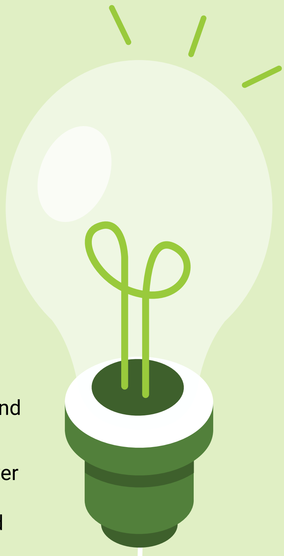
SYNOPSYS® | BSIMM

5 Lessons Learned From the BSIMM



The Building Security In Maturity Model (BSIMM) is a study of real-world software security initiatives (SSI). Learning about the quantified practices carried out by real SSIs can help your security team plan, carry out, and measure initiatives of your own.

After conducting hundreds of BSIMM assessments over the last 10 years, we've uncovered some undeniable trends and truths. Here are the top 5 things you should keep in mind as you build or tweak your program.

1. There are no special snowflakes.

How do you decide which activities will make your software secure? The 119 security activities described in the BSIMM fit every organization in every industry. What works to keep financial services or technology firms secure will work for retailers, healthcare, manufacturers, and you.

2. Your firm's risk drivers are unique.

The BSIMM describes what firms are doing to make software secure. But the risk drivers in your firm will result in unique prioritization, scale, implementation, depth, breadth, and other characteristics of the activities you implement. Customizing your SSI for your firm is a foundational necessity for success.

3. Your software security team can't do everything.

There isn't a single group within the organization that controls every tool, system, configuration, or entry point. Software security is everyone's responsibility. Provide everyone with awareness training, and recruit other people or teams to help you secure the nooks and crannies of your organization.

4. Security still needs people.

You can buy any number of tools that go "ding" in the night when they discover vulnerabilities. But someone must read the results, prioritize findings, and fix the issues. Good people, not tools, make the difference. Increasing software security skill sets on your team is essential to creating an effective SSI.

5. Software security is more than penetration testing.

No single tool can solve the software security problem, even penetration testing. Every strong SSI performs 12 core activities across four domains—governance, intelligence, secure software development, and deployment—and there are over 100 more to consider for your own SSI.

By providing actual measurement data from the field, the BSIMM makes it possible for you to build a long-term plan for a software security initiative and track your progress against the plan.

Learn how to join the BSIMM Community

SYNOPSYS®

The Synopsys difference

Synopsys 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. For more information, go to www.synopsys.com/software