Black Duck Newsroom

Synopsys Publishes BSIMM11 Study Highlighting Fundamental Shifts in Software Security Initiatives in Response to DevOps and Digital Transformation

The 11th iteration of the Building Security In Maturity Model reflects how organizations are adapting their software security efforts to support modern software development paradigms

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

MOUNTAIN VIEW, Calif., Sept. 15, 2020 /PRNewswire/ -- Synopsys, Inc. (Nasdaq: SNPS) today published BSIMM11, the latest version of the Building Security In Maturity Model (BSIMM), created to help organizations plan, execute, measure, and improve their software security initiatives (SSIs). BSIMM11 reflects the software security practices observed across 130 firms from multiple industry verticals including financial services, FinTech, independent software vendors, cloud, healthcare, Internet of Things, insurance, and retail. BSIMM11 describes the work of 8,457 software security professionals who guide the efforts of over 490,000 developers.

BSIMM is used by organizations as a measuring stick to compare and contrast their own initiatives with the data from the broader BSIMM community. BSIMM11 shows that many organizations are adapting their software security efforts to support digital transformation and modern software development paradigms like DevOps.

Read the BSIMM11 Digest or download the full BSIMM11 study.

"The BSIMM is an excellent resource for security leaders interested in learning from the collective experiences of their peers, particularly to solve new or emerging challenges," said Mike Newborn, CISO of Navy Federal Credit Union, a member organization of the BSIMM community. "Today, most organizations face the challenge of securing a growing portfolio of applications against the backdrop of rapidly evolving and accelerating software development practices. BSIMM11 reflects how many of these organizations are adapting their software security strategies to protect themselves and their customers without stifling innovation or impeding the speed of development."

Emerging trends in BSIMM11

- **Engineering-led software security efforts are successfully contributing to DevOps value streams in pursuit of resiliency.** BSIMM11 shows that CI/CD instrumentation and operations orchestration have become standard components of many organizations' software security initiatives, and are influencing how they are organized, designed, and executed. For example, software security teams increasingly report into a technology group or CTO (as opposed to an IT security team or CISO) and are changing how they recruit and organize talent internally.
- **Software-defined security governance is no longer just aspirational.** Organizations are replacing some high-friction, out-of-band security activities with automated activities triggered by events in the CI/CD pipeline execution. Converting human processes and decision-making to algorithms is one of the ways organizations are increasingly addressing resource constraints and cadence management problems.

- **"Shift left" is becoming "shift everywhere."** The implementation of the "shift left" concept has evolved from the literal interpretation of performing some security testing earlier in the development cycle to performing security activities as soon as the artifacts to be reviewed are available. That could mean to the left of where activities have historically been performed, but often, it's to the right, including in production.
- **Introduction of FinTech vertical to BSIMM data pool.** Upon carefully reviewing the growing data pool of firms in the financial vertical, it became apparent that there was a need to add a separate vertical to account for firms that are effectively ISVs specifically for financial services software.

"The way modern software is built and deployed has transformed dramatically over the past few years, so naturally the efforts required to secure that software are changing as well," said Michael Ware, BSIMM co-author and senior director of technology at Synopsys. "Businesses are critically dependent on software, and modern methodologies have accelerated the speed of development. As a result, there is more software everywhere, and we still need to worry about all the pre-existing software. As a model that constantly evolves to represent the actual practices in use by hundreds of software security groups around the world—including some of the most advanced teams in the world—the BSIMM provides a near-real-time view into how these changes are being implemented to protect the growing software portfolios."

New activities in the BSIMM represent a shift toward DevSecOps

The three activities added to BSIMM10 saw exceptional growth within the past year (SM3.4 Integrate software-defined lifecycle governance, AM3.3 Monitor automated asset creation, CMVM3.5 Automate verification of operational infrastructure security). This reflects how some organizations are actively working to accelerate software security efforts to match the pace of software delivery. Furthermore, the two activities added in BSIMM11 represent a continuation of that trend (ST3.6 Implementing event-driven security testing, CMVM3.6 Publishing risk data for deployable artifacts).

BSIMM across industries

BSIMM provides unique, data-driven insight to understanding and comparing the relative strengths and weaknesses of software security initiatives across a variety of industries. Cloud, Internet of Things, and high technology firms are three of the most mature verticals in the BSIMM11 data pool. BSIMM11 also highlights differences between three highly regulated industries: financial services, healthcare, and insurance. The financial services industry, which had software security groups in place earlier than other industries, was seen to have more mature practices compared to their counterparts in healthcare and insurance. For the first time, the BSIMM presents data on the FinTech vertical, and found that it tracks fairly closely to financial services, with the primary deltas (in favor of FinTech) occurring in the training, security testing, and code review practices.

Read the BSIMM11 Digest or download the full BSIMM11 study.

For an interactive discussion of the key findings in BSIMM11, register for our October 15 webinar.

Acknowledgments

Sammy Migues, principal scientist at Synopsys, Michael Ware, senior director of technology at Synopsys, and John Steven, founding principal at Aedify Security, authored BSIMM11 after analyzing data collected over nearly 12 years of software security research. Some of the companies participating in the BSIMM study include: Adobe, Aetna, Alibaba, Ally Bank, Autodesk, Axway, Bank of America, Bell, BMO Financial Group, Black Knight Financial

Services, Box, Canadian Imperial Bank of Commerce, City National Bank, Cisco, Citigroup, Dahua, Depository Trust & Clearing Corporation, Eli Lilly, Equifax, Experian, F-Secure, Fannie Mae, Freddie Mac, General Electric, Genetec, Global Payments, HCA Healthcare, Highmark Health Solutions, Honeywell, Horizon Healthcare Services, HSBC, iPipeline, Johnson & Johnson, JPMorgan Chase & Co., Lenovo, MassMutual, McKesson, Medtronic, Morningstar, Navient, Navy Federal Credit Union, NCR, NEC Platforms, NetApp, NewsCorp, NVIDIA, PayPal, Pegasystems, Principal Financial Group, Royal Bank of Canada, SambaSafety, ServiceNow, Synopsys, TD Ameritrade, The Home Depot, The Vanguard Group, Trainline, Trane, U.S. Bank, Veritas, Verizon, Verizon Media, Wells Fargo, and Zendesk.

About the BSIMM

Started in 2008, the Building Security In Maturity Model (BSIMM) is a tool for creating, measuring, and evaluating software security initiatives. A data-driven model and measurement tool developed through the careful study and analysis of over 200 software security initiatives, BSIMM11 includes current, real-world data from 130 organizations. The BSIMM is an open standard that includes a framework based on software security practices, which an organization can use to assess and mature 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 Contact:
Mark Van Elderen
Synopsys, Inc.
650-793-7450
mvanelde@synopsys.com

SOURCE Synopsys, Inc.

---

https://news.blackduck.com/2020-09-15-Synopsys-Publishes-BSIMM11-Study-Highlighting-Fundamental-Shifts-in-Software-Security-Initiatives-in-Response-to-DevOps-and-Digital-Transformation