SYNOPSYS®
Silicon to Software™

BSIMM

Building Security In Maturity Model

杨国梁

2017-10-17


主办方 Geekbang. InfoQ
ArchSummit
全球架构师峰会 2017
12月8-9日 北京 · 国际会议中心


AiCon
全球人工智能技术大会 2018
助力人工智能落地
2018.1.13 - 1.14 北京国际会议中心
AiCon
扫描关注大会官网

Agenda

BSIMM是什么？不是什么？

BSIMM发展史及使用方法

当前BSIMM评估的数据展示及分析

我应该如何利用BSIMM提升软件安全成熟度

Descriptive vs. Prescriptive Models

Descriptive vs. Prescriptive Models

Prescriptive Models

- Prescriptive models describe what you should do.
  - SAFECode
  - SAMM
  - SDL
  - Touchpoints
- Every firm has a methodology they follow (often a hybrid).
- You need an SSDL.

Descriptive Models

- Descriptive models describe what is actually happening.
- The BSIMM is a descriptive model that can be used to measure any number of prescriptive SSDLs.

BSIMM 发展史

SYNOPSYS®

2008: Building BSIMM

- BIG idea: Build a maturity model from actual data gathered from 9 well-known large-scale software security initiatives.
  - Create a software security framework.
  - Interview 9 firms in-person.
  - Discover 110 activities through observation (1 removed, 4 added later).
  - Organize the activities in 3 levels.
  - Build a scorecard.
- The model has been validated with data from 146 firms (109 in BSIMM8).
  - 321 distinct measurements over time
  - 36 over time (one firm 5 times)
- There is no special snowflake.

BSIMM: Software security measurement

- 146 firms measured (data freshness)
- BSIMM8 = data from 109 real initiatives
- McGraw, Migues, and West

109 firms in BSIMM8 community

BSIMM 使用方法

SYNOPSYS®

113 个 安全事件

3 个 等级

现场访谈

结果展示

Who ------ 跟谁谈？

SYNOPSYS®

高管

CTO

产品安全总监

安全开发生命周期工程经理

企业架构总监

CISO

CIO

网络安全副总裁

安全运营和情报副总裁

全球安全与合规总监

首席数据安全和隐私官

CSO

产品运营
执行总监

企业信息安全总监

应用安全高级副总裁

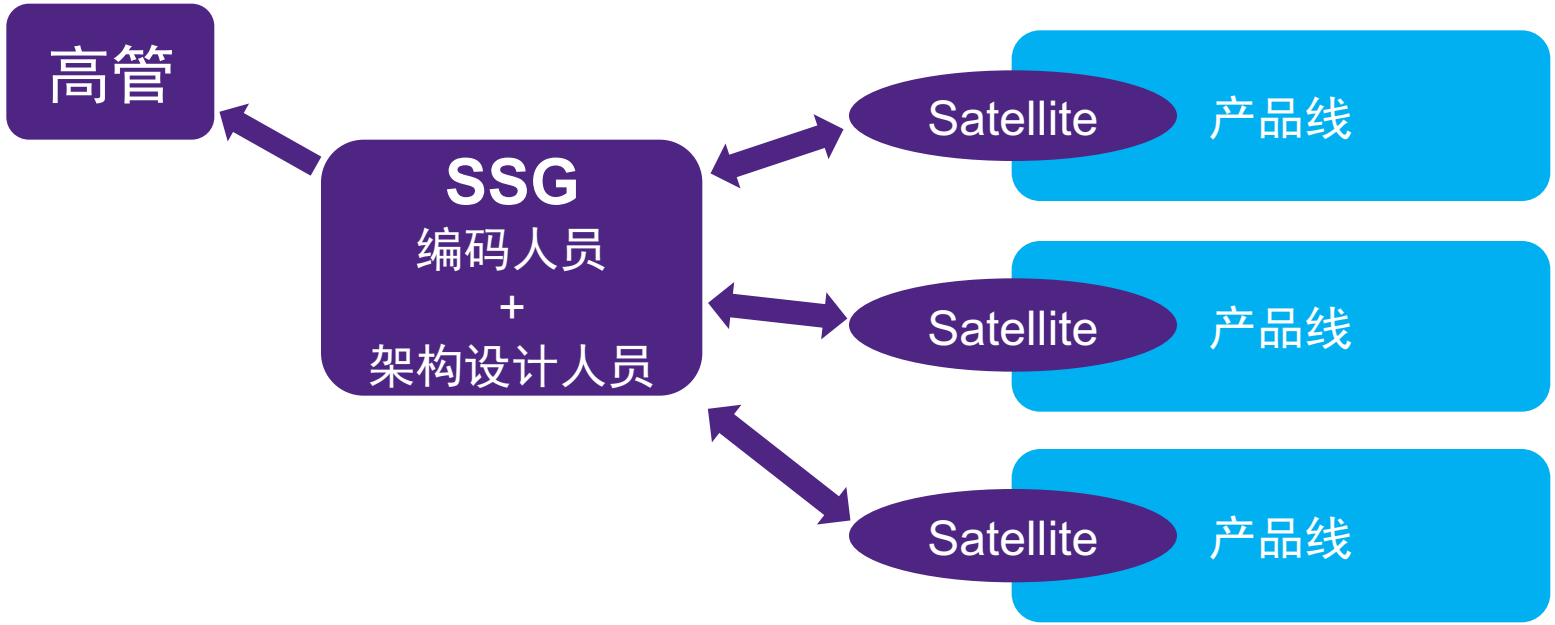
应用安全高级副总裁

应用安全全球负责人

标准、质量和安全副总裁

SYNOPSYS®

软件安全小组（SSG） + 辅助小组（Satellite） + 其他



Satellite

开发人员
测试人员
架构师

Gartner: Security Champion

Bug(50) vs Flaw(50)

