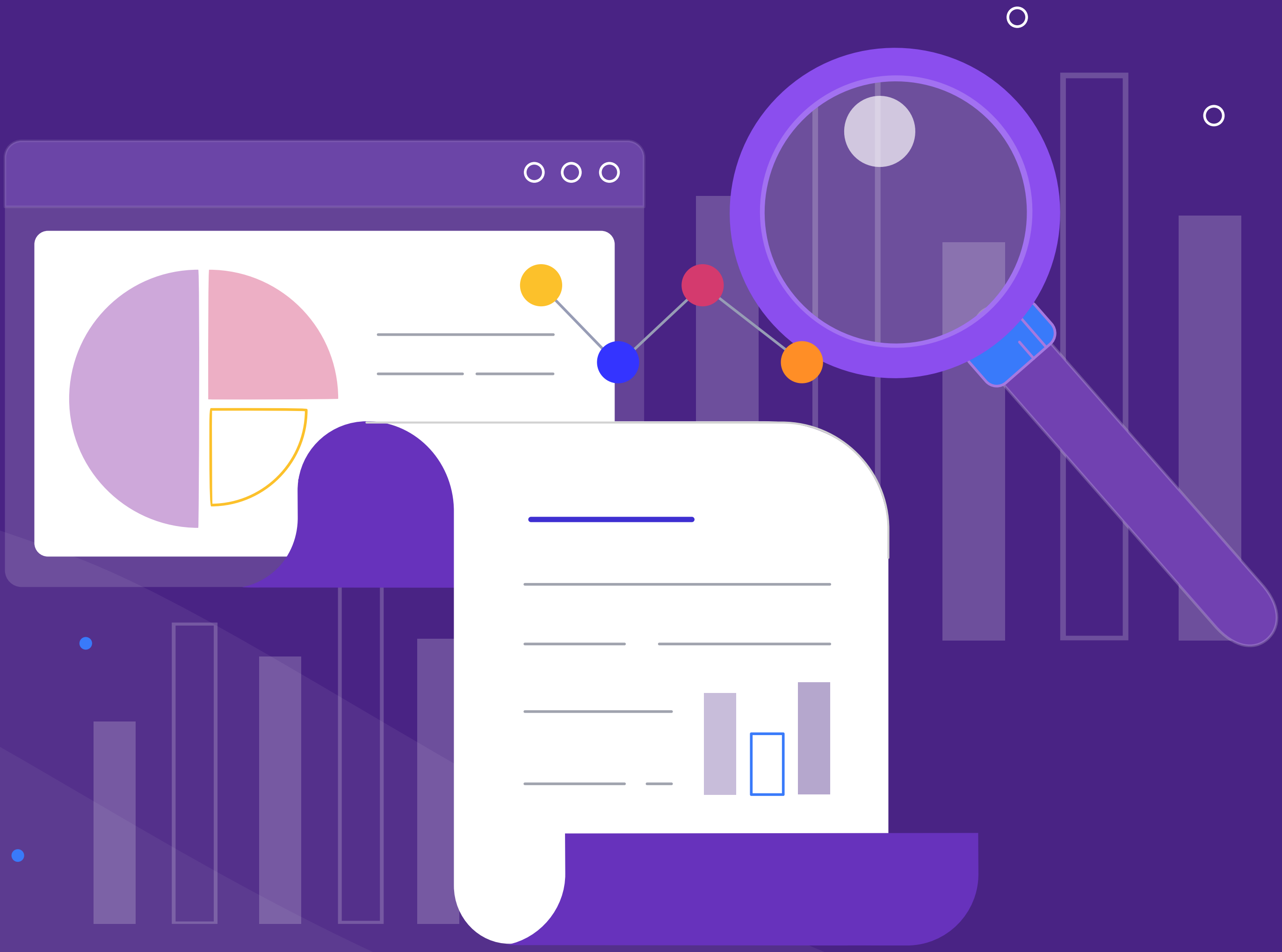
Purple Book Community

# State of Application Security 2023

## Approaches and results from modern AppSec programs



# Executive Summary

AppSec is coming to the forefront as DevSecOps comes of age. But we still, as an industry, have a ways to go. Developers need embedded, advanced automation, Security needs to get the message across more clearly, and tooling needs to be effectively orchestrated. Software supply chain vulnerabilities pose a growing threat. The State of Application Security 2023 from the Purple Book Community captures the pulse of the industry now.

> **“Too many vulnerabilities, not enough prioritization” is the #1 stumbling block reported by software security teams**

> **“86% agree that security tools are interchangeable, it’s the process that’s most important”**

> **“53% of teams have unmanaged risk in their application portfolio”**

## AppSec is slowly maturing

- 14% of orgs are leaders in next-gen AppSec maturity, but for 58% there is still a lot of work to be done to get to baseline levels.
- 31% of orgs use an Application Security Maturity Model and track usage of security tools across teams (30%).”

## Prioritization is still a struggle

- 58% of organizations say ‘too many vulnerabilities, not enough prioritization’ is one of their biggest stumbling blocks.

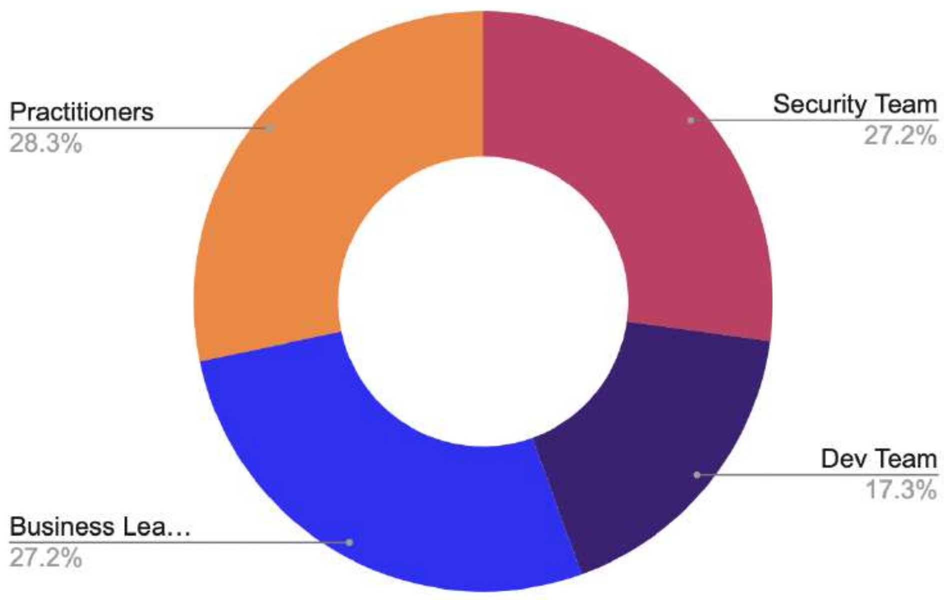
## SBOM for the software supply chain

- 4% of orgs say securing the software supply chain via Software Bill Of Materials is their #1 priority.
- 21% had no SBOM usage at all.

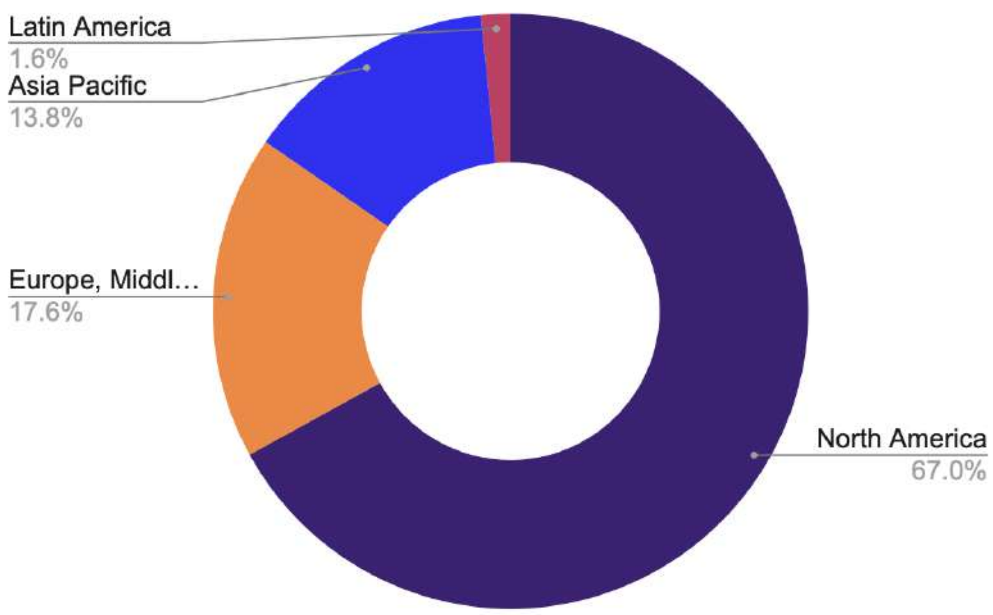
# Who took the survey?

We collected 443 survey responses in 2023 from both individuals and leaders in security, development, and analysis, across a variety of industries and business sizes.

