BYTES | Smarter together

DevOps Market Report

December 2022

A Bytes Market Report in partnership with

snyk

TREND MICRO

Introduction

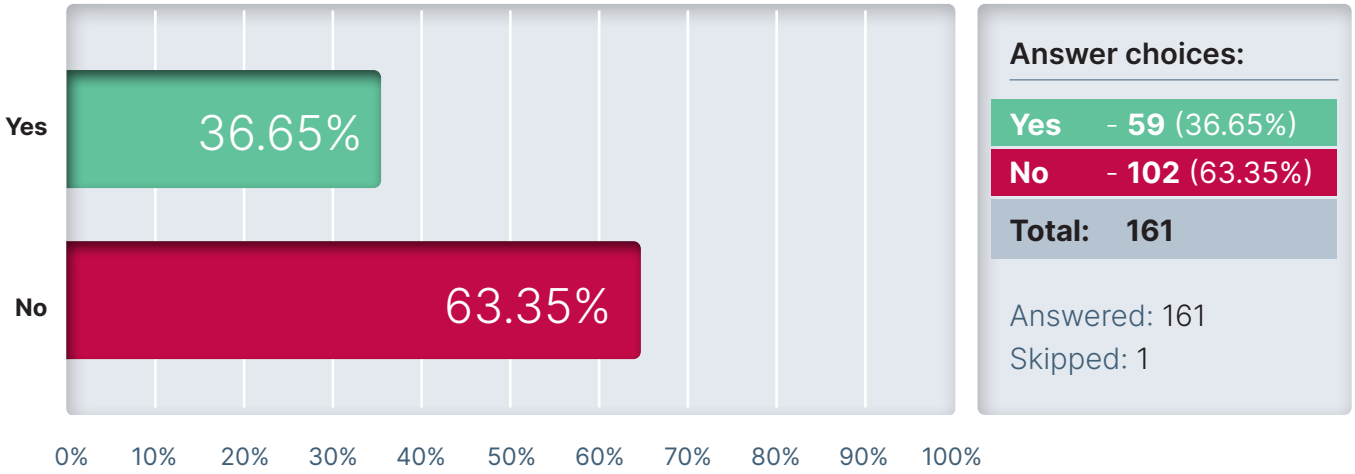
More organisations are choosing to use and develop applications to give them a competitive edge. If left unchecked, some developed applications can pose an avoidable security risk to organisations. It is no surprise therefore that DevOps and SecOps teams are working more closely together and becoming more closely integrated.

We surveyed 161 DevOps and SecOps professionals to understand how they are using and securing developed applications. This Market Report provides an insight into the findings and includes commentary from Paul Harland (Solution Architect at Synk), Nick Ross (Channel Sales Engineer at Trend Micro), Toby Noble (Security Business Manager at Bytes), and Ed Fenton (Application and Risk Security Specialist at Bytes).

If you would like to discuss the findings in this Report further, or have a conversation with Bytes about how you could improve your security posture, please speak with your Account Manager, or email tellmemore@bytes.co.uk

Q1.

Do you have a dedicated SecOps within your IT function?



Answer choices:

