DEVSECOPS COMMUNITY SURVEY 2018

Sonatype

Signal Sciences

Software Engineering Institute
Carnegie Mellon

DZone

ranger4

SJ Technologies
Resources. Responsiveness. Reliability.

CONTINO

DEREK E. WEEKS

Vice President and DevOps Advocate, Sonatype

As the world witnessed record breaches in 2017, leading IT teams were integrating and automating more security practices throughout the software development lifecycle to better fortify applications and protect their data.

Over the past several years, our survey has revealed the growth in enterprise DevSecOps initiatives that have successfully incorporated automated security practices, strengthened their cybersecurity posture, and readied themselves for government regulations on the horizon. This survey, representing the voice of 2,076 IT professionals, demonstrates that DevSecOps practices continue to mature rapidly and that, once automated, security is difficult to ignore.

While some results of our survey may surprise you, I hope they also encourage you to begin new conversations with your peers and across our industry. Sharing these results can help motivate all of us to further mature DevSecOps practices everywhere and to establish new benchmarks for speed, quality, and security.

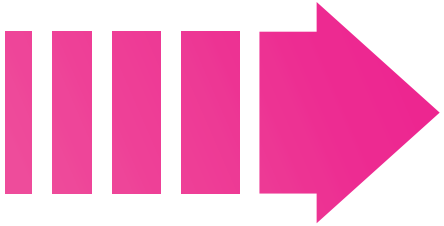
Thank you to all who participated in the survey and to our community partners: Carnegie Mellon's Software Engineering Institute, Contino, DZone, Ranger4, Signal Sciences, and SJ Technologies for helping us build this year's survey and promote its awareness.

2,076

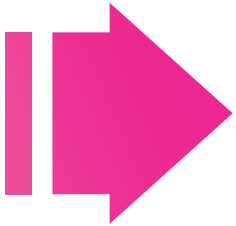
people shared their views with us this year.

How mature is your adoption of DevOps practices?

25%
have **mature**
DevOps practices



49%
are **improving**
their maturity.



26%
immature
practices

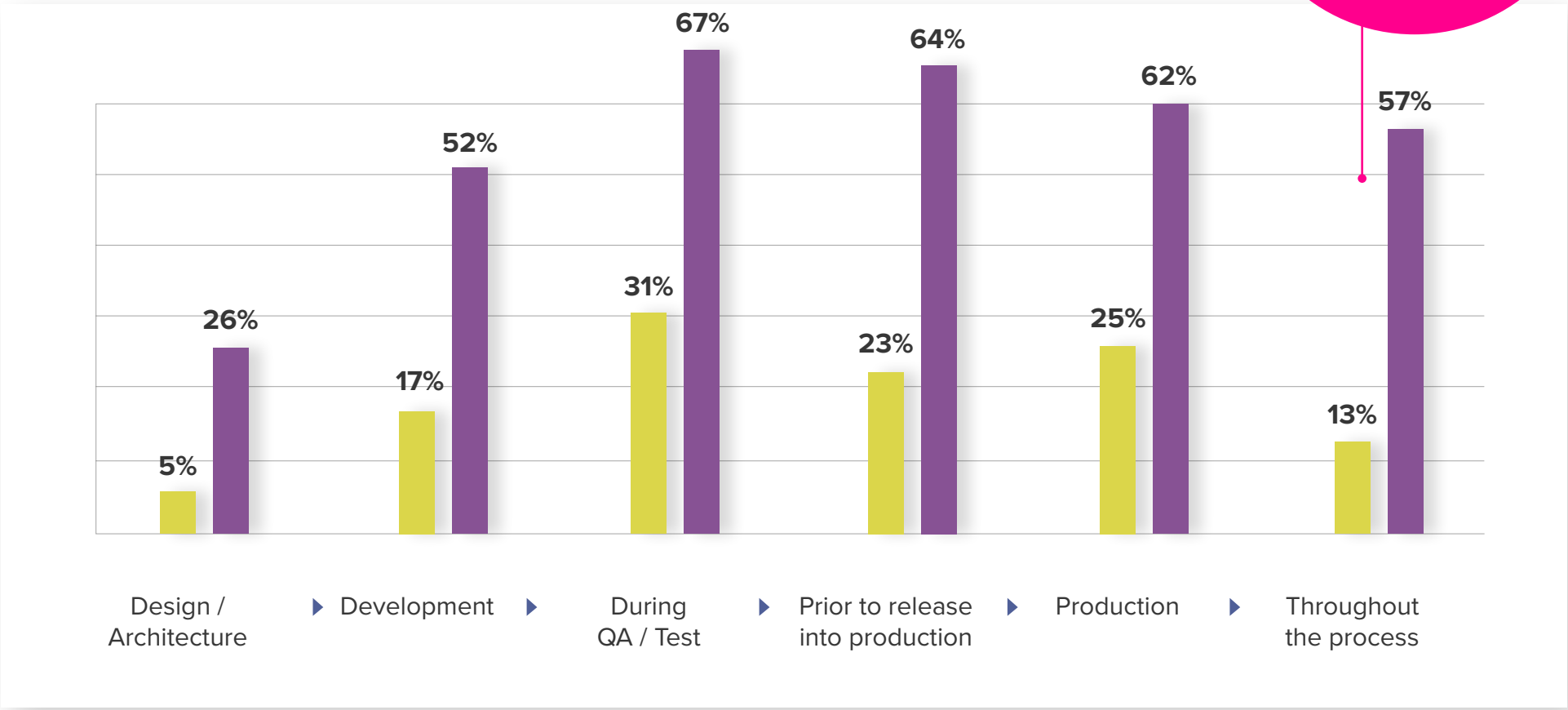
48%

of developers know security is important but don’t have enough time to spend on it.

DEVOPS RAMPS SECURITY INVESTMENTS

At what point in the development process does your organization perform automated application security analysis?

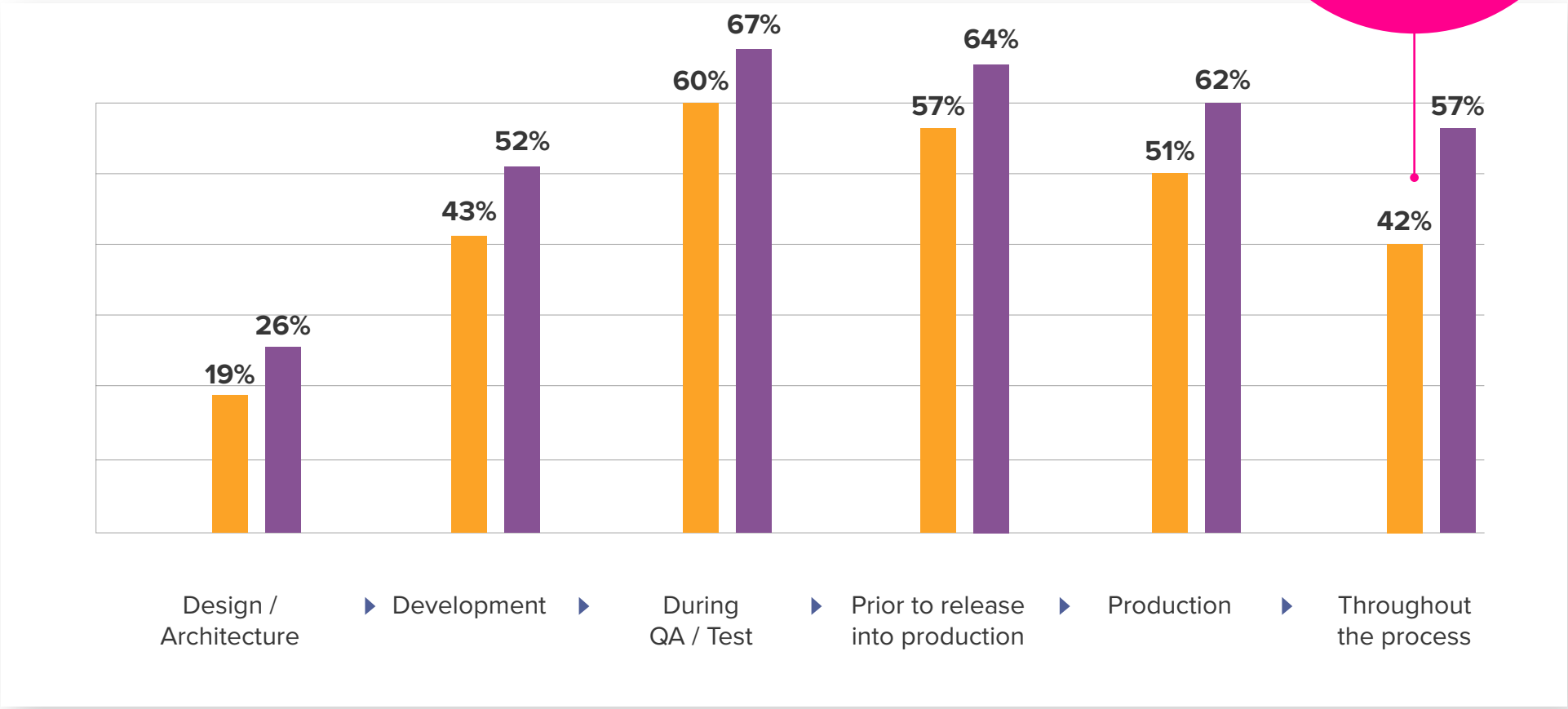
Mature DevOps practices are 338% more likely to integrate automated security.



