SYNOPSYS®

CASE STUDY

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.

"We've incorporated AppSec activities into every sprint."

—Gopal Addada, senior software engineering manager, Synopsys

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 journey to a secure SDLC

To help the Synopsys development teams build secure, high-quality software while still maximizing their speed and productivity, the company changed internal processes, nurtured a security-focused culture, and brought in new tools and best practices for a secure software development life cycle.

"In our old process, most security activities were done towards the end of the spiral," says Addada. "We modified that spiral approach to incorporate AppSec activities into every sprint. Now, each sprint has a definitive scope, and our goal is to be production-ready at the end of every sprint. Additionally, security stories have been created as a part of sprint requirements. Because tests are automated in each sprint, we have defined our exit criteria for a sprint as 100% test automation coverage."

"A one-time comprehensive architectural risk analysis (ARA) is performed on the application and a threat model created. ARA is done in a sprint only if the security stories implemented during the sprint change any assets, security controls, attack surface, or threat agents."

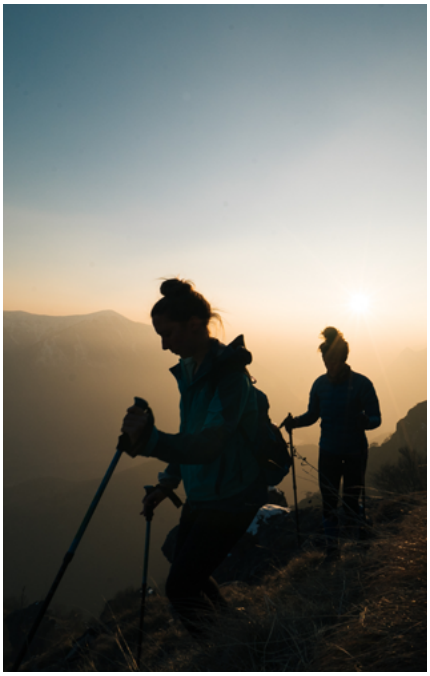
Shifting left: Tools and best practices

Implementing a lightweight IDE static analysis tool was the first major step Synopsys took toward shifting security left. The company initiated peer and development lead reviews to ensure that new or modified code follows security coding standards and doesn't have obvious security issues. And the first thing engineering teams do every morning is triage and address the results from nightly SAST and SCA testing.

In addition, the AppSec team, working closely with the engineering team, performs a penetration test for every release. This collaborative effort is helping Synopsys achieve the goal of continuous security testing.

Outcome: Toward a secure SDLC

"The R&D team really love moving towards a secure SDLC," says James Reynolds, group director of software engineering. "People who take a job at Synopsys are already security-focused and have a security mindset. They love learning how to write more secure code because they firmly believe in the necessity of secure code."



"R&D loves moving towards a secure SDLC. People who take a job at Synopsys are already security-focused and have a security mindset."

—James Reynolds, group director of software engineering, Synopsys

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.

Synopsys, Inc.
185 Berry Street, Suite 6500
San Francisco, CA 94107 USA

U.S. Sales: 800.873.8193
International Sales: +1 415.321.5237
Email: sig-info@synopsys.com

SYNOPSYS®
Silicon to Software™

06/12/18.synopsys-devsecops-cs-ul.