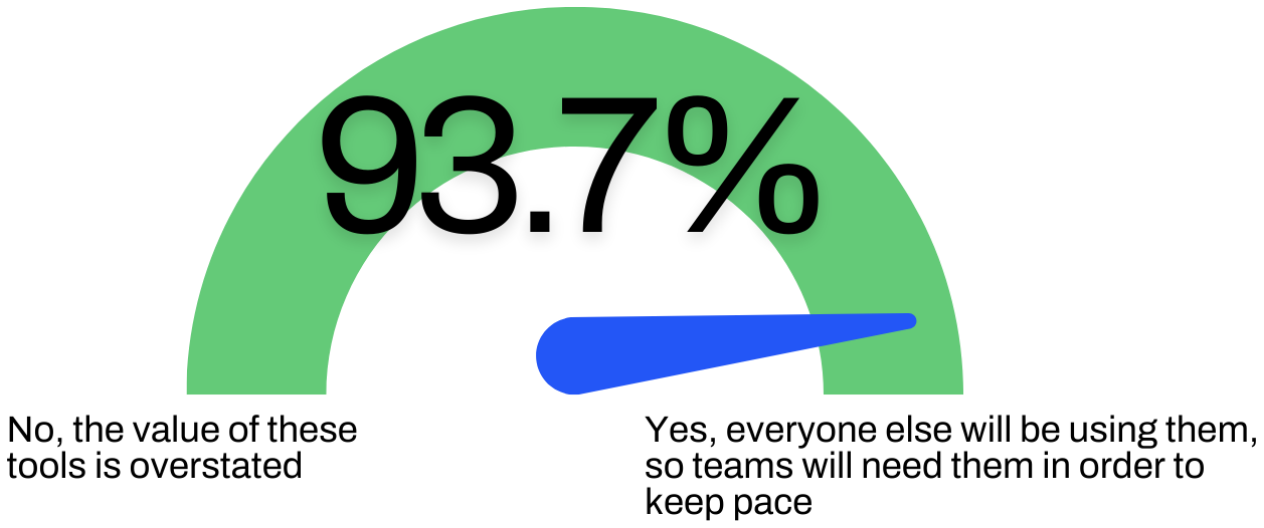
Question: Do you trust the output of these tools?



Question: What are you looking for in these tools? (Multiple answers accepted)



Question: Will AI-based tools become necessary in the next few years?



A Look at Licensing

Many organizations also have some form of compliance or standards their code needs to adhere to. Often the AppSec team collects this information along with vulnerabilities detected to create a bigger overall picture of compliance.

Question: Are you required to provide a Software Bill of Materials (SBOM) with your applications?

Yes	62.8%
Yes, but it's handled by a different group	21%
No, but we do anyway for best practices	10%
No	6.3%

Question: Do you have software library restrictions? (e.g. cannot use GPL)

Yes	51.5%
Yes, but it's handled by a different group	22.4%
No, but we track for best practices	11.9%
No, we don't use open-source libraries	4%
No	10.1%

It's worth noting that only 4% of the respondents said they did not use open-source libraries.

Releasing Code

After planning, writing, debugging, and fixing vulnerabilities comes the next step in the process: putting code into production.

Question: How often does your team deploy code into production?

Daily	29%
Every week	41.5%
Every two weeks	13.9%
Every month	9.4%
Every two months	4%
Twice a year	1.1%
Once a year	0.4%
Other	0.7%

Question: What's holding your company back from deploying more often? (Multiple answers accepted)

Question: Which of the following capabilities would help your teams iterate faster? (Multiple answers accepted)

Help in QA	56.6%
See where each error originates	51.7%
Access to rich contextual information	56.6%
Prioritization of security fixes	59.6%
Real-time capabilities	60%
Other	0.3%
None of above	2%

Question: Do you feel the security team's priorities are properly aligned with your development goals?

No, they are misaligned	27%
No, they are somewhat misaligned	21.9%
There is a good balance between development goals and security goals	33.8%
Yes, they are completely aligned	17.2%

Conclusion

This survey revealed some of the challenges and opportunities that developers face in their daily work. The prevailing thread throughout the results shows that developers spend a lot of time fixing bugs instead of writing code, often due to a lack of clearly prioritized results from application security scans. This suggests that there is a need for better tools and processes to help developers identify and resolve the most critical bugs.

In line with the rest of the findings, developers want fewer false positives from their security tools, as they can waste time and resources. This implies that security tools should be more accurate and reliable and that developers should be more involved in the security testing process. Finally, the survey showed that developers are bullish about the future of AI tools, as they believe they can improve their productivity and quality. This indicates that developers are open to adopting new technologies and methods and that they are eager to learn and innovate.

As organizations look to improve their overall productivity while also reducing risk to the business, it's important to take into account the impact of disrupting developer workflow. To truly optimize the process, it is important that AppSec tools provide the most advanced security protections available while also being streamlined to fit the existing development environment. The only way to truly provide secure code is by making AppSec a welcome part of the process and not a burden on already overworked development teams.

About Qwiet AI

Qwiet AI is the AI-enhanced application security testing platform that provides SAST, SCA, Container Scanning, and Secrets Detection all in one fast and comprehensive scan. Qwiet AI customers benefit from targeted results with scans that are 10x faster and 12x more accurate than traditional application security tools.