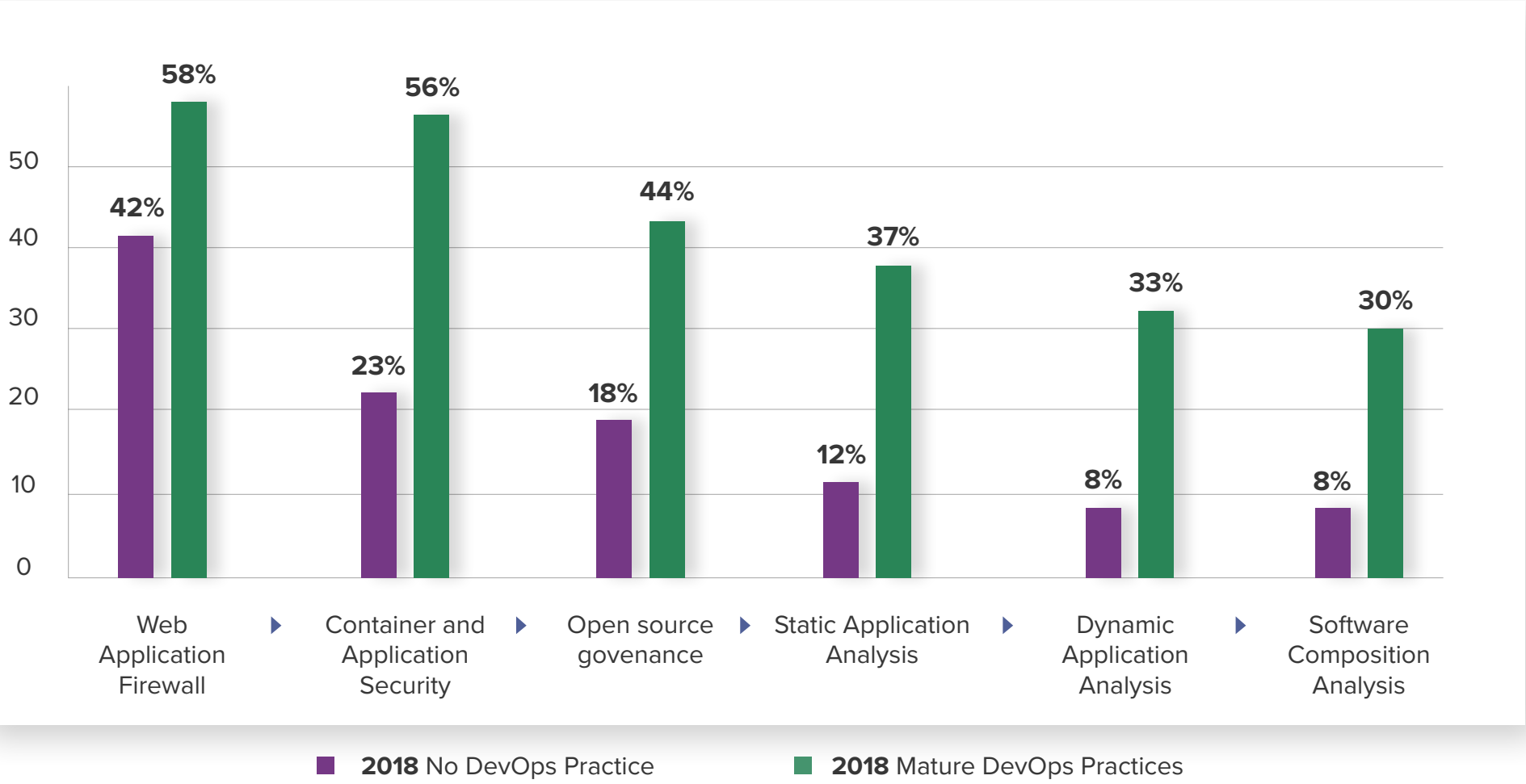

Mature DevOps practices are
338% MORE
likely to integrate security across the SDLC.

At what point in the development process does your organization perform automated application security analysis?

Mature DevOps practices ramped their investment in automated security by 15%.

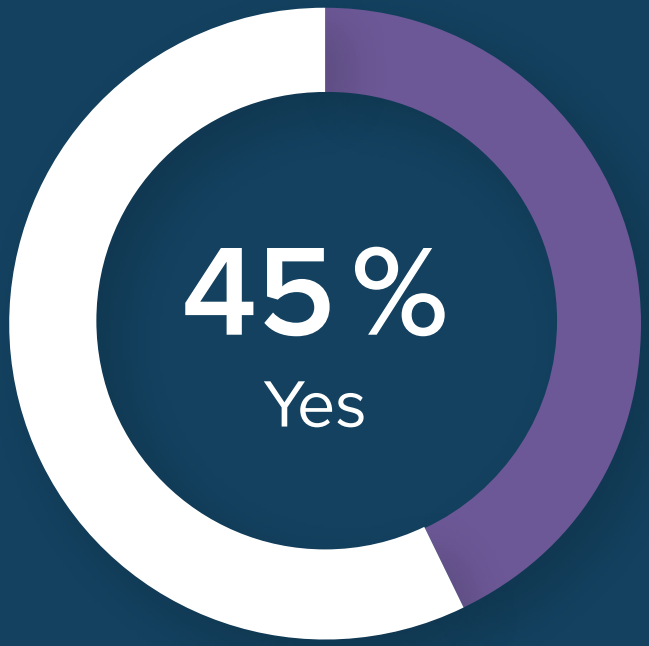


Which application security tools are critical to your organization?

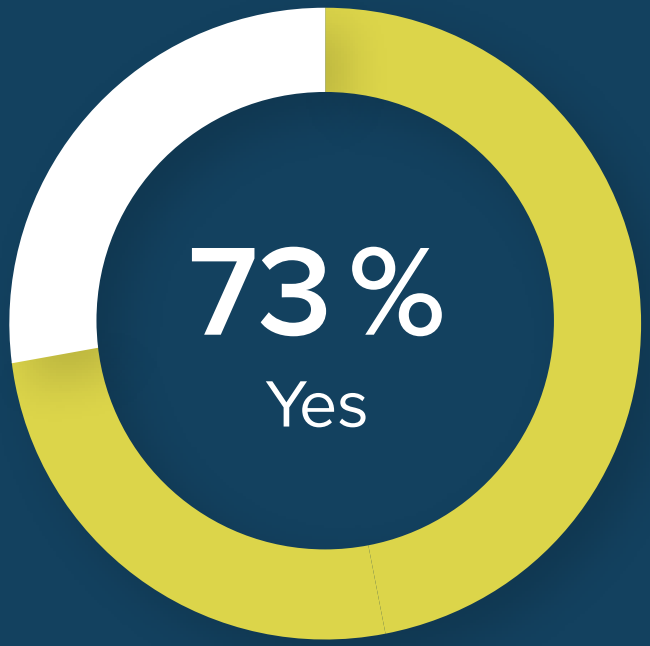


BREACHES HAPPEN

Have recent high profile breaches heightened interest in DevSecOps practices for your organization?