SYNOPSYS®

What ------ 谈什么？

软件安全框架 SSF（Software Security Framework）

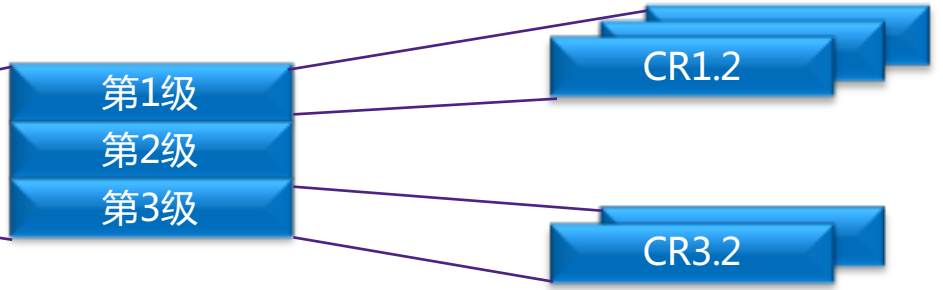
4 12 3 113

治理
1. 战略和指标(SM)
2. 合规和策略(CP)
3. 培训(T)

智能
4. 攻击模型(AM)
5. 安全功能和设计(SFD)
6. 标准和要求(SR)

SSDL触点
7. 架构分析(AA)
8. 代码审查(CR)
9. 安全测试(ST)

部署
10. 渗透测试(PT)
11. 软件环境(SE)
12. 配置管理和安全漏洞管理(CMVM)



SYNOPSYS®

BSIMM：活动示例

[CR2.6: 16] 使用支持自定义规则的自动化工具。

定制静态分析以提高效率并减少误报。使用自定义规则查找特定于企业编码标准或自定义中间件的错误。关闭不相关的检查。负责提供工具使指导的小组很可能也会牵头开展定制工作。定制的规则应通过积极的方式与技术堆栈的合理使用明确挂钩，以免出现公司码库中常见的消极错误。

BSIMM8 结果数据展示

Real-World Data (109 Firms)	
Initiative age	**Satellite size**
• Average: 3.9	• Average: 32.1
• Newest: 0.1	• Smallest: 0
• Oldest: 19	• Largest: 1,400
• Median: 2.5	• Median: 0
SSG size	**Development size**
• Average: 11.6	• Average: 2,666
• Smallest: 1	• Smallest: 20
• Largest: 130	• Largest: 35,000
• Median: 5.0	• Median: 800

BSIMM8 SCORECARD

GOVERNANCE		INTELLIGENCE		SSDL TOUCHPOINTS		DEPLOYMENT	
ACTIVITY	BSIMM8 FIRMS (109)	ACTIVITY	BSIMM8 FIRMS (109)	ACTIVITY	BSIMM8 FIRMS (109)	ACTIVITY	BSIMM8 FIRMS (109)
Strategy & Metrics		**Attack Models**		**Architecture Analysis**		**Penetration Testing**	
[SM1.1]	55	[AM1.2]	68	[AA1.1]	90	[PT1.1]	95
[SM1.2]	56	[AM1.3]	36	[AA1.2]	30	[PT1.2]	71
[SM1.3]	52	[AM1.5]	50	[AA1.3]	24	[PT1.3]	68
[SM1.4]	92	[AM2.1]	9	[AA1.4]	49	[PT2.2]	23
[SM2.1]	46	[AM2.2]	8	[AA2.1]	14	[PT2.3]	20
[SM2.2]	36	[AM2.5]	14	[AA2.2]	12	[PT3.1]	8
[SM2.3]	40	[AM2.6]	14	[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	[SFD1.1]	85	[CR1.2]	69	[SE1.1]	49
[CP1.2]	89	[SFD1.2]	70	[CR1.4]	65	[SE1.2]	91
[CP1.3]	56	[SFD2.1]	29	[CR1.5]	34	[SE2.2]	33
[CP2.1]	27	[SFD2.2]	41	[CR1.6]	37	[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			[CR3.2]	3		
[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	[SR1.1]	66	[ST1.1]	87	[CMVM1.1]	92
[T1.5]	31	[SR1.2]	69	[ST1.3]	79	[CMVM1.2]	96
[T1.6]	22	[SR1.3]	71	[ST2.1]	25	[CMVM2.1]	78
[T1.7]	44	[SR2.2]	33	[ST2.4]	11	[CMVM2.2]	83
[T2.5]	16	[SR2.3]	25	[ST2.5]	9	[CMVM2.3]	44
[T2.6]	18	[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	[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						

