New Synopsys Research Finds Significant Increase in Practices to Bolster Software Supply Chain Security

BSIMM13 data reveals nearly 50 percent surge in activities to secure open source components and integrate security into developer toolchains

MOUNTAIN VIEW, Calif., Sept. 21, 2022 /PRNewswire/ -- Synopsys, Inc. (Nasdaq: SNPS), today published BSIMM13, the latest edition of the annual Building Security In Maturity Model (BSIMM) report analyzing the software security practices across 130 organizations—including Adobe, PayPal and Lenovo—in their cumulative efforts to secure more than 145,000 applications built and maintained by nearly 410,000 developers.

The findings highlight a significant increase in activities that indicate BSIMM member organizations are implementing a "shift everywhere" approach to perform automated and continuous security testing throughout the software development lifecycle (SDLC) and manage risk across their complete application portfolio.

To learn more, download the BSIMM13 Trends & Insights report.

"The BSIMM13 findings suggest that with the attention placed on software supply chains, most enterprise organizations are taking a risk-based approach to application security. Such an approach recognizes that security isn't limited to the codebase; it includes the process of software development where security reviews and testing 'shift everywhere' to continuously improve security outcomes." said Jason Schmitt, general manager of the Synopsys Software Integrity Group. "The findings also demonstrate that BSIMM member organizations' software security initiatives are maturing, and they're now looking for ways to drive the scalability, efficiency and overall effectiveness of their programs."

Conducted by the Synopsys Software Integrity Group, BSIMM13 highlights evolving trends among member organizations' software security initiatives over the last 12 months, including:

- **Managing Software Supply Chain Risk and the Rise of SBOMs**
  Likely as a result of recent high-profile supply chain attacks, managing software supply chain risk—most commonly performed through identifying and securing open source software—appears to be a top priority for BSIMM member organizations**.** BSIMM13 reports a 51% increase in activities associated with controlling open source risk over the last 12 months, as well as a 30% increase in organizations building and maintaining a Software Bill of Materials (SBOM) to fully catalog the components within their deployed software.

- **Integrating Security into Developer Toolchains**
  As part of their efforts to "shift everywhere" BSIMM organizations made significant progress in integrating security options into CI/CD pipelines and developer toolchains over the last 12 months. BSIMM13 data notes a 48% growth in activities that enable organizations to include security tests in QA automation.

- **Expanding Software Security Beyond Products and Applications**
  BSIMM13 data also shows tremendous growth in activities that indicate security teams are working with operations to secure software that is not an application—such as automation created for CI/CD— as observations of activities for leveraging operational data for continuous improvement grew by 95% over the last 12 months.

- **"Shift Everywhere" with Automated and Continuous Testing**
  BSIMM13 data reports that 82% of BSIMM member organizations now use automated code review tools—ranking among the top-10 most-observed activities in BSIMM13—which unlocks their ability to perform faster, incremental security tests and identify vulnerabilities as they are introduced throughout the SDLC.

Established in 2008, the BSIMM is a maturity model that observes and quantifies the activities performed by software security professionals to help members of the wider security community plan, execute and measure their organizations' initiatives. BSIMM data originates in interviews conducted with member organizations during a BSIMM assessment. Following the assessment, observation data is anonymized and added to the BSIMM data pool, where statistical analysis is performed to highlight trends around how BSIMM organizations are securing their software.

In addition to publishing its annual report, BSIMM provides members with a private community to engage with peers, learn best practices and gain new insights through community discussions, blogs, e-learning courses, webinars and more exclusive content focused on securing software in today's dynamic business environment.

"Having joined the BSIMM community in 2015, we have found significant value in leveraging the insights drawn from the annually refreshed observations to help us plan and measure our own security program, and also gain a sense of the practice areas that are most important to our customers," said Bill Jaeger, Executive Director of Lenovo's Infrastructure Solutions Group Product Security Office. "Additionally, the BSIMM community itself is a fantastic resource, with members generously sharing experiences and lessons learned; we're all on a similar journey, and firms just beginning their software security initiatives can learn so much from those that started earlier."

Those interested in learning more about the findings and the BSIMM program can download the BSIMM13 Trends & Insights report or the full-length BSIMM13 Foundations, which provides an in-depth analysis of the data and explores industry-specific trends.

Acknowledgements

Synopsys would like to thank Jamie Boote, Eli Erlikhman, Stephen Gardner, and Sammy Migues, authors of the BSIMM13, as well as Kathy Clark-Fisher and Ryan Francis, whose behind-the-scenes work keeps the BSIMM science project, conferences, and community on track.

Some of the companies participating in the BSIMM study include: AARP, Adobe, Aetna, Ally Bank, Axway, Bank of America, Bell Network, CIBC, Cisco, Citi, Diebold Nixdorf, Depository Trust & Cleaning Corporation, Egis, Eli Lilly and Company, eMoney Advisor, EQBank, Equifax, Fidelity, Finastra, Freddie Mac, F-Secure, Genetec, HCA Healthcare, Honeywell CE, HSBC, Imperva, Inspur Software, Intralinks, iPipeline, Johnson & Johnson, Landis+Gyr, Lenovo, MassMutual, MediaTek, Medtronic, Navient, Navy Federal Credit Union, NEC, NetApp, Oppo, PayPal, Pegasystems, Principal Financial, Realtek, SambaSafety, ServiceNow, Signify, SonicWall, Synchrony Financial, TD Ameritrade, Teradata, Trainline, Trane, U.S. Bank, Veritas, Verizon Media, Vivo, World Wide Technology, ZoomInfo.

About BSIMM

Established in 2008, the Building Security In Maturity Model (BSIMM) is a data-driven tool for creating, measuring, and evaluating software security initiatives. Developed through the careful study and analysis of over 250 software security initiatives, BSIMM13 includes current, real-world data from 130 organizations across the globe. In addition to publishing its annual report, BSIMM provides member organizations with a private community to engage with peers, learn best practices and gain new insights through community discussions, blogs, e-learning courses, webinars and more. To learn more about the BSIMM program, visit www.bsimm.com

About the Synopsys Software Integrity Group

Synopsys Software Integrity Group 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. 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.