



RSA CONFERENCE 2010

SECURITY DECODED

Mathematical Profile of a Winner—BSIMM Data Analyzed

Sammy Miguez
Cigital, Inc.

Elizabeth A. Nichols, Ph.D.
PlexLogic LLC

Session ID: SIP-108
Session Classification: Advanced

BSIMM Overview

Data Analyzed

Key Findings

Next Steps



BSIMM Overview

BSIMM Software Security Framework

The Software Security Framework (SSF)

Governance	Intelligence	SSDL Touchpoints	Deployment
Strategy and Metrics	Attack Models	Architecture Analysis	Penetration Testing
Compliance and Policy	Security Features and Design	Code Review	Software Environment
Training	Standards and Requirements	Security Testing	Configuration Management and Vulnerability Management

An “archaeology grid” of four domains and 12 practices used to capture and organize ongoing activity

Building Security In Maturity Model (bsi-mm.com)

- Take a science approach; get real data from real initiatives and build a model
 - Started with a Software Security Framework
 - Held in-person executive interviews with nine firms
 - Harmonized data onto the SSF and assigned maturity levels
 - Published model comprising 110 observed activities, each with:
 - An objective against which you can measure
 - A real-world example of how someone does it
- Model now validated with data from 30 firms
 - Available in English, German, Italian
 - English addendum for BSIMM EU data

Monkeys Eat Bananas



- BSIMM is not about good or bad ways to eat bananas or banana best practices
- BSIMM is about observations
- BSIMM is descriptive, not prescriptive

Sample BSIMM Practice and Activities

GOVERNANCE: TRAINING		
Objective	Activity	Level
[T1.1] promote culture of security throughout the organization	provide awareness training	1
[T1.2] ensure new hires enhance culture	include security resources in onboarding	
[T1.3] act as informal resource to leverage teachable moments	establish SSG office hours	
[T1.4] create social network tied into dev	identify satellite during training	
[T2.1] build capabilities beyond awareness	offer role-specific advanced curriculum (tools, technology stacks, bug parade)	2
[T2.2] see yourself in the problem	create/use material specific to company history	
[T2.3] keep staff up-to-date and address turnover	require annual refresher	
[T2.4] reduce impact on training targets and delivery staff	offer on-demand individual training	
[T2.5] educate/strengthen social network	hold satellite training/events	
[T3.1] align security culture with career path	reward progression through curriculum (certification or HR)	3
[T3.2] spread security culture to providers	provide training for vendors or outsource workers	
[T3.3] market security culture as differentiator	host external software security events	

- [T1.3] **Establish SSG office hours.** The SSG offers help to any and all comers during an advertised lab period or regularly scheduled office hours. By acting as an informal resource for people who want to solve security problems, the SSG leverages teachable moments and emphasizes the carrot over the stick. Office hours might be held one afternoon per week in the office of a senior SSG member.



Data Analyzed

- Organization data

- Software security group size
- Satellite size
- Development team size
- Software security group age
- Vertical market

- Observed activity data

- 110 1's and 0's

- The Verticals*

- Financial Services – 12
- ISVs – 7
- High Tech – 7
- Health, Insurance, Media, Energy, Telecomm – 9

*A few firms assigned to more than one vertical

Adobe, DTCC, EMC, Google, Microsoft, Nokia, QUALCOMM, Standard Life, SWIFT, Telecom Italia, Thomson Reuters, Wells Fargo



BSIMM Study Set - Basic Numbers

- Initiative age
 - Average: 4.5 years
 - Newest: 0
 - Oldest: 14
 - Median: 4
- SSG size
 - Average: 21.9
 - Smallest: 0
 - Largest: 100
 - Median: 13
- Satellite size
 - Average: 39.7
 - Smallest: 0
 - Largest: 300
 - Median: 11
- Dev size
 - Average: 5061
 - Smallest: 40
 - Largest: 30,000
 - Median: 3000