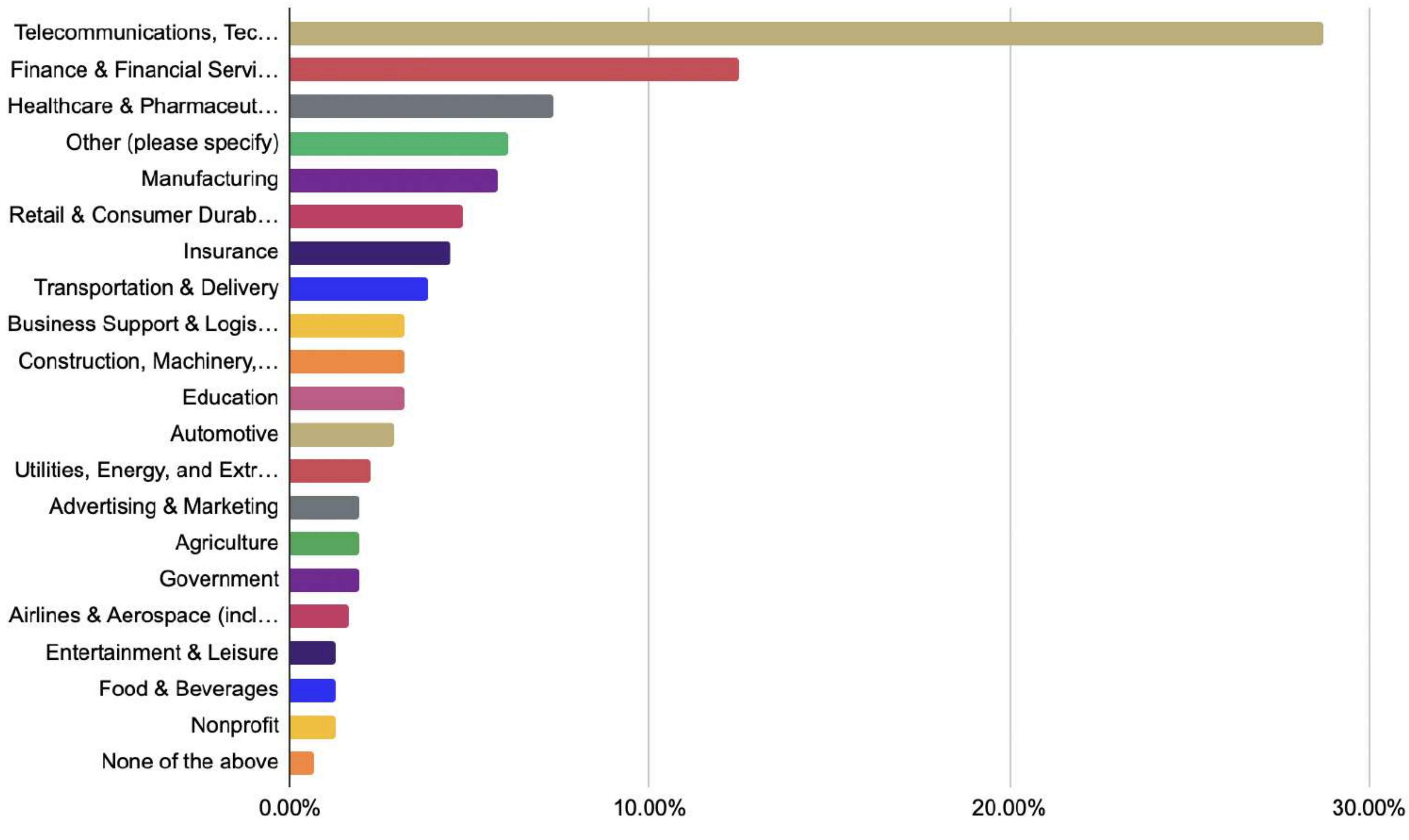
## Respondents



## Location



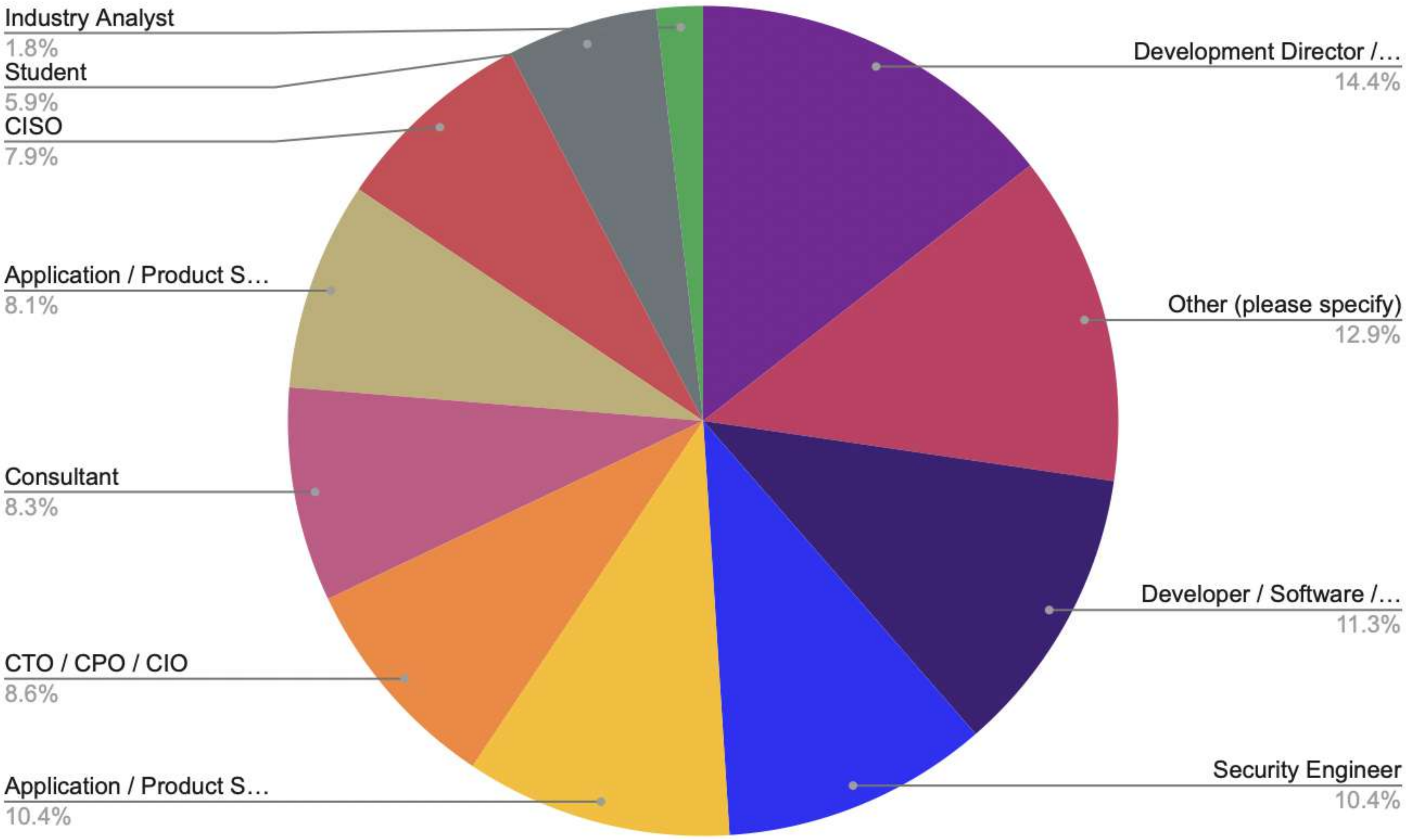
## Industry



# Who does what?

### What is your job role?

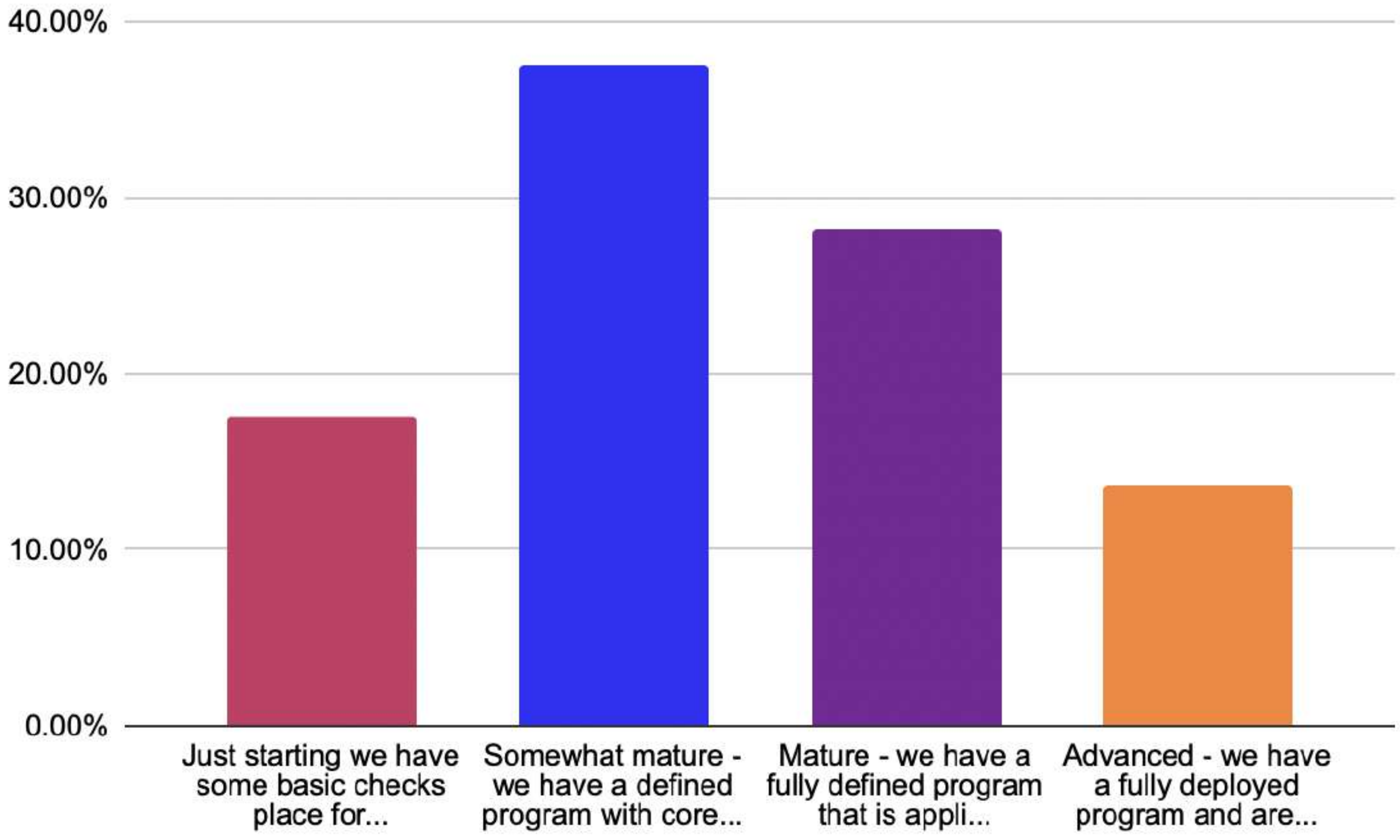
| Answer Choices | Response Percent |
|---|---|
| Development Director / Manager | 14.45 % |
| Others (Please specify) | 12.87 % |
| Developer / Software / QA /DevOps Engineer | 11.29 % |
| Security Engineer | 10.38 % |
| Application / Product Security Director | 10.38 % |
| CTO / CPO / CIO | 8.58 % |
| Consultant | 8.35 % |
| Application / Product Security Engineer | 8.13 % |
| CISO | 7.90 % |
| Student | 5.87 % |
| Industry Analyst | 1.81 % |