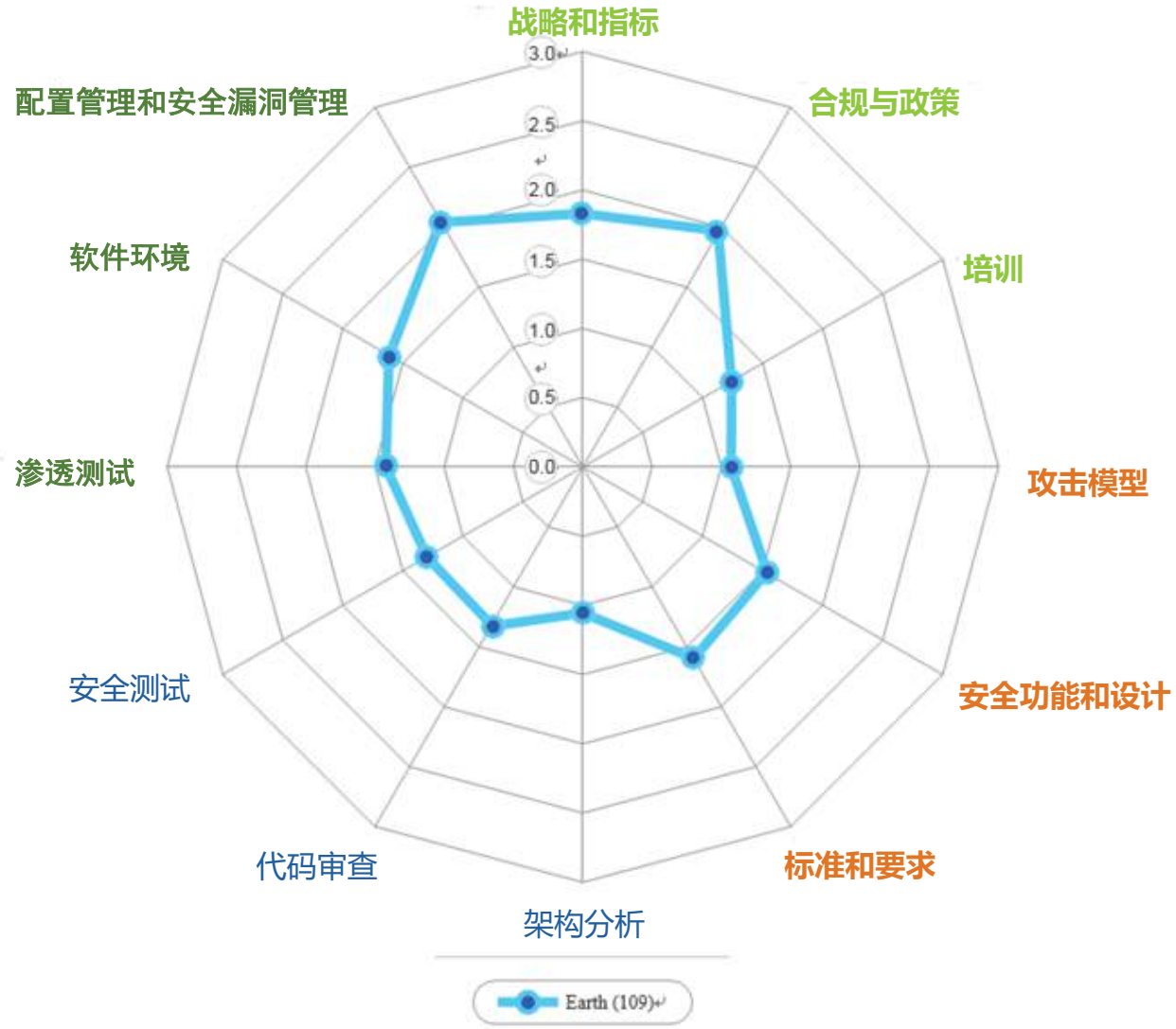
代码审查(CR)

活动描述	活动	开展这项活动的企业占比(%)
第1级		
责令SSG开展特别审查。	CR1.2	63%
自动和手动审查并行。	CR1.4	60%
所有的项目都必须强制执行代码审查。	CR1.5	31%
使用集中报告来构建知识环路并推动培训。	CR1.6	34%
第2级		
安排导师教授工具使用方法。	CR2.5	24%
使用支持自定义规则的自动化工具。	CR2.6	15%
使用top N bugs列表（最好是真实数据）。	CR2.7	21%
第3级		
构建工厂模式。	CR3.2	3%
培养从整个代码库中消除特定bug的能力。	CR3.3	2%
自动执行恶意代码检测任务。	CR3.4	3%
执行编码标准。	CR3.5	5%

