MEASURING APPSEC SUCCESS

4 Metrics for Managing Your Application Security Program

Metrics play an important role in managing your application security program. They allow you quantify risk. Metrics also enable you to communicate areas for improvement to the security and development teams, and report progress to senior management or the board.

SCAN ACTIVITY

As you scale your AppSec program, you might be scanning more applications, more frequently. And if you're shifting to DevOps, you're likely integrating security testing within your developer workflow, enabling developers with manual Sandbox scanning and automated scanning at check-in.

METRICS

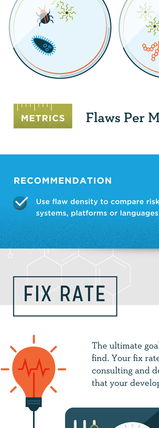
Number of Scans

- Daily / Monthly / Yearly
- Automated vs. Manual
- Policy vs. Sandbox

RECOMMENDATIONS

- Engage development teams to better integrate testing within the development lifecycle
- Train developers on using plugins to increase scans

POLICY COMPLIANCE



You can define a policy according to industry regulations and standards like PCI, or according to the security goals of your organization (e.g., no SQL injection).

A policy helps boil all your results down to a simple pass/fail. Applications failing policy, but within a flaw remediation grace period, can be given a Conditional pass.

METRICS

Compliance Rate

Pass / Fail / Conditional Pass

RECOMMENDATIONS

- Review a sample of non-compliant applications
- Require consultation calls for developers of non-compliant applications

FLAW DENSITY

As your scans increase, the number of flaws increases, too. Flaw density – measured as the number of flaws divided by the size of the application – makes it easier to compare apples to apples.

METRICS

Flaws Per MB of Code

RECOMMENDATION

- Use flaw density to compare risk across different systems, platforms or languages, and over time

FIX RATE

The ultimate goal of your program is to fix the flaws you find. Your fix rate illuminates where you need remediation consulting and developer training to fix the kinds of flaws that your developers might struggle with.

METRICS

$$\text{Fix Rate} = \frac{\text{Fixed Flaws}}{\text{(Fixed + Open Flaws)}}$$

Open Flaws

High and Very High Severity

RECOMMENDATIONS

- Dynamic Vulnerability Rescan keeps track of flaws as new, fixed, open or re-opened, since the last scan
- Require consultation calls, eLearning, or instructor-led coaching for developers with Very High severity open flaws

BOTTOM LINE

WHAT YOU MEASURE IMPROVES

Schedule a consultation call, or contact your Veracode account rep or Security Program Manager for help implementing and maturing your AppSec program.

CONTACT US

Veracode gives companies a comprehensive and accurate view of software security defects so they can create secure software, and ensure the software they are buying or downloading is free of vulnerabilities. As a result, companies using Veracode are free to boldly innovate, explore, discover, and change the world.

With its combination of automation, integrations, process, and speed, Veracode helps companies make security a seamless part of the development process. This allows them to both find and fix security defects so that they can use software to achieve their missions.

Learn more at veracode.com, on the Veracode Blog and on Twitter.

Veracode serves more than 2,000 customers worldwide across a wide range of industries. The veracode Platform has assessed more than 8 trillion lines of code and helped companies fix more than 36 million security flaws.

Learn more at www.veracode.com, on the Veracode blog and on Twitter.

VERACODE