Black Duck Newsroom

BSIMM8 Study Reinforces Benchmarking as a Critical Exercise in Early Stages of Software Security Initiatives

Latest Iteration of the Building Security in Maturity Model Shows More Organizations Jumpstarting their Software Security Initiatives with Assessments and Improving Over Time

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

MOUNTAIN VIEW, Calif., Sept. 20, 2017 /PRNewswire/ -- Synopsys, Inc. (Nasdaq: SNPS) today released BSIMM8, the latest version of a leading software security maturity model, which is based on real-world data and helps organizations plan, execute, and measure their software security initiatives (SSIs). The eighth iteration of the Building Security in Maturity Model (BSIMM) is based on data collected from the largest community to date. BSIMM8 shows that software security is becoming a critical business priority with more organizations benchmarking their efforts early in their SSI lifecycle and using the results strategically to improve their risk posture over time. To download the report, visit https://www.bsimm.com/download.html.

"With the rise of widely distributed and increasingly disruptive attacks targeting vulnerable software, we're seeing a shift from the reactive 'penetrate and patch' approach toward more proactive strategies that empower organizations to build secure software systematically from the ground up," said Dr. Gary McGraw, vice president of security technology at Synopsys. "Organizations are beginning to understand that they can mitigate risk more effectively by establishing a software security initiative, assessing their strengths and weaknesses early on through instruments like the BSIMM, and focusing their efforts on the most appropriate practices and activities."

BSIMM8 includes data collected from 109 firms and describes the work of 4,769 software security professionals. Their work guides and maximizes the security efforts of almost 300,000 developers across approximately 95,000 applications. BSIMM8 firms represent industry verticals including financial services, independent software vendors (ISVs), cloud, healthcare, Internet of Things (IoT), and insurance.

Key findings from the BSIMM8 study:

- **Organizations use the BSIMM to jumpstart their SSIs**. BSIMM8 introduces firms in the early stages of the SSI lifecycle, as evidenced by a slight decrease in the average maturity score[1] (33.1, down from 33.9 in BSIMM7) and average software security group age (3.88 years, down from 3.94 in BSIMM7) of the BSIMM population. SSI benchmarking is one of the pivotal first steps in the software security journey.
- **BSIMM firms mature over time.** Firms that have participated in multiple BSIMM assessments show a clear trend of improvement, with scores increasing by an average of 10.3, or 33.4 percent. Benchmarking is an effective exercise in guiding organizations along the optimal path toward building secure software consistently.
- **Maturity varies by industry**. Each industry prioritizes certain activities over others, and every industry and individual organization has a different path toward building security in. On average, cloud, financial services, and ISV firms are more mature than firms in healthcare, IoT, and insurance. Financial services and cloud firms have notably higher scores in compliance and policy practices, while IoT firms have the most mature

software environment practices.

According to Gartner, "Application security requires a structured, programmatic approach to deal with the seeming chaos of new technology and an evolving threat landscape. A successful application security program must be a balanced combination of people, process, and technology."[2]

The BSIMM observes firms that have established real software security initiatives, quantifying the occurrence of 113 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.

Acknowledgments

Dr. McGraw along with Sammy Migues, principal scientist at Synopsys, and Jacob West, chief architect at NetSuite, analyzed data collected during the past nine years of software security research. Companies participating in the assessments include: Adobe, Aetna, Amgen, ANDA, Autodesk, Axway, Bank of America, Betfair, BMO Financial Group, Black Knight Financial Services, Box, Canadian Imperial Bank of Commerce, Capital One, City National Bank, Cisco, Citigroup, Citizen's Bank, Comerica Bank, Cryptography Research (a division of Rambus), Dell EMC, Depository Trust & Clearing Corporation, Elavon, Ellucian, Epsilon, Experian, F-Secure, Fannie Mae, Fidelity, Freddie Mac, General Electric, Genetec, Highmark Health Solutions, Horizon Healthcare, Services, Inc., HPE Fortify, HSBC, Independent Health, iPipeline, JPMorgan Chase & Co., Lenovo, LGE, LinkedIn, McKesson, Medtronic, Morningstar, Navient, NetApp, NVIDIA, NXP Semiconductors N.V., Oracle NSGBU, PayPal, Principal Financial Group, Qualcomm, Royal Bank of Canada, Scientific Games, Siemens, Sony Mobile, Splunk, Symantec, Synopsys SIG, Target, TD Ameritrade, The Advisory Board, The Home Depot, The Vanguard Group, Trainline, Trane, U.S. Bank, Veritas, Verizon, Wells Fargo, Zendesk, and Zephyr Health.

- The BSIMM score reflects the total number of software security activities observed during the assessment of a firm's software security initiative. Each activity is worth one point and the BSIMM framework includes 113 activities.
- Source: Gartner, "A Guidance Framework for Establishing and Maturing an Application Security Program", 23 December 2016, Michael Isbitski & Ramon.

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 100 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 https://www.bsimm.com.

About the Synopsys Software Integrity Platform

Synopsys offers the most comprehensive solution for building integrity—security and quality—into the software development lifecycle and supply chain. The Software Integrity Platform unites leading testing technologies, automated analysis, and experts to create a robust portfolio of products and services. This portfolio enables

companies to develop personalized programs for detecting and remediating defects and vulnerabilities early in the development process, minimizing risk and maximizing productivity. Synopsys, a recognized leader in application security testing, is uniquely positioned to adapt and apply best practices to new technologies and trends such as IoT, DevOps, CI/CD, and the Cloud. For more information, go to 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:

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

SOURCE Synopsys, Inc.

---

https://news.blackduck.com/2017-09-20-BSIMM8-Study-Reinforces-Benchmarking-as-a-Critical-Exercise-in-Early-Stages-of-Software-Security-Initiatives