SYNOPSYS®

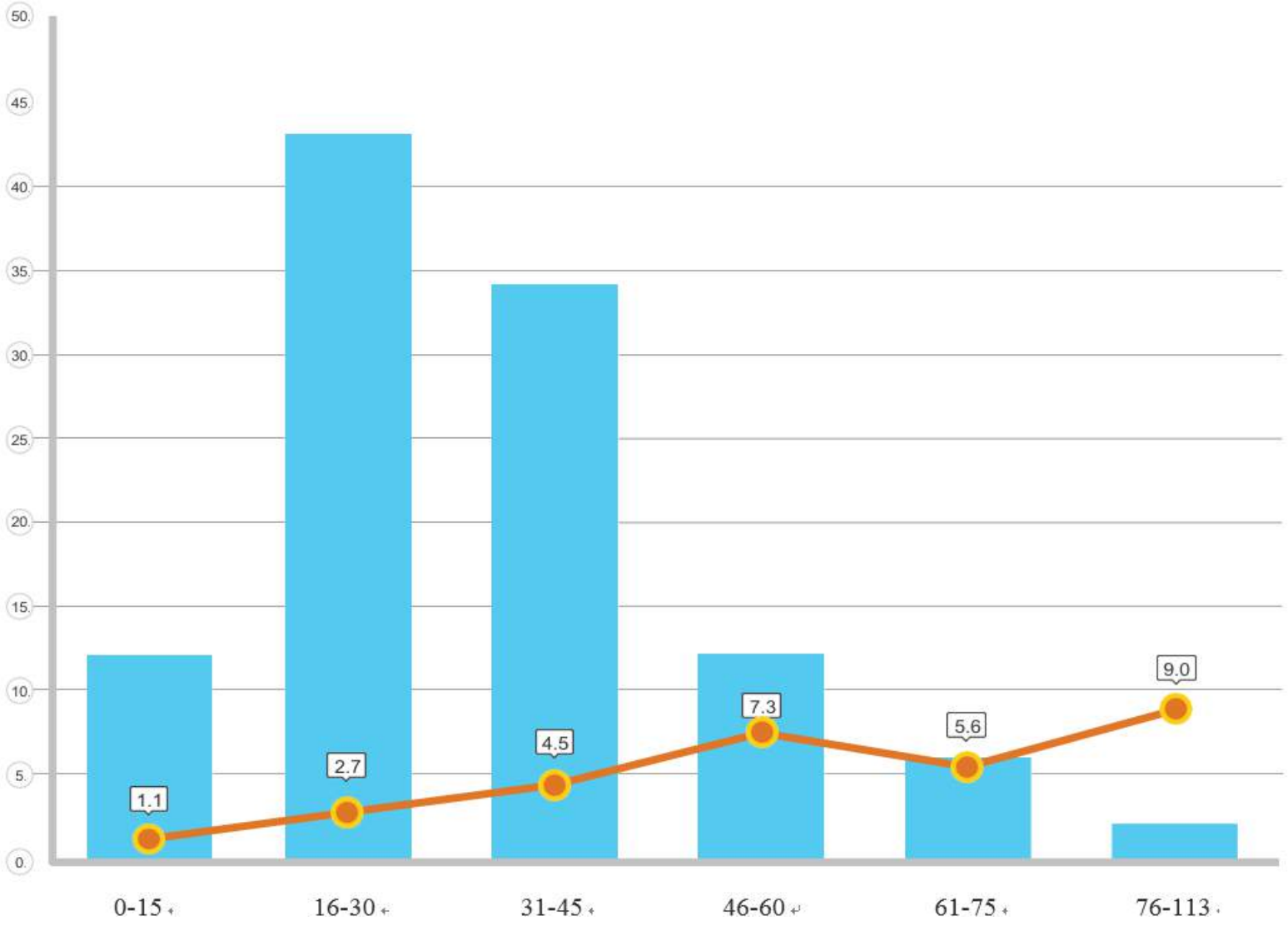
109家企业平均得分蛛网图

[5:84]



SYNOPSYS®

BSIMM企业得分情况柱状分布



SYNOPSYS®

	BSIMM8	BSIMM7	BSIMM6	BSIMM-V	BSIMM4	BSIMM3	BSIMM2	BSIMM1
公司数量	109	95	78	67	51	42	30	9
评估次数	256	237	202	161	95	81	49	9
第2轮评估	36	30	26	21	13	11	0	0
第3轮评估	16	15	10	4	1	0	0	0
SSG团队成员数量	1,268	1,111	1,084	976	978	786	635	370
辅助小组成员数量	3,501	3,595	2,111	1,954	2,039	1,750	1,150	710
开发人员数量	290,582	272,782	287,006	272,358	218,286	185,316	141,175	67,950
应用数量	94,802	87,244	69,750	69,039	58,739	41,157	28,243	3,970
企业SSG建立平均时长（年）	3.88	3.94	3.98	4.28	4.13	4.32	4.49	5.32
SSG平均占比	1.60 / 100	1.61 / 100	1.51 / 100	1.4 / 100	1.95 / 100	1.99 / 100	1.02 / 100	1.13 / 100
金融服务	47	42	33	26	19	17	12	4
ISVs	38	30	27	25	19	15	7	4
技术	16	14	17	14	13	10	7	2
医疗卫生	17	15	10					
物联网	12	12	13					
云	16	15						
保险	11	10						