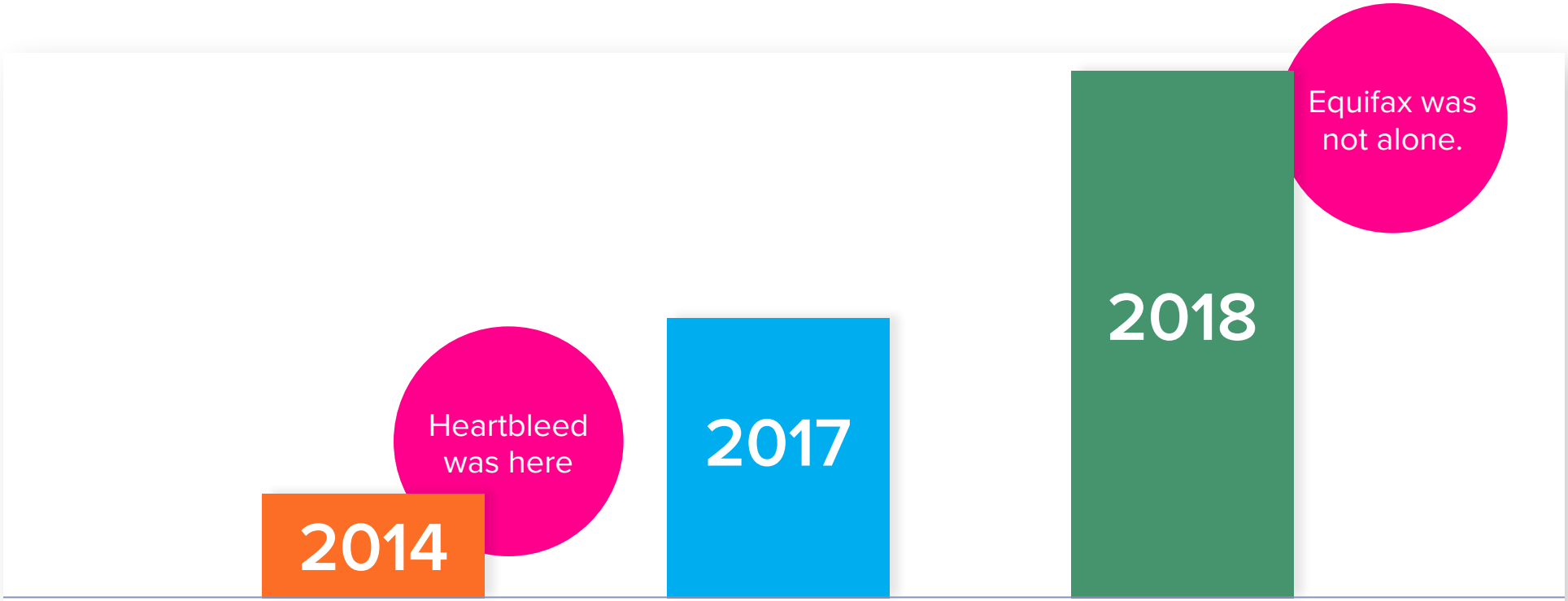
2018
No DevOps Practice



2018
Mature DevOps Practices

1-in-3 had or suspected a **breach due to web application** vulnerabilities in the last 12 months.

Has your organization had a breach that can be attributed to a vulnerability in an open source component or dependency in the last 12 months?



14%
suspect or have verified a breach related to open source components in the **2014 survey.**

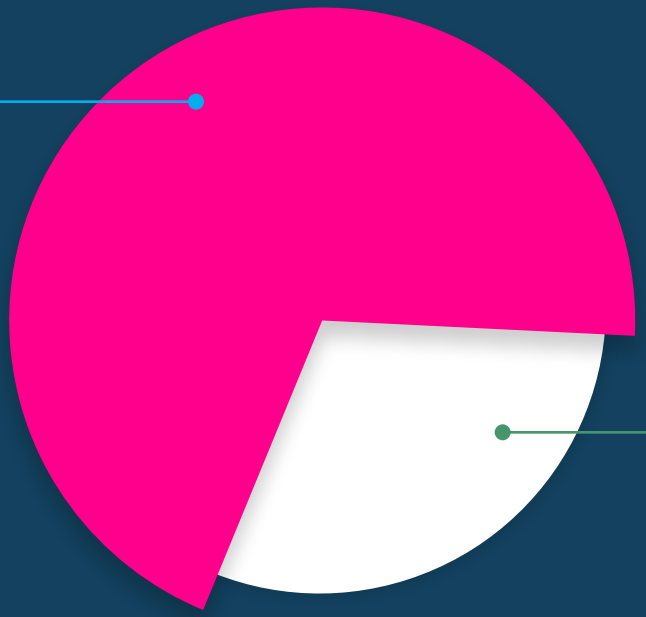
20%
suspect or have verified a breach related to open source components in the **2017 survey.**

31%
suspect or have verified a breach related to open source components **in the last 12 months.**

How well does your organization control which open source and third-party components are used in development?

62 %

of organizations **do not have meaningful controls** over what components are in their applications.

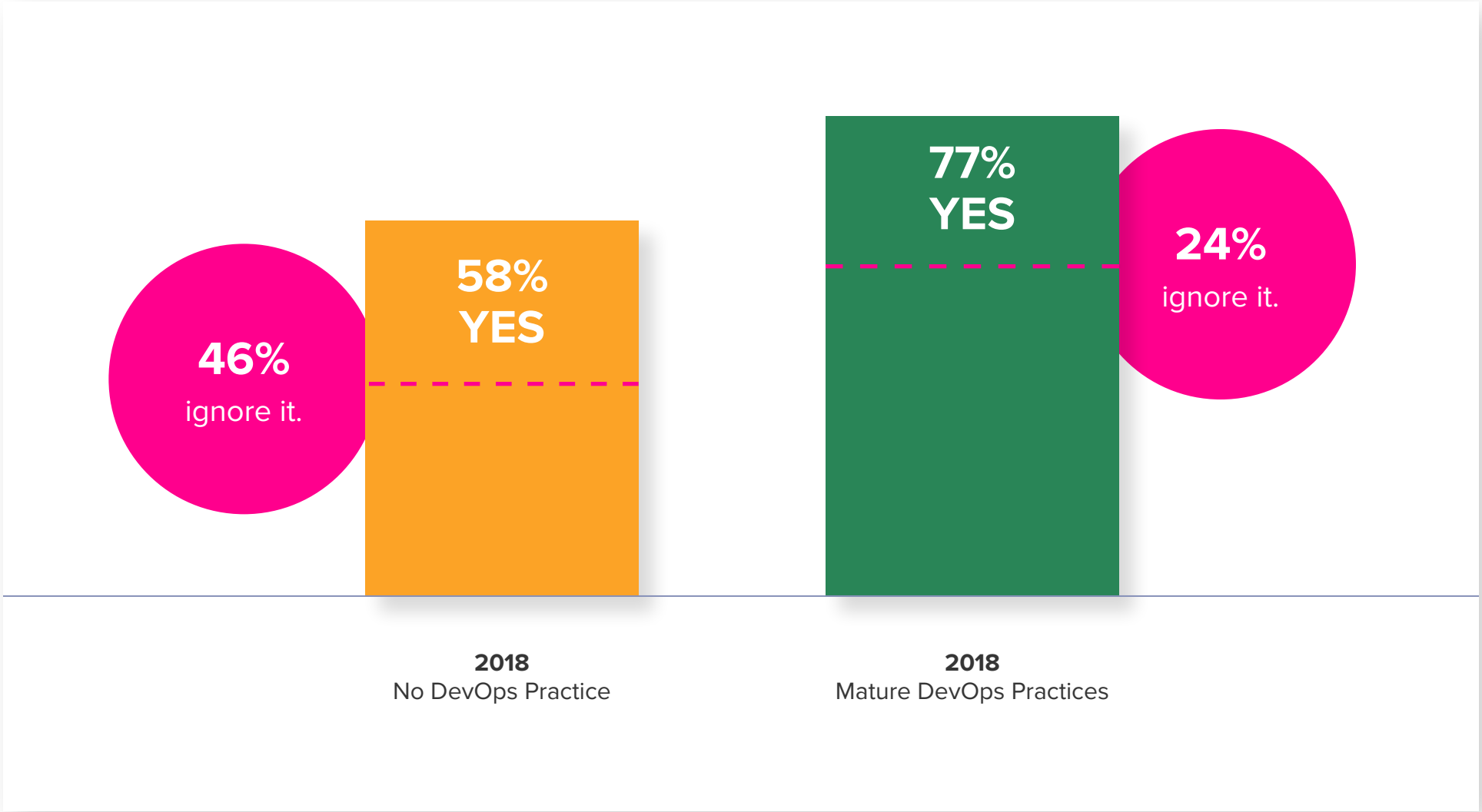


38 %

have a **complete software bill of materials** for each application.

Automation is difficult to ignore.

Question: Does your organization have an open source governance policy? If yes, do you follow it?



ARE YOU PREPARED?

