SYNOPSYS®

Building Security In Maturity Model
(BSIMM)

Bringing science to software security

BSIMM results provide a way to assess the current state of your software security initiative, identify gaps, prioritize change, and determine how and where to apply resources for immediate improvement.

What the BSIMM enables you to do

1. Start a software security initiative (SSI) using real data.

If you don't have a software security initiative yet, you need one. Before you start down that path, the BSIMM will help you identify the core activities that all successful initiatives undertake—no matter what industry you're in.

2. Compare your SSI to other firms in your industry.

The BSIMM is one of the best yardsticks available today for measuring how your SSI stacks up against the rest of your industry peers. With your goals in mind, you can quickly determine where you stand relative to your needs.

3. Benchmark and track your SSI growth.

The BSIMM is the best and only repeatable way to measure your SSI's effectiveness. Once your SSI is established, you can use it to measure your continuous improvement year over year. It will also provide concrete details to show your executive team and board how your security efforts are making a difference.

4. Evolve your initiative using lessons learned from mature initiatives.

The BSIMM is a "what works" report on building and evolving a software security initiative. It comprises proven activities that mature organizations are performing today. You can use your assessment results, the BSIMM activities, and your objectives to set strategies and priorities for real improvement.

5. Interact with professionals facing common issues.

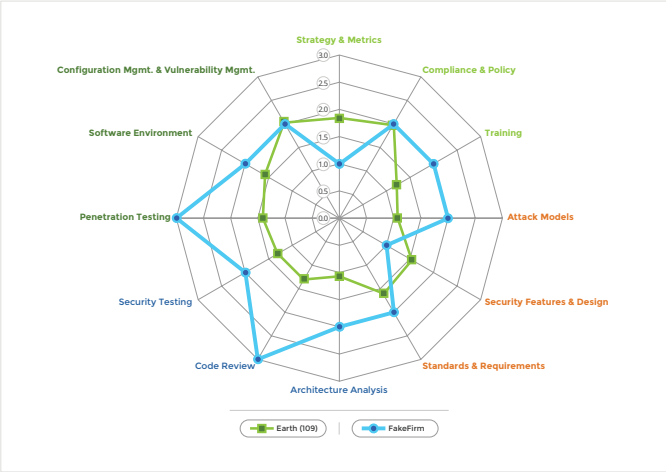
Along with your BSIMM, you gain access to our exclusive BSIMM community, which includes monthly newsletters, specialized quarterly webinars, U.S.- and U.K.-based annual conferences, RSA conference networking events, and a vibrant online community.

Get a personalized report

Every BSIMM comes with a detailed report highlighting your areas of strength and where you need improvement:

- **Customized Spider Chart:** This diagram shows at a glance where you are ahead of the game and where you might be behind. As you switch from measuring-stick mode to SSI-planning mode, these results provide objective guidance that you can implement immediately.
- **BSIMM Company Scorecard:** This table shows where you stand relative to all other initiatives. You can use it to look at your entire initiative over time, your individual business units, your business partners, and the vendors you work with.

EARTH vs. FAKE FIRM SPIDER CHART



What BSIMM participants are saying

Software is influencing more and more of our daily lives as consumers, professionals, and humans are embracing a digital experience. Leading organizations that use BSIMM to benchmark their software security resiliency practices have a significant competitive advantage in the marketplace.

~ JIM ROUTH, CHIEF SECURITY OFFICER, AETNA

Since 2009, each new version of BSIMM demonstrates how software security is becoming more mainstream and adopted by an always larger number of organizations. BSIMM7 is no exception and possibly represents an inflection point where software security is increasingly part of the development practices and less an independent discipline of software engineering.

~ ERIC BAIZE, SENIOR DIRECTOR, PRODUCT SECURITY OFFICE, DELL EMC

BSIMM7 is a fundamental resource for those looking for solid foundations or improvement for a software security initiative based on real data about what organizations worldwide actually do and a consistent, systematic approach to classify and understand them.