Average SSG size: 1% of dev group size

BSIMM Scorecard - Activity Observations

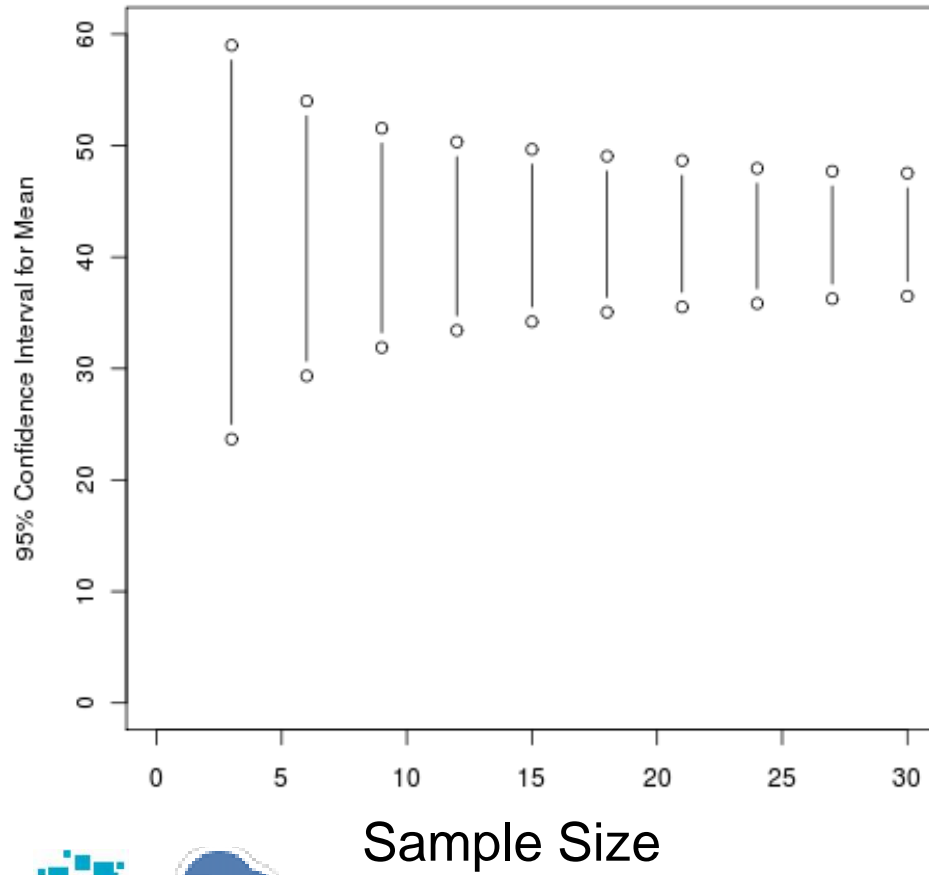
Governance		Intelligence		SSDL Touchpoint		Deployment	
Activity	Observed	Activity	Observed	Activity	Observed	Activity	Observed
[SM1.1]	18	[AM1.1]	11	[AA1.1]	22	[PT1.1]	28
[SM1.2]	18	[AM1.2]	20	[AA1.2]	18	[PT1.2]	17
[SM1.3]	16	[AM1.3]	14	[AA1.3]	19	[PT2.1]	17
[SM1.4]	24	[AM1.4]	10	[AA1.4]	15	[PT2.2]	10
[SM1.5]	13	[AM2.1]	7	[AA2.1]	9	[PT2.3]	11
[SM2.1]	12	[AM2.2]	9	[AA2.2]	6	[PT3.1]	9
[SM2.2]	13	[AM2.3]	13	[AA2.3]	11	[PT3.2]	5
[SM2.3]	16	[AM2.4]	9	[AA3.1]	5		
[SM2.4]	19	[AM3.1]	2	[AA3.2]	3		
[SM3.1]	7	[AM3.2]	2				
[SM3.2]	4						
[CP1.1]	24	[SFD1.1]	29	[CR1.1]	10	[SE1.1]	11
[CP1.2]	24	[SFD1.2]	15	[CR1.2]	19	[SE1.2]	30
[CP1.3]	26	[SFD2.1]	18	[CR1.3]	3	[SE2.1]	6
[CP2.1]	13	[SFD2.2]	11	[CR2.1]	20	[SE2.2]	16
[CP2.2]	18	[SFD2.3]	10	[CR2.2]	11	[SE2.3]	7
[CP2.3]	12	[SFD3.1]	5	[CR2.3]	8	[SE3.1]	13
[CP2.4]	9	[SFD3.2]	10	[CR2.4]	12		
[CP2.5]	17			[CR2.5]	11		
[CP3.1]	4			[CR3.1]	7		
[CP3.2]	7			[CR3.2]	1		
[CP3.3]	5			[CR3.3]	2		
[T1.1]	24	[SR1.1]	22	[ST1.1]	21	CMVM1.1	21
[T1.2]	6	[SR1.2]	13	[ST1.2]	9	CMVM1.2	22
[T1.3]	5	[SR1.3]	12	[ST2.1]	18	CMVM2.1	18
[T1.4]	11	[SR1.4]	11	[ST2.2]	16	CMVM2.2	11
[T2.1]	14	[SR2.1]	10	[ST2.3]	5	CMVM2.3	11
[T2.2]	13	[SR2.2]	8	[ST3.1]	7	CMVM3.1	2
[T2.3]	2	[SR2.3]	13	[ST3.2]	10	CMVM3.2	4
[T2.4]	14	[SR2.4]	13	[ST3.3]	3		
[T2.5]	7	[SR2.5]	11	[ST3.4]	4		
[T3.1]	4	[SR3.1]	10				
[T3.2]	3						
[T3.3]	4						

- SM1.4 – Identify gate locations, gather artifacts
- CP1.1 – Know regulatory pressures, unify approach
- CP1.2 – Identify PII obligations
- CP1.3 – Create policy
- T1.1 – Provide awareness training
- AM1.2 – Create data classification scheme/inventory
- SFD1.1 – Build/publish security features
- SR1.1 – Create security standards
- AA1.1 – Perform security feature review
- CR2.1 – Use automated tools with manual review
- ST1.1 – QA supports edge/boundary testing
- PT1.1 – Use external pen testers to find problems
- SE1.2 – Ensure host/network security basics
- CMVM1.1 – Create/interface with incident response
- CMVM1.2 – Identify software bugs found in Ops monitoring and feed back to Dev

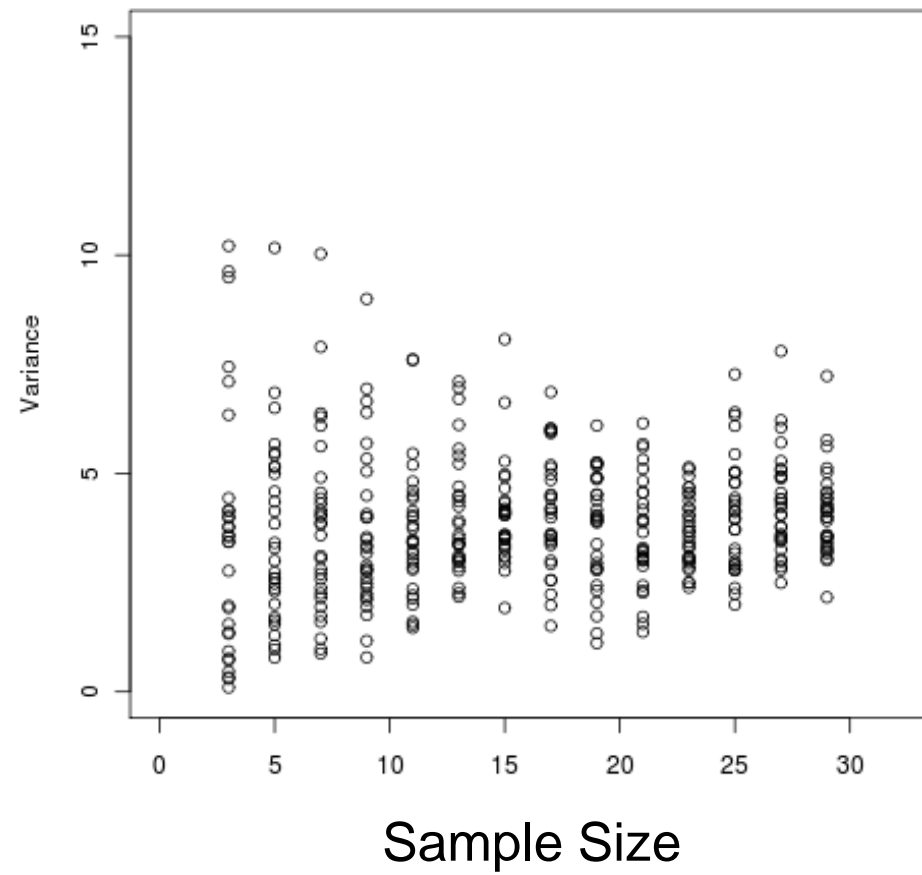
Key Findings

The Importance of Being “30”