# Let’s talk maturity

Application Security maturity isn’t something that just happens. Organizations weren’t just born with best practices across application security.

Choosing the right Maturity Model, benchmarking your organization regularly, committing to achievable goals, and rolling out to the wider organization need to be a priority for ongoing progress in maturation of AppSec programs. Modern models like the Scalable Software Security Maturity Model (S3M2) can help with this.



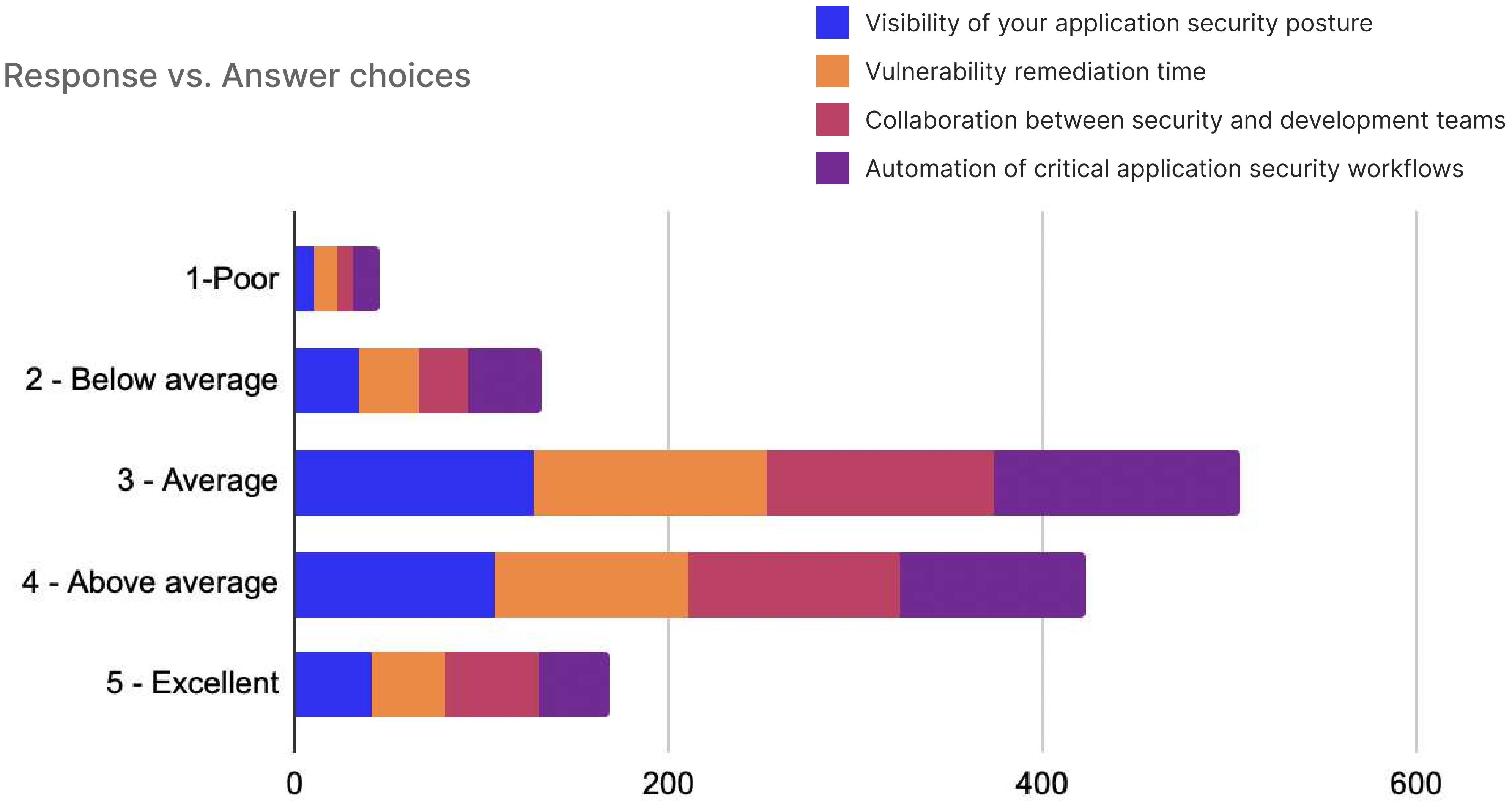
“14% are leaders in next-gen AppSec maturity, but for 58% there is still a lot of work to be done to get to baseline levels.”

# Security check - How are we doing?

While gauging the maturity of an AppSec program using an Application Security Maturity Model like S3M2 remains the gold standard, we can also get a pulse of the organization through self-assessment of different elements that make up a successful AppSec program.

As a whole, respondents believe their organizations are generally average or above average across most key vectors, with collaboration between security and development teams the strongest element and automation of critical AppSec workflows the weakest.

**How would you rate the following aspects of your current software security program?**



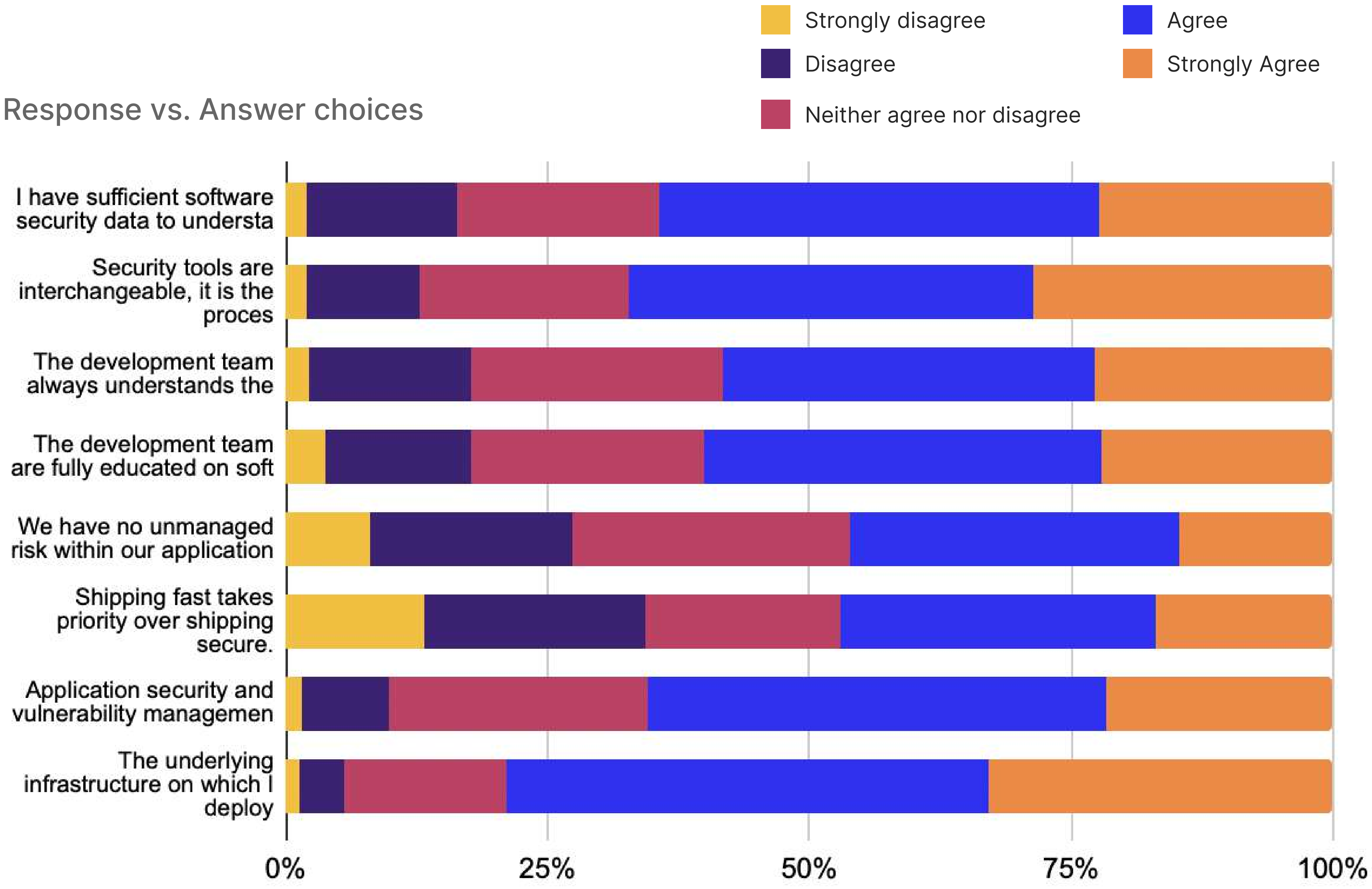
# Are we doing DevSecOps right?