~ IVAN ARCE, DIRECTOR OF SECURITY, ICT PROGRAM, SADOSKY FOUNDATION

BSIMM8 SCORECARD FOR: FAKEFIRM | OBSERVATIONS: 37

GOVERNANCE			INTELLIGENCE			SSDL TOUCHPOINTS			DEPLOYMENT		
ACTIVITY	BSIMM8 FIRMS (109)	FAKEFIRM	ACTIVITY	BSIMM8 FIRMS (109)	FAKEFIRM	ACTIVITY	BSIMM8 FIRMS (109)	FAKEFIRM	ACTIVITY	BSIMM8 FIRMS (109)	FAKEFIRM
Strategy & Metrics			Attack Models			Architecture Analysis			Penetration Testing		
[SM1.1]	55	1	[AM1.2]	68		[AA1.1]	90	1	[PT1.1]	95	1
[SM1.2]	56		[AM1.3]	36		[AA1.2]	30	1	[PT1.2]	71	1
[SM1.3]	52	1	[AM1.5]	50	1	[AA1.3]	24	1	[PT1.3]	68	
[SM1.4]	92	1	[AM2.1]	9		[AA1.4]	49		[PT2.2]	23	1
[SM2.1]	46		[AM2.2]	8	1	[AA2.1]	14		[PT2.3]	20	
[SM2.2]	36		[AM2.5]	14	1	[AA2.2]	12	1	[PT3.1]	8	1
[SM2.3]	40		[AM2.6]	14	1	[AA3.1]	2		[PT3.2]	7	
[SM2.5]	21		[AM2.7]	10		[AA3.2]	0				
[SM2.6]	33		[AM3.1]	4		[AA3.3]	2				
[SM3.1]	15		[AM3.2]	1							
[SM3.2]	9										
Compliance & Policy			Security Features & Design			Code Review			Software Environment		
[CP1.1]	66	1	[SFD1.1]	85		[CR1.2]	69	1	[SE1.1]	49	
[CP1.2]	89		[SFD1.2]	70	1	[CR1.4]	65	1	[SE1.2]	91	1
[CP1.3]	56	1	[SFD2.1]	29		[CR1.5]	34		[SE2.2]	33	1
[CP2.1]	27		[SFD2.2]	41		[CR1.6]	37	1	[SE2.4]	29	
[CP2.2]	37		[SFD3.1]	5		[CR2.5]	26		[SE3.2]	15	
[CP2.3]	35		[SFD3.2]	11		[CR2.6]	16		[SE3.3]	4	
[CP2.4]	40		[SFD3.3]	2		[CR2.7]	23		[SE3.4]	4	
[CP2.5]	41	1				[CR3.2]	3	1			
[CP3.1]	22					[CR3.3]	2				
[CP3.2]	14					[CR3.4]	3				
[CP3.3]	5					[CR3.5]	5				
Training			Standards & Requirements			Security Testing			Config. Mgmt. & Vuln. Mgmt.		
[T1.1]	73	1	[SR1.1]	66	1	[ST1.1]	87	1	[CMVM1.1]	92	1
[T1.5]	31		[SR1.2]	69		[ST1.3]	79	1	[CMVM1.2]	96	
[T1.6]	22	1	[SR1.3]	71	1	[ST2.1]	25	1	[CMVM2.1]	78	1
[T1.7]	44		[SR2.2]	33	1	[ST2.4]	11		[CMVM2.2]	83	
[T2.5]	16		[SR2.3]	25		[ST2.5]	9		[CMVM2.3]	44	
[T2.6]	18	1	[SR2.4]	25		[ST2.6]	10		[CMVM3.1]	4	
[T3.1]	3		[SR2.5]	26		[ST3.3]	4		[CMVM3.2]	6	
[T3.2]	6		[SR2.6]	15	1	[ST3.4]	3		[CMVM3.3]	7	
[T3.3]	5		[SR3.1]	10		[ST3.5]	4		[CMVM3.4]	12	
[T3.4]	7		[SR3.2]	9							
[T3.5]	4										
[T3.6]	5										

The Synopsys difference

Synopsys offers the most comprehensive solution for building integrity—security and quality—into your SDLC and supply chain. We've united leading testing technologies, automated analysis, and experts to create a robust portfolio of products and services. This portfolio enables companies to develop customized 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. We don't stop when the test is over. We offer onboarding and deployment assistance, targeted remediation guidance, and a variety of training solutions that empower you to optimize your investment. Whether you're just starting your journey or well on your way, our platform will help ensure the integrity of the applications that power your business.

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

Synopsys, Inc.
185 Berry Street, Suite 6500
San Francisco, CA 94107 USA

U.S. Sales: 800.873.8193
International Sales: +1 415.321.5237
Email: sig-info@synopsys.com

SYNOPSYS®
Silicon to Software™

09/06/17.CS11536_SIG_BSIMM_DS7_v3.