SYNERCOMM
SECURE • INTELLIGENT • NETWORKS

Maturing Your SDLC: Ch 1. BSIMM Framework

By: William Kiley
Managing Consultant - DevSecOps

Why use a framework?

- Efficiency
  - Built-in abstractions to reduce complexity/wheel reinvention
- Quality
  - Consistent design
  - Battle-tested components
- Documentation

Why? efficiency

- Abstractions
- Direction

Why? quality

- Consistent design
- Battle-tested components

Framework… for software security?

BSIMM Framework History

- Since 2009
- Collaborative, quantitative approach to software security

Our philosophy

We understand that not all organizations need to achieve the same security goals, but we believe all organizations can benefit from using the same measuring stick.

(Publicly) Participating Firms

Core Domains

Governance

Practices that help organize, manage, and measure a software security initiative

Learn more

Intelligence

Practices that result in collections of corporate knowledge used in carrying out software security activities throughout the organization

Learn more

SSDL Touchpoints

Practices associated with analysis and assurance of particular software development artifacts and processes

Learn more

Deployment

Practices that interface with traditional network security and software maintenance organizations

Learn more

All about the activities

- [SM1.4] Identify gate locations and gather necessary artifacts.
- [CP1.2] Identify PII obligations.
- [T1.1] Provide awareness training.
- [AM1.2] Create a data classification scheme and inventory.
- [SFD1.1] Build and publish security features.
- [SR1.2] Create a security portal.
- [AA1.1] Perform security feature review.
- [CR1.2] Have SSG perform ad hoc code review.
- [ST1.1] Ensure QA supports edge/boundary value condition testing.
- [PT1.1] Use external penetration testers to find problems.
- [SE1.2] Ensure host and network security basics are in place.
- [CMVM1.2] Identify software bugs found in operations monitoring and feed them back to development.

How to begin?

- ✔ Prep your org
- Assess the current state of affairs

BSIMM Scorecard

GOVERNANCE		INTELLIGENCE		SSDL TOUCHPOINTS		DEPLOYMENT	
ACTIVITY	BSIMM9 FIRMS (out of 120)	ACTIVITY	BSIMM9 FIRMS (out of 120)	ACTIVITY	BSIMM9 FIRMS (out of 120)	ACTIVITY	BSIMM9 FIRMS (out of 120)
Strategy & Metrics		**Attack Models**		**Architecture Analysis**		**Penetration Testing**	
[SM1.1]	71	[AM1.2]	75	[AA1.1]	101	[PT1.1]	105
[SM1.2]	66	[AM1.3]	38	[AA1.2]	33	[PT1.2]	89
[SM1.3]	67	[AM1.5]	53	[AA1.3]	27	[PT1.3]	74
[SM1.4]	101	[AM2.1]	10	[AA1.4]	57	[PT2.2]	26
[SM2.1]	47	[AM2.2]	10	[AA2.1]	15	[PT2.3]	21
[SM2.2]	42	[AM2.5]	16	[AA2.2]	14	[PT3.1]	10
[SM2.3]	44	[AM2.6]	14	[AA3.1]	4	[PT3.2]	7
[SM2.6]	39	[AM2.7]	11	[AA3.2]	2		
[SM3.1]	15	[AM3.1]	4	[AA3.3]	3		
[SM3.2]	7	[AM3.2]	2				
[SM3.3]	18						
Compliance & Policy		**Security Features & Design**		**Code Review**		**Software Environment**	
[CP1.1]	79	[SFD1.1]	95	[CR1.2]	82	[SE1.1]	58
[CP1.2]	101	[SFD1.2]	70	[CR1.4]	76	[SE1.2]	104
[CP1.3]	66	[SFD2.1]	34	[CR1.5]	40	[SE2.2]	39
[CP2.1]	39	[SFD2.2]	46	[CR1.6]	44	[SE2.4]	31
[CP2.2]	38	[SFD3.1]	9	[CR2.5]	28	[SE3.2]	17
[CP2.3]	43	[SFD3.2]	9	[CR2.6]	20	[SE3.3]	4
[CP2.4]	42	[SFD3.3]	2	[CR2.7]	25	[SE3.4]	11
[CP2.5]	47			[CR3.2]	4	[SE3.5]	0
[CP3.1]	21			[CR3.3]	1	[SE3.6]	0
[CP3.2]	12			[CR3.4]	4	[SE3.7]	0
[CP3.3]	5			[CR3.5]	3		
Training		**Standards & Requirements**		**Security Testing**		**Config. Mgmt. & Vuln. Mgmt.**	
[T1.1]	80	[SR1.1]	75	[ST1.1]	100	[CMVM1.1]	101
[T1.5]	34	[SR1.2]	78	[ST1.3]	88	[CMVM1.2]	102
[T1.6]	26	[SR1.3]	76	[ST2.1]	30	[CMVM2.1]	82
[T1.7]	47	[SR2.2]	38	[ST2.4]	14	[CMVM2.2]	87
[T2.5]	21	[SR2.3]	23	[ST2.5]	12	[CMVM2.3]	57
[T2.6]	23	[SR2.4]	39	[ST2.6]	13	[CMVM3.1]	5
[T3.1]	4	[SR2.5]	29	[ST3.3]	4	[CMVM3.2]	7
[T3.2]	8	[SR3.1]	17	[ST3.4]	3	[CMVM3.3]	9
[T3.3]	9	[SR3.2]	10	[ST3.5]	3	[CMVM3.4]	13
[T3.4]	9	[SR3.3]	10				
[T3.5]	5						
[T3.6]	3						

How to begin?

- ✔ Prep your org
- ✔ Assess the current state of affairs
- Make a realistic plan and execute

Questions