SHIFTING SECURITY LEFT & RIGHT

HOW VERACODE ENABLES DevSecOps

VERACODE

STATIC ANALYSIS IS ONLY THE BEGINNING.

You're already using Veracode for static application security testing as part of your development process, which puts you in a good place for achieving a mature application security program. But, as advanced development teams are shifting to DevOps and CI/CD to increase quality while adding velocity, security teams like yours may be having a hard time keeping up. If you're going to support your business goals for new applications and features, while securing DevOps, you need to move beyond static analysis to make security a truly integrated part of the entire software development lifecycle (SDLC), what we call DevSecOps. In this paper, we'll look at how Veracode can provide you with the technologies and services you need to make the journey to DevSecOps.

DevSecOps defined

DevSecOps combines culture, process, and technology to make everyone responsible for secure code. The key characteristics of DevSecOps include:

Development and security teams together are responsible for software throughout the application lifecycle, from inception to production and customer use

Continuous, incremental security testing and remediation, with security shifting left into development, where it is the most cost-effective

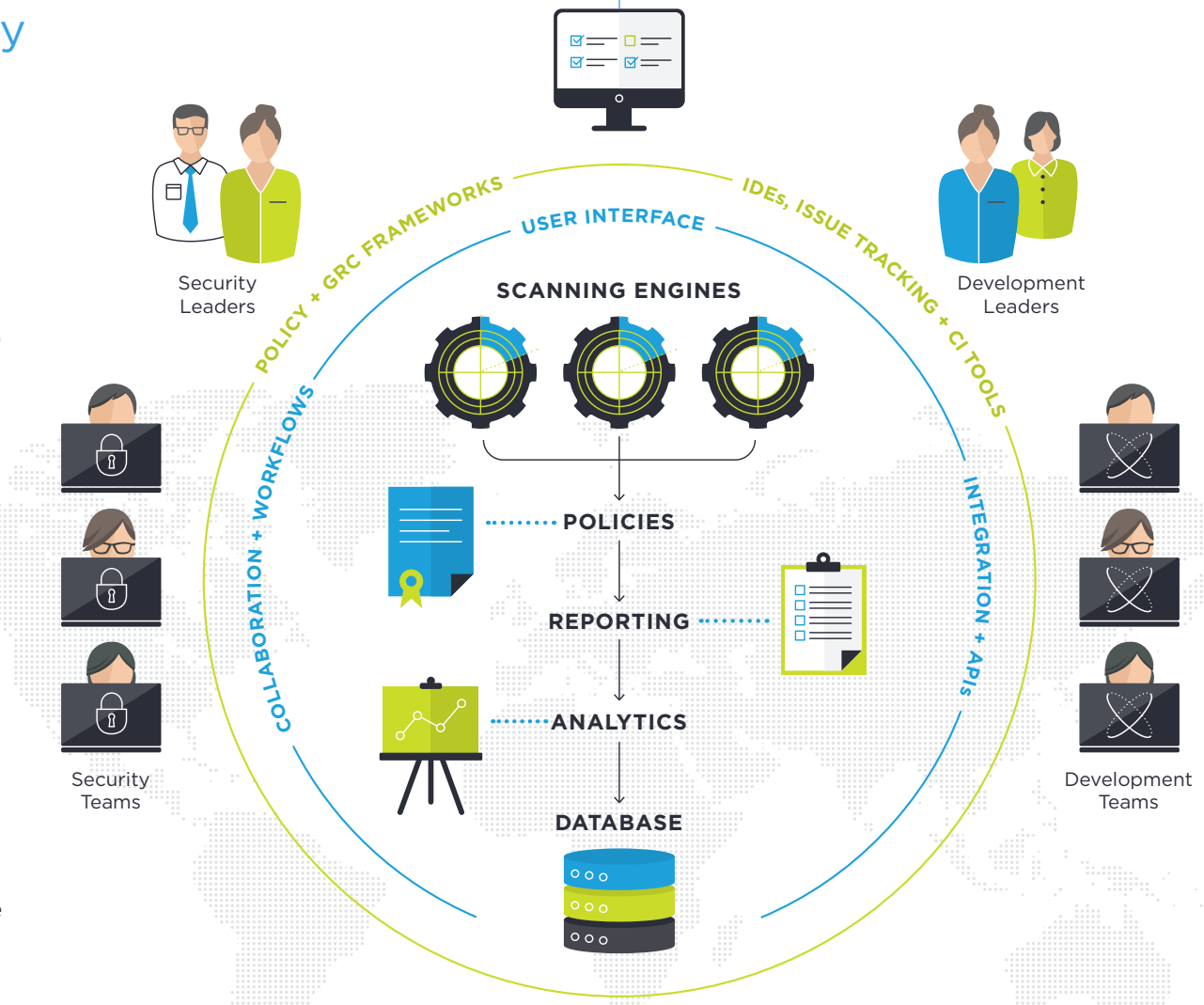
Use of security technologies and processes that won't get in the way of rapid development by fitting seamlessly with developers' workflow