OUTNUMBERED

100 : 10 : 1

Developement

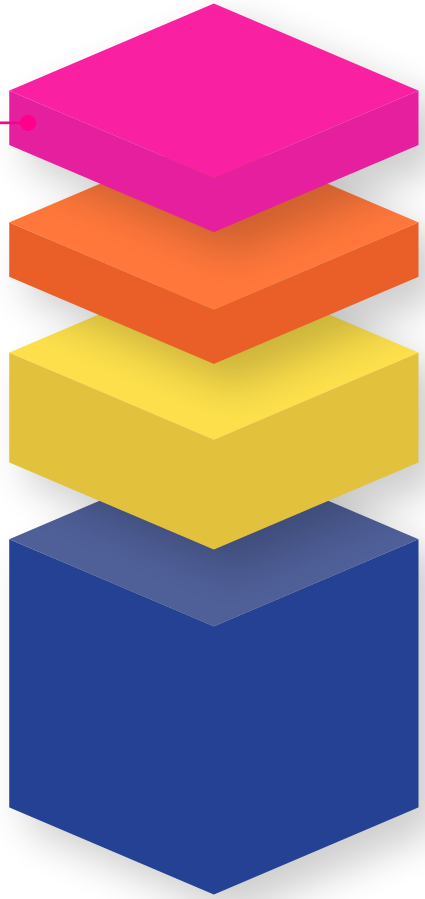
Operations

Security

What application security training is available to you?

