Black Duck Newsroom

Synopsys Publishes BSIMM12 Study Highlighting Notable Growth in Open Source, Cloud, and Container Security Efforts

The 12th iteration of the Building Security In Maturity Model reflects high-profile ransomware and software supply chain disruptions driving increased attention on software security.

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

MOUNTAIN VIEW, Calif., Sept. 28, 2021 /PRNewswire/ -- Synopsys, Inc. (Nasdaq: SNPS) today published BSIMM12, the latest version of the Building Security In Maturity Model (BSIMM) report, created to help organizations plan, execute, measure, and improve their software security initiatives. BSIMM12 reflects the software security practices observed across 128 firms from multiple industry verticals including financial services, FinTech, independent software vendors, cloud, healthcare, and Internet of Things. BSIMM12 describes the work of nearly 3,000 software security group members and over 6,000 satellite members. The BSIMM is used by organizations around the globe as a measuring stick to compare and contrast their own initiatives with the data from the broader BSIMM community.

BSIMM12 data indicates a 61% increase in software security groups' identification and management of open source over the past two years, almost certainly due to the prevalence of open source components in modern software and the rise of attacks using popular open source projects as vectors.

The growth in activities related to cloud platforms and container technologies show the dramatic impact these technologies have had on how organizations use and secure software. For example, observations of "use orchestration for containers and virtualized environments" increased 560% over the past two years.

Read about the BSIMM12 insights and trends or download the BSIMM12 digest.

"Over the last 18 months, organizations experienced a massive acceleration of digital transformation initiatives. This has resulted in increased adoption of software-defined approaches for deploying and managing software environments and cloud technology stacks," said Mike Ware, Information Security Principal at Navy Federal Credit Union, a member organization of the BSIMM community. "Given the complexity and pace of these changes, it's never been more important for security teams to have the tools which allow them to understand where they stand and have a reference for where they should pivot next. The BSIMM is a management tool for serving such a purpose. The BSIMM provides a unique lens into how organizations are shifting strategies for implementing software-defined security features like policy as code to align with modern software development principles and practices."

"The BSIMM study allows organizations to benchmark their current security practices so that they may establish priorities and maintain perspective in response to the emerging trends in the security landscape," said Mathieu Chevalier, Principal Security Architect and Manager, Genetec Inc., a member organization of the BSIMM community. "The descriptive model of the BSIMM helps organizations to determine how to get started building a software security initiative and to mature it effectively. BSIMM12's observations concerning shared responsibility

models in particular should encourage security leaders to consider how they're evolving to meet and mitigate any potential gaps in their security strategy."

"The BSIMM study is very aligned in terms of accessing industry best practices. It can be used to understand the level of maturity in a variety of development security activities as observed across multiple development teams," said Todd Wiedman, CISO at Landis+Gyr, a member organization of the BSIMM community. "With rapidly accelerating software development practices, BSIMM12 data illustrates the actual shifts taking place in security development programs. With this information, organizations can adapt their own strategies to protect their organization and customers without dampening innovation."

"As part of our Product and Data Security Program we have been using the BSIMM framework to help us in advancing our security strategy," said Vinod Raghavan, Director, Product & Data Security Program at Finastra, a member organization of the BSIMM community. "It has been instrumental in helping us to benchmark against other organizations in both financial services and other industries, supporting security maturity."

Emerging trends in BSIMM12

- **High-profile ransomware and software supply chain disruptions are driving increased attention on software security.** Over the past two years, BSIMM data shows a 61% increase in the "identify open source" activity and a 57% increase in the "create SLA boilerplates" activity among participant organizations.

- **Businesses are learning how to translate risk into numbers.** Organizations are exerting more effort to collect and publish their software security initiative data, demonstrated by a 30% increase of the "publish data about software security internally" activity over the past 24 months.

- **Increased capabilities for cloud security.** Increased executive attention, likely combined with engineering-driven efforts, has also resulted in organizations developing their own capabilities for managing cloud security and evaluating their shared responsibility models. There was an average of 36 new observations over the past two years across activities typically related to cloud security.