Shifting security to the left and right

With DevSecOps, security shifts both to the left — to prevent issues in software development — and to the right — to help protect applications in production.

This expands the visibility and velocity of application security throughout the entire SDLC. Development makes prevention a priority by fixing flaws as they occur, while operations maintains quality long after the product has shipped. Security can then focus on governance and on providing development and operations with the training they need to integrate security into their work.

To support these shifts, Veracode can provide your development, operations, and security teams with a range of tools that will help make application security seamless.



Development: An ounce of prevention

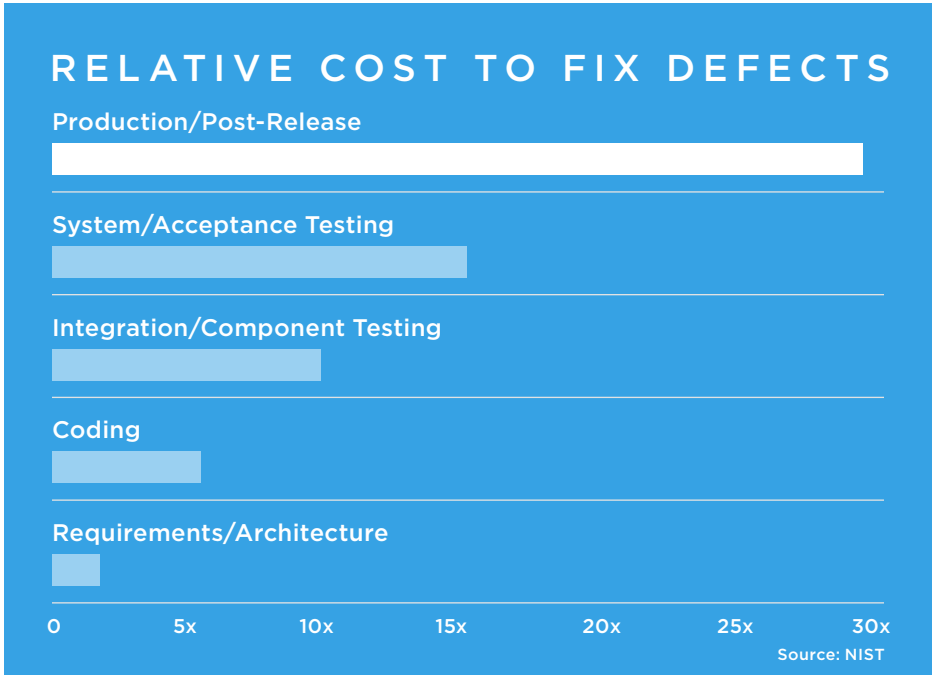
By incorporating security at the beginning of the software development process, developers have the potential to reap the greatest security returns. The more you can make code secure during development, the more you can maximize velocity later by reducing the number of security flaws that developers and operations must fix at the end of the process.

Not only that, but according to NIST, flaws fixed during coding can reduce costs by as much as six times compared to making the exact same fix in production, providing a strong business case for investing in DevSecOps' technologies and processes.

SO WHERE DO YOU BEGIN? Let's start with the tool you're already familiar with: Veracode Static Analysis (SAST), the foundation of our Application Security Platform. A SAST test looks at your application from the inside out, scanning the application in a static environment for signs of vulnerabilities without executing the program.

With DevSecOps, SAST is integrated early in the development process and used in conjunction with other tools, such as developer SAST (Veracode Greenlight), private sandbox scanning (Veracode Developer Sandbox), and developer training. Developers using Veracode Static Analysis can get quick security feedback to improve code incrementally, while security uses it to conduct an overall test on the full application.

