VERACODE

4 Ways to Increase Developer Buy-In of AppSec

Today, most organizations are in a race to deliver new, innovative software before their competitors. In turn, they have gone from bi-annual software releases to daily, hourly, or even by-the-minute releases. To keep up with these rapid deployments, security has had to shift from being a late-stage blocker, to an integrated part of the development process. Developers have been doing their best to implement these security measures, but since their performance is often tied to the rate of deployments, speed tends to take precedence. As a security professional, what are some steps you can take so that security doesn't take a back seat to speed?

ONE:
Automate and Integrate

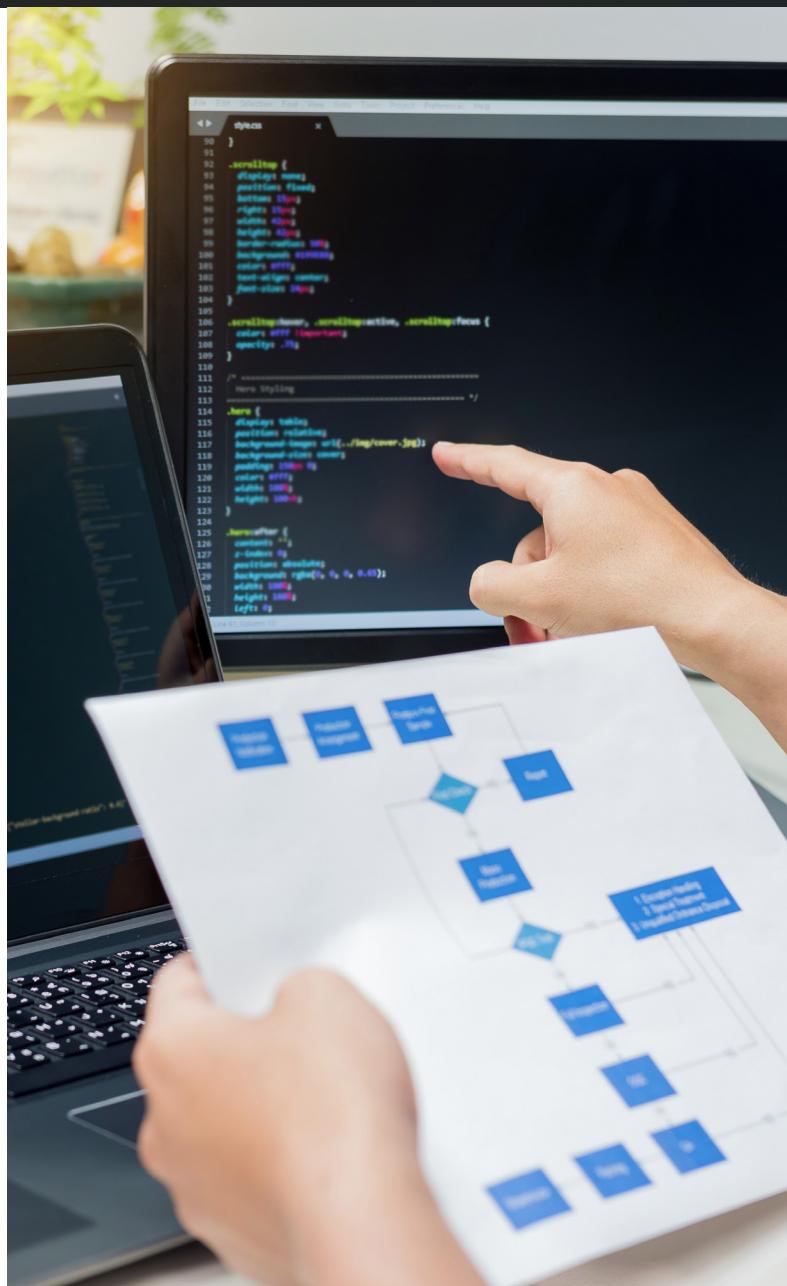
The easier you make it for developers to run AppSec tests, the more likely the tests will happen. Integrate the AppSec scans into the developers' existing tools and processes and automate the tests.

> *Did you know that organizations can integrate Veracode products into their tooling with more than 30 out-of-the-box integrations, plus APIs and code samples to support continuous scanning in any environment?*

TWO:
Break Down Silos

In a perfect world, every development team would include a security professional; but, since there are far fewer security professionals than there are developers, this usually isn't feasible. What your organization can and should do is work on building a "one team" approach where security professionals and developers interact more frequently and work together to support systems and structures.

> *Tip: Attend developer sprint planning meetings to get a better idea of the developers' priorities and to make sure AppSec scans and remediation practices are top of mind.*



THREE:
Educate

Developers take pride in their code and want it to be secure. Unfortunately, most developers have never been taught secure coding best practices. Computer engineering programs typically do not teach secure coding. And at organizations, security professionals are supposed to train developers, but they usually don't have the time or resources. To address this concern, consider security solutions that provide real-time security feedback to developers as they code. Supplement that feedback with online and in-person security training, but make sure it's the right type of training. If the tools and trainings are engaging and interactive, there is a higher chance that developers will participate in the courses and leverage the tools.

Veracode offers several products to help developers write secure code:

The ***IDE Scan*** provides focused, real-time security feedback while the developer codes. It also helps developers remediate faster and learn on the job through positive reinforcement, remediation guidance, code examples, and links to Veracode AppSec Tutorials.

The ***Pipeline Scan*** happens in the build phase. It directly embeds into teams' CI tooling and provides fast feedback on flaws being introduced on new commits. It helps answer the question, "is the code my team is writing secure?"

Veracode Security Labs trains developers to tackle evolving security threats by exploiting and patching real code. Through hands-on labs that use modern web apps, developers learn the skills and strategies that are directly applicable to their organization's code. Detailed progress reporting, email assignments, and a leaderboard encourage developers to continuously level up their secure coding skills.

FOUR:
Implement Security Champions

Since most organizations do not have enough security professionals to put one on every scrum team, find developers who are interested in learning more about security and train them to be the "security champion" for their team. The security champions should be responsible for ensuring that their scrum team is implementing proper security measures, and the security professionals should be responsible for making sure that the champions are up to date on the latest security practices. Consider scheduling bi-weekly or monthly check-ins with the security champions.

For more ideas on aligning roles, check out our recent video,

Tips for Unifying the Security Professional and Developer Roles.