BSIMM平均结果的演进趋势

- 36 家公司做了两次BSIMM评估（平均相隔26个月）

- 我们所观测到的进展：
  - 安全事件得分平均进展33.4%

SYNOPSYS®

垂直行业对比结果

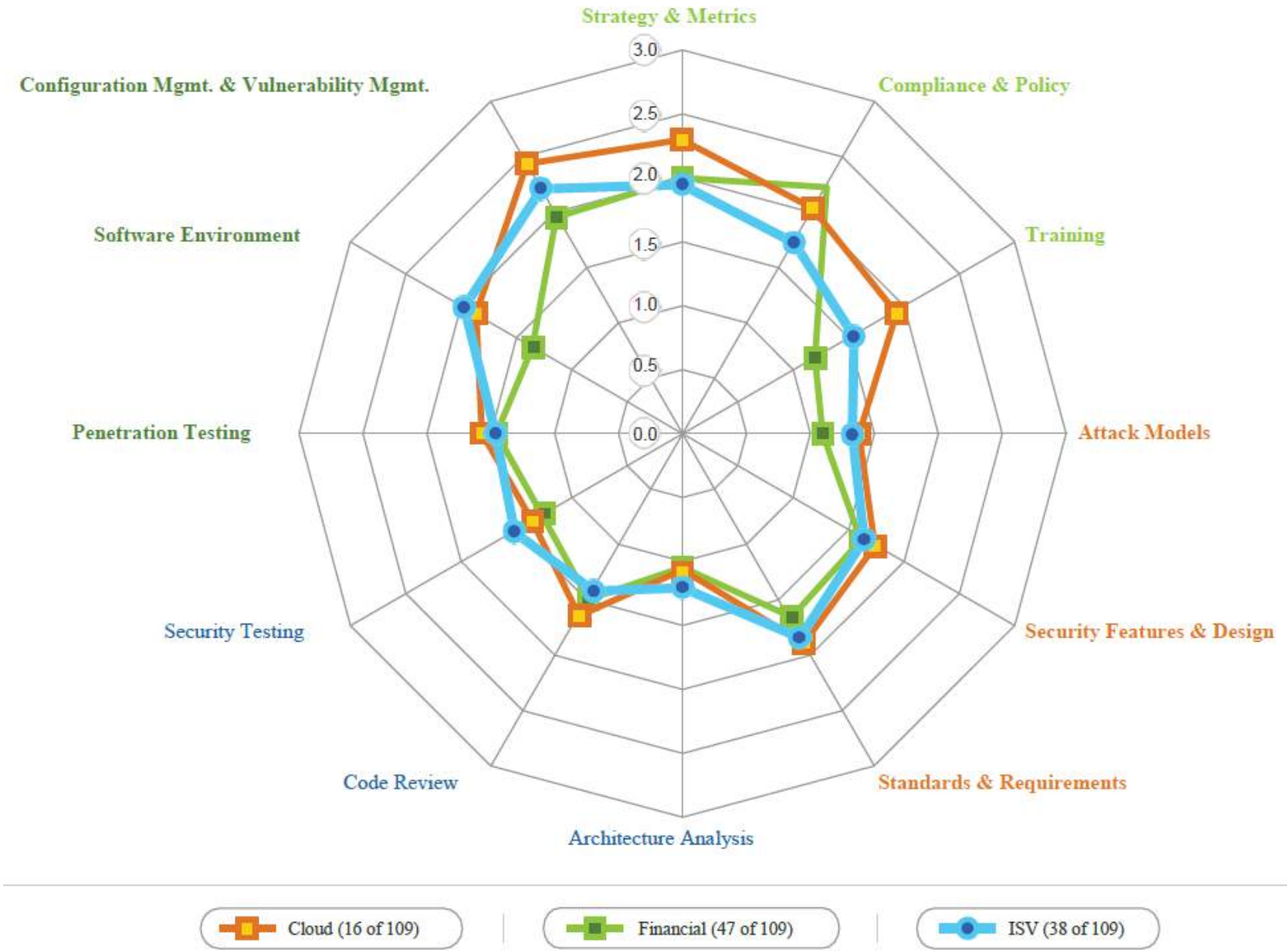
云

vs

金融

vs

软件商



SYNOPSYS®

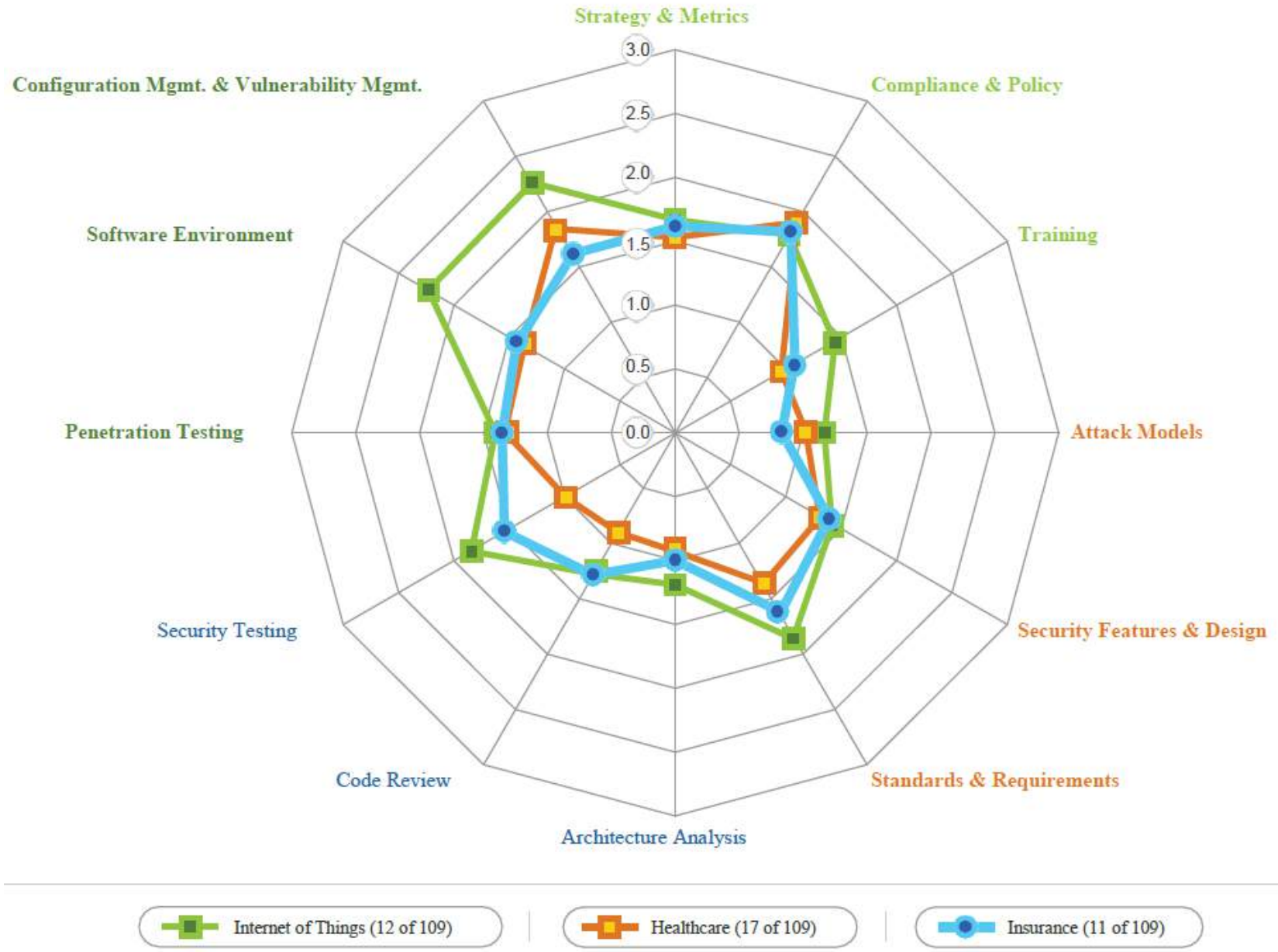
物联网

vs

医疗卫生

vs

保险

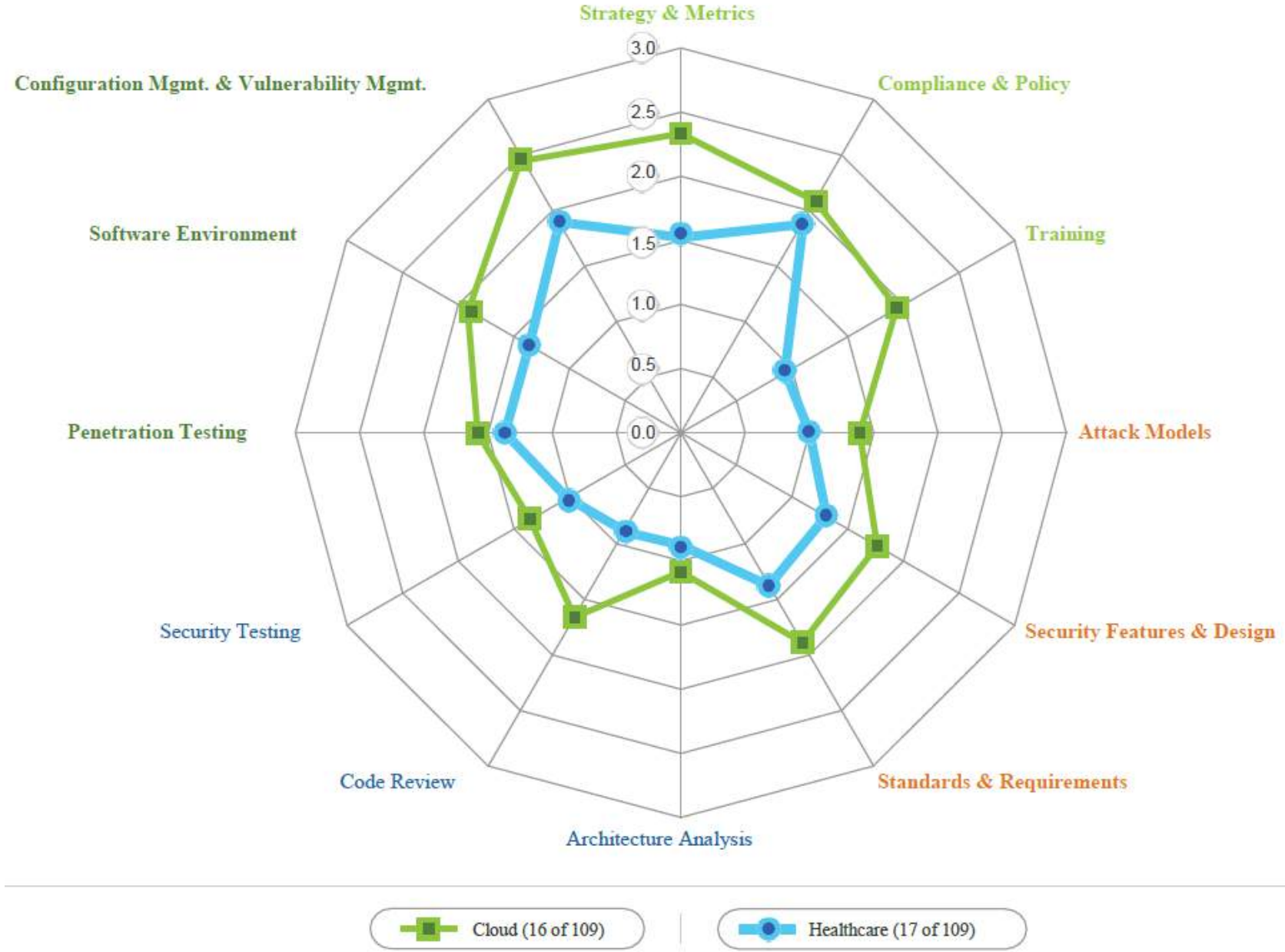


SYNOPSYS®

云

vs

医疗卫生



SYNOPSYS®

12项最常见的安全事件

活动	描述
[SM1.4]	确定门控的位置，收集必要的工件。
[CP1.2]	确定PII义务。
[T1.1]	提供意识培训。