Mean Estimation



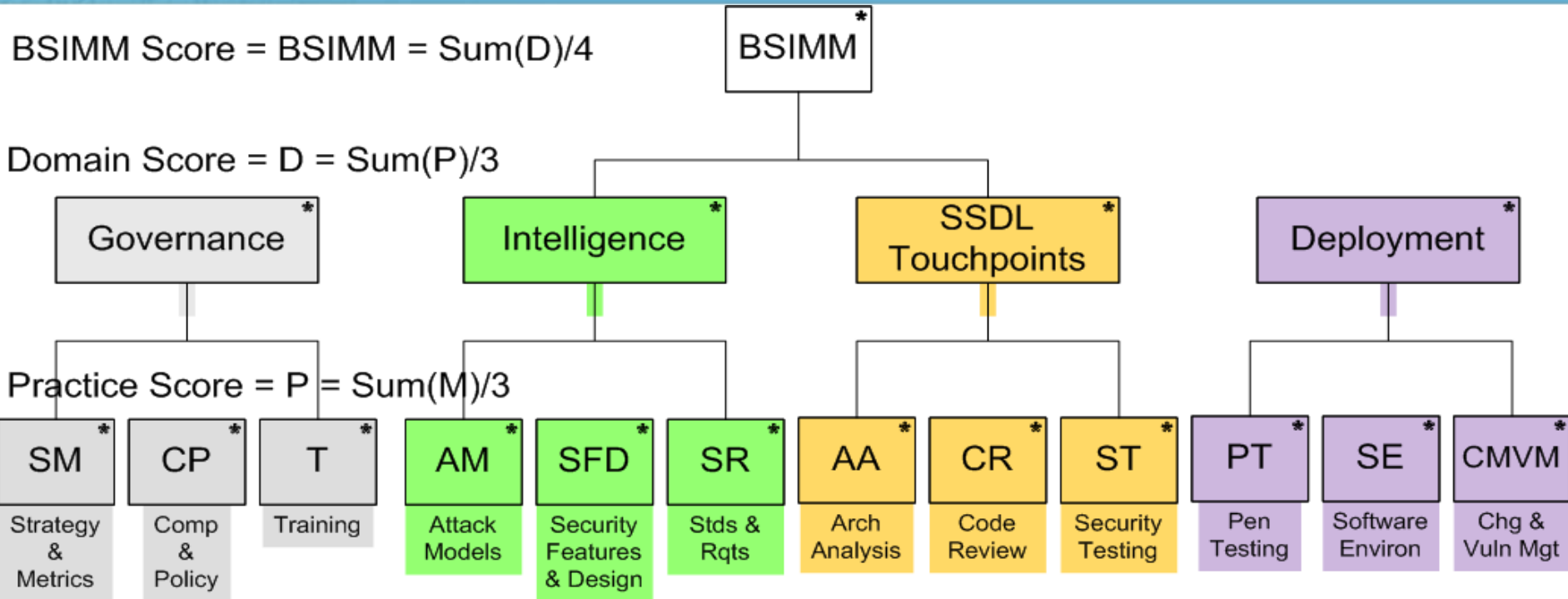
Variance Estimation



BSIMM Recursive Mean Score

$$\text{BSIMM Score} = \text{BSIMM} = \text{Sum}(D)/4$$

$$\text{Domain Score} = D = \text{Sum}(P)/3$$



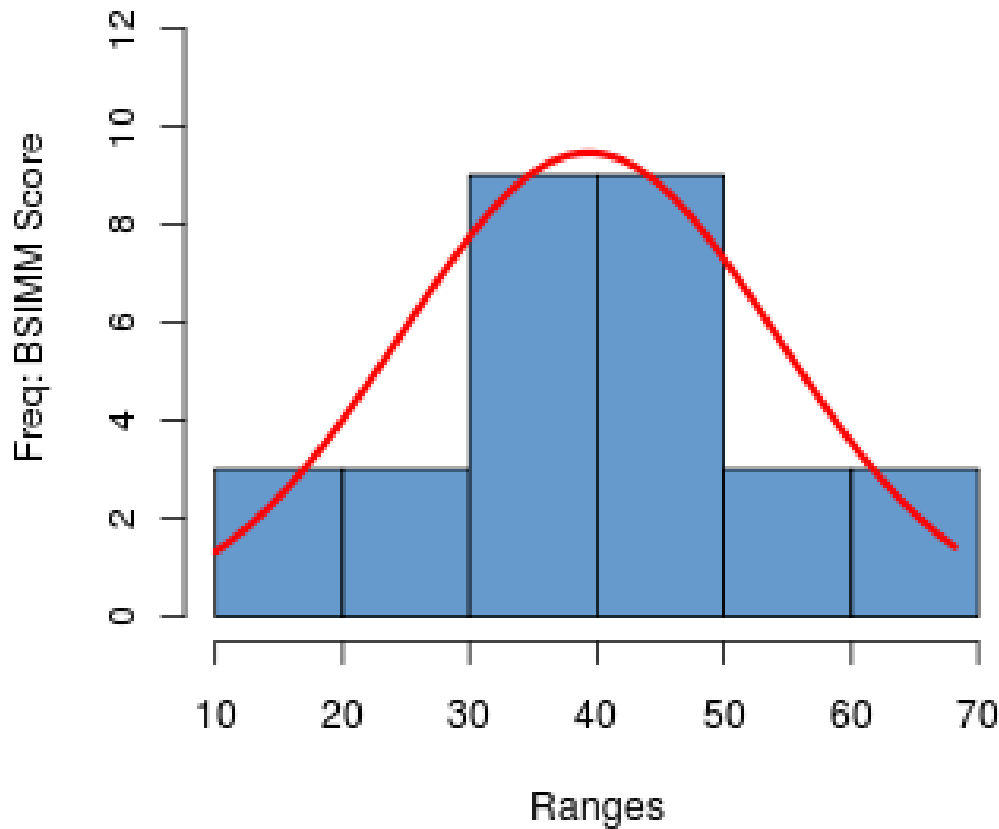
$$\text{Practice Score} = P = \text{Sum}(M)/3$$

