BSIMM14 Report: Application Security Automation Soars

Synopsys Software Integrity Group report highlights how customers embracing automation are improving security processes throughout the software life cycle.

SUNNYVALE, Calif., Dec. 5, 2023 /PRNewswire/ -- Synopsys, Inc. (Nasdaq: SNPS) today published BSIMM14, the latest edition of the annual Building Security In Maturity Model (BSIMM) report analyzing the software security practices across 130 organizations, including some of the most advanced companies in cloud, financial services, FinTech, ISV, insurance, IoT, healthcare, and technology industries. The report found that the use of automated security technology is growing rapidly, which in turn is propagating the "shift everywhere" philosophy – performing security tests throughout the entire software development life cycle – across more organizations.

Automation Adoption on the Rise
This year's findings revealed a clear trend of firms increasingly taking advantage of security automation to replace manual, subject matter expert–driven security activities to reduce cost and improve effectiveness.

Greater automation has enabled organizations to embrace the shift everywhere philosophy, with automated, event-driven security testing increasing by 200% over the last two years. Additional notable findings around the power of automation include:

- **Improved ease of review:** Automation has led to a 68% growth in mandatory code review in the last five years.
- **Enhanced affordability:** Recent economic conditions have caused a reduction in expensive, subject matter expert–driven activities that are not easy to automate. Centralized defect reporting and attack lists all decreased in usage by more than 17%.
- **Greater toolchain usage:** Organizations are embracing modern toolchain technology that allows security testing in the QA stage to be automated – leading to a 10% growth in several related security activities.

"Everyone has gone all-in on automation across a range of security functions, and that's leading directly to better practices," said Jason Schmitt, general manager of the Synopsys Software Integrity Group. "Companies are seeing firsthand that eliminating human error with consolidated, integrated security tooling makes security programs more effective and affordable — a compelling combination. With cyberattacks on the rise and coming from every angle, automation is proving essential to defend against myriad threats that are targeting software, while enabling companies to do more with less in this uncertain economy."

Maturing Culture of Security
The report also found that customers have made valuable strides in improving the culture of security at their organizations. Key findings include:

- **Security champions make a difference:** Firms with security champion programs made up of developers, QA analysts, or architects in a security-enabler role, earned an average 25% higher BSIMM score than firms without one.
- **Higher vendor standards:** Firms are also demanding more from service providers and partners. Expectations for strong vendor security practices grew by 21% as firms held vendors to standards similar to those they use internally.

Secure Software Supply Chain Practices Gain Traction
Customers also reported that security processes made impressive progress adhering to industry best practices:

- **SBOM usage grows:** Organizations are increasingly building Software Bills of Materials (SBOMs), with a 22% increase in SBOM creation from last year.
- **Open source awareness:** Identifying and controlling open source risk increased by just under 10% from last year.

Those interested in learning more about the findings and the BSIMM program can download the BSIMM14 report, which provides an in-depth analysis of the data and explores industry-specific trends or read the detailed blog post.

Acknowledgements
Some of the companies participating in the BSIMM study include AARP, Aetna, Bank of America, Bell Network, CIBC, Citi, Diebold Nixdorf, Egis Technology, Eli Lilly and Company, EQ Bank, Fidelity, Finastra, Genetec, HCA Healthcare, Honeywell, Imperva, Inspur Software, Intralinks, iPipeline, Johnson & Johnson, Landis+Gyr, Lenovo, MassMutual, MediaTek, Medtronic, Navient, Navy Federal Credit Union, NEC, NetApp, Oppo, Pegasystems, Principal Financial, Realtek, Reckitt, ServiceNow, Signify, SonicWall, Synchrony Financial, TD Ameritrade, Teradata, Trainline, U.S. Bank, Vanguard, Veritas, Verizon Media, Vivo, and ZoomInfo.

About the Synopsys Software Integrity Group
Synopsys Software Integrity Group provides integrated solutions that transform the way development teams build and deliver software, accelerating innovation while addressing business risk. Our industry-leading portfolio of software security products and services is the most comprehensive in the world and interoperates with third-party and open source tools, allowing organizations to leverage existing investments to build the security program that's best for them. Only Synopsys offers everything you need to build trust in your software. 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 an S&P 500 company, Synopsys has a long history of being a global leader in electronic design automation (EDA) and semiconductor IP and offers the industry's broadest portfolio of application security testing tools and services. Whether you're a system-on-chip (SoC) designer creating advanced semiconductors, or a software developer writing more secure, high-quality code, Synopsys has the solutions needed to deliver innovative products. Learn more at www.synopsys.com.

Editorial Contact:
Liz Samet
Synopsys, Inc.
336-414-6753
esamet@synopsys.com

SOURCE Synopsys, Inc.