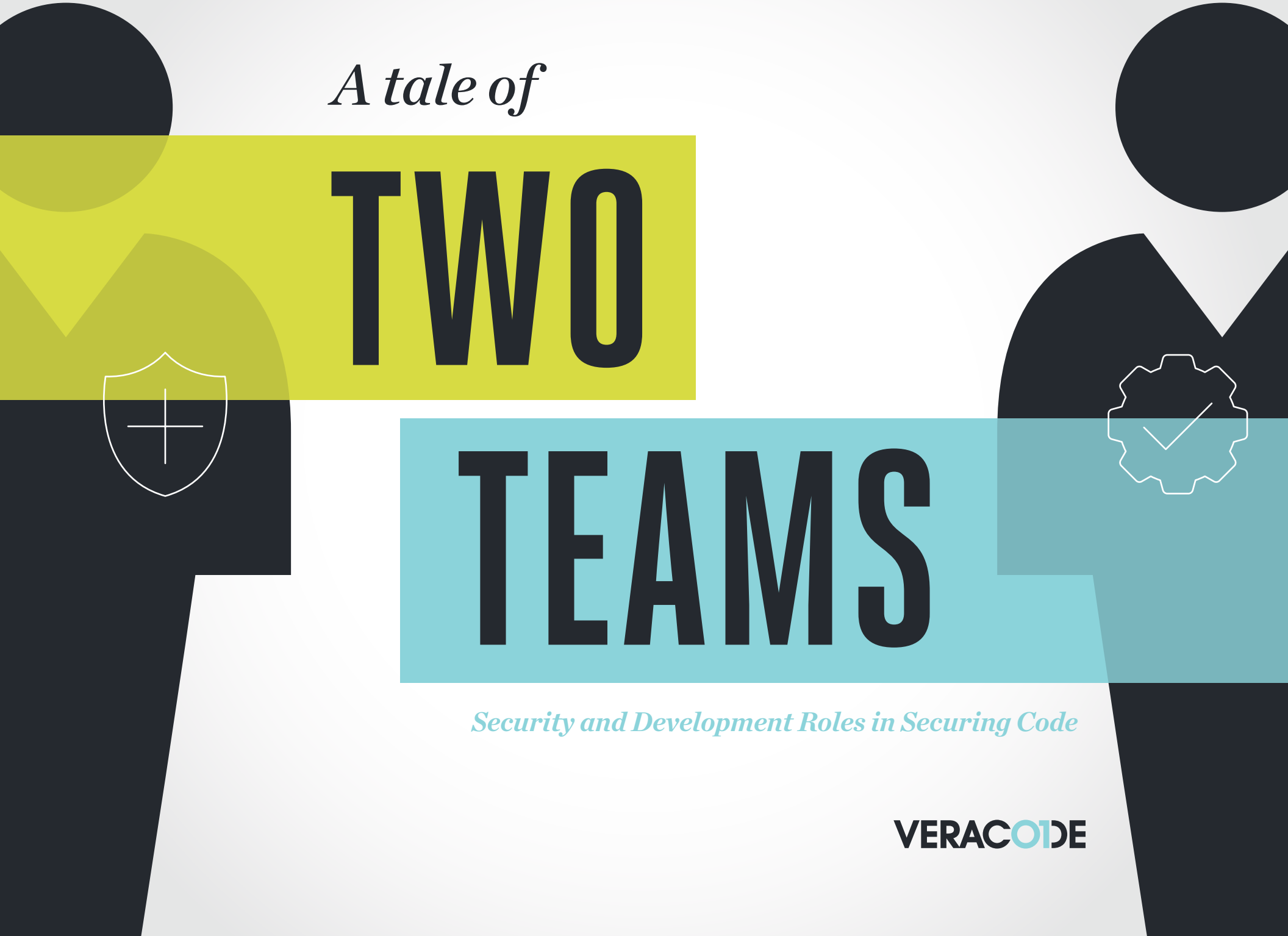
