Synopsys: Changing Our Culture to Follow a Secure Software Development Life Cycle

As a company, Synopsys consistently evangelizes that any software development life cycle (SDLC) should systematically address software security during the development phase. Such a secure SDLC ensures that vulnerabilities are more likely to be found and fixed before application deployment, thereby reducing the total cost of software development. The National Institute of Standards and Technology (NIST) estimates that code fixes performed after release can cost over 30 times more than fixes performed during the design phase.

The primary advantages of pursuing a secure SDLC approach include these:

- More secure software
- Awareness of security considerations by stakeholders
- Early detection and resolution of issues
- Cost reduction and productivity improvements
- Reduction of business risks

But evangelists must practice what they preach for their message to ring true. So when we realized we weren’t supporting our internal secure development efforts as much as we were those of our customers, it was time to turn our view inward. As a leader in static analysis, software composition analysis, and application security testing, we believed it was essential for our development teams to apply the same tools and best practices we use with our customers to create our own secure SDLC.

The challenge for Synopsys

Like members of many other development teams, Synopsys engineers initially resisted anything that might slow developer productivity. However, their reluctance to adopt security practices during development was hindering their achievement of agile release cycles and continuous delivery. Security testing as the last sprint before release resulted in lengthy production deployment delays.

“It was being left to the AppSec engineers to perform the heavy security lifting at the very end of the release cycle,” says Gopal Addada, senior software engineering manager.
The Synopsys difference

Synopsys helps development teams build secure, high-quality software, minimizing risks while maximizing speed and productivity. Synopsys, a recognized leader in application security, provides static analysis, software composition analysis, and dynamic analysis solutions that enable teams to quickly find and fix vulnerabilities and defects in proprietary code, open source components, and application behavior. With a combination of industry-leading tools, services, and expertise, only Synopsys helps organizations optimize security and quality in DevSecOps and throughout the software development life cycle.

For more information, go to www.synopsys.com/software.

©2019 Synopsys, Inc. All rights reserved. Synopsys is a trademark of Synopsys, Inc. in the United States and other countries. A list of Synopsys trademarks is available at www.synopsys.com/copyright.html. All other names mentioned herein are trademarks or registered trademarks of their respective owners.