53% of teams have unmanaged risk in their software portfolio

86% agree that security tools are interchangeable, it’s the process that’s most important

66% say that shipping fast takes priority over shipping secure

How strongly do you agree with the following statements?



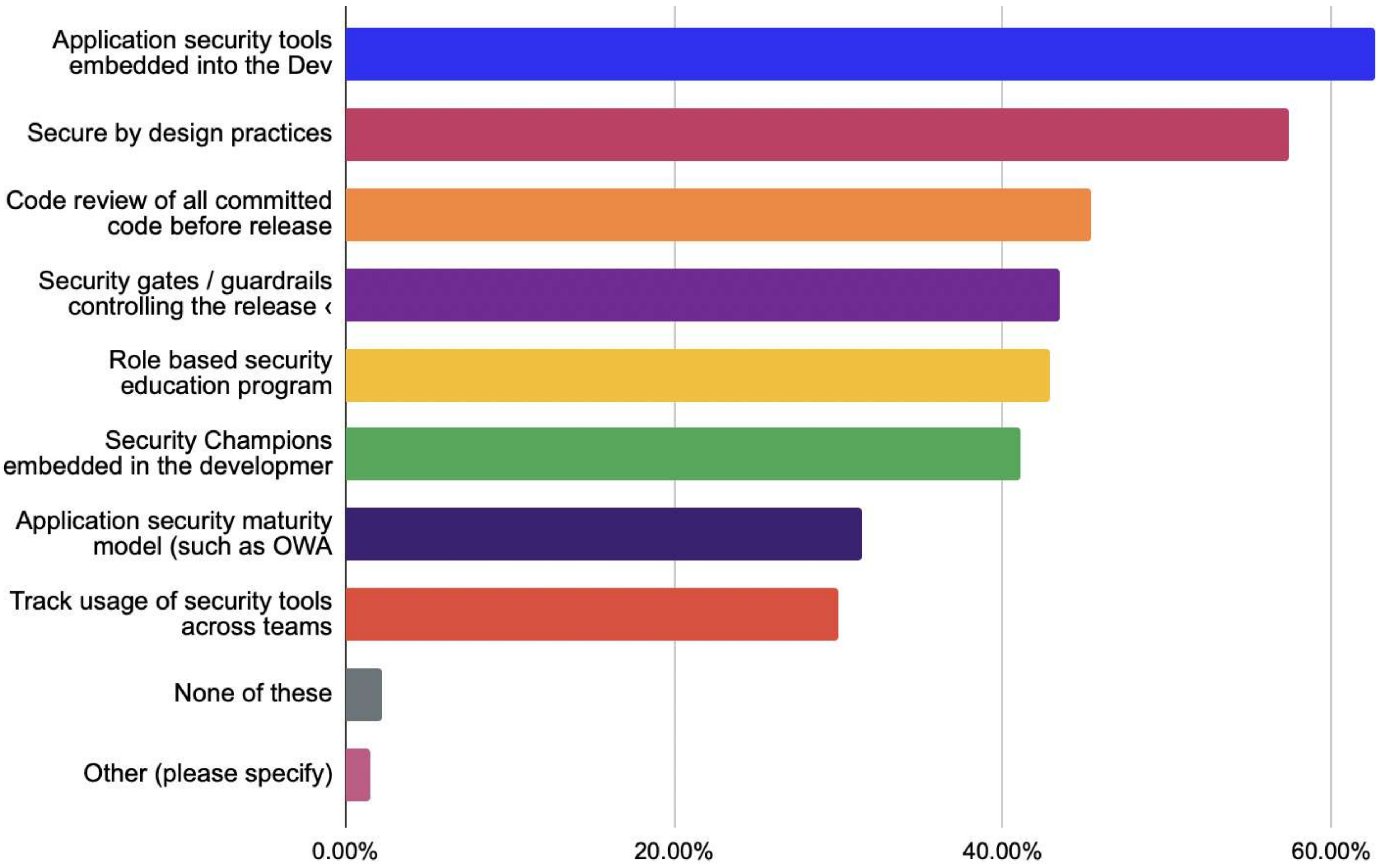
# A stocktaking of best practices

Strong AppSec is built on the back of DevOps best practices, including core practices like continuous integration / continuous deployment (CI/CD), bringing together mixed teams of people from both operations and software development, and building out infrastructure as code.

Adding in elements like secure by design coding practices, Security Champions, and AppSec tooling leads to an organization's best line of defense in building secure apps.

Since 2022, we've seen a 10% jump in the number of organizations deploying guardrails for release, although other best practices remain steady.

> "Industry leaders (31%) use an Application Security Maturity Model and track usage of security tools across teams (30%)."



**What initiatives do you leverage as part of your software security program?**

| Answer Choices | Responses |
|---|---|
| Application security tools embedded into the DevOps pipeline | 62.65% |
| Secure by design practices | 57.41% |
| Code review of all committed code before release | 45.37% |
| Security gates / guardrails controlling the release of software into production | 43.52% |
| Role based security education program | 42.90% |
| Security Champions embedded in the development teams | 41.05% |
| Application security maturity model (such as OWASP SAMM) | 31.48% |
| Track usage of security tools across teams | 29.94% |
| None of these | 2.16% |

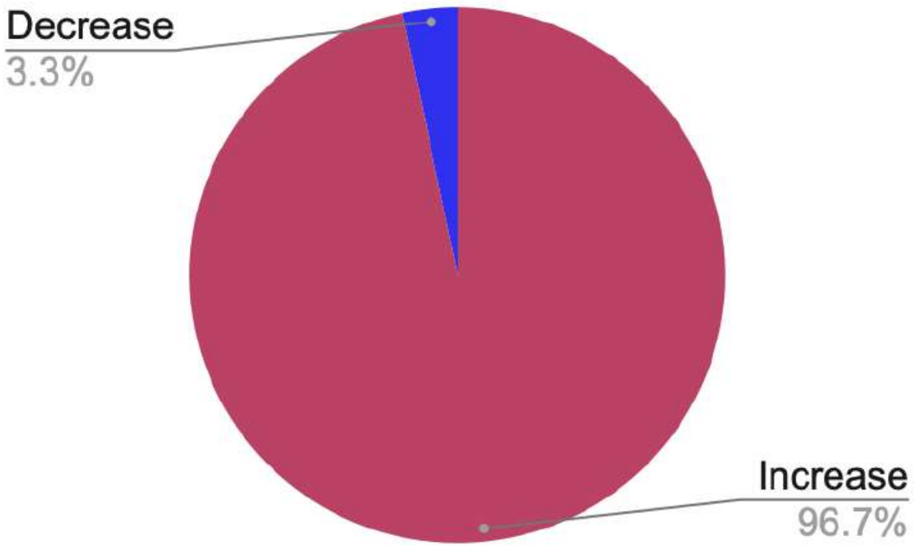
# Investment into security

Without investment into security, organizations will find they fail to keep up with competition.

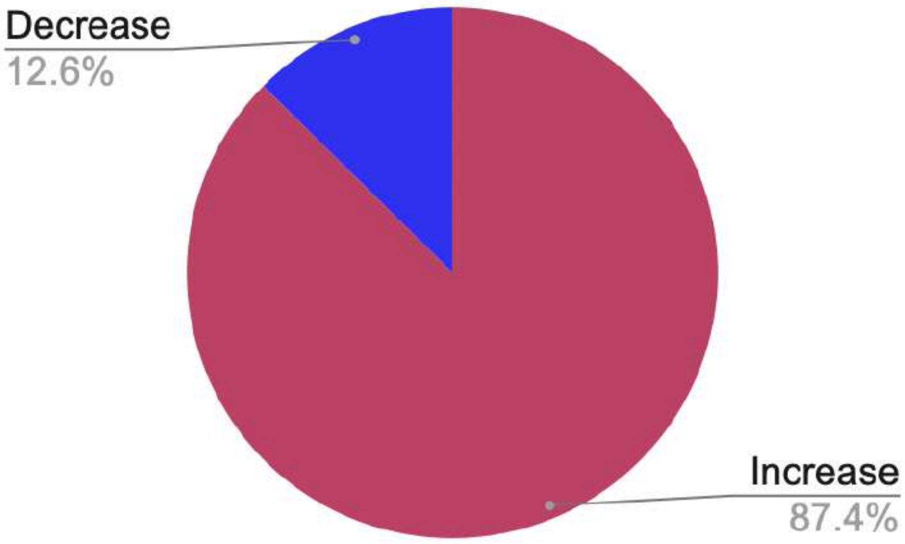
Balancing investment into security alongside speed of development and deployment is critical in the Agile space we find ourselves in.