With computer science courses generally not covering cybersecurity, developers aren't prepared for security requirements early in their careers. Many developers will struggle to write secure code if they don't have the right understanding about best practices. One of the most effective things you can do to improve application security is to provide preventive training to developers to help eliminate bad code early in development, where it's most cost-effective. Veracode Developer Training provides a combination of training options designed to get developers up to par.



VERACODE DEVELOPER TRAINING OPTIONS

eLearning

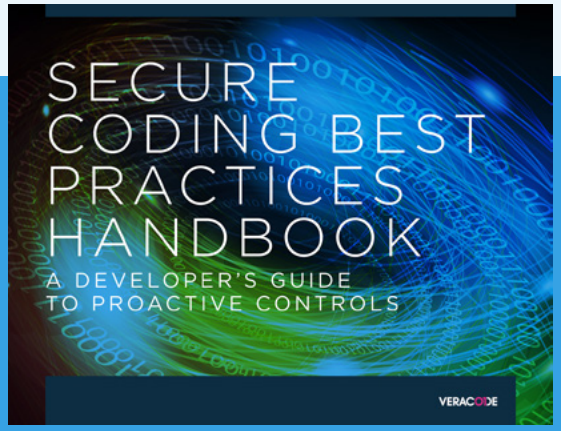
Veracode eLearning offers a library of on-demand, web-based training content so developers can learn on their own schedule or whenever they're in the process of fixing a particular vulnerability.

Remediation Consulting

Bugs are a fact of development. Veracode Remediation Consulting provides one-on-one results analysis and guidance, so a developer can understand how to address a specific security finding while learning how to avoid introducing a similar finding in the future.

Instructor-Led Training

Veracode Instructor-Led Training gives developers the chance to learn directly from the same application security consultants who provide remediation coaching for your team so they can learn best practices in a way that's specific to your application.



Give developers the tools they need for self-training.
Get our Secure Coding Best Practices Handbook.

As developers write code, Veracode Greenlight accelerates the speed of feedback by helping developers find security flaws on small batches of code while they're still working in the IDE. When a flaw is found, Greenlight provides instant remediation advice to help fix the issue before check-in and a full policy scan.

The best thing about Greenlight is that it easily incorporates into the developer's workflow with scan times that take just a few seconds and contextual remediation advice. Scanning at the speed of code means developers can fix flaws right away and learn how to avoid mistakes. With Greenlight, developers can spot-test their code dozens or even hundreds of times a week, compared to the monthly or even yearly testing you might be doing now.

Developers don't always respond well to the old "scan-and-shame" of security teams providing feedback at the end of the development lifecycle with all the flaws in the developer's code. Veracode Developer Sandbox lets developers experiment by scanning their code for feedback on the security results each would get during a policy scan. Developers can then address that feedback before check-in. This lets developers find the best method for solving a security problem without affecting compliance reporting for the version of the application currently in production.

But even the most security-minded developer in your company can only prevent flaws in the code they write. Development teams rely on third-party components to accelerate their application development and cut costs. Veracode Software Composition Analysis (SCA) analyzes third-party code at the same time you scan your proprietary code during static analysis, alerting developers to the presence of components with known vulnerabilities. Scanning both at the same time gives you complete visibility into your application's security in a single report. SCA allows developers to keep an up-to-date inventory of components and versions, so they can quickly update their components when new vulnerabilities are discovered.

Security: From tactical to strategic

As DevSecOps empowers development to create more secure code, security can begin to take a holistic, overall view of an application's security, instead of having to put out a hundred little fires as they occur. As you move from Agile to DevOps to DevSecOps, security can work with development teams to help them understand why rules have been set up in a certain way, or why an application is failing to meet security requirements. The more security can educate developers, the easier security's job becomes.

Rather than enacting complex security rules and confusing development teams out of the gate, start simple by curating the list of security filings the team should handle. For example, by beginning with just very high severity findings, such as SQL injection, development can prioritize flaws that need to be fixed. As developers work through those findings, security can then begin introducing additional requirements and applications over time. This lets development focus on the most important things first, while giving security high-impact wins.

Another move security can make is to simplify the mitigation process. In mitigation, a developer provides documentation about how the risk for a particular finding is alleviated so it won't be an issue. Your security experts can then approve or reject that mitigation. This process helps development and security teams focus on the things that truly need to be fixed. Minor bugs are then well-documented so they can be understood should there be an issue in the future.

