Black Duck Newsroom

Security in DevOps Is Lagging Despite Advantages and Opportunities, According to New Study by 451 Research and Synopsys

Survey Reveals Only Half of CI/CD Workflows Include Application Security Testing Elements

Disclaimer: The Synopsys Software Integrity Group is now Black Duck®. Click here to learn more.

MOUNTAIN VIEW, Calif., April 25, 2018 /PRNewswire/ -- Synopsys, Inc. (Nasdaq: SNPS) today released new data that highlights the opportunities and challenges of DevSecOps, an emerging paradigm in which DevOps teams incorporate application security into their continuous integration and continuous delivery (CI/CD) workflows. The 451 Research report commissioned by Synopsys, DevSecOps Realities and Opportunities, analyzes survey results from 350 enterprise decision-makers at large enterprises across a variety of industries. The study found that only half of CI/CD workflows include application security testing elements despite respondents citing awareness of the importance and advantages of doing so.

"While some DevOps teams are starting to incorporate application security into their CI/CD workflows, driven by factors such as improved software quality, compliance, and risk avoidance, there is ample room for improvement," said Jay Lyman, principal analyst at 451 Research. "In many cases, security testing is not being integrated often or early enough in the process for organizations to fully benefit from reduced risk and rework headaches."

DevOps teams today are working with large-scale infrastructures, releasing software faster, and doing so with significant code changes in each release. Sixty-three percent of respondents say they expect to deploy software at least four times faster in a DevOps model. Without a clear and informed strategy, this can make establishing and scaling application security testing within these processes complex and difficult.

While organizations cited a lack of automation and consistency, reduced speed, and the noise of false positives as the primary challenges of DevSecOps, the survey also showed that the use of automated tools integrated early in the software development life cycle can have a positive impact on both the speed and the overall quality and security of software.

The survey also revealed that software composition analysis (SCA), or the identification of open source software components affected by known vulnerabilities, is the most critical application security element that needs to be incorporated into CI/CD workflows. Interestingly, the survey also showed that nearly 40% of organizations either do not perform SCA or claim not to use any open source components – which may represent a lack of awareness given that a previous Open Source Security and Risk Analysis report by Black Duck Software found that over 95% of applications contain open source. Synopsys acquired Black Duck Software, the global leader in software composition analysis solutions, in December 2017.

"DevSecOps presents an opportunity to make application security part of the cultural and technological fabric of modern, high-velocity development and deployment models," said Andreas Kuehlmann, general manager of the Synopsys Software Integrity Group. "This study highlights many of the opportunities and challenges DevOps team face in adapting and applying application security tools and best practices. It also validates that automation,

speed, accuracy, and CI/CD integration—attributes Synopsys has built into its application security solutions—are critical to making DevSecOps successful."

To read the full report, click here.

To register for the joint 451 Research and Synopsys webinar exploring the result of this study on May 15, click here.

About the Synopsys Software Integrity Group

Synopsys Software Integrity Group helps organizations 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 maximize security and quality in DevSecOps and throughout the software development life cycle. Learn more at www.synopsys.com/software.

About Synopsys

Synopsys, Inc. (Nasdaq: SNPS) is the Silicon to Software™ partner for innovative companies developing the electronic products and software applications we rely on every day. As the world's 15th largest software company, Synopsys has a long history of being a global leader in electronic design automation (EDA) and semiconductor IP and is also growing its leadership in software security and quality solutions. Whether you're a system-on-chip (SoC) designer creating advanced semiconductors, or a software developer writing applications that require the highest security and quality, Synopsys has the solutions needed to deliver innovative, high-quality, secure products. Learn more at www.synopsys.com.

Editorial Contacts:
Mark Van Elderen
Synopsys, Inc.
650-793-7450
mark.vanelderen@synopsys.com

Simone Souza
Synopsys, Inc.
650-584-6454
simone@synopsys.com

SOURCE Synopsys, Inc.

---

https://news.blackduck.com/2018-04-25-Security-in-DevOps-Is-Lagging-Despite-Advantages-and-Opportunities-According-to-New-Study-by-451-Research-and-Synopsys