Synopsys Releases BSIMM10 Study Highlighting Impact of DevOps on Software Security

10th Iteration of the Building Security In Maturity Model Reflects Software Security Initiatives of 122 Firms

MOUNTAIN VIEW, Calif., Sept. 18, 2019 /PRNewswire/ -- Synopsys, Inc. (Nasdaq: SNPS) today released BSIMM10, the latest version of the Building Security In Maturity Model (BSIMM), designed to help organizations plan, execute, mature, and measure their software security initiatives (SSIs). Synopsys has used the BSIMM nearly 450 times across 185 firms over the past decade, and this 10th iteration reflects software security activities observed across 122 firms. BSIMM10 also highlights the impact of DevOps on software security initiatives, the emergence of a new wave of engineering-driven security efforts, and how firms progress through three phases of software security maturity. To download the report, visit www.bsimm.com/download.html.

"Since 2008, the BSIMM has served as an effective tool for understanding how organizations of all shapes and sizes, including some of the most advanced security teams in the world, are executing their software security strategies," said Jim Routh, head of enterprise information risk management at MassMutual. "The current BSIMM data reflect how many organizations are adapting their approaches to address the new dynamics of modern development and deployment practices, such as shorter release cycles, increased use of automation, and software-defined infrastructure."

BSIMM10 describes the work of 7,900 software security professionals whose efforts guide and maximize the security efforts of nearly 470,000 developers working on more than 173,000 applications. BSIMM10 represents firms in industry verticals including financial services, high tech, independent software vendors (ISVs), cloud, healthcare, Internet of Things (IoT), insurance, and retail.

Key findings from the BSIMM10 study:

- **DevOps' impact on software security:** The BSIMM data show that the DevOps movement and the adoption of continuous integration and continuous delivery (CI/CD) tooling are affecting the way that firms approach software security. This is seen in the BSIMM's addition of three new activities that reflect how firms are actively working to automate security activities to match the speed at which their business delivers functionality to market. BSIMM10 also includes updated descriptions and examples of existing activities to reflect how they are being implemented as part of modern DevOps organizations.
- **The new wave of engineering-driven security culture:** BSIMM10 is the first study to formally reflect changes in SSI culture, observed in a new wave of engineering-led software security efforts originating bottom-up in development and operations teams rather than top-down from a centralized software security group. In some organizations, an engineering-led security culture has overcome its struggle to establish and grow meaningful software security efforts. This new wave of engineering-driven security culture is emerging in response to both the demands of modern software delivery practices such as Agile and DevOps and undesirable friction with existing SSIs.
- **Firms use the BSIMM to navigate their software security journey:** BSIMM10 is the first edition to define three phases of SSI maturity—emerging, maturing, optimizing—and describe how different firms typically progress through them. The BSIMM data show that organizations improve demonstrably over time, and many achieve a level of maturity where they focus on the depth, breadth, and scale of the activities they're conducting rather than always striving for more activities.

"Leading an effective software security initiative is challenging, and the dramatic technological and organizational shifts brought on by DevOps and CI/CD are not making that task easier," said Sammy Migues, principal scientist at Synopsys. "As a tool that constantly evolves to reflect the experiences of hundreds of software security groups around the world, the BSIMM and its community are invaluable resources, whether you're just beginning your journey, looking to optimize your program, or grappling with new challenges."

The BSIMM includes data collected from firms that have established real SSIs, quantifying the occurrence of 119 activities to show the common ground shared by many initiatives as well as the variations that make each initiative unique. The BSIMM data show that high-maturity initiatives are well-rounded, carrying out numerous activities in all 12 of the practices described by the model. Organizations can use the BSIMM to compare initiatives and determine which additional activities might be useful to support their overall strategies.

Acknowledgments
Sammy Migues, principal scientist at Synopsys, Michael Ware, managing principal at Synopsys, and John Steven, chief technology officer at ZeroNorth, authored BSIMM10 after analyzing data collected over the past 11 years of software security research. Some of the companies participating in the BSIMM study include: Adobe, Aetna, Alibaba, Ally Bank, Amadeus, Amgen, Autodesk, Axway, Bank of America, Betfair, BMO Financial Group, Black Duck Software, Black Knight Financial

Services, Box, Canadian Imperial Bank of Commerce, Capital One, City National Bank, Cisco, Citigroup, Citizens Bank, Comerica Bank, Dahua, Depository Trust & Clearing Corporation, Eli Lilly, Ellucian, Experian, F-Secure, Fannie Mae, Fidelity, Freddie Mac, General Electric, Genetec, Global Payments, HCA Healthcare, Highmark Health Solutions, Horizon Healthcare Services, HSBC, iPipeline, Johnson & Johnson, JPMorgan Chase & Co., Lenovo, LGE, McKesson, Medtronic, Morningstar, Navient, NCR, NetApp, News Corp, NVIDIA, PayPal, Principal Financial Group, Royal Bank of Canada, Scientific Games, Synopsys Software Integrity Group, TD Ameritrade, The Home Depot, The Vanguard Group, Trainline, Trane, U.S. Bank, Veritas, Verizon, Wells Fargo, and Zendesk.

About the BSIMM
Started in 2008, the Building Security In Maturity Model (BSIMM) is a tool for measuring and evaluating software security initiatives. A data-driven model and measurement tool developed through the careful study and analysis of software security initiatives, the BSIMM includes real-world data from more than 120 organizations. The BSIMM is an open standard that includes a framework based on software security practices, which an organization can use to assess its own efforts in software security. For more information, 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 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.