Yes	- **59** (36.65%)
No	- **102** (63.35%)
Total:	**161**

Answered: 161
Skipped: 1

Summary

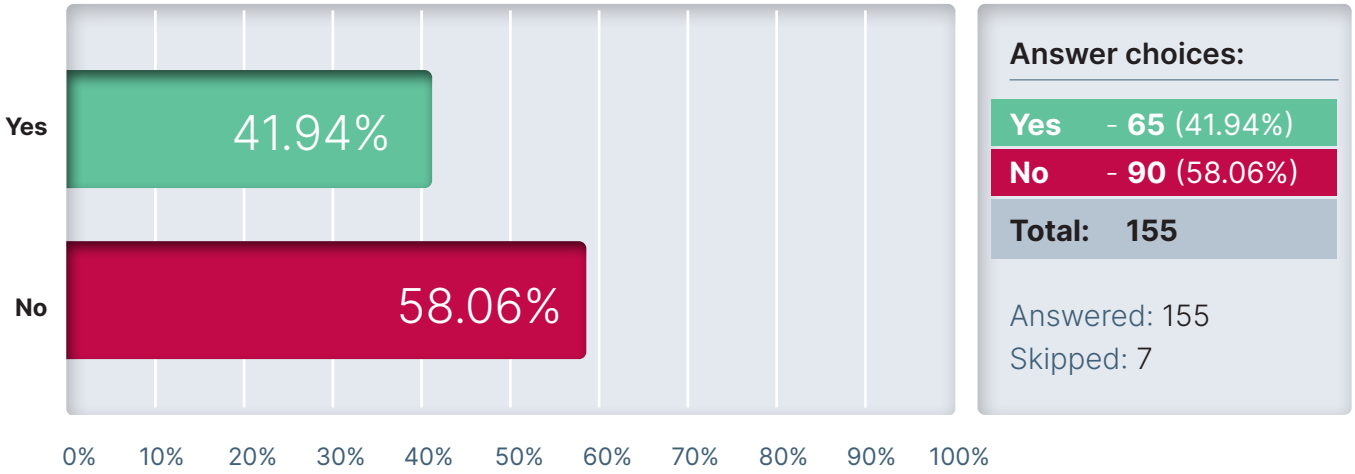
Whether they have a dedicated security operations team or not, given the growing insider and external threats, it is essential that every organisation has a robust security posture and strategy in place.

In the instance that organisations do not have a dedicated SecOps team, the various security activities are typically distributed among the broader IT team. While a distributed approach can be effective, we tend to find that in those instances the job of security is broadly reactive-based and not proactive, so teams are largely responding to threats rather than getting ahead of them.

The larger percentage of "Nos" in this question also highlights the lack of available talent in the security job market and unfortunately the situation is not looking likely to improve anytime soon. To overcome the skills shortage, organisations have two options. One, is to invest in cross training their existing team, and the other is to outsource parts of the security requirement to specialist organisations, typically on a managed service basis. Bytes are often called upon to provide both solutions - training services and managed services.

Q2.

Do you have a dedicated DevOps team?



Answer choices:

Yes	**65** (41.94%)
No	**90** (58.06%)
Total:	**155**

Answered: 155
Skipped: 7

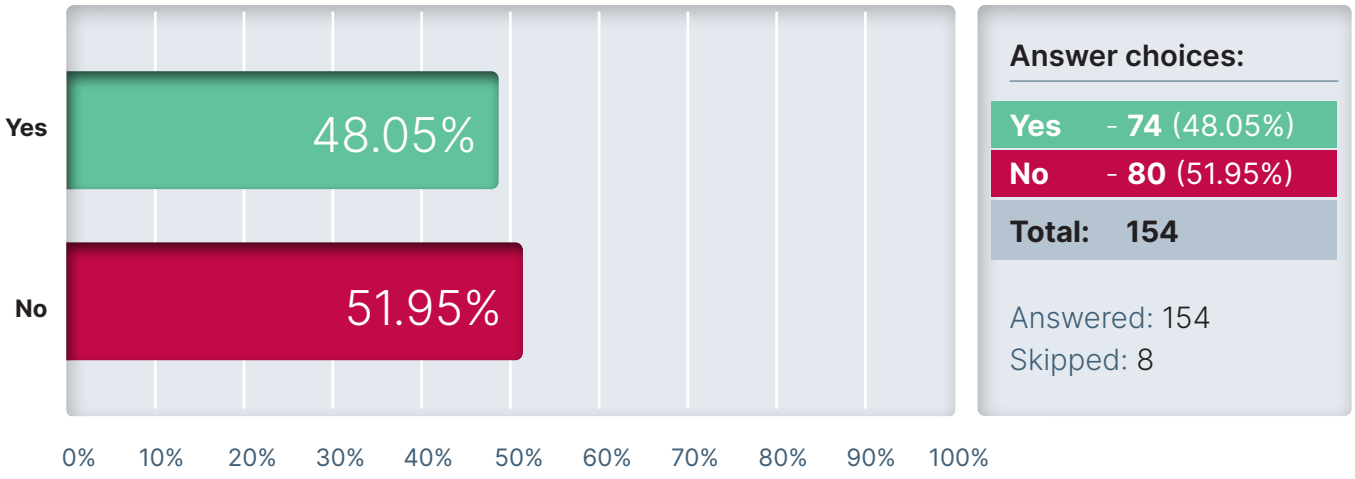
Summary

When the answers provided to the various other questions asked in this survey, we reach a different conclusion to the outcome of this specific question. For example, 140 out of the 161 respondents are currently using Open Source so we know most organisations have a development capability. It is very likely therefore that many will also have a DevOps team.

This is not surprising as organisations are forever competing and looking for the next competitive advantage. Using development teams to develop Apps that improve operational efficiencies is one effective way of doing this. It is essential however that development teams are not working in isolation of the security teams. We expand on this in the next question.

Q3.

Do your IT/SecOps team work directly with your DevOps function to ensure security is by design and not an afterthought?



Answer choices:

Yes	**74** (48.05%)
No	**80** (51.95%)
Total:	**154**

Answered: 154
Skipped: 8

Summary

The findings from this question are broadly in line with what we are seeing in the market, as there has been a trend towards closer alignment for many months now. This is because organisations are recognising the direct correlation between closer alignment and improved security.

A good example of this was the Log4j vulnerability that caught a lot of organisations out when it was disclosed in November 2021. Those organisations with more closely aligned SecOps and DevOps teams were more able to rapidly assess the risk in their applications and take the necessary remedial actions.

Closer aligned teams also make the developers think more about how their Apps are designed to adhere to the latest security best practices, and specifically think what would happen if there was a breach. The SecOps teams are also able to communicate breach intel more efficiently to the developers, enabling them to contain the threat.

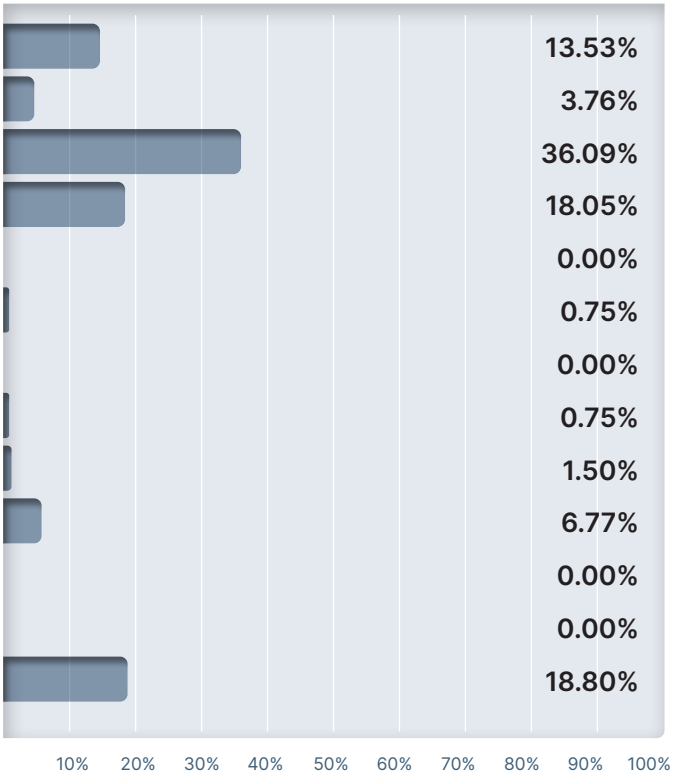
Often the driving force behind closer alignment is the need for organisations to have the right processes in place to detect how vulnerable they are, and in what Apps, and be able to move quickly should a threat be detected. That translation from the SecOps team therefore to the developers is critical.