With difficult economic conditions over the past year or two, organizations have tightened the belt across the board, and security has not escaped. Many security budgets have been frozen over the past year, but there are some signs of thaw, as over 50% of respondents report plans to grow their budgets over the next 12 months.

**How do you expect your software security budget to change over the next 12months?**



**Last year**



> “Despite economic downturn globally, over 50% of organizations are increasing their security spend - a telling figure”

# Vulnerabilities in production

## Q: How many vulnerabilities in production is too many?

A: Just one if there is a catastrophic exploit.

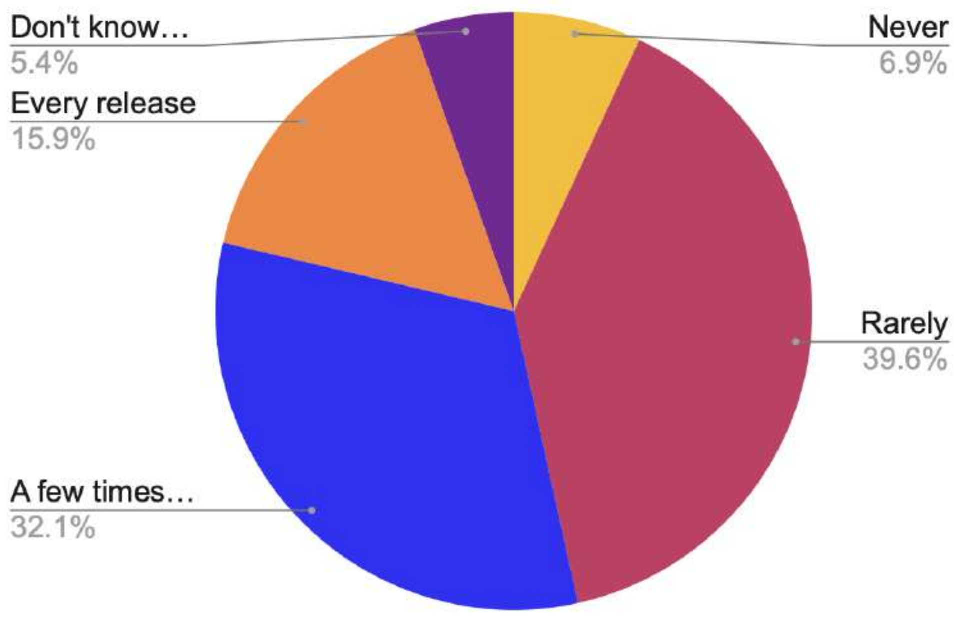
While it's not feasible to fully eliminate vulnerabilities from reaching production code, minimizing and remediating them based on best practices, DevSecOps tooling, and effective prioritization makes a significant difference to risk levels.

Respondents report that Critical and High severity vulnerabilities make their way to production with consistency and can take significant time to be remediated, meaning there is still plenty of work to do here.

> "AppSec leaders - the top 20% of organizations - remediate critical vulnerabilities in less than one day"

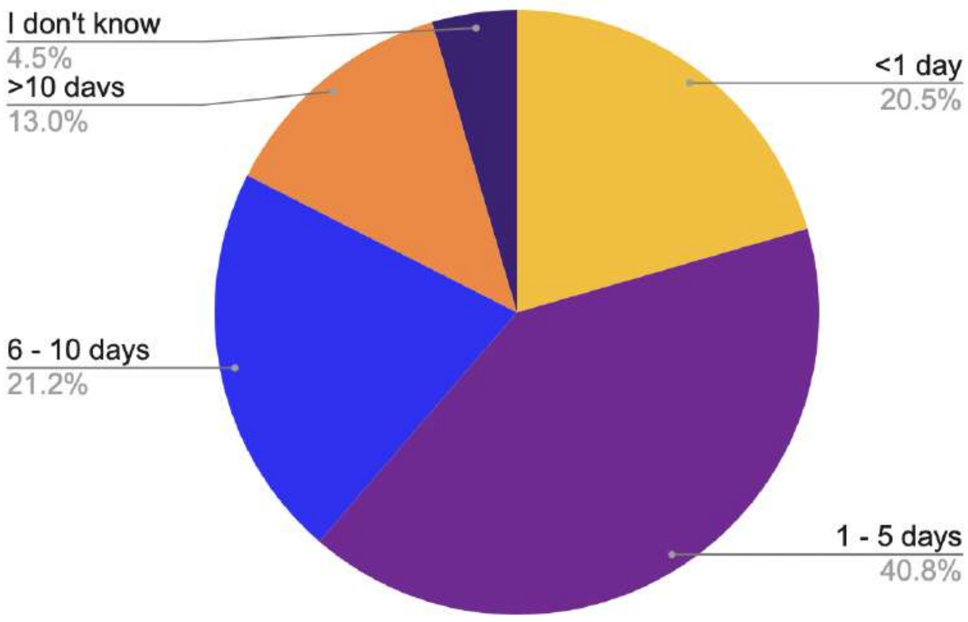
**How often do critical or high Severity vulnerabilities make their way into production?**

Response vs. Answer choices



**What is your typical remediation time for Critical Severity vulnerabilities?**

Response vs. Answer choices



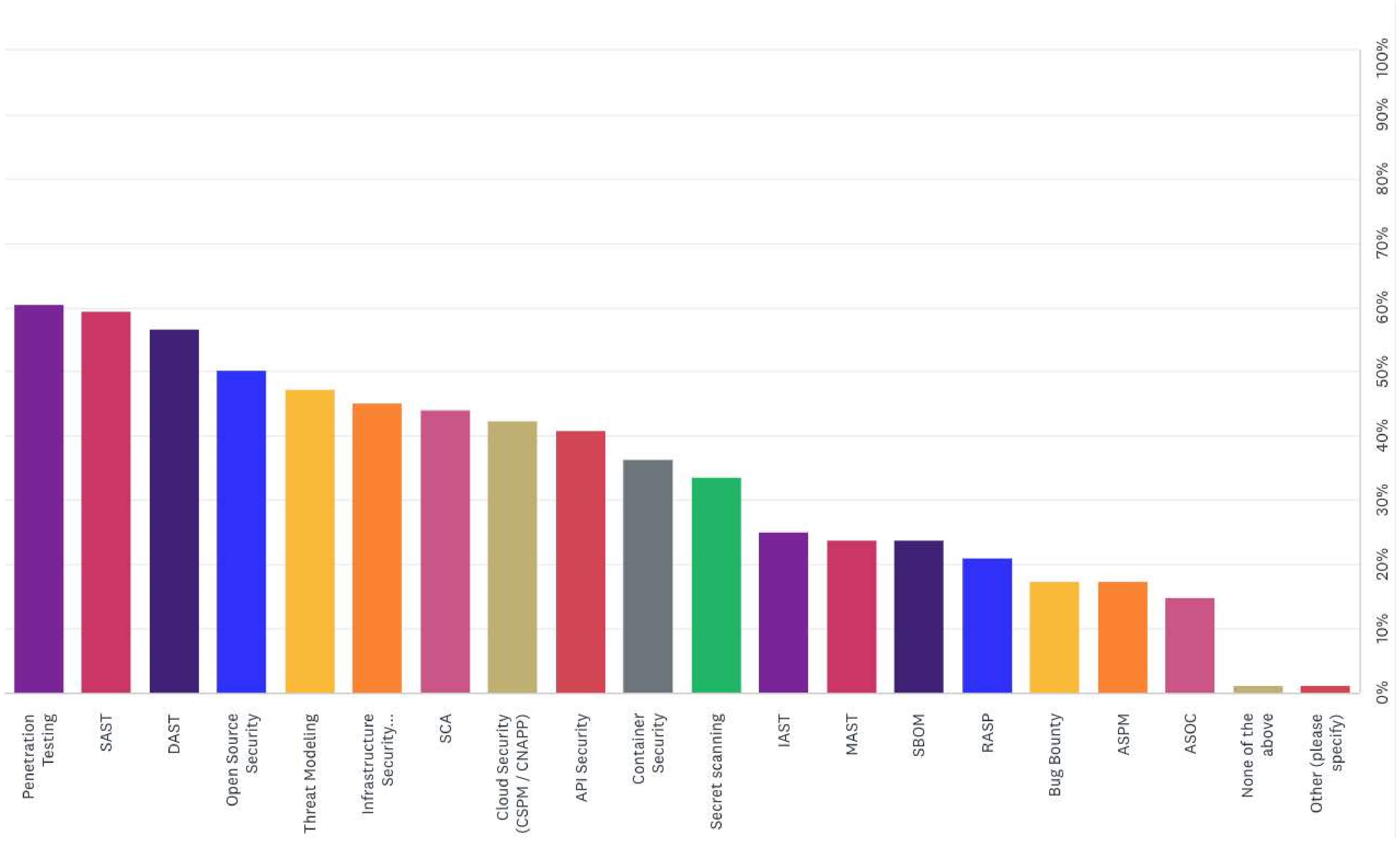
# The toolset

The right tools for the job make it easy to spot and fix vulnerabilities, decrease developer workload, speed time-to-production, enhance security posture, and automate and orchestrate for fully integrated security practices.

While this list is not exhaustive, it provides a solid baseline for a mature AppSec program.