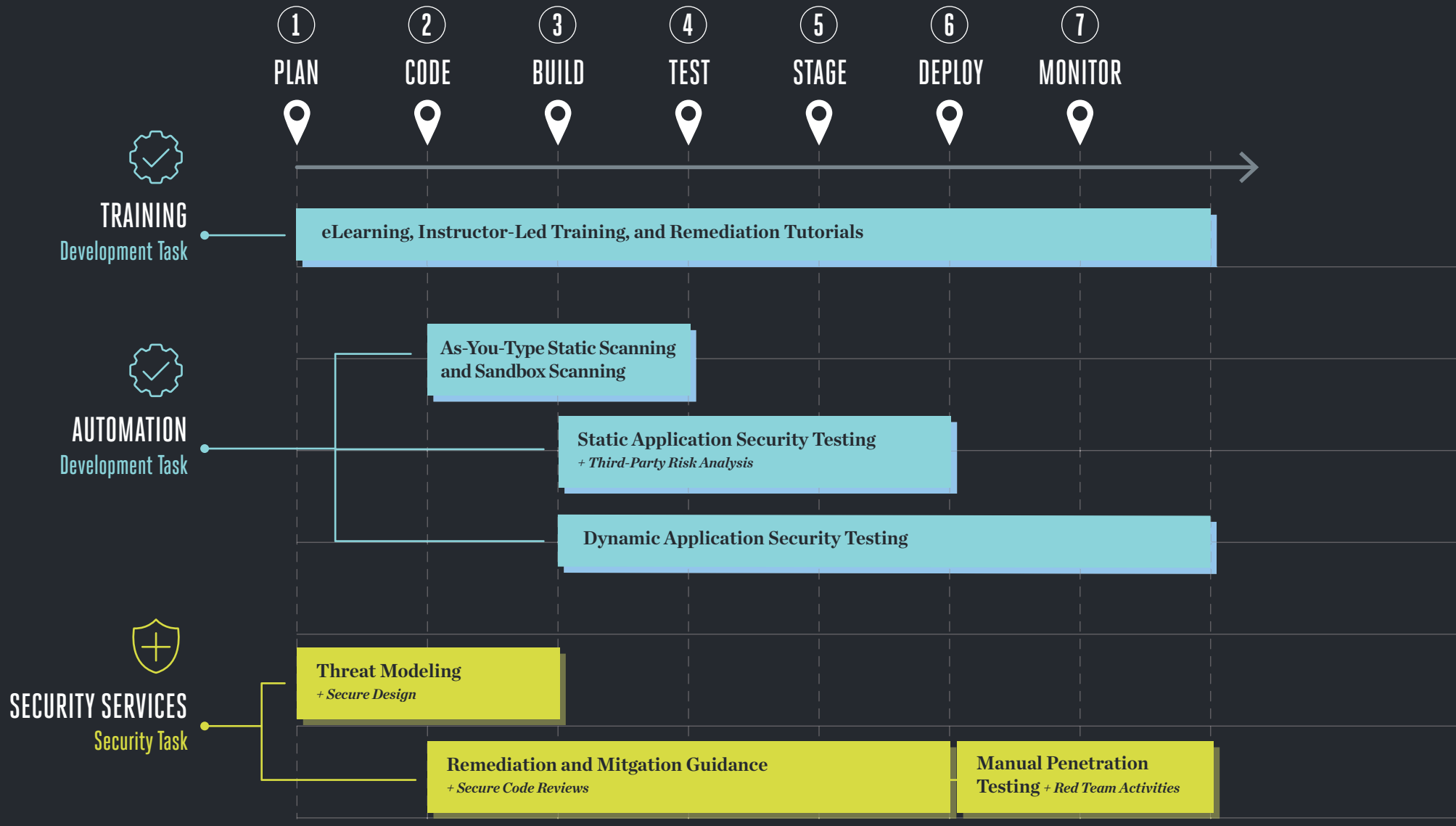