Maturity Levels 1, 2 and 3: Maturity Score = $M = \text{Sum}(\text{ActivityValues})/\text{ActivityCount}$

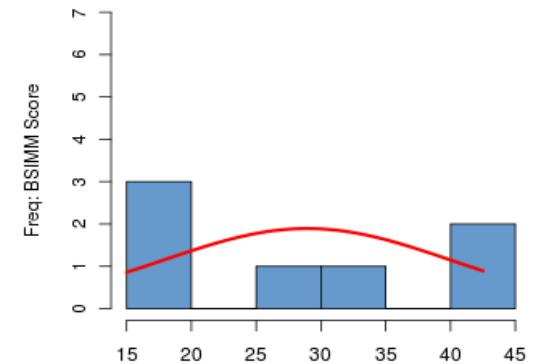
110 Activities: ActivityValue in { 0, 1 }

BSIMM Recursive Mean Score Distribution

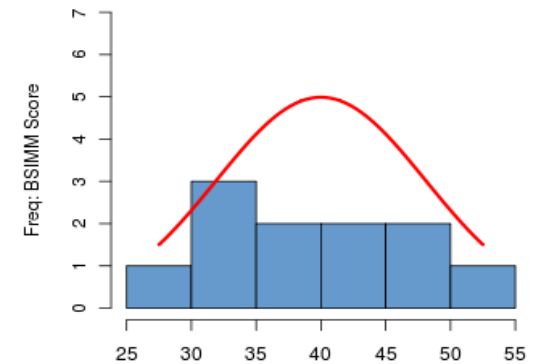
BSIMM Recursive Mean Score Distribution
Mon Feb 15 16:30:13 2010