**What initiatives do you leverage as part of your software security program?**

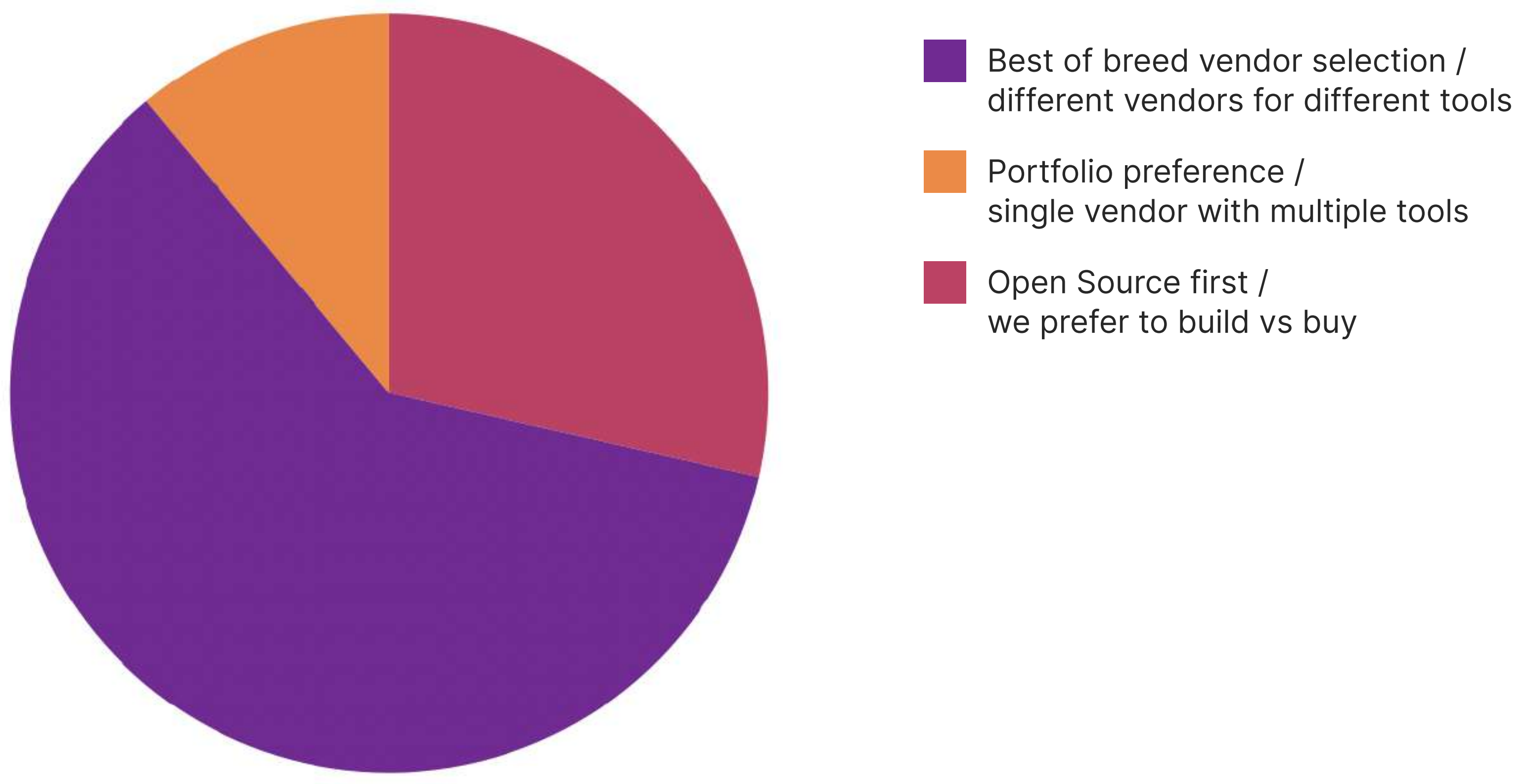
| Answer Choices | Response Percentage |
|---|---|
| Penetration Testing | 60.49% |
| Static Application Security Testing (SAST) | 59.27% |
| Dynamic Application Security Testing (DAST) | 56.53% |
| Open Source Security / Licensing | 50.15% |
| Threat Modeling | 47.11% |
| Infrastructure Security (Vulnerability Management) | 44.98% |
| Source Composition Analysis (SCA) | 44.07% |
| Cloud Security (CSPM / CNAPP) | 42.25% |
| API Security | 41.03% |
| Container Security | 36.17% |
| Secret scanning | 33.43% |
| Interactive Application Security Testing (IAST) | 24.92% |
| Software Bill of Materials (SBOM) | 24.01% |
| Mobile Application Security Testing (MAST) | 23.71% |
| Runtime Application Security Protection (RASP) | 20.97% |
| Bug Bounty | 17.33% |
| Application Security Posture Management (ASPM) | 17.33% |
| Application Security Orchestration and Correlation (ASOC) | 14.89% |
| None of the above | 1.22% |



# The vendors and buying approaches

The right tools for the job make it easy to spot and fix vulnerabilities, decrease developer workload, speed time-to-production, enhance security posture, and automate and orchestrate for fully integrated security practices.

The majority of respondents take a best-of-breed approach to tool selection, looking for the best vendor for any given tooling category, rather than opting to be a single vendor shop or build tools themselves.



While this list is not exhaustive, it provides a solid baseline for a mature AppSec program.

### Which of the following security vendors are you using in your software security program?

| Answer Choices | Responses |
|---|---|
| AWS Security Hub | 32.42% |
| Amazon Inspector | 26.30% |
| Synk | 24.16% |
| SonarQube | 23.55% |
| Bitbucket | 22.63% |
| OWASP Zap | 21.41% |
| OWASP Dependency Check | 19.88% |
| Tenable | 18.35% |
| JFrog | 18.04% |
| Rapid7 | 16.51% |
| Fortify | 14.98% |
| Black Duck (Synopsis) | 14.07% |
| Other (please specify) | 13.76% |
| Prisma Cloud (Palo Alto Networks) | 13.46% |
| Qualys | 13.46% |
| Checkmarx | 13.15% |
| Veracode | 10.70% |
| ArmorCode | 10.40% |
| HackerOne | 9.48% |
| Wiz | 8.87% |
| Coverity(Synopsys) | 7.34% |
| BugCrowd | 7.03% |
| Contrast Security | 7.03% |
| Orca | 7.03% |
| Security Scorecard | 5.81% |
| Cloud Optix | 5.50% |
| Bionic | 5.20% |
| Thread Modeler | 5.20% |
| WhiteHat(NTT Application Security) | 5.20% |
| Semgrep | 4.89% |
| Lacework | 4.59% |
| Nucleus Security | 4.28% |
| WhiteSource | 4.28% |
| Brakeman | 3.36% |
| Apiiro | 3.06% |
| Kenna (Cisco) | 3.06% |

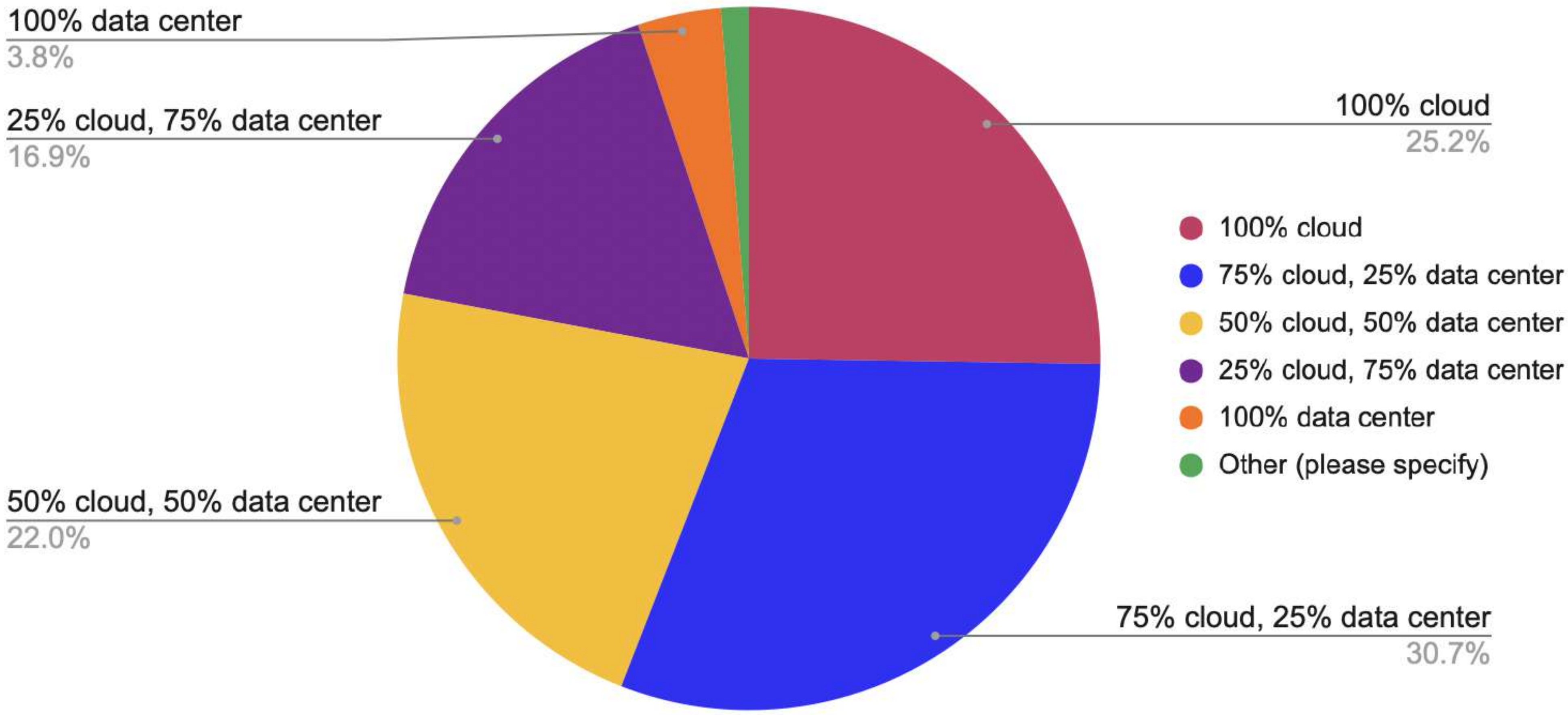
# Where do we deploy?