- **Security teams are lending resources, staff, and knowledge to DevOps practices.** BSIMM data shows a shift by software security groups away from mandating software security behaviors and toward a partnership role—providing resources, staff, and knowledge to DevOps practices with an objective to include security efforts in the critical path for software delivery.

- **Software Bill of Materials activities increased by 367%.** BSIMM data shows an increase in capabilities focused on inventorying software; creating a software Bill of Materials (BOM); understanding how the software was built, configured, and deployed; and increasing the organization's ability to re-deploy based on security telemetry. Demonstrating that many organizations have taken to heart the need for a comprehensive, up-to-date software BOM, the BSIMM activity related to those capabilities ("enhance application inventory with operations Bill of Materials") grew from 3 to 14 observations over the past two years—a 367% increase.

- **"Shift left" progresses to "shift everywhere."** The concept of "shift left" focuses on moving security testing earlier in the development process. "Shift everywhere" extends the idea to making security testing

continuous throughout the software lifecycle, including smaller, faster, pipeline-driven security tests conducted at the earliest opportunity, which might be during design or even all the way over in production.

The move away from maintaining traditional operational inventories and toward automated asset discovery and creating Bills of Material includes adding "shift everywhere" activities such as using containers to enforce security controls, orchestration, and scanning infrastructure as code. Increased BSIMM observation rates of activities such as "enhance application inventory with operations Bill of Materials," "use orchestration for containers and virtualized environments," and "monitor automated asset creation" all demonstrate this trend.

"Since 2008, BSIMM consulting, research, and data experts have been gathering data on the different paths that organizations take to address the challenges of securing software," said Jason Schmitt, general manager of the Synopsys Software Integrity Group. "With an average age of 4.4 years, BSIMM participating organizations' software security initiatives reflect how organizations are adapting their approaches to address the new dynamics of modern development and deployment practices. With this information, organizations can then adapt their own strategies to protect their organization and customers without dampening innovation."

To learn more, download the BSIMM12 Insights and Trends or read the blog post.

For an interactive discussion of the key findings in BSIMM12, register for our October 21 webinar.

Acknowledgments

Sammy Migues, principal scientist at Synopsys, Eli Erlikhman, managing principal at Synopsys, Jacob Ewers, principal security consultant at Synopsys, and Kevin Nassery, director of application security at Gemini authored BSIMM12 after analyzing data collected over nearly 13 years of software security research. Some of the companies participating in the BSIMM study include: AARP, Adobe, Aetna, Alibaba, Ally Bank, Autodesk, Axway, Bank of America, Bell, Black Knight Financial Services, Canadian Imperial Bank of Commerce, Cisco, Citigroup, Depository Trust & Clearing Corporation, Eli Lilly, eMoney Advisor, EQ Bank, Equifax, F-Secure, Fannie Mae, Finastra, Freddie Mac, Genetec, Global Payments, HCA Healthcare, Highmark Health Solutions, Honeywell, HSBC, iPipeline, Johnson & Johnson, Landis+Gyr, Lenovo, MassMutual, McKesson, Medtronic, MediaTek, Morningstar, Navient, Navy Federal Credit Union, NCR, NEC Platforms, NetApp, NewsCorp, NVIDIA, Oppo, PayPal, Pegasystems, Principal Financial Group, RB, SambaSafety, ServiceNow, Synopsys, TD Ameritrade, Teradata, The Home Depot, The Vanguard Group, Trainline, Trane, U.S. Bank, Veritas, Verizon Media.

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, BSIMM12 includes current, real-world data from 128 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 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.
703-657-4218
esamet@synopsys.com

SOURCE Synopsys, Inc.

---

https://news.blackduck.com/2021-09-28-Synopsys-Publishes-BSIMM12-Study-Highlighting-Notable-Growth-in-Open-Source,-Cloud,-and-Container-Security-Efforts