A tale of

TWO TEAMS

Security and Development Roles in Securing Code

VERACODE

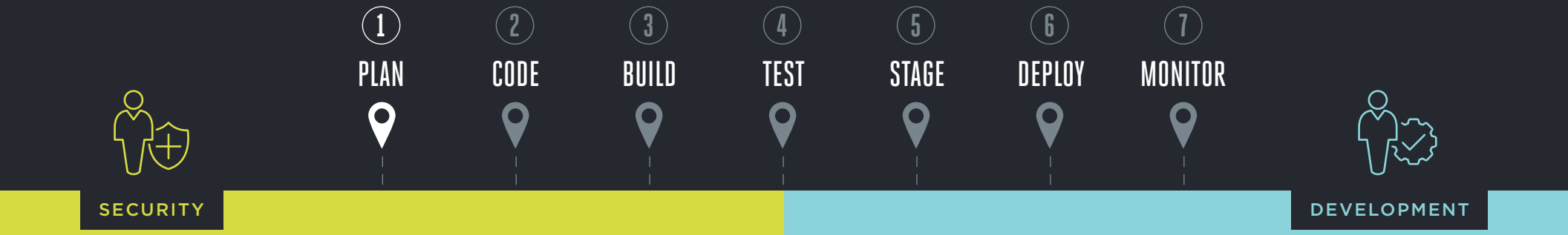


SOFTWARE LIFECYCLE

INTRODUCTION

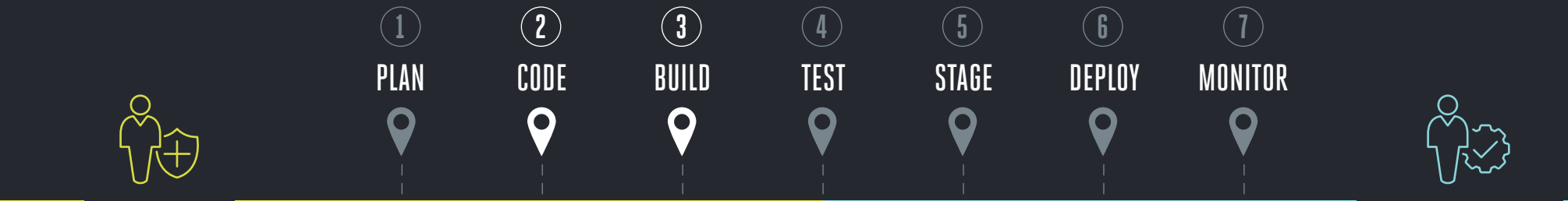
As DevSecOps changes the way software is created and distributed, it is also changing the roles and responsibilities of the development and security teams.

As security shifts left, and right, each team has new tasks, concerns, priorities, and things to learn. And they each need to understand what the other team is doing and prioritizing in order to work together more closely than ever before. Here's a glimpse of what those new processes and priorities are for each team throughout the software lifecycle.



What's a security champion?

Designate developers with an interest in security as security champions. These champions help to reduce culture conflict between development and security by amplifying the security message on a peer-to-peer level. They don't need to be experts, more like the "security consciousness" of the group.



SECURITY

DEVELOPMENT

Help developers to embed security into their processes seamlessly.

Investigate automated security testing tools that can integrate with their existing tools and processes, and help them get up to speed on using these tools. Help developers fix what they find. Do this by providing:

- Training
- Remediation and mitigation guidance
- Secure code reviews: Include security considerations into existing peer reviews of code.

- Take security training.
- Conduct security scans early and often — and automate if possible.
- Tie security findings into bug tracking system.
- Fix policy violations.

Our recent State of Software Security report, which analyzes the code we scan over the course of the year, found that developer training has an essential role in reducing flaws.

eLearning

IMPROVED FIX RATES BY

19%

Remediation Coaching

IMPROVED FIX RATES BY

88%

Early scanning makes a big security difference.

