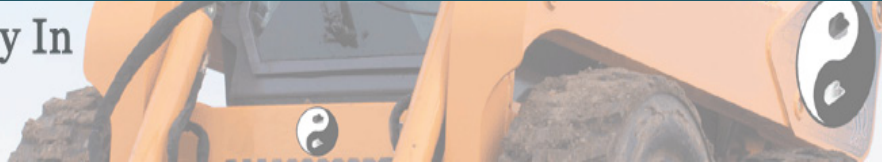




Building Security In Maturity Model



SOFTWARE SECURITY SCIENCE

Whether you run a software security initiative today or are charged with starting one tomorrow, you will find BSIMM to be a useful measurement and planning tool.

The Building Security In Maturity Model (BSIMM) allows you to:

- Measure your software security initiative relative to organizations like yours
- Start a new software security initiative
- Evolve your software security initiative by executing proven activities that mature organizations carry out today

“It’s not much of a secret that a lot of software has security flaws. One reason is that there aren’t any real standards for designing secure software. In fact, the right way to secure programs is rarely discussed at all. A new group is hoping to change that.”

Ben Worthen
Wall Street Journal

Based on in-depth interviews with leading firms from three verticals, including Adobe, EMC, Google, Microsoft, QUALCOMM, Wells Fargo, and The Depository Trust & Clearing Corporation (DTCC), BSIMM identifies a set of activities practiced by nine of the most successful software security initiatives in the world.

To view the full report, visit <http://bsi-mm.com>

MEASURE YOUR INITIATIVE

BSIMM is a yardstick for measuring your software security initiative. You will immediately see which activities you routinely carry out and which you don’t as compared to top software security initiatives. With your goals in mind, you can quickly determine where you stand relative to your needs.

START YOUR INITIATIVE

If you don’t have a software security initiative, you need one. In building BSIMM, we discovered ten things everyone does and these core activities will help you get started. They include building support for software security throughout the organization, providing awareness training, driving automation, using the attacker perspective, and publishing security features for other groups to use.

EVOLVE YOUR INITIATIVE

BSIMM is a “what works” guide for building and evolving a software security initiative. BSIMM is built from proven activities that mature organizations are performing today. Use your assessment results, the BSIMM activities, and your objectives to set strategy and priorities for real improvements.

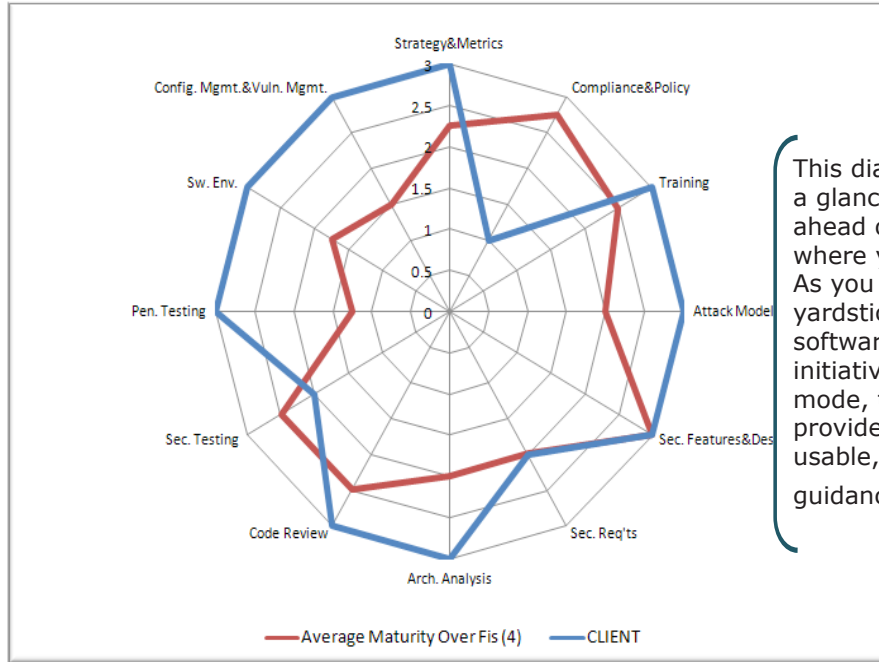
CIGITAL THOUGHT LEADERSHIP

We developed BSIMM to bring science to software security. It is a fact-based model of what is being done in mature software security initiatives. Download BSIMM from <http://bsi-mm.com> and use it. If you prefer a more detailed assessment, we can add your company to the model and help you to determine the next steps for your program.