Shifted to the cloud or running in data centers? In 2023, more organizations than ever are running most of their workloads in the cloud. However, on-premises is still a major force and something organizations can’t ignore from a security perspective.

### Where do you deploy applications today?

| Answer Choices | Responses % |
|---|---|
| 100% cloud | **25.24%** |
| 75% cloud, 25% data center | **30.67%** |
| 50% cloud, 50% data center | **22.04%** |
| 25% cloud, 75% data center | **16.93%** |
| 100% data center | **3.83%** |
| Other (Please specify) | **1.28%** |

> **“More than half of respondents deploy 75% or more of their applications in the cloud, and a quarter run full cloud.”**



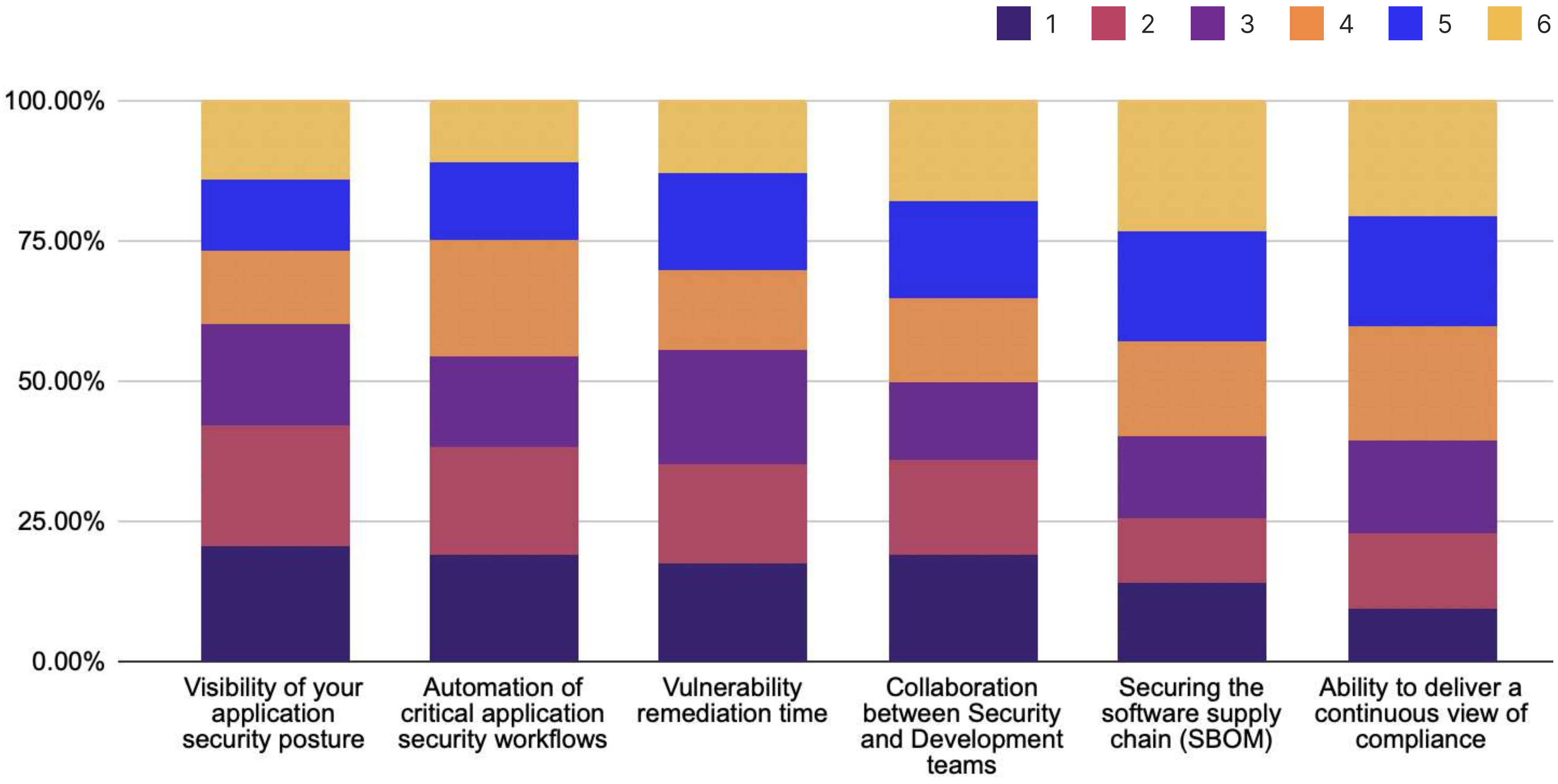
# AppSec prioritization

**What's the most important focus of your AppSec program for the 12 months?**

For most organizations, visibility of application security posture and automation of critical application security workflows will be the main focus for the year. While securing the software supply chain (SBOM) comes in last, supply chain attacks continue to rise, increasing risk in this key area.

**What do you plan to focus on over the next 12 months?**

Ranked from 1-6, with 1 being the highest



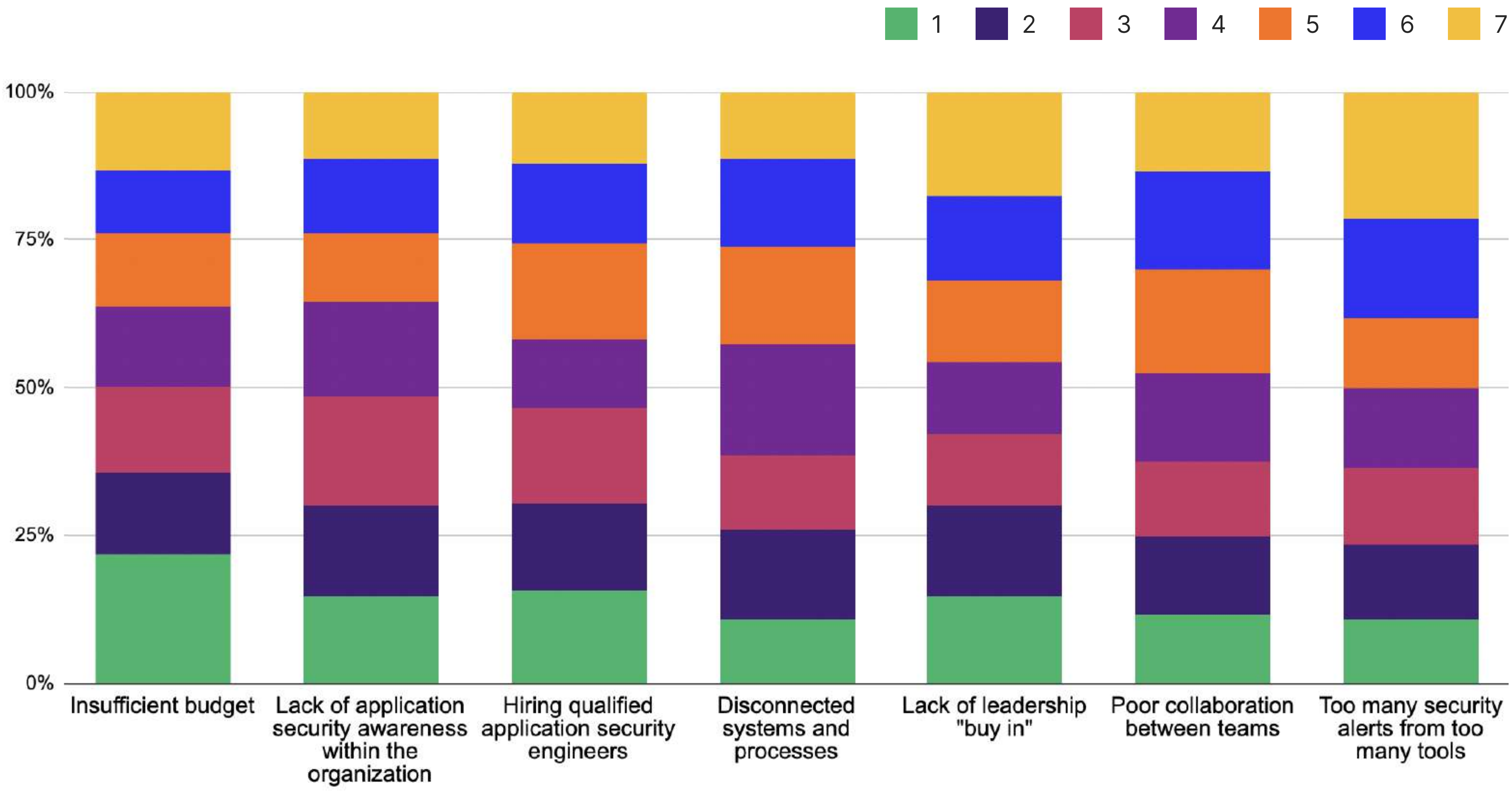
# Challenges in running a successful AppSec program

**You're working on culling too many AppSec alerts. You're finally un-siloing systems and data effectively. So what are the new challenges?**

Not having enough funding is a standout challenge in running a successful AppSec program among respondents. Other notables are in hiring, broader AppSec awareness and lack of leadership buy-in.