Our State of Software Security report found that DevOps organizations that tested frequently with sandbox scanning had

48%

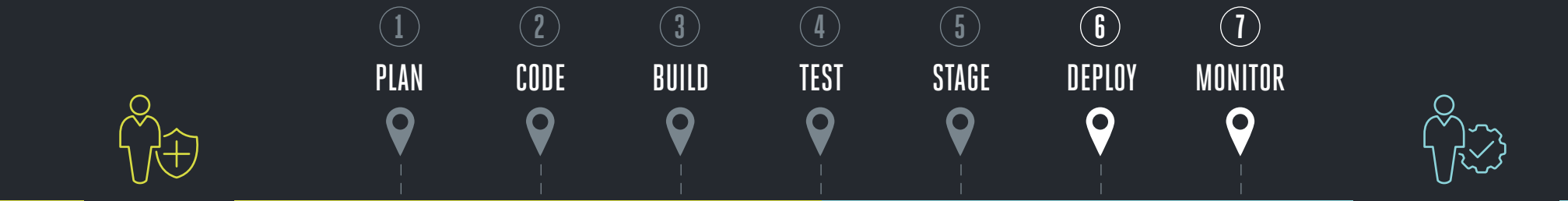
BETTER FIX RATE THAN THOSE DOING POLICY-ONLY SCANNING

Again, help developers fix what they find with remediation and mitigation guidance.

- Conduct dynamic and static testing, automating as much as possible.
- Fix policy violations.

> *It is going to take more than one automated technique and manual processes to secure your applications. Gather the strengths of multiple testing techniques along the entire application lifetime to drive down application risk in your organization.*

CHRIS WYSOPAL, VERACODE CTO + CO-FOUNDER



SECURITY

DEVELOPMENT

- Re-assess applications for security as they are updated or changed.

- Conduct pen testing: There are some vulnerabilities only a human can identify.

- Consider red team activities: Get your team to think like an attacker to find the flaws in your code.

Our 2017 State of Software Security report, which looked at 400,000 application scans, found that, among applications undergoing security testing for the first time:

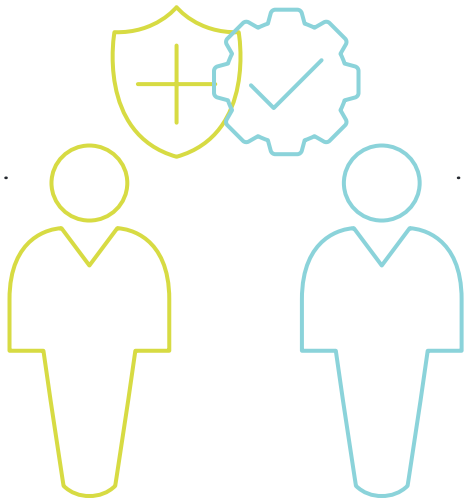
70%
FAIL TO PASS OWASP TOP 10 POLICY

77%
HAVE AT LEAST ONE VULNERABILITY

12%
HAVE AT LEAST ONE HIGH OR VERY HIGH SEVERITY VULNERABILITY

CONCLUSION

The days of security and development working in silos are over. Each team needs to understand and work closely with the other.



NEED TO BUMP UP YOUR DEVELOPMENT KNOWLEDGE?

Understanding the Dev in DevSecOps: A Toolkit for the Security Team

NEED TO BUMP UP YOUR SECURITY KNOWLEDGE?

What Developers Don't Know About Security, but Should

SECURITY

DEVELOPMENT

VERACODE

Veracode delivers the application security solutions and services today's software-driven world requires. Veracode's unified platform assesses and improves the security of applications from inception through production so that businesses can confidently innovate with the web and mobile applications they build, buy and assemble as well as the components they integrate into their environments.

With its powerful combination of automation, process and speed, Veracode seamlessly integrates application security into the software lifecycle, effectively eliminating vulnerabilities during the lowest-cost point in the development/deployment chain, and blocking threats while in production. By protecting each and every application throughout its entire lifecycle, Veracode not only prevents cyberthreats, but also responds to them—delivering application security unmatched in coverage and effectiveness.

Veracode serves hundreds of customers across a wide range of industries, including nearly one-third of the Fortune 500, three of the top four U.S. commercial banks and more than 20 of Forbes' 100 Most Valuable Brands.

LEARN MORE AT WWW.VERACODE.COM,
ON THE VERACODE BLOG, AND ON TWITTER.