# State of Application Security Operations 2022

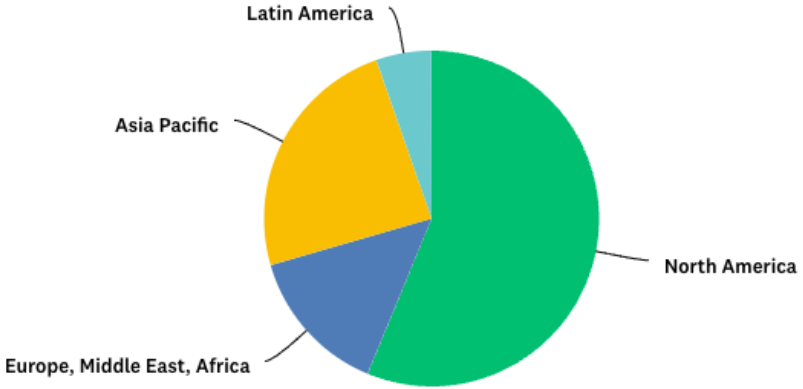
## How industry leaders ship secure software and ship it fast

Brought to you by

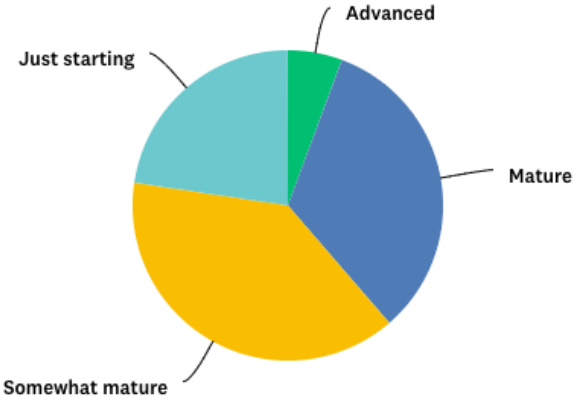
# Over 500 Respondents so far …

65% Security Team, 35% Development Team
59% Leaders, 41% Practitioners

Where are you currently working?



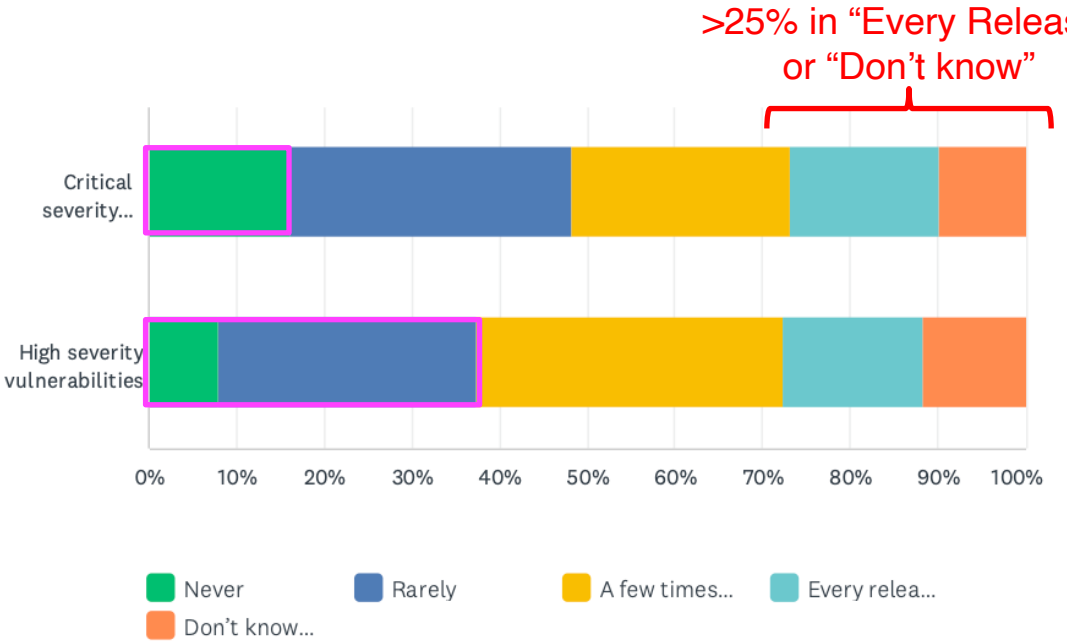

How would you rate the maturity of your application security program?