BSIMM RESULTS

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



This diagram shows at a glance where you are ahead of the game and where you are behind. As you switch from yardstick-mode to software security initiative planning-mode, these results provide immediately usable, objective guidance.

“Comprehensive software security involves a combination of people, processes, and technologies, and it almost always requires some change to the way the organization operates. As software security comes of age, using a maturity model will only help to accelerate your enterprise security initiative.”

**Joseph Feiman
Gartner**

This table is an example of BSIMM results. It shows where you stand relative to leading initiatives.

Governance			Intelligence			SDL Touchpoints			Deployment		
Activity	Obs.	CLIENT	Activity	Obs.	CLIENT	Activity	Obs.	CLIENT	Activity	Obs.	CLIENT
[SM1.1]	4	1	[AM1.1]	5	1	[AA1.1]	5		[PT1.1]	9	
[SM1.2]	8	1	[AM1.2]	6		[AA1.2]	4		[PT1.2]	2	
[SM1.3]	6	1	[AM1.3]	2		[AA1.3]	8	1	[PT2.1]	3	1
[SM1.4]	7	1	[AM1.4]	7		[AA1.4]	3		[PT2.2]	2	
[SM1.5]	7	1	[AM2.1]	3		[AA2.1]	4		[PT2.3]	1	
[SM2.1]	7	1	[AM2.2]	6		[AA2.2]	2	1	[PT3.1]	2	1
[SM2.2]	4	1	[AM2.3]	5		[AA2.3]	5		[PT3.2]	2	
[SM2.3]	7	1	[AM2.4]	5		[AA3.1]	2				
[SM2.4]	4	1	[AM3.1]	1		[AA3.2]	1	1			
[SM3.1]	3	1	[AM3.2]	1	1						
[SM3.2]	1	1									
[SFD1.1]	6	1	[SFD1.1]	9	1	[CR1.1]	3	1	[SE1.1]	2	1
[SFD1.2]	6		[SFD1.2]	6	1	[CR1.2]	7	1	[SE1.2]	9	1
[SFD1.3]	9	1	[SFD2.1]	6	1	[CR1.3]	3	1	[SE2.1]	1	1
[SFD2.1]	3		[SFD2.2]	5	1	[CR2.1]	7	1	[SE2.2]	4	1
[SFD2.2]	4		[SFD2.3]	4	1	[CR2.2]	5	1	[SE2.3]	2	1
[SFD2.3]	5		[SFD3.1]	1	1	[CR2.3]	4	1	[SE3.1]	3	1
[SFD3.1]	3		[SFD3.2]	5	1	[CR2.4]	5	1			
[SFD3.2]	5					[CR2.5]	5	1			
[SFD3.3]	1					[CR3.1]	2	1			
	2					[CR3.2]	1	1			
	2					[CR3.3]	1	1			
[T1.1]	9		[SR1.1]	5	1	[ST1.1]	5	1	CMVM1.1	4	1
[T1.2]	5		[SR1.2]	3		[ST1.2]	5		CMVM1.2	6	
[T1.3]	5	1	[SR1.3]	3	1	[ST2.1]	9	1	CMVM2.1	6	1
[T1.4]	7		[SR1.4]	4		[ST2.2]	2		CMVM2.2	4	
[T2.1]	6		[SR2.1]	3	1	[ST2.3]	3	1	CMVM2.3	2	1
[T2.2]	8	1	[SR2.2]	1		[ST3.1]	5		CMVM3.1	1	
[T2.3]	1		[SR2.3]	4	1	[ST3.2]	7		CMVM3.2	2	1
[T2.4]	6		[SR2.4]	5		[ST3.3]	2				
[T2.5]	4	1	[SR2.5]	4	1	[ST3.4]	2				
[T3.1]	2		[SR3.1]	3							
[T3.2]	1										
[T3.3]	1	1									

Legend: Activity 110 activities from BSIMM, shown in 4 domains and 12 practices
 Obs. observed count of firms performing this practice out of the original nine firms
 yellow an activity performed by 8 or 9 of the original nine firms
 light blue the activity most commonly performed in remaining practices, to ensure coverage
 red where you do not perform a most common activity
 green where you do perform a most common activity
 light blue a practice where your high-water mark score is below the average of the nine
 dark blue a data-driven candidate activity for increasing overall maturity

Contact us today for an assessment of your software security initiative and guidance on a strategy that works for you.

Call us at 703-404-9293 or email sales@cigital.com