Q4.

Which programming languages and package managers are you using?

(Mulitple choice)

Answer choices:	Responses	%
JavaScript	18	13.53%
Java (Gradle, Maven)	5	3.76%
.NET	48	36.09%
Python	24	18.05%
GoLang	0	0.00%
Swift	1	0.75%
Objective-C	0	0.00%
Scala	1	0.75%
Ruby	2	1.50%
PHP	9	6.77%
Elixir	0	0.00%
Bazel	0	0.00%
Other	25	18.80%
TOTAL	133	



Summary

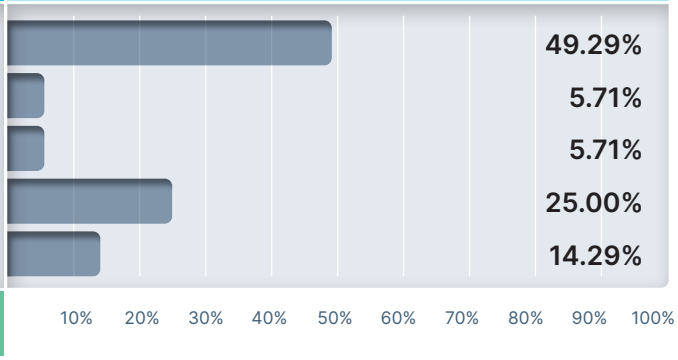
It is no surprise, given that most of Bytes' customers are Microsoft users, that .NET is the dominate programming language here. It is also not too much of a stretch to think they are deploying Apps to Azure.

What is striking however is there are more Python users than Java Script users as this is not aligned with the broader development community. One explanation for this is the growing popularity of Python in relation to Machine Learning and AI.

Q5.

What source control repositories are you using?

Answer choices:	Responses	%
GitHub	69	49.29%
GitLab	8	5.71%
BitBucket	8	5.71%
Azure Repo	35	25.00%
Other	20	14.29%
TOTAL	140	



Summary

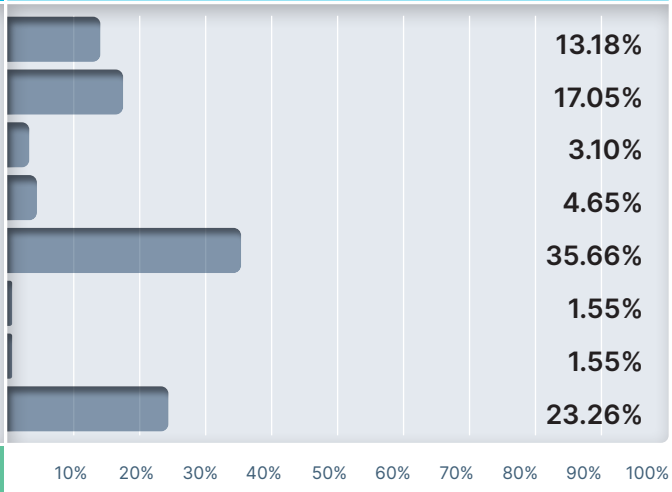
As with the last question, it is no surprise that GitHub, being a Microsoft company, is popular with the responders of this survey. What is interesting however is that most organisations responded, suggesting most have a development capability. This supports the conclusions drawn earlier in this Report that more organisations have a DevOps team than the findings suggest.

The large percentage of Azure Repo users can be explained by the inclusion of it in most Microsoft subscriptions. .NET users will be using Azure Repo.

Q6.

What CI/CD tools are you using?

Answer choices:	Responses	%
CLI	17	13.18%
Jenkins	22	17.05%
TeamCity	4	3.10%
BitBucket Pipeline	6	4.65%
Azure Pipeline	46	35.66%
Circle CI	2	1.55%
Synk API	2	1.55%
Other	30	23.26%
TOTAL	129	



Summary

The findings of this question are self-explanatory but we should highlight that the “Snyk API” here is used as an additional capability integrated into the tools stated above.