Because every organization usually has far more developers than application security experts, Veracode Mitigation Proposal Review can provide an independent evaluation of mitigation proposals against your customized risk tolerance guidelines. By leveraging Veracode to review mitigations, security teams can increase compliance, speed up time to resolution, and increase the consistency of risk acceptance without increasing headcount.

Many application security policies were built when we did not have fast, automated security tools that could be plugged into the SDLC … It is important to revisit and build new policies that work with, and not against, the developer goal of "getting good code out quickly."

PEJMAN POURMOUSA,
VP, Program Management,
Veracode

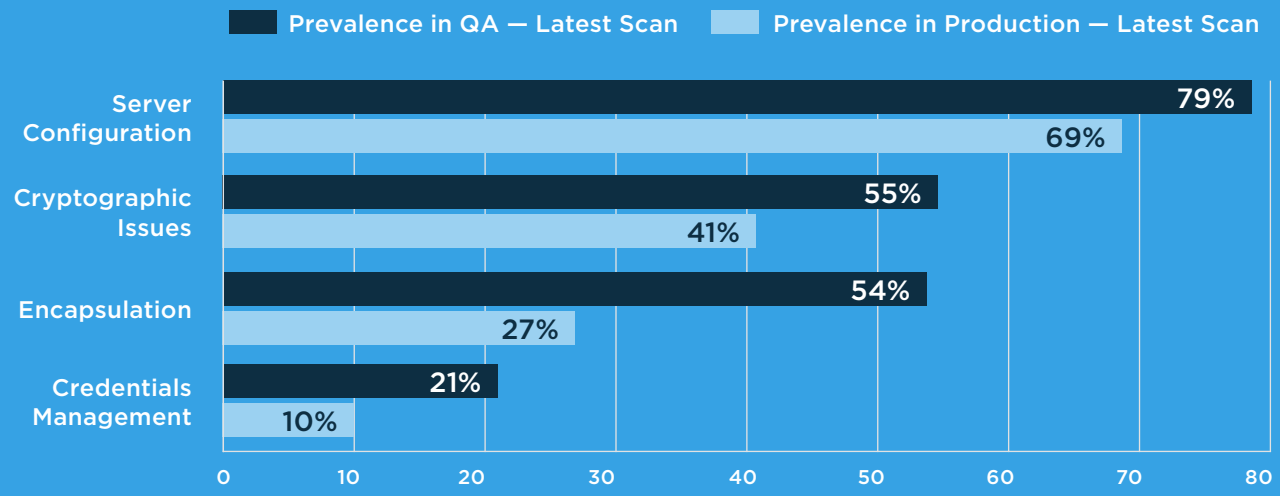
Operations: Protecting production

As the last line of defense, the operations team is responsible for protecting the production instance from security threats.

As with development and security, operations can take advantage of Veracode training and tools, like Software Composition Analysis, to ensure the security of your organization's applications.