ANSWERS FROM
Mature DevOps organizations

35%
of those with Agile or Waterfall practices received no training



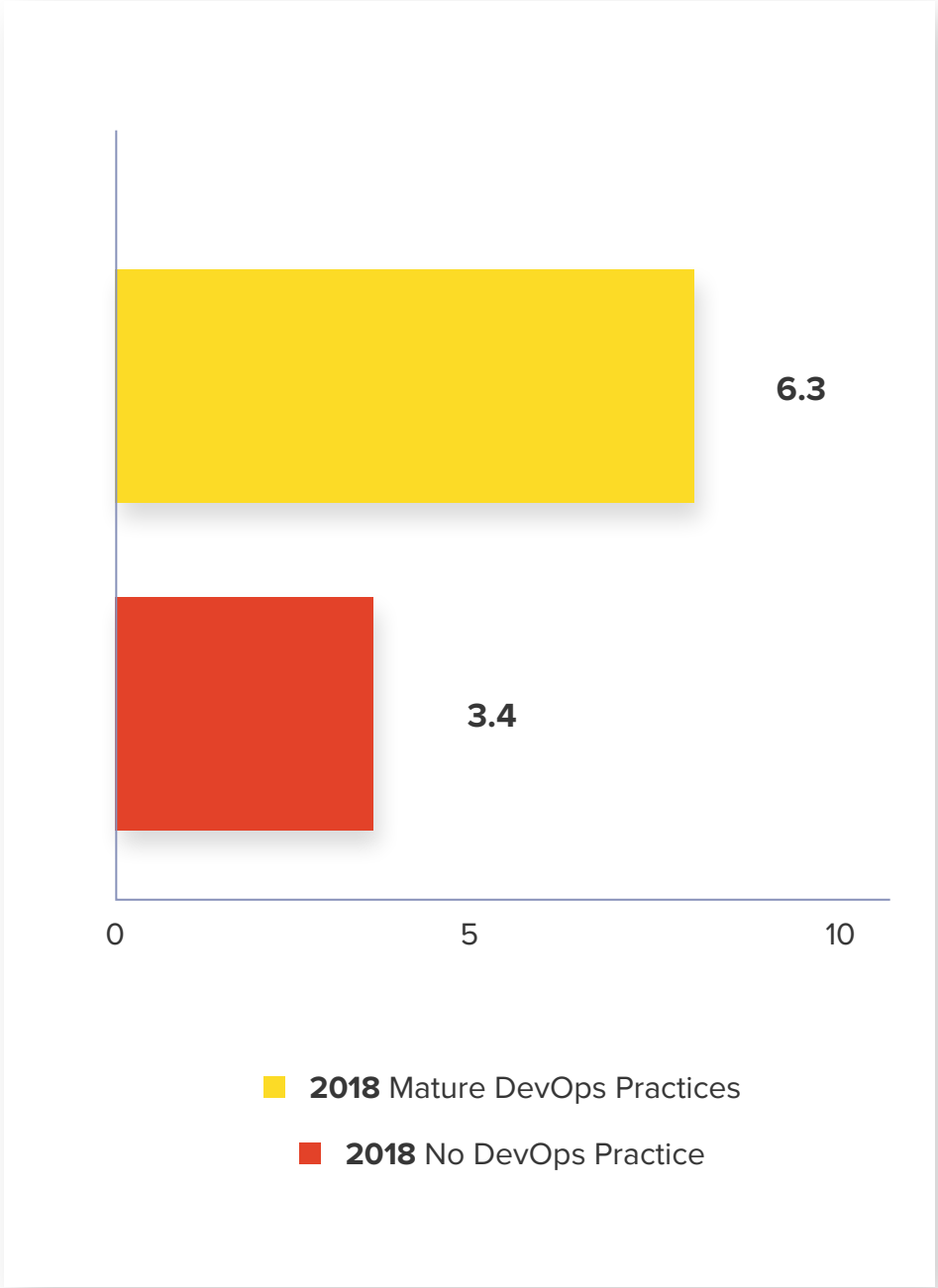
None
12 %

Instructor Led
12 %

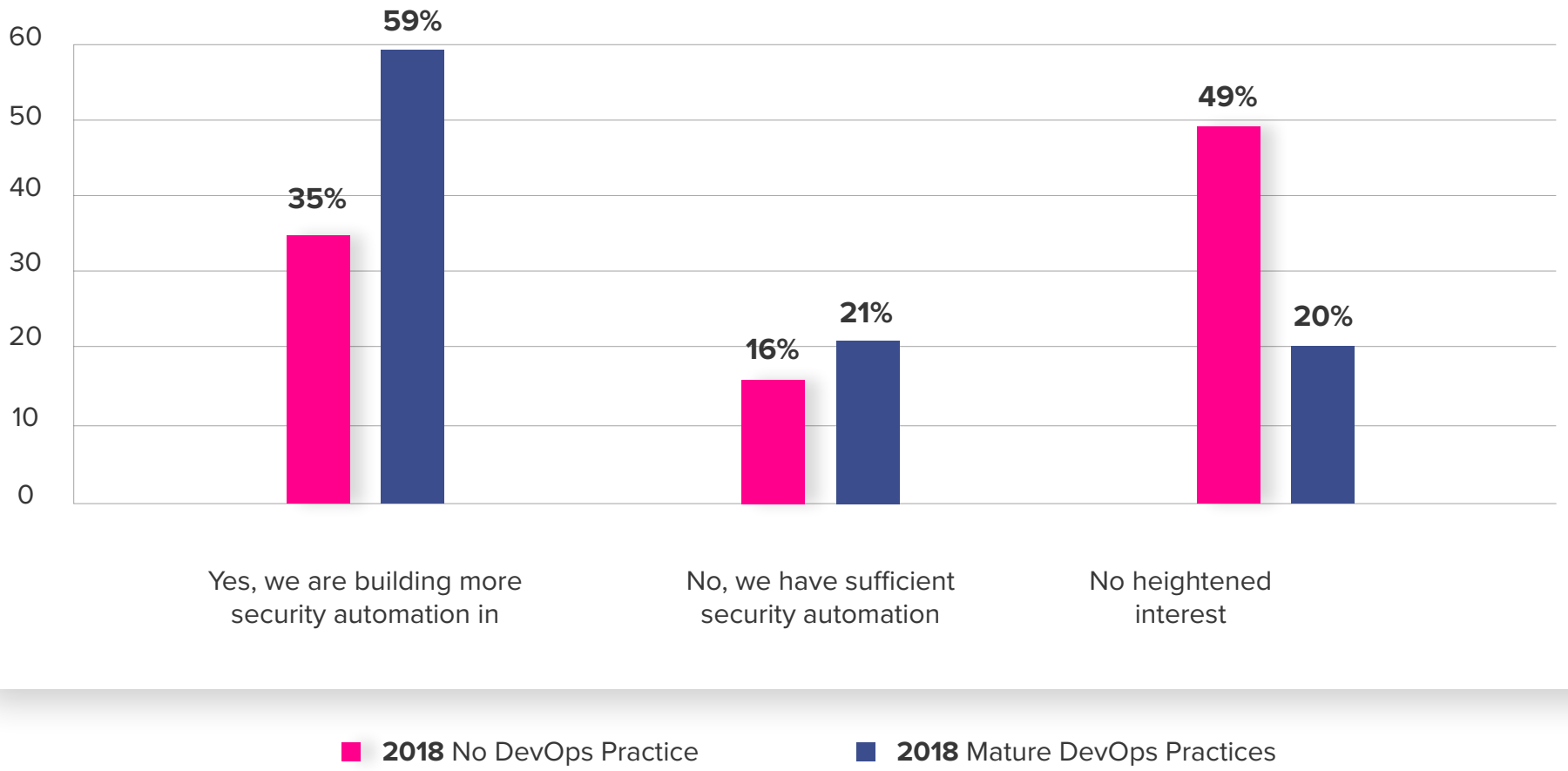
Secure coding/ programming
22%

E-learning
54%

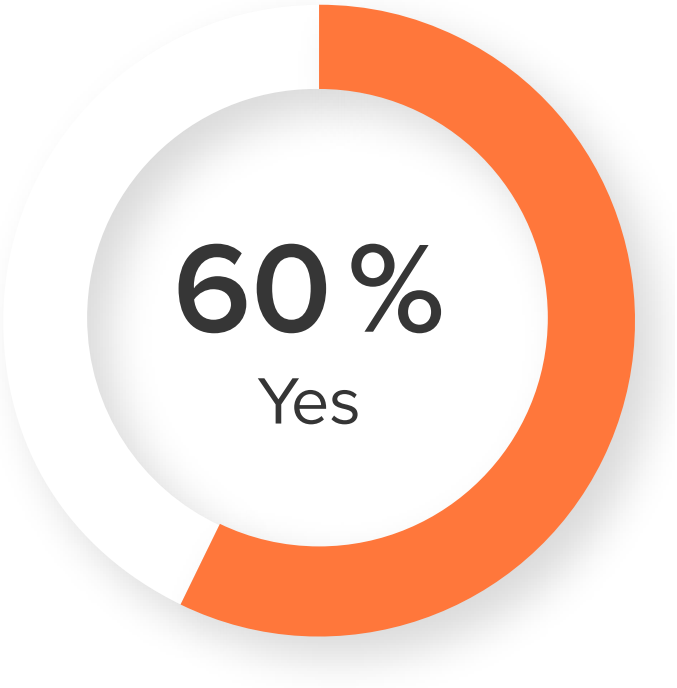
Rate your cybersecurity preparedness



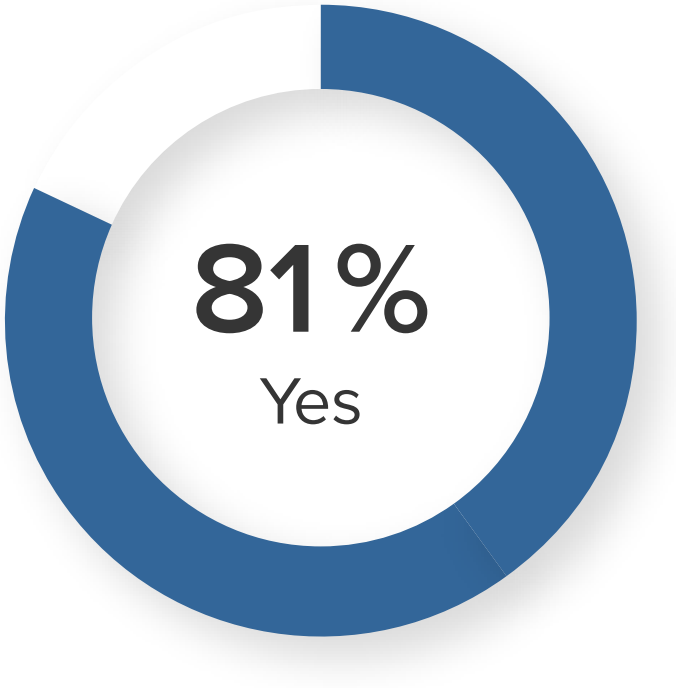
GDPR regulation heightened interest in building security automation into the SDLC.



Do you have a cybersecurity incident response plan in place?