>42% of Respondents have

“Unmanaged risk in the portfolio”

# How often do critical or high severity vulnerabilities make their way into production?




What does a Leader look like?

- Never release a Critical
- Never/Rarely release a High

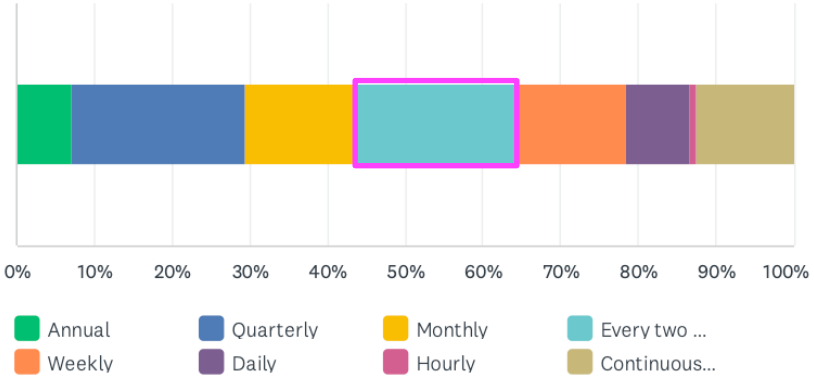
Only 7.6% of Respondents

>63% of Respondents agree

“Shipping fast takes priority over shipping secure.”

# How fast do we release? How fast do we remediate?

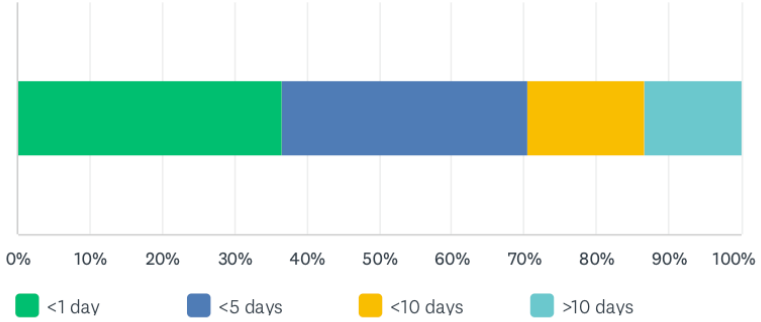
What is the typical frequency of your organization's software releases?



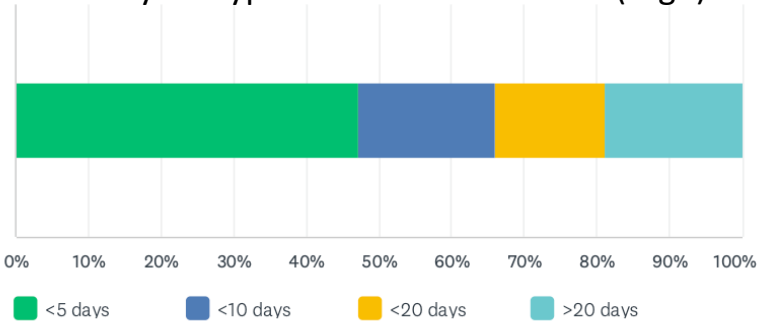

The Leaders:

- **Never release more often than "Weekly"**
- Most common is "Every two weeks"

What is your typical remediation time? (Critical)