[AM1.2]	制定数据分类方案并制作数据清单。
[SFD1.1]	构建并发布安全功能。
[SR1.3]	将合规约束转变成要求。
[AA1.1]	开展安全功能审查。
[CR1.2]	责令SSG开展特别审查。
[ST1.1]	确保QA支持边缘/边界值条件测试。
[PT1.1]	聘请外部渗透测试人员，以发现问题。
[SE1.2]	确保主机和网络安全基础知识到位。
[CMVM1.2]	在操作监控期间发现软件缺陷并将其反馈给开发人员。

如何用BSIMM8来自我评估？

用于虚构公司的BSIMM8记分卡| 观察到的活动数量：37

治理			智能			SSDL接触点			部署		
ACTIVITY 活动	BSIMM8 FIRMS (109) BSIMM8 公司(109)	FAKEFIRM 虚构公司	ACTIVITY 活动	BSIMM8 FIRMS (109) BSIMM8 公司(109)	FAKEFIRM 虚构公司	ACTIVITY 活动	BSIMM8 FIRMS (109) BSIMM8 公司(109)	FAKEFIRM 虚构公司	ACTIVITY 活动	BSIMM8 FIRMS (109) BSIMM8 公司(109)	FAKEFIRM 虚构公司
战略和指标			攻击模型			架构分析			渗透测试		
[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										
合规与政策			安全功能和设计			代码审查			软件环境		
[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				
培训			标准和要求			安全测试			配置管理和安全漏洞管理		
[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										