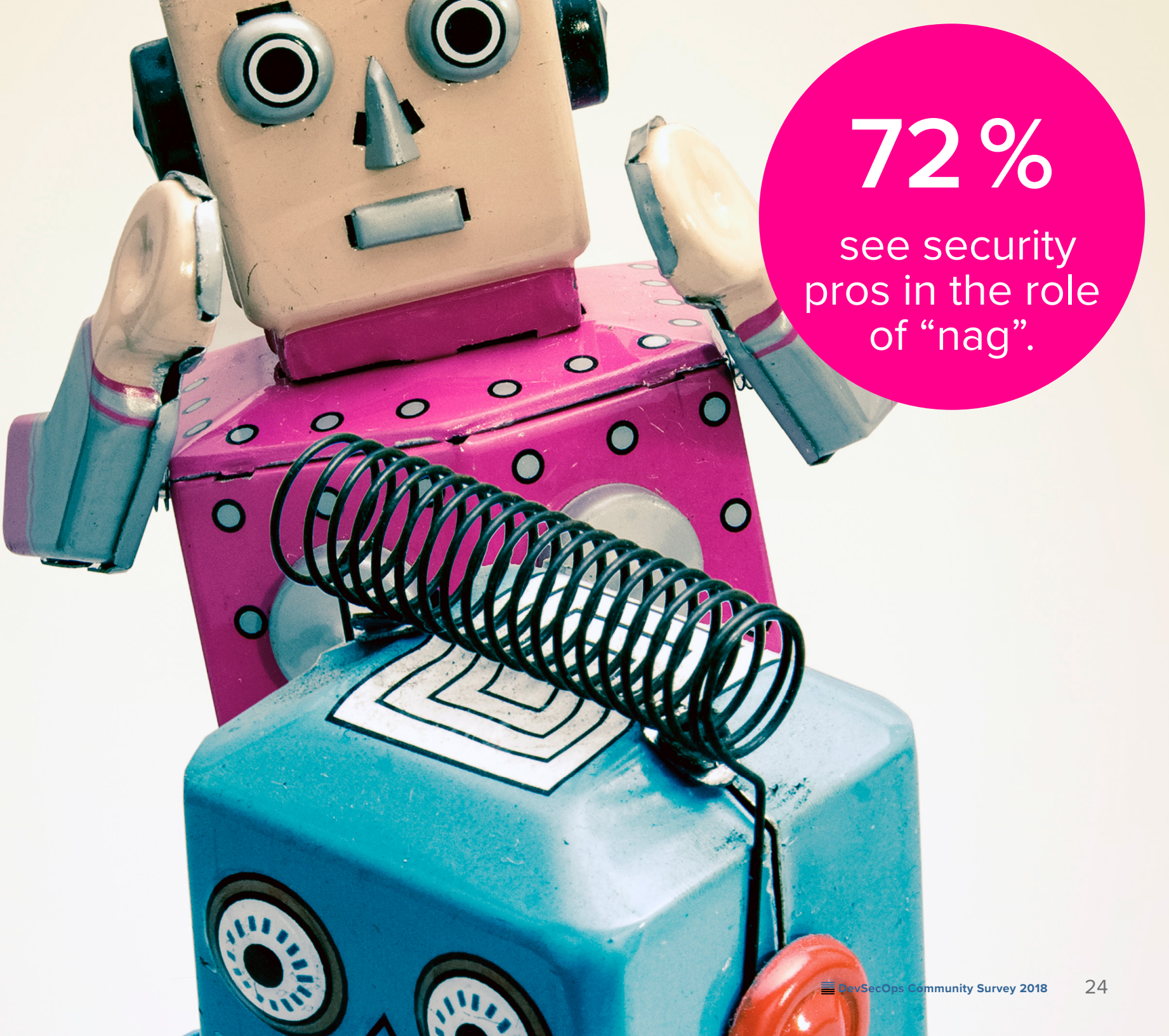


2018
No DevOps Practice



2018
Mature DevOps Practices

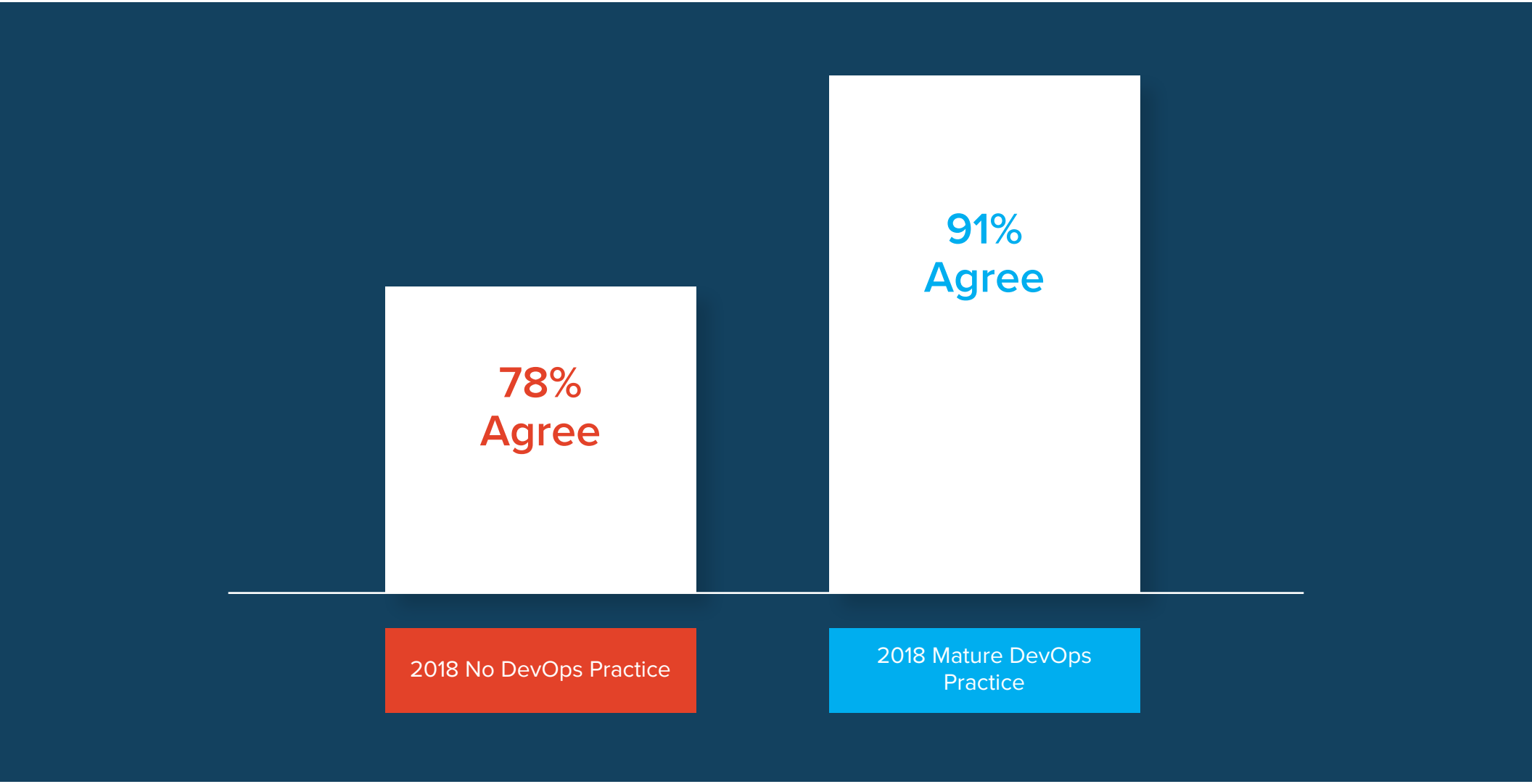
DEVSECOPS MINDSET



72%

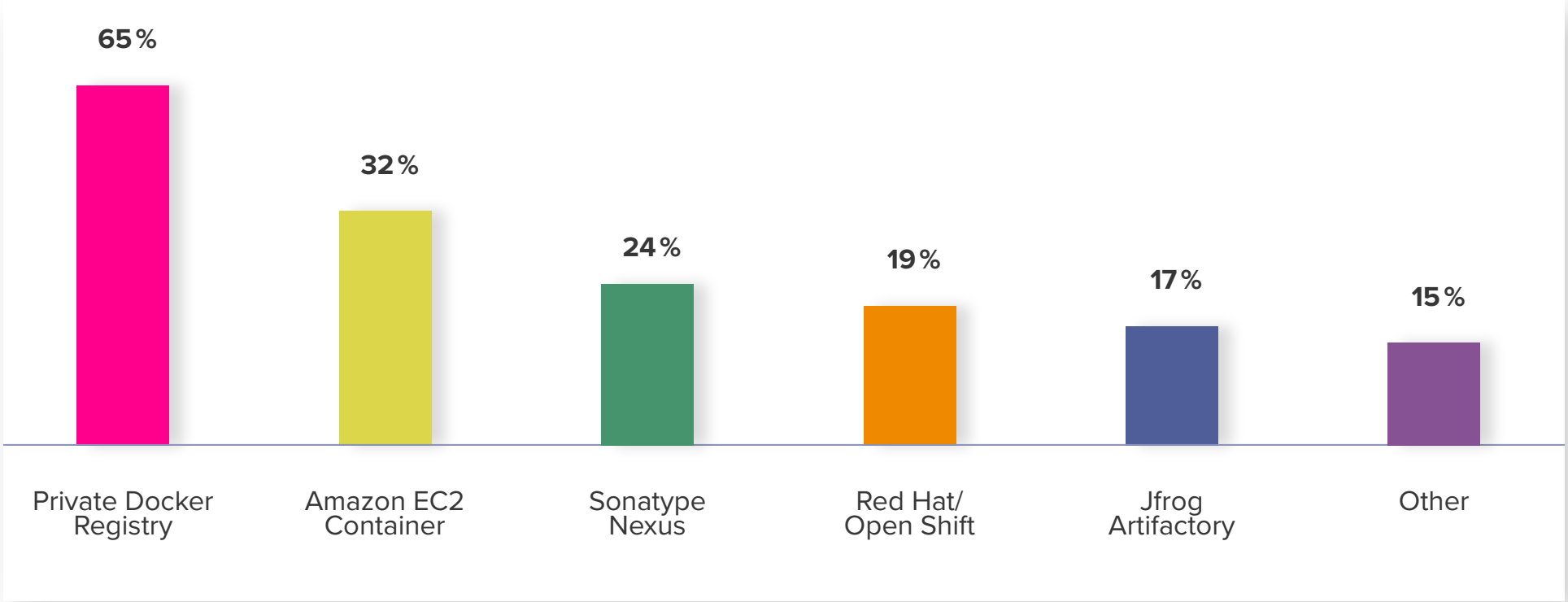
see security pros in the role of “nag”.

Security is part of everyone's role.

