Black Duck Newsroom

Black Duck's BSIMM15 Report Highlights How Companies Are Tackling Security Risk in AI and Software Supply Chains

Key BSIMM15 Highlights:

- The number of organizations conducting adversarial tests (abuse cases) has doubled year-over-year.
- The number of organizations performing software composition analysis (SCA) on code repositories has increased by 67%.
- The number of organizations employing research groups to develop new attack methods has grown by 30%.
- The number of organizations generating software bills of materials (SBOMs) for deployed software has risen by 22%.

BURLINGTON, Mass., Jan. 14, 2025 /PRNewswire/ -- Black Duck® Software, Inc. ("Black Duck"), a leading provider of application security solutions, today released BSIMM15, the latest edition of its annual Building Security In Maturity Model (BSIMM) report. The report highlights how organizations are addressing software security challenges, including securing complex software supply chains and emerging technologies such as artificial intelligence (AI).

BSIMM15 analyzes the software security practices of 121 organizations, including some of the most advanced companies worldwide across industries like cloud computing, financial services, fintech, healthcare, IoT, and technology. Collectively, the BSIMM data pool represents the work of 11,100 security professionals supporting 270,000 developers and securing 96,000 applications.

"Over the past year, AI has gone mainstream across organizations of all sizes, bringing both opportunities and new risks," said Jason Schmitt, CEO of Black Duck. "Prioritizing security in the face of emerging technologies—especially rapidly evolving fields like AI—has never been more critical or challenging. BSIMM15 offers valuable insights into how organizations are navigating these hurdles and can serve as a guide for others looking to innovate securely and build trust in their software."

The BSIMM15 study reveals several key trends and insights, including:

- **Secure Innovation**: As organizations grapple with the opportunities and risks of AI and machine learning (ML), many are struggling to define and secure this new, evolving attack surface. A key trend observed is a ~30% increase in organizations engaging research groups to develop new attack methods. Additionally, the use of adversarial tests (abuse cases) has more than doubled since the previous report (BSIMM14).
- **Software Supply Chain Security**: With self-attestation requirements for selling software to the U.S. government, organizations are increasingly prioritizing activities that support compliance. For example, there has been a 22% rise in the number of organizations creating SBOMs for deployed software, and a 67% increase in organizations performing software composition analysis (SCA) on code repositories.
- **Declining Security Awareness Training**: In 2008, 100% of organizations in BSIMM1 conducted software security awareness training. However, this rate has steadily declined, and in BSIMM15, only 51.2% of organizations are still providing basic security training to their teams, marking the lowest rate observed to date.

Established in 2008, BSIMM is a maturity model that tracks the activities of software security professionals. It helps organizations plan, execute, and measure their software security initiatives. BSIMM data is collected through comprehensive interviews conducted during assessments by security professionals, after which the anonymized data is analyzed to identify trends in software security practices.

To learn more, download the BSIMM15 report, read the detailed blog post, or register for the February 27th webinar.

Acknowledgements
Black Duck would like to thank Jamie Boote, Ben Hutchison, Mike Lyman, Sammy Migues, and Sam Schueller, authors of the BSIMM15, as well as special guest authors, Tim Mackey and David Benas. Additional thanks to the nearly 165 individuals who helped gather the data for the BSIMM data pool, along with the 121 executives from the SSIs we studied to create BSIMM15.

Some of the companies participating in the BSIMM study include AARP, Aetna, Airoha, AON, Arlo, Axway, Bank of America, Bell Network, CIBC, Citi, Diebold Nixdorf, Egis Technology, Eli Lilly and Company, EQ Bank, Fidelity, Finastra, Genetec, HCA Healthcare, Honeywell, HUMAN Security, Imperva, Inspur Software Intralinks, iPipeline, Johnson & Johnson, Landis+Gyr, Lenovo, MassMutual, MediaTek, Medtronic, MiTAC, Navient, Navy Federal Credit Union, NetApp, Oppo, Pegasystems, Phison, QlikTech International AB, Realtek, Reckitt, Sammons Financial, ServiceNow, Signify, SonicWall, Synchrony Financial, TD Ameritrade, Teradata, U.S. Bank, Unisoc, Vanguard, Veritas, Vivo, and ZoomInfo.

About Black Duck

Black Duck®, formerly known as the Synopsys Software Integrity Group, offers the most comprehensive, powerful, and trusted portfolio of application security solutions in the industry. We have an unmatched track record of helping organizations around the world secure their software quickly, integrate security efficiently in their development environments, and safely innovate with new technologies. As the recognized leaders, experts, and innovators in software security, Black Duck has everything you need to build trust in your software. Learn more at www.blackduck.com.

SOURCE Black Duck Software

For further information: Liz Samet, Black Duck, 336.414.6753, esamet@blackduck.com

---

https://news.blackduck.com/2025-01-14-Black-Ducks-BSIMM15-Report-Highlights-How-Companies-Are-Tackling-Security-Risk-in-AI-and-Software-Supply-Chains