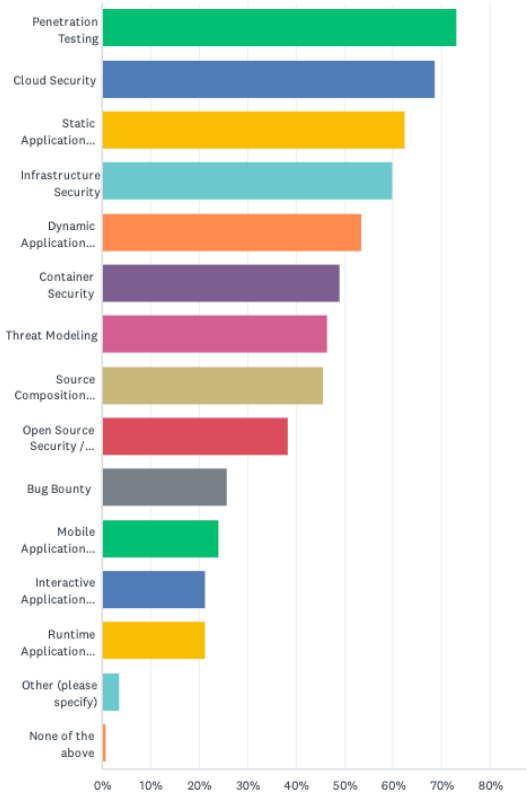



What is your typical remediation time? (High)