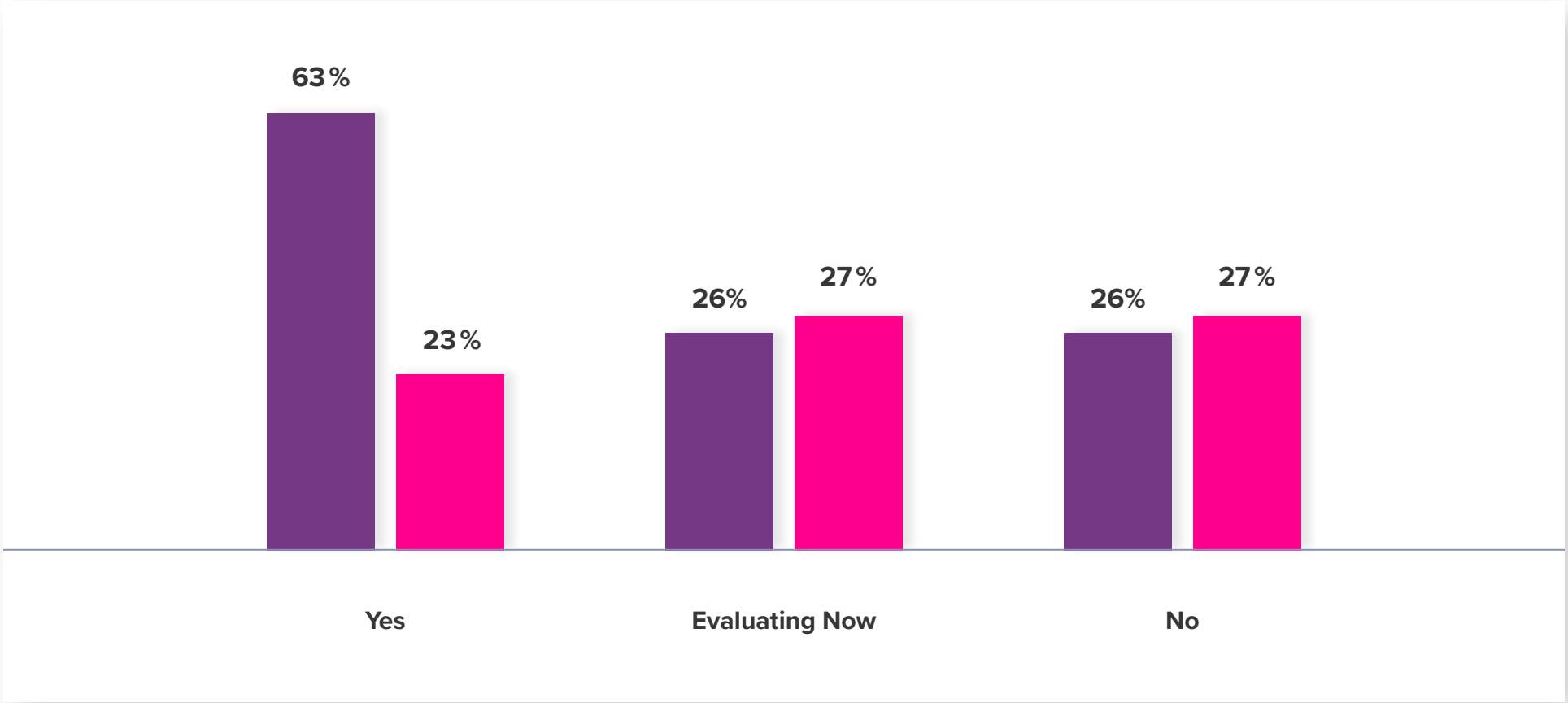


CONTAINERS AND CODE

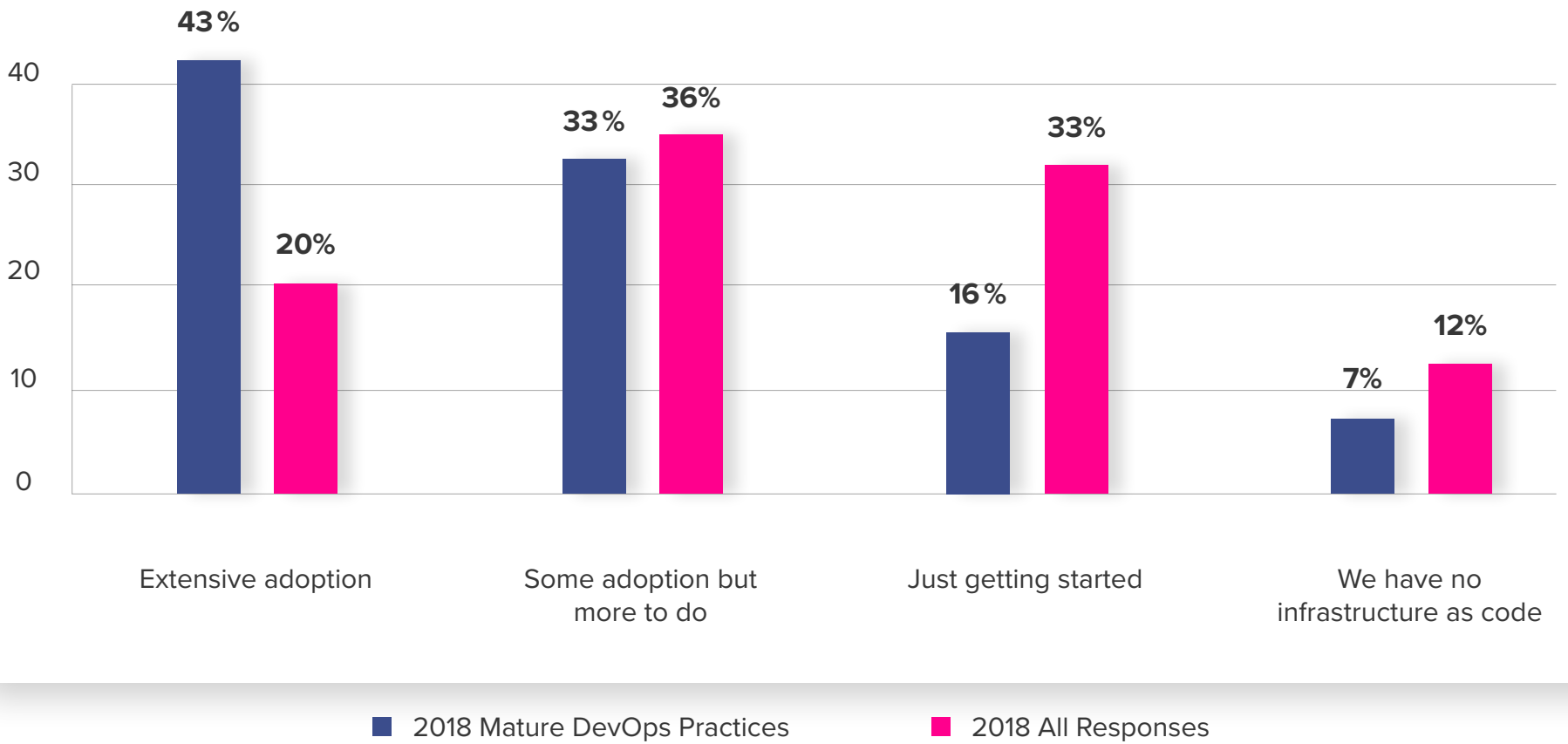
Which private container registries does your organization use?



Do you leverage security products to identify vulnerabilities in containers?



Infrastructure as code adoption (e.g., Docker containers, Chef cookbooks, Vagrant boxes).

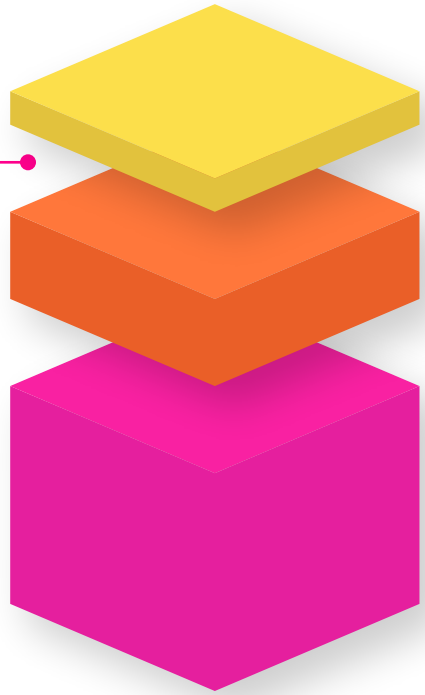


WHO PARTICIPATED?

What is your level of seniority within the organization?