SYNOPSYS®

将BSIMM8用作衡量标尺

平均水平

vs

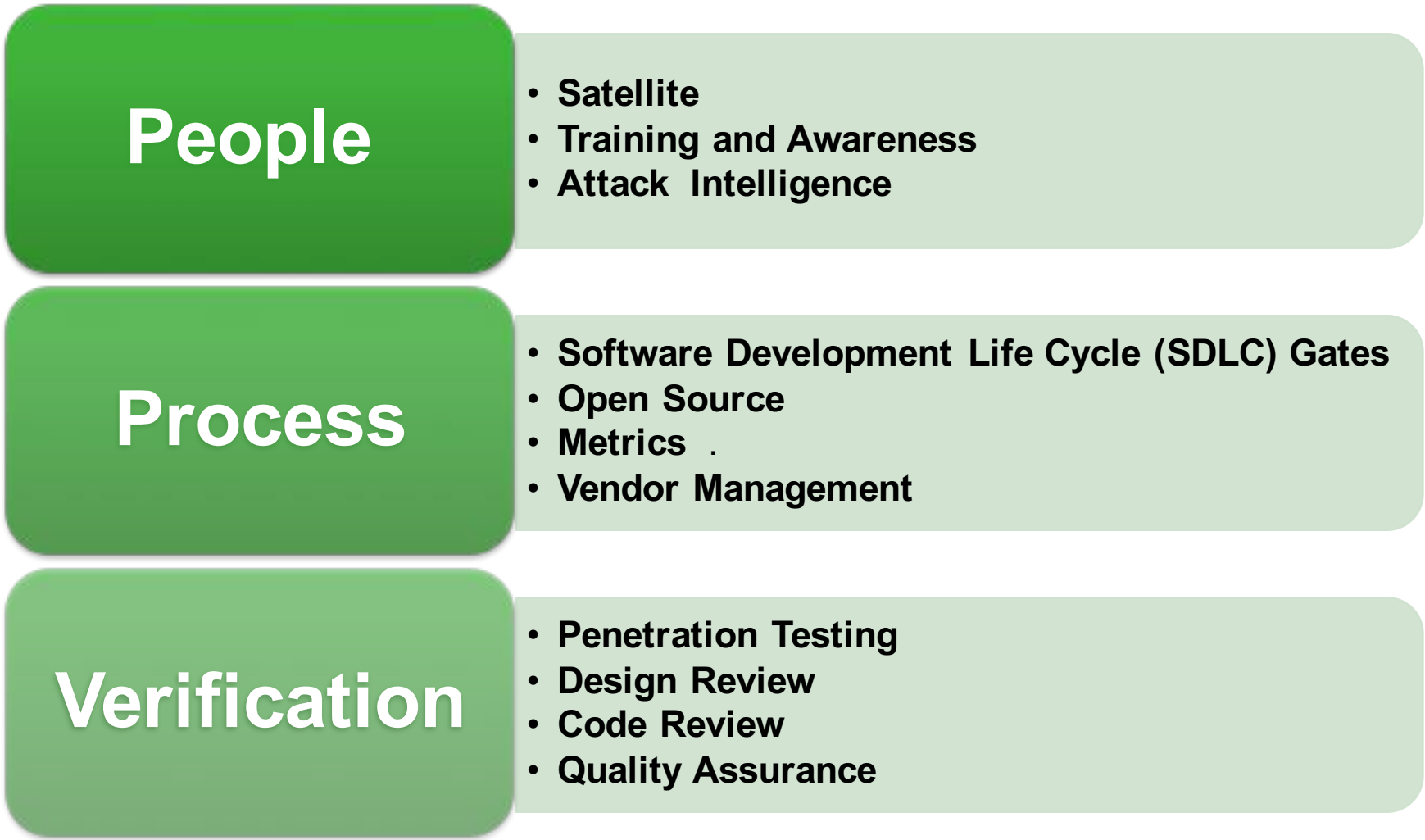
你

我知道差在哪了，下一步怎么办？

The Maturity Action Plan roadmap

SYNOPSYS®

Capability areas considered in a MAP



Sample Deliverables – Implementation Roadmap

Implementation Plan Description

DEVELOPER ENABLEMENT – Security Training

Develop and implement application security curriculum

Timeline

	Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8
Internal	Define	Pilot			Operationalize			
External								

Key Activities

Develop training curriculum

- Inventory development languages and frameworks in use across development teams. Focusing on the most common development languages and frameworks. Identify areas within application security and/or compliance that needs immediate attention.
- Determine the number of developers, architects, QA, business owners and third-party contractors who will be part of curriculum. Update the application security policy to include the training requirement for all SSDLC participants.

Implement training curriculum

- Identify internal resources to build the curriculum. Alternatively, evaluate externally available courses that are current and updated regularly
- Structure the curriculum to build knowledge sequentially. Use a mix of instructor-led, computer-based delivery methods to deliver courses for maximum impact.

Enforcement

- SSG works with HR to enforce security training as part of the new-hire on-boarding for SDLC participants. Encourage attendance to ongoing training by incentivizing employees during performance reviews.
- Build and enhance security champions group using training data.

Key Considerations

- HR: CISO-governance and SSG resources to work together to develop a role-based training program focused on application security
- Technical: Learning management system to deliver and report student attendance, progress etc.
- Business: Incentivize on-going training for employees
- Operations: New-hire employee and contractor training. Identify security champions

Dimensions

Key Dependencies

- Learning management system
- Role-based curriculum
- Common development languages, frameworks and compliance requirements

Drivers

- Governance
- SDLC Touchpoints
- Developer Enablement

Implementation Risks

- Lack of regular updates to the training material will render it obsolete and will result in an ineffective training program.
- Lack of attendance or enforcement will result in poor implementation of the program

Expected Improvement

Initial Cost Driver Analysis

Cost Category	Internal	External	Ongoing	Assumptions
Resources				▪ A third-party developed role-based curriculum focused on application security would be faster and efficient to implement than using internal resources to do the same.
Expenditure		 $100K – $300K	 $100K – $300K	▪ External cost assumes building a role-based CBT curriculum delivered on an annual basis to 500 developers along with some ILT courses delivered to targeted audience