“AppSec tools embedded into the DevOps pipeline” is the #1 AppSec initiative

# What are the techniques needed?

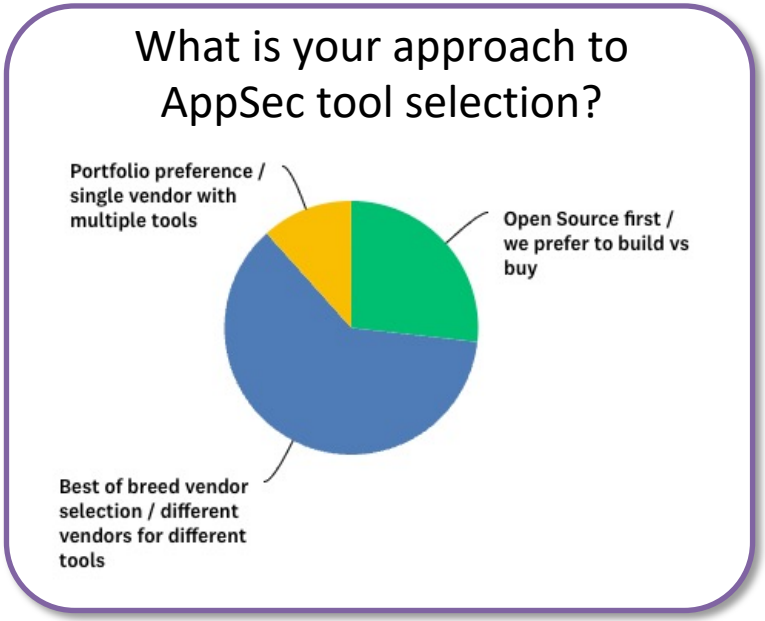


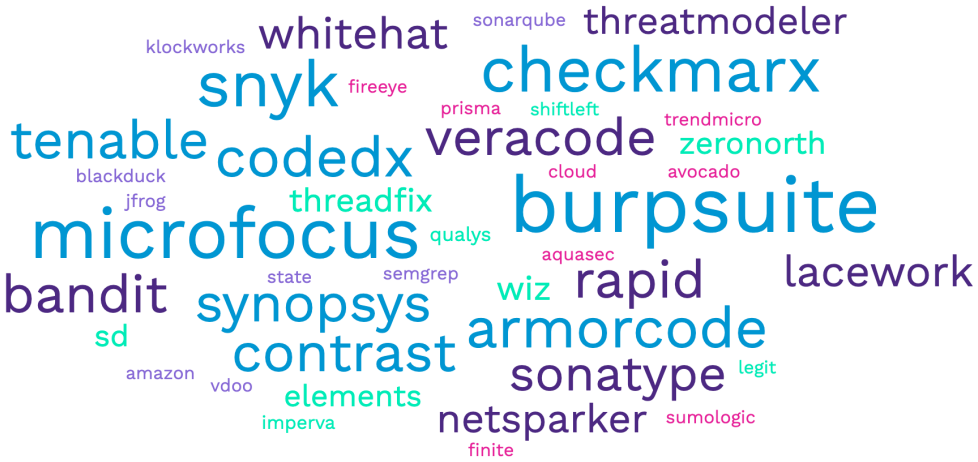

| ANSWER CHOICES | RESPONSES |
|---|---|
| Penetration Testing | 73.21% |
| Cloud Security | 68.75% |
| Static Application Security Testing (SAST) | 62.50% |
| Infrastructure Security | 59.82% |
| Dynamic Application Security Testing (DAST) | 53.57% |
| Container Security | 49.11% |
| Threat Modeling | 46.43% |
| Source Composition Analysis (SCA) | 45.54% |
| Open Source Security / Licensing | 38.39% |
| Bug Bounty | 25.89% |
| Mobile Application Security Testing (MAST) | 24.11% |
| Interactive Application Security Testing (IAST) | 21.43% |
| Runtime Application Security Protection (RASP) | 21.43% |

**The Leaders …**

- SAST, DAST, and Penetration Testing are core capabilities
- >80% also leverage SCA, Cloud, Container, Infrastructure security tools

# What are the tools used?




**The Leaders …**

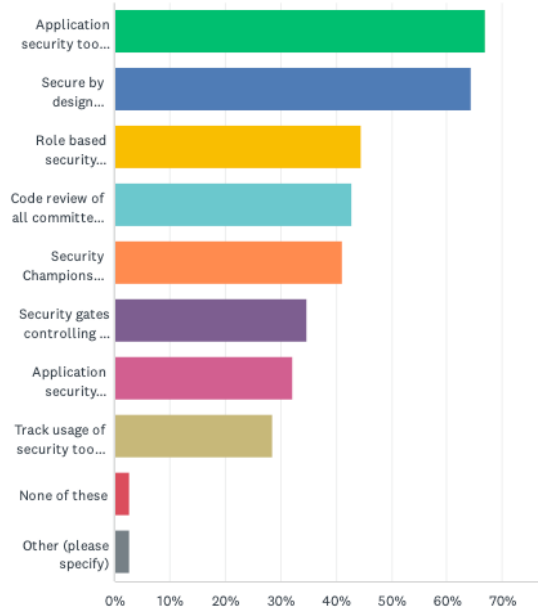
- >75% take "Best of Breed" approach

>86% of Respondents agree

“Security tools are interchangeable;

it is the process that is most important.”

# What initiatives are part of your AppSec program?




| ANSWER CHOICES | RESPONSES |
|---|---|
| Application security tools embedded into the DevOps pipeline | 66.96% |
| Secure by design practices | 64.29% |
| Role based security education program | 44.64% |
| Code review of all committed code before release | 42.86% |
| Security Champions embedded in the development teams | 41.07% |
| Security gates controlling the release of software into production | 34.82% |
| Application security maturity model (such as OWASP SAMM) | 32.14% |
| Track usage of security tools across teams | 28.57% |

**The Leaders …**

1. AppSec tools embedded into DevOps
2. Code review of all committed code before release
3. Secure by design practices

# >40% of Respondents leverage “Security Champions”

# How are AppSec programs structured and budgeted?

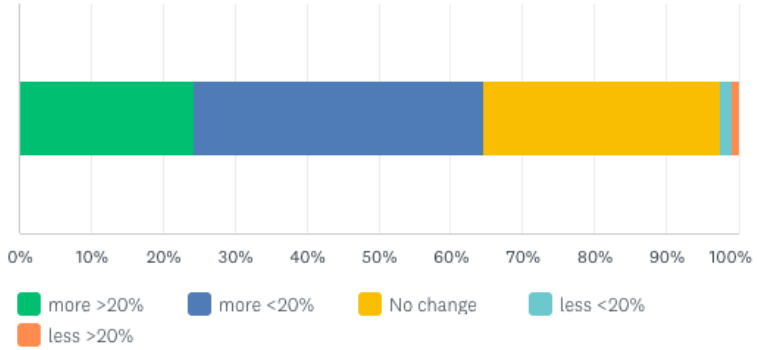
**Size of AppSec Team**
(Dev:AppSec ratio)