20 %

of participants were **managers or executives.**



Executive

3.3 %

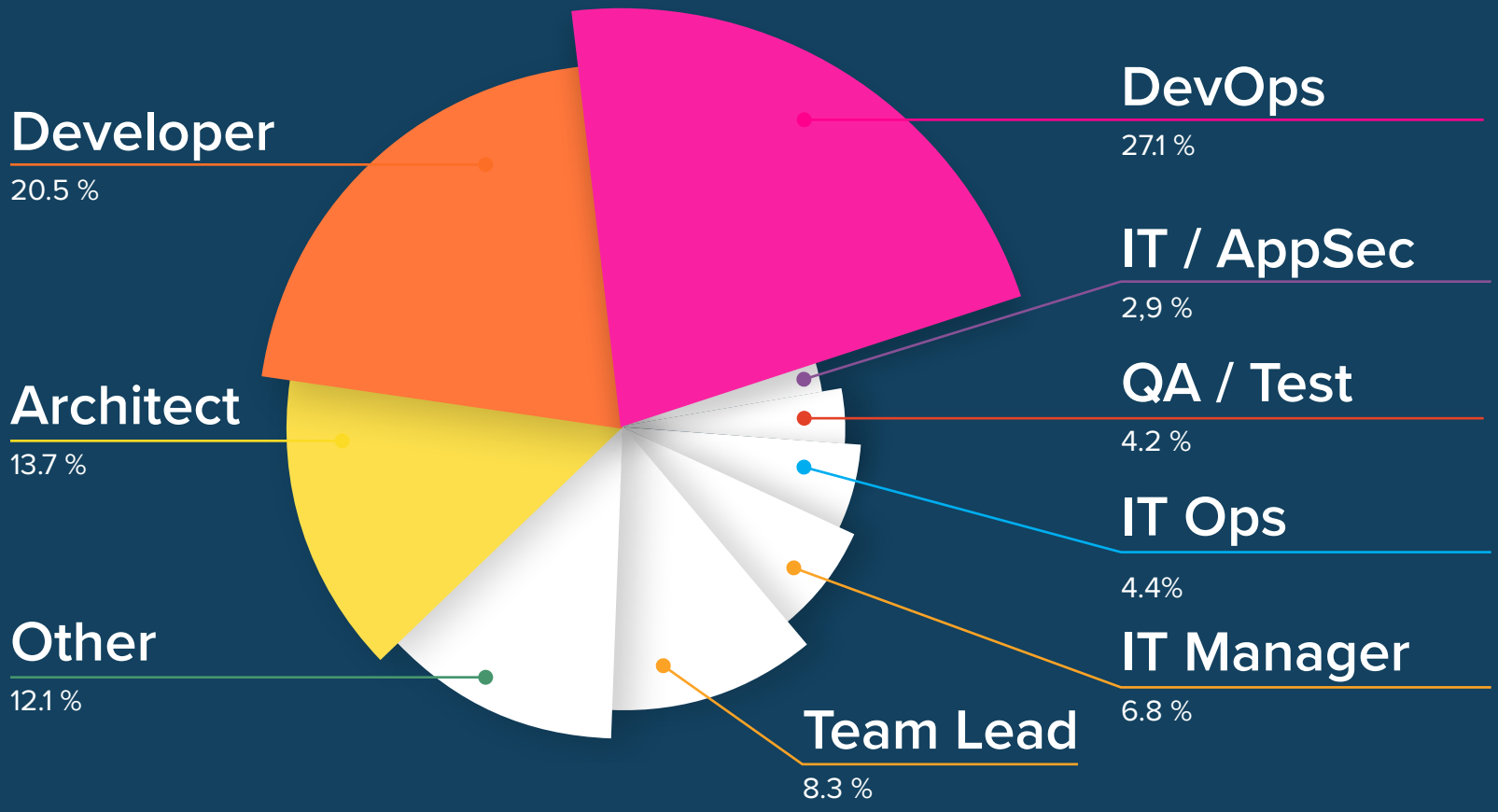
Manager

16.7 %

Individual contributor

80%

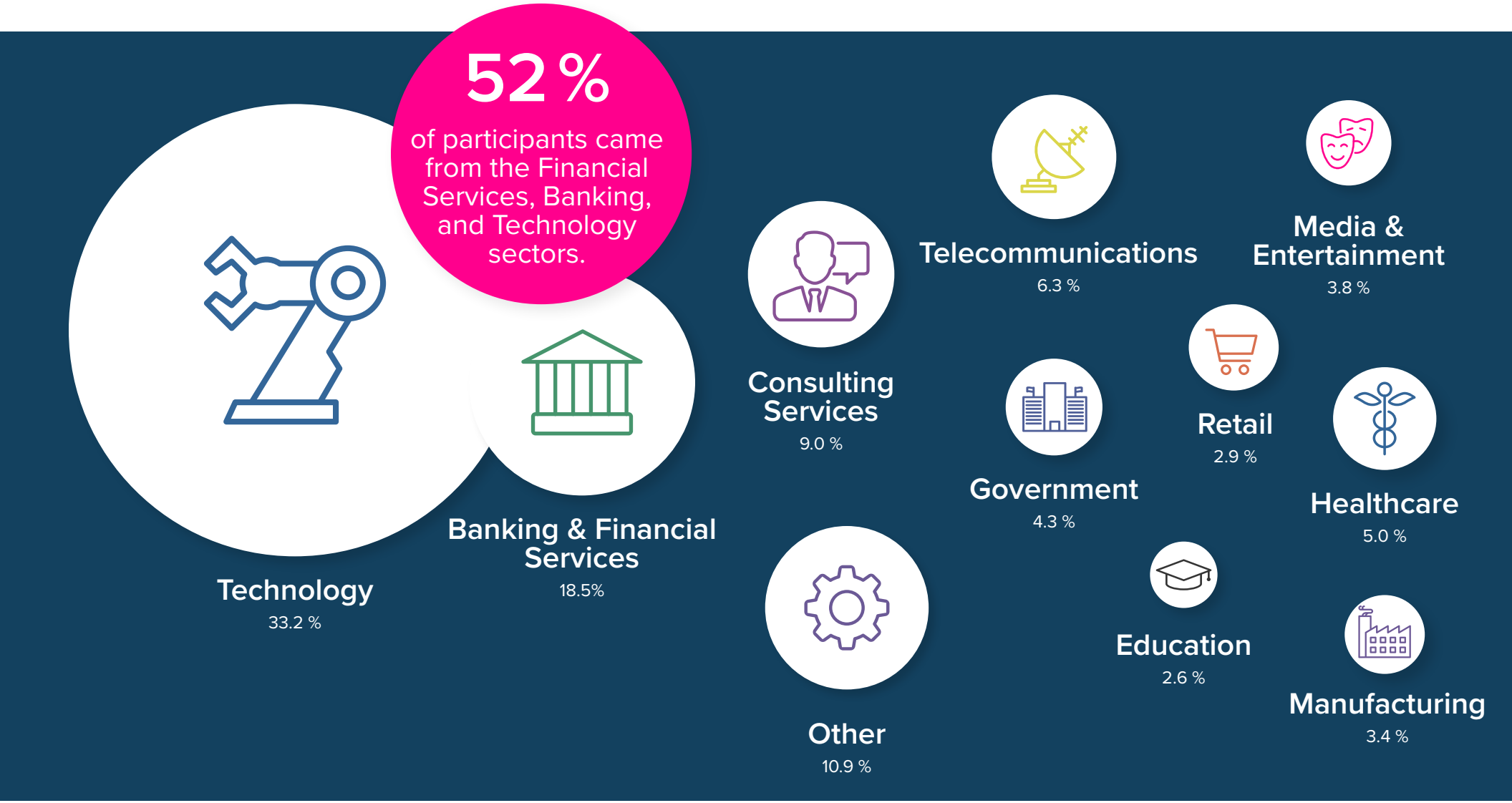
What is your role within the organization?



How many developers are in your organization?

50% HAVE MORE THAN **100** DEVELOPERS.

In what industry is your company?



ABOUT
The Survey

DEVSECOPS COMMUNITY SURVEY 2018

Just as the DevOps community has rapidly grown over the past several years, we have witnessed very strong interest in security practices that run within higher velocity, more collaborative, and highly integrated environments across this popular. Traditional waterfall-native security practices often don't fit in the DevOps native world and we wanted to use this survey to get a better sense of how organizations are adapting, what challenges they've overcome, and what approaches they are prioritizing.

The results reported here came in response to 44 questions asked by the Sonatype and our DevOps community partners, including Carnegie Mellon's Software Engineering Institute, Contino, DZone, Emerasoft, Ranger4, SJ Technologies, and Signal Sciences. The online survey was conducted between March 7, 2018 and March 21, 2018.

This is the fifth such survey conducted by Sonatype since 2011 focused on application development and security practices that have recently evolved into what we now call DevSecOps. The data collected in the DevSecOps Community Survey the provides statistically representative results on the adoption, practices, and challenges of managing DevOps practices with regard to security requirements.

For this project, 2,076 IT professionals responded to the survey with 1,287 (62%) completing it in its entirety. In a few cases where we were seeking definitive knowledge by the participants, we chose to not include "I don't know" responses in the final results.

To establish historical trends, a number of the questions in our 2014 and 2017 surveys were identical. Although we invited past participants to our 2017 survey, not all participants between the two surveys were the same. For people who self-identified, we saw that 40% live in North America, 23% live in Europe, 23% live in Asia, and the remainder of the people participated from other regions of the world. The survey's margin of error is ±2.02 percentage points for 2,076 IT professionals at the 95% confidence level.

SPEAKING OF DEV**SEC**OPS

Security feels too widely regarded as a hurdle, to be overcome once, when it should be a fluent part of everyday development.

SKJALG TEIG
Capra Consulting, Norway

Security should be an integral part of your build and run strategy. Everybody within the process should show their own responsibility in delivering stable and secure applications!

JAAP VAN ARRAGON
Capgemnini, Netherlands

Involving external groups to perform security tests (e.g., pen testing) is expensive and doesn't scale when we're releasing frequently. We need to build security in, the same way that we build quality in.

LIZ KEOGH
Lunivore Limited, United Kingdom

Making security a natural part of the SDLC will make it more resilient and valuable. It should be "something we do" rather than "something we are told to do".

PAULY COMTOIS
Hearst Business Media, United States

SPEAKING OF DEVSECOPS

Who can sleep if they are worried that their code is insecure?

BARRY O'CONNELL
Deutsche Bank, United Kingdom

Security should be built into the application, not around it.

PRAVEEN MANTHENA
MGM, United States

Security is everyone's responsibility.

MITCH MITCHELL
Duke Energy, United States

I come from a system administration and operations background. I understand the challenges and performance markers facing other teams. Having faced security "across the fence", my mission as an information security professional is to consider how security can fit in. Through DevSecOps, security can be an integral part of existing and planned business practices, rather than a clumsy bolt-on.

LOIS GARCIA
Consensus, United States

SPEAKING OF DEVSECOPS

DevSecOps is the next step. If our applications aren't build from the ground up with security as a concern, we may as well leave the apps without any security at all and just watch them carefully. DevOps has enabled security to actually be built into organizations, instead of as an annoying afterthought in a spreadsheet.

MARCY NUGENT
RealEyes Media, United States

Just like testing and refactoring have been recognized everyday, isolated steps in the development cycle, so to should security.

JOOST VAN DER GRIENDT
ABN AMRO, The Netherlands

Most teams focus on the DevOps benefits but forget about security until its too late, when code is in production. This leads to vulnerabilities and extended time to market as fixes (or worse redesign) are needed. It is important to my team to build security in as soon as possible to ensure we address risks as early as possible.

STEVEN VAN HEERDEN
Derivco, South Africa