We recommend seeing a higher adoption from our customers here as Snyk allows developers to fail builds based on vulnerabilities or policy deviations found, and stops the promotion to live, bringing automation and scale to the security effort.

Conclusion

Provided by **Ed Fenton, Application and Risk Security Specialist at Bytes**

This Report shows some very interesting outcomes. I am not surprised that there is a separation between SecOps and DevOps, this was a common occurrence throughout 2022. What I am surprised about is the lack of dedicated SecOps professionals, my thoughts here are that the industry still faces a lack of good quality cyber security professionals.

For me, what is becoming clearer is the need and inevitability for SecOps and DevOps to become more intertwined. With one of the largest open-source vulnerabilities for Java hitting organisations in 2021 (Log4), there is widespread agreement within Organisations for better security protocols within their CI/CD so remedial action can be taken as early as possible. Furthermore, if organisations don't have a key security champion within the Developer Team as a minimum then a breach is more likely to occur.

Speaking to developer teams daily, the wide range of languages being used wasn't a surprise to me. However, the rise of Infrastructure as Code will play a big part in which languages will be most common in 2023.

I believe the shift from DevOps to DevSecOps will continue to gather momentum through 2023, with more organisations shifting left and embedding security earlier in their SDLC, with the majority of organisations adopting either a SAST or SCA tool set as a starting point. However, it must be added that doing this must not be taken lightly and setting up a true AppSec needs to be managed correctly, as from a culture shift perspective, it is hard to do. Security Champions within the developer teams is going to be crucial to securing the SDLC in the future.

If you would like to discuss the findings in this Report further, or have a conversation with Bytes about how you could improve your security posture, please speak with your Account Manager, or email tellmemore@bytes.co.uk

About Bytes

Bytes provides leading insights, expertise and practical help to over 3,600 organisations nationwide. We enable effective and cost-efficient technology sourcing, adoption, security and management of software, hardware and cloud services.

Our UK business began in 1982 and has grown profitably each year to reach a turnover in excess of £1bn, making us one of the largest software services and solutions businesses in the country.

The most important aspect of our business is our people. We value initiative, teamwork and achievement. Together, we focus on providing the highest levels of service so we can deliver our ultimate goal – customer satisfaction and success.

Our customers include leading brands, such as Marks & Spencer, BBC, NHS, Clifford Chance, BUPA, Thames Water, Hiscox, Allen & Overy LLP and thousands more across retail, media, finance, manufacturing, legal, healthcare and the public sector.

We work closely with the majority of IT vendors and are delighted to regularly receive honours from them in addition to being named a Sunday Times Best Company to Work For 2020.

Within our business we have over 150 members of staff qualified as Microsoft Certified Professionals (MCP) and Microsoft Certified Technology Specialists, who are experts in licensing, software asset management and technology, so you can get the best advice at every moment.

As well as being a Gold certified Partner with a deep understanding of all the latest Microsoft technology, we're also a Microsoft certified FastTrack deployment partner, therefore we're in the best position to help you plan and deliver your next modernisation project.

---

snyk

About Snyk

Snyk combines the power of developer-first tooling with best-in-class security intelligence. The Snyk platform quickly finds and fixes security issues in proprietary code, open source dependencies, container images, and cloud infrastructure so businesses can build security directly into their continuous development process.

TREND MICRO

About Trend Micro

Trend Micro, is a global cybersecurity leader in cloud and enterprise cybersecurity, and their platform delivers central visibility for better, faster detection and response and a powerful range of advanced threat defense techniques optimized for environments, like AWS, Microsoft, and Google.

UK Head Office
Bytes House
Randalls Way
Leatherhead
Surrey
KT22 7TW

01372 418 500
tellmemore@bytes.co.uk
bytes.co.uk

BYTES | Smarter together