**What are the challenges for a successful application security program?**

The challenges for a successful application security program, ranked from 1-7



# All about the SBOM

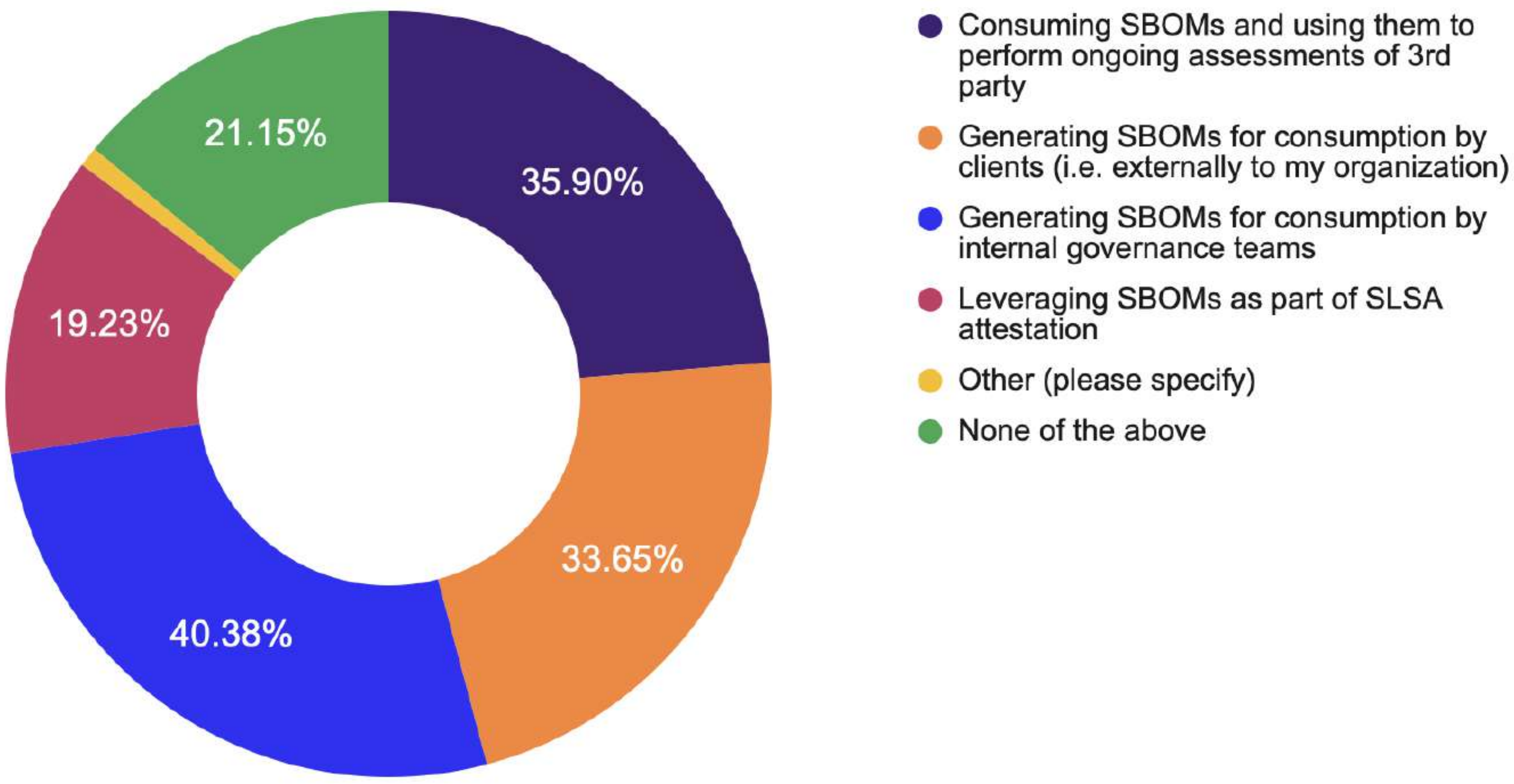
While we're on the topic of software supply chain risk, a Software Bill of Materials goes a long way to understanding the full extent of an application's threat surface.

Generating, consuming, and leveraging SBOMs provides a far more comprehensive and fair assessment of and organization's AppSec posture.

> "Over 20% of respondents had no SBOM usage at all"

**How are you currently leveraging SBOMs within your organizations?**

| Answer Choices | Response Percentage |
|---|---|
| Consuming SBOMs and using them to perform ongoing assessments of 3rd party | 35.9% |
| Generating SBOMs for consumption by clients (i.e externally to my organization) | 33.65% |
| Generating SBOMs for consumption by internal governance teams | 40.38% |
| Leveraging SBOMs as part of SLSA attestation | 19.23% |
| Other(Please specify) | 1.28% |
| None of the above | 21.15% |



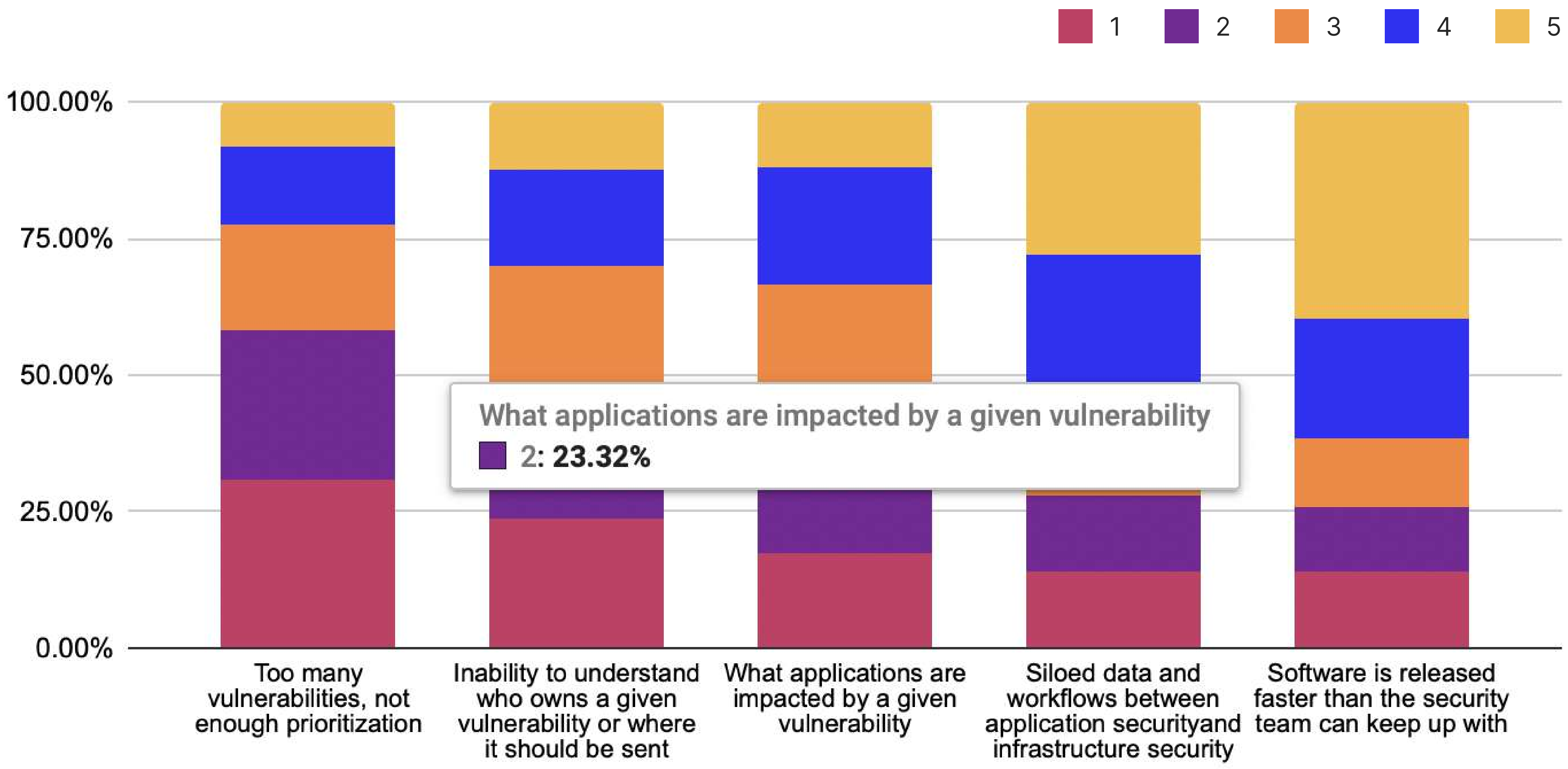
# Challenges for AppSec on the ground

For AppSec teams, on the ground, the challenges faced day to day are different.

We've learned that teams are still extremely concerned that there are too many vulnerabilities with not enough prioritization. Being able to analyze and triangulate results across a variety of tools and highlight risk priorities - even when they're constantly shifting - remains difficult.

**What are the biggest stumbling blocks your software security team runs into?**

Ranked from 1-5, with 1 being the biggest obstacle



# Methodology

This survey was run by the Purple Book Community, and was circulated among Purple Book Community members, extended security networks, and across social media.