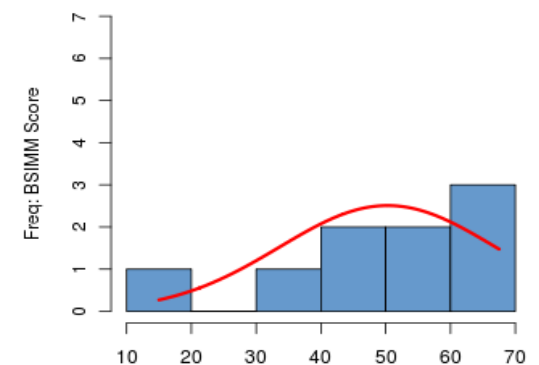
0 to 2
yrs old



2+ to 5
yrs old

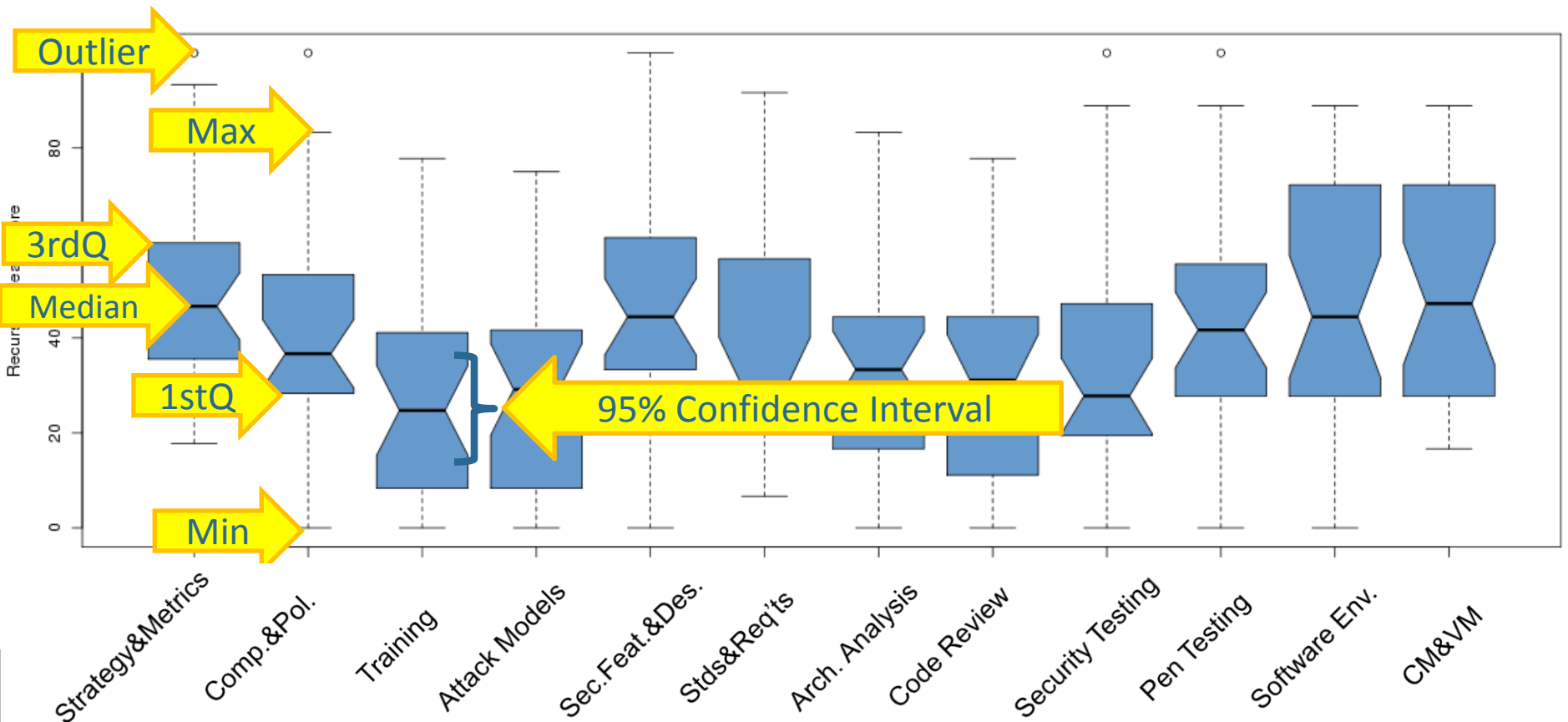


5+
yrs old



Software Security “Effort” Per Practice

BSIMM Recursive Mean Score: Practice Distribution



Governance

Intelligence

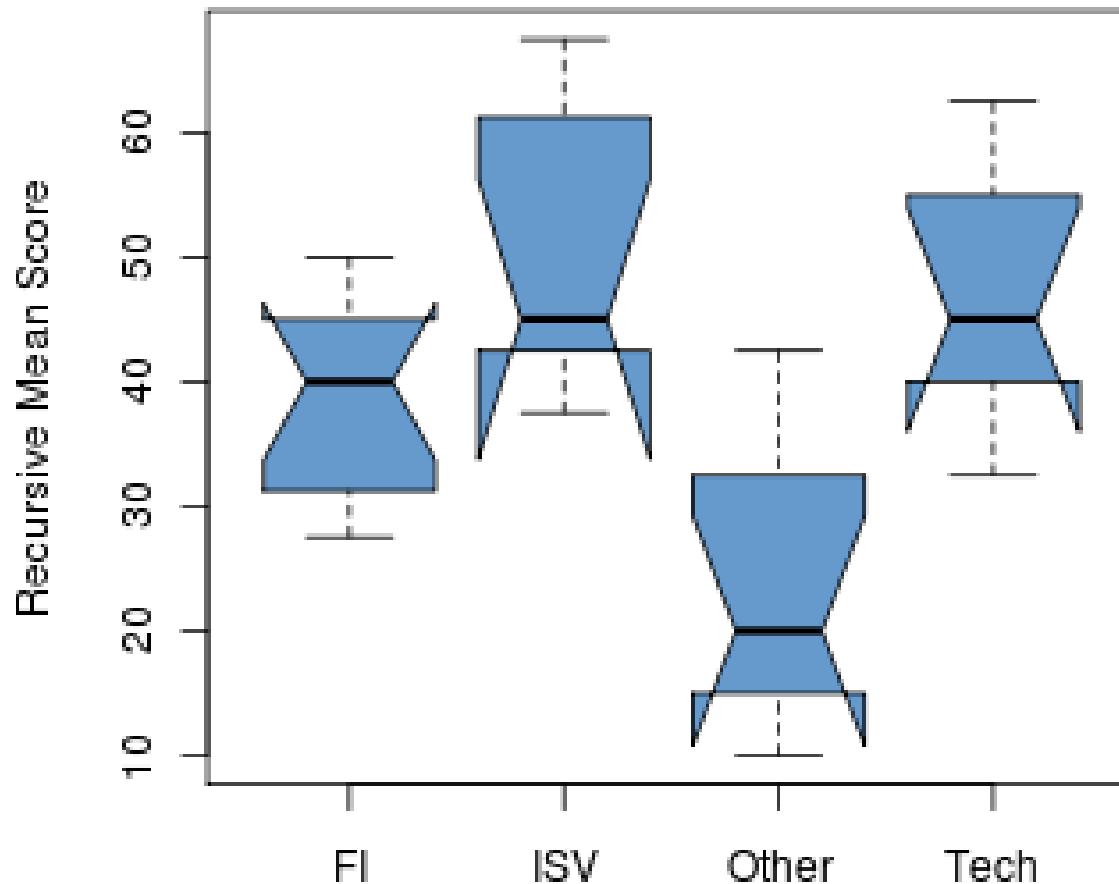
SSDL Touchpoints

