Building Security In Maturity Model (BSIMM)

Bringing science to software security

Change is a constant. Is your SSI keeping up?

- Uptick in development velocity
- Use of automation to drive application lifecycle management processes
- Engineering-led software security efforts
- Shift to containers, microservices, and virtualized environments
- Conflicts in multicloud deployment strategies
- Everything as code
- New application architectures

Overview

Whether software security changes are being driven by engineering team evolution, such as with agile, CI/CD, and DevOps, or originating top-down from a centralized software security group (SSG), maturing your software security initiative (SSI) is critical to your success in managing risk. But what if your team has neither the visibility into the current state of your SSI nor the data they need to create an improvement strategy and prioritize SSI change?

Your solution is to use the Building Security In Maturity Model (BSIMM), a decade-long study of SSIs resulting in a unique industry model and yardstick for measuring SSIs. By quantifying the activities of many different organizations, the BSIMM describes the common ground they share as well as the variations that make each unique. A BSIMM assessment scorecard provides a way to assess the current state of your SSI, 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 an SSI yet, you need one. As you start down that path, the BSIMM will help you understand the core activities that all successful initiatives undertake—no matter what industry you're in, your company size, your deployment models, or your compliance requirements.

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

The BSIMM is the only yardstick available today for measuring your SSI and determining how your results compare with other results across multiple industry groups. 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 breadth and depth. Once your SSI is established, you can use the BSIMM to measure your continuous improvement year over year. The BSIMM also provides concrete details to show your executive team and board how your security efforts are making a difference.

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

The BSIMM is a "what works" report on building and evolving an SSI. 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.

Get a personalized report

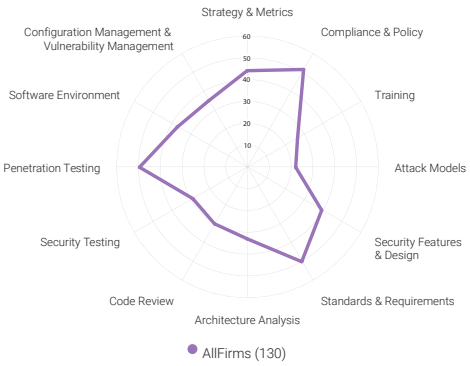
Every BSIMM assessment comes with a detailed report highlighting your SSI areas of strength and where it could use improvement. For use with executives and the board, you also get:

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 feedback so you can track progress.

BSIMM Scorecard. This table shows where you stand relative to other initiatives. You can use it to look at your entire initiative over time, your individual business units, business partners, and the vendors you work with.

Extracting value

"Having joined the BSIMM community in 2015, we have found significant value in leveraging the insights drawn from the annually refreshed observations to help us plan and measure our own security program, and also gain a sense of the practice areas that are most important to our customers," said Bill Jaeger, executive director of Lenovo's Infrastructure Solutions Group Product Security Office.



GOVERNANCE			INTELLIGENCE			SSDL TOUCHPOINTS			DEPLOYMENT		
ACTIVITY	BSIMM14 FIRMS (OUT OF 130)	EXAMPLE FIRM	ACTIVITY	BSIMM14 FIRMS (OUT OF 130)	EXAMPLE FIRM	ACTIVITY	BSIMM14 FIRMS (OUT OF 130)	EXAMPLE FIRM	ACTIVITY	BSIMM14 FIRMS (OUT OF 130)	EXAMPLE FIRM
STRATEGY & METRICS			**ATTACK MODELS**			**ARCHITECTURE ANALYSIS**			**PENETRATION TESTING**		
[SM1.1]	101	1	[AM1.2]	73		[AA1.1]	108	1	[PT1.1]	114	
[SM1.3]	80		[AM1.3]	49	1	[AA1.2]	59	1	[PT1.2]	102	1
[SM1.4]	118		[AM1.5]	81		[AA1.4]	63		[PT1.3]	85	1
[SM2.1]	73		[AM2.1]	16		[AA2.1]	35		[PT2.2]	42	
[SM2.2]	71		[AM2.6]	16	1	[AA2.2]	34	1	[PT2.3]	55	
[SM2.3]	71		[AM2.7]	15	1	[AA2.4]	40	1	[PT3.1]	30	1
[SM2.6]	77		[AM2.8]	20		[AA3.1]	20		[PT3.2]	21	
[SM2.7]	62	1	[AM2.9]	16		[AA3.2]	8				
[SM3.1]	32		[AM3.2]	8		[AA3.3]	17				
[SM3.2]	23		[AM3.4]	13							
[SM3.3]	32		[AM3.5]	11							
[SM3.4]	8										
[SM3.5]	0										
COMPLIANCE & POLICY			**SECURITY FEATURES & DESIGN**			**CODE REVIEW**			**SOFTWARE ENVIRONMENT**		
[CP1.1]	103	1	[SFD1.1]	100	1	[CR1.2]	84	1	[SE1.1]	88	
[CP1.2]	114	1	[SFD1.2]	95	1	[CR1.4]	112	1	[SE1.2]	113	1
[CP1.3]	101	1	[SFD2.1]	45		[CR1.5]	74		[SE1.3]	92	1
[CP2.1]	58		[SFD2.2]	70		[CR1.7]	55		[SE2.2]	68	1
[CP2.2]	63		[SFD3.1]	18		[CR2.6]	26	1	[SE2.4]	45	
[CP2.3]	72		[SFD3.2]	22		[CR2.7]	20		[SE2.5]	63	1
[CP2.4]	62		[SFD3.3]	9		[CR2.8]	28	1	[SE2.7]	47	1
[CP2.5]	80	1				[CR3.2]	17		[SE3.2]	18	
[CP3.1]	38					[CR3.3]	5		[SE3.3]	18	
[CP3.2]	34					[CR3.4]	3		[SE3.6]	22	
[CP3.3]	15					[CR3.5]	4		[SE3.8]	2	
									[SE3.9]	0	
TRAINING			**STANDARDS & REQUIREMENTS**			**SECURITY TESTING**			**CONFIG. MGMT. & VULN. MGMT.**		
[T1.1]	76	1	[SR1.1]	94	1	[ST1.1]	110	1	[CMVM1.1]	117	1
[T1.7]	64	1	[SR1.2]	103	1	[ST1.3]	91	1	[CMVM1.2]	95	
[T1.8]	59		[SR1.3]	98		[ST1.4]	62		[CMVM1.3]	98	1
[T2.5]	44		[SR1.5]	101	1	[ST2.4]	23		[CMVM2.1]	92	
[T2.8]	27	1	[SR2.2]	75		[ST2.5]	34		[CMVM2.3]	53	
[T2.9]	32	1	[SR2.5]	63	1	[ST2.6]	25		[CMVM3.1]	14	
[T2.10]	26		[SR2.7]	58		[ST3.3]	16		[CMVM3.2]	24	
[T2.11]	30		[SR3.2]	18		[ST3.4]	4		[CMVM3.3]	18	
[T2.12]	28		[SR3.3]	19		[ST3.5]	3		[CMVM3.4]	30	1
[T3.1]	8		[SR3.4]	21		[ST3.6]	6		[CMVM3.5]	16	1
[T3.2]	14								[CMVM3.6]	3	
[T3.6]	8								[CMVM3.7]	35	
									[CMVM3.8]	0	

About Black Duck

Black Duck® 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.