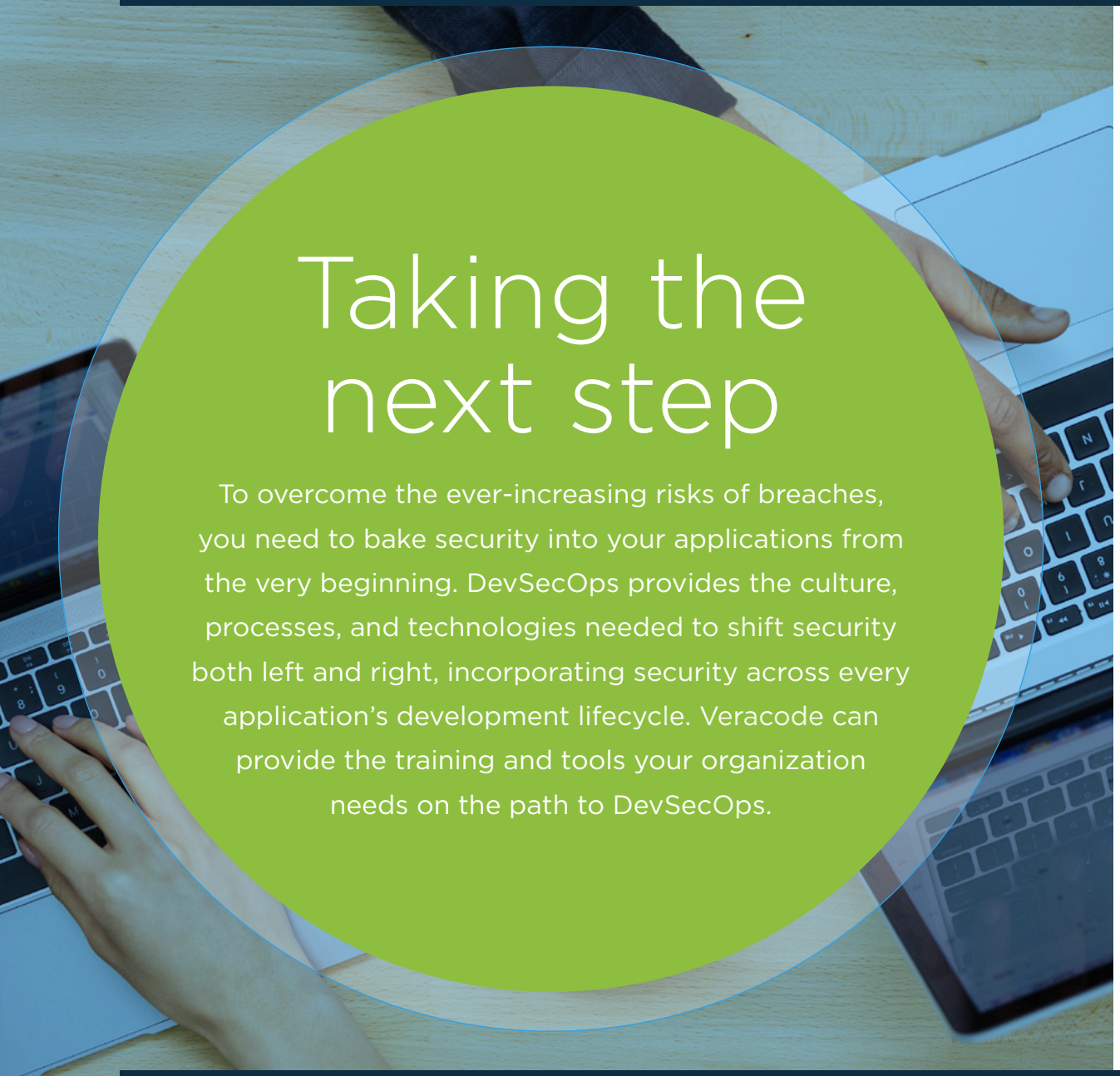
In addition, Veracode's open APIs and plugins let you create integrations with other build systems, like Ansible and Hygieia, to automate dynamic scanning. Veracode Dynamic Analysis also automates the scanning of web applications in a dynamic environment, auditing those applications for flaws in a run-time environment, providing insights into application behavior and detecting flaws in production. This results in few, if any, false positives, ensuring any returned issues get high prioritization.

PRODUCTION FIXES MOST LIKELY TO BE IMPACTED BY OPS



	Difference	Fix Rate
Server Configuration	-10% ▼	12.7%
Cryptographic Issues	-14% ▼	25.5%
Encapsulation	-27% ▼	50%
Credentials Management	-11% ▼	52.4%

Source: *2017 State of Software Security*



Taking the next step

To overcome the ever-increasing risks of breaches, you need to bake security into your applications from the very beginning. DevSecOps provides the culture, processes, and technologies needed to shift security both left and right, incorporating security across every application's development lifecycle. Veracode can provide the training and tools your organization needs on the path to DevSecOps.

LEARN MORE

In our webinar The Path From DevOps to DevSecOps, we explore how to build an application security program that works for you and your development needs. You'll learn:

- How current application security technologies should adapt to fit DevSecOps trends
- What capabilities application security should adopt and the technologies that should be embraced by development, operation, and security specialists
- How to forecast the pace of adoption for these technologies and understand their place in integrating security seamlessly into the DevOps process

VERACODE

Veracode is a leader in helping organizations secure the software that powers their world. CA Veracode's SaaS platform and integrated solutions help security teams and software developers find and fix security-related defects at all points in the software development lifecycle, before they can be exploited by hackers. Our complete set of offerings help customers reduce the risk of data breaches, increase the speed of secure software delivery, meet compliance requirements, and cost effectively secure their software assets- whether that's software they make, buy or sell.

Veracode serves more than 1,400 customers across a wide range of industries, including nearly one-third of the Fortune 100, 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**, on **Twitter** and in the CA Veracode Community.

Copyright © 2018 Veracode, Inc. All rights reserved. All other brand names, product names, or trademarks belong to their respective holders.