Deployment

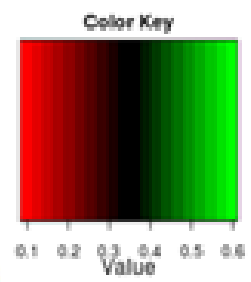
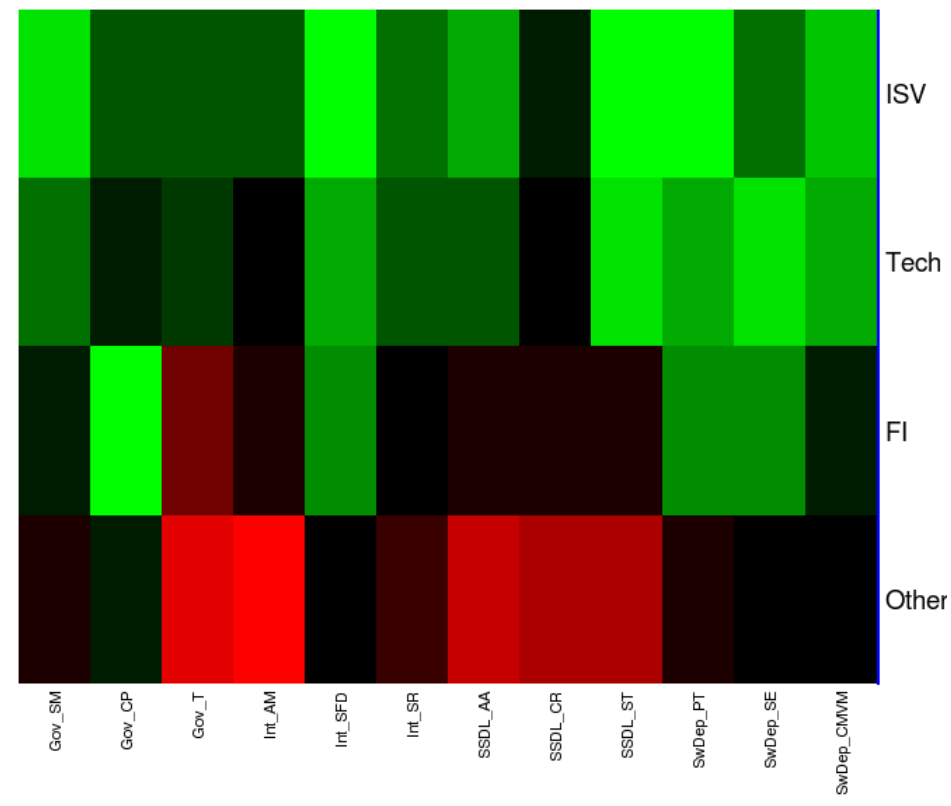
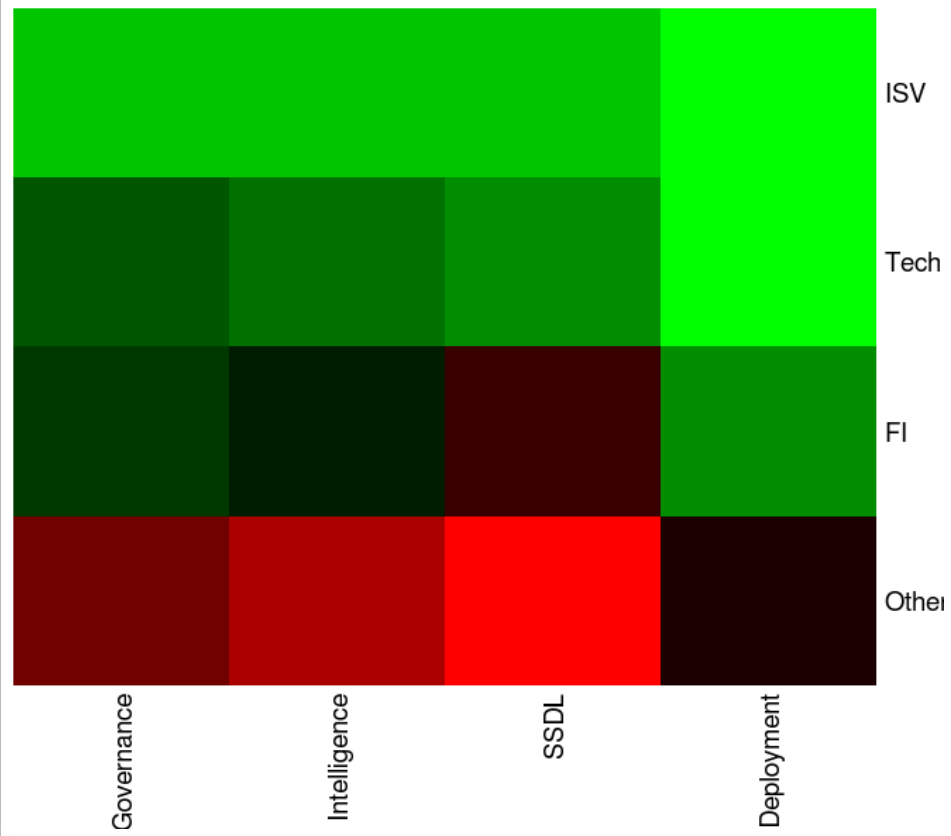


Software Security “Effort” Per Vertical

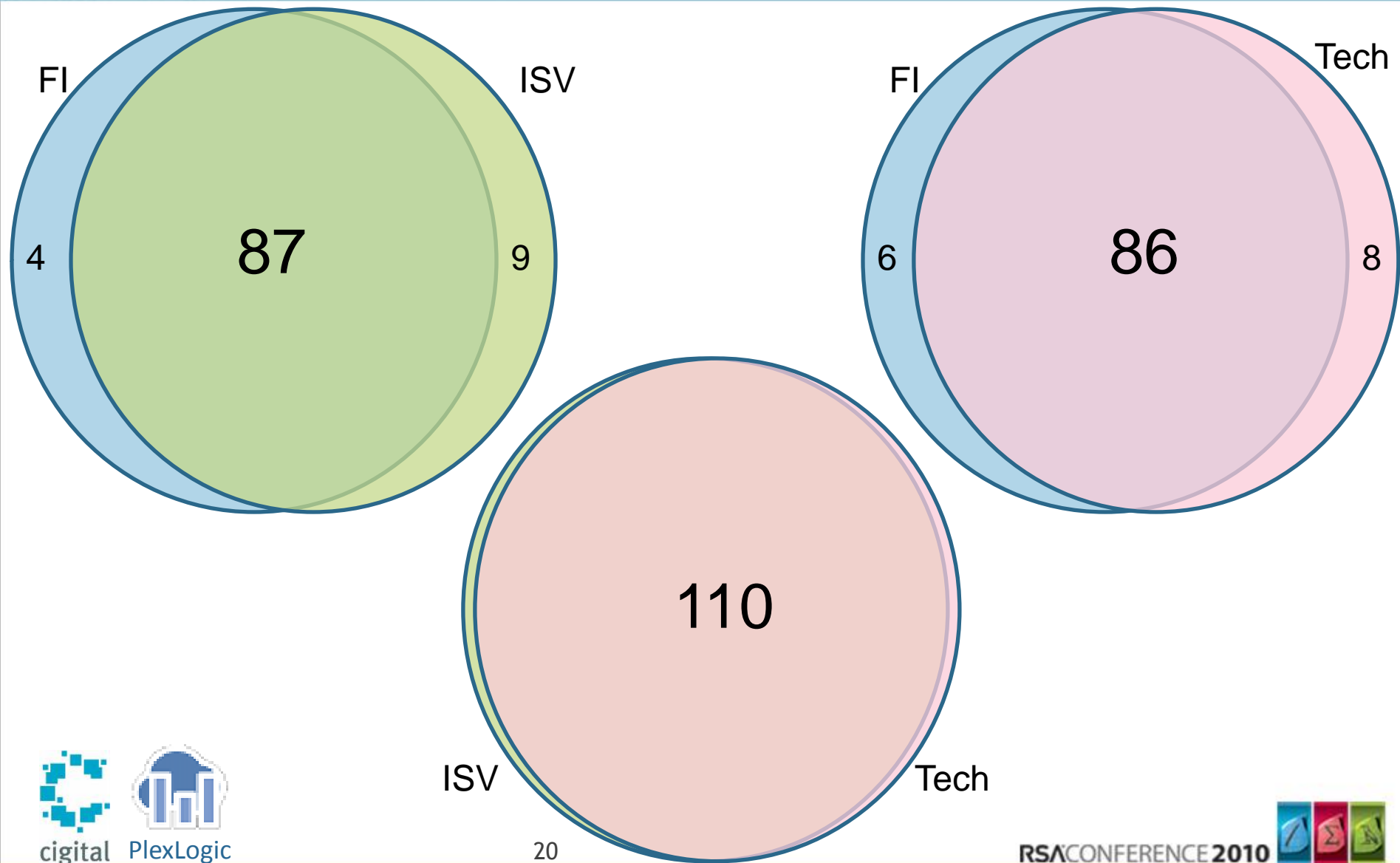
BSIMM RecMean Score: Segment Distribution
Mon Feb 15 16:38:28 2010



Are They Doing The Same Things?