- Average: 90:1
- Max: 500:1
- **Leaders**: 50:1

**Budget (tools, training, AppSec engineers)**
($ / Developer)

- Average: $7000
- Most common: $5000
- **Leaders**: $3500

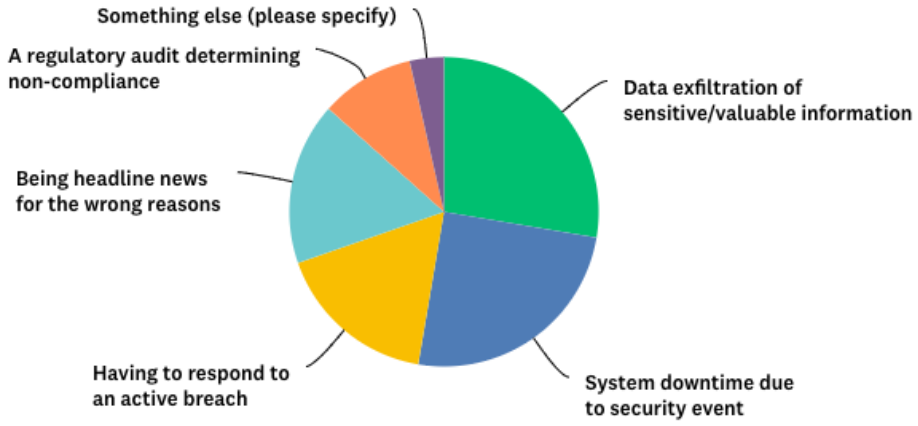
How do you expect your application security budget to change over the next 12 months?



“Hiring qualified application security engineers” is the #1 challenge for building a successful AppSec program

# What about the next 12 months?

**What is your biggest fear for the coming 12 months?**



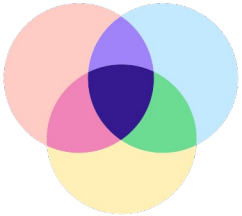

**The top 3 challenges for a successful AppSec program?**

1. Hiring qualified AppSec engineers
2. Disconnected systems and processes
3. Poor collaboration between teams

**Focus on over the next 12 months**

1. Automation of critical AppSec workflows
2. Visibility of application security posture
3. Collaboration between Security and Development teams

Brought to you by



ArmorCode

ArmorCode is the industry leading AppSecOps platform. ArmorCode delivers continuous visibility and actionable insights so that AppSec teams can successfully identify, prioritize and remediate the highest risk application security issues, vulnerabilities, and coverage and compliance gaps - all in a single integrated AppSecOps platform. ArmorCode eliminates manual, repetitive and low value work across the DevSecOps pipeline and lets AppSec teams enroll and enable their development teams as security partners; scaling AppSec effectiveness and impact by 10x or more across the organization. ArmorCode customers use the platform for AppSec Posture, Vulnerability, and Compliance Management and DevSecOps orchestration and automation.

Enterprises like Shutterfly, SnapDoc, SnapFinance, Guardant Health and ChargePoint use ArmorCode to measure and improve application security posture, coverage and compliance while empowering development and Ops teams to ship and deploy more secure code faster; all without increased security staffing, developer training or workload. With the ArmorCode AppSecOps platform, application teams ship secure software, and ship it fast.

For more information visit: [http://www.armorcode.com](http://www.armorcode.com)