There Are No Special Snowflakes



digital



PlexLogic

ISV

20

Tech

RSA CONFERENCE 2010

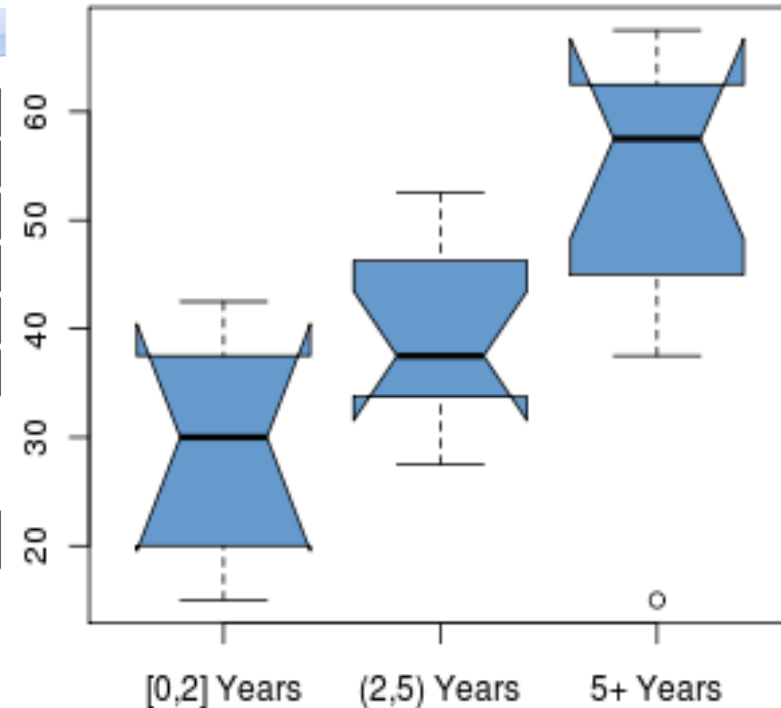
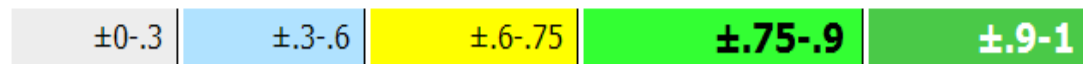


There is No Big Bang Here

Company Facts vs Score

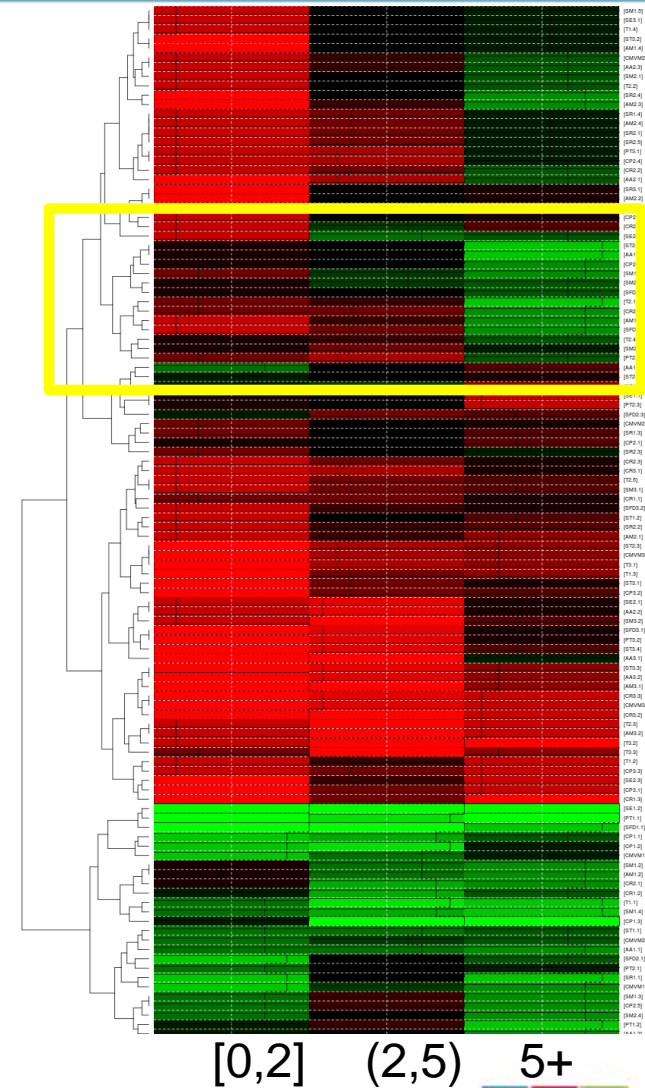
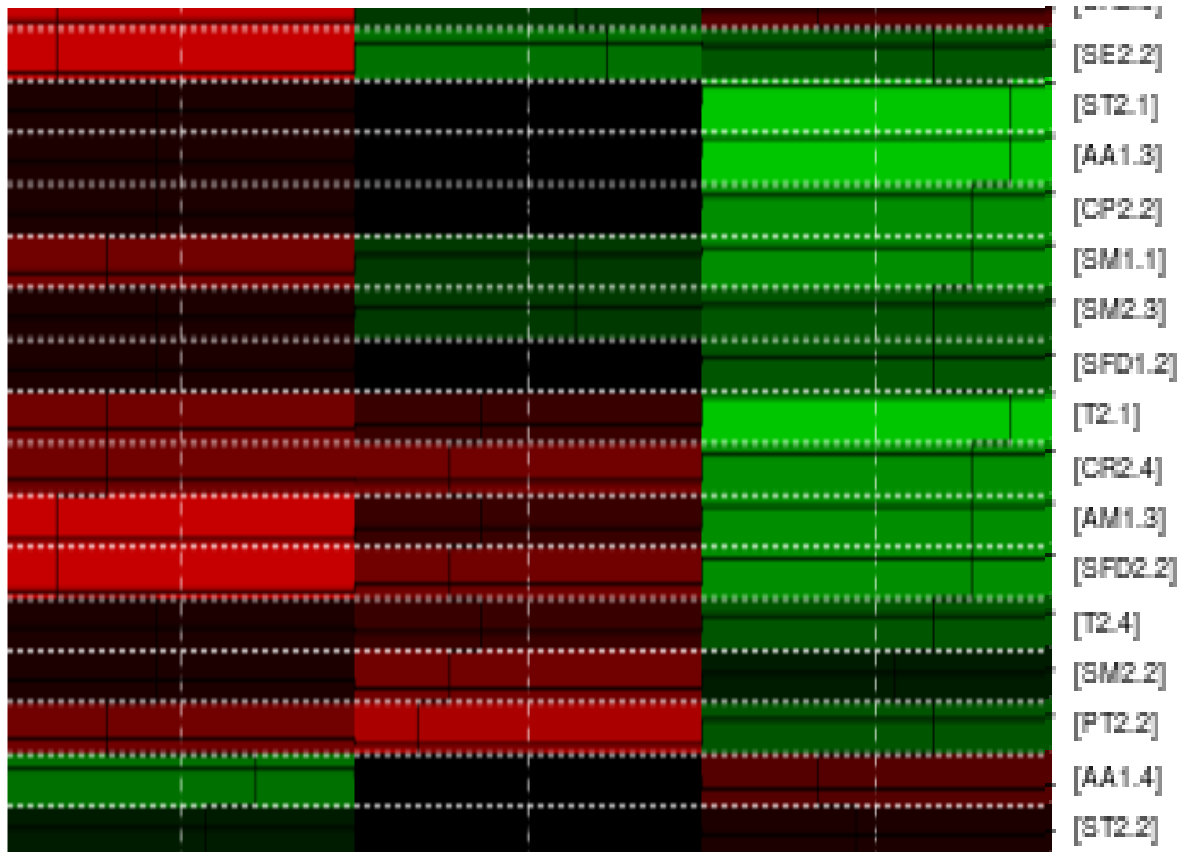
	BSIMM	SSG_Size	Sat_Size	Dev_Size	SSG_Age
BSIMM	1	0.41	0.36	0.6	0.62
SSG_Size	0.41	1	0.6	0.59	0.34
Sat_Size	0.36	0.6	1	0.4	0.15
Dev_Size	0.6	0.59	0.4	1	0.4
SSG_Age	0.62	0.34	0.15	0.4	1

Legend: Correlation Levels



- SSG Age is the factor most correlated with score
- Development team size follows closely

With Age Comes (Sometimes Weird) Activity

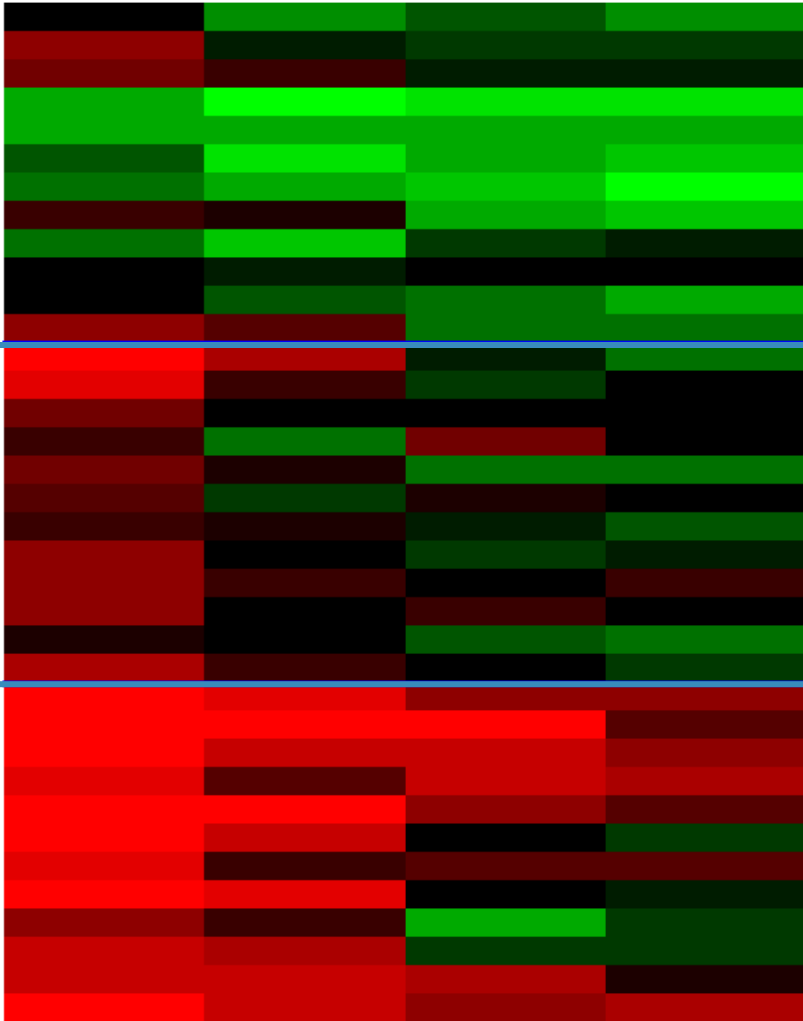


Self-Reflection

Maturity Level 1

Maturity Level 2

Maturity Level 3



Next Steps

The Big Take-Aways

- Use BSIMM to compare yourself with your peers
- BSIMM objectives immediately useful as governance tool
- Data indicate SSG and Satellite are anchor for activity
- No software security special snowflakes across verticals
- Big bang is very rare; activity directly correlated with age
- Be Yourself! No prescriptive pattern of activity adoption has emerged

- Continue to observe
 - Expanded data set enables more possibilities
 - Attempt correlation with selected “outcome” metrics – tying BSIMM scorecards to investments and other success measures
 - Model refinement over time
 - BSIMM Begin
 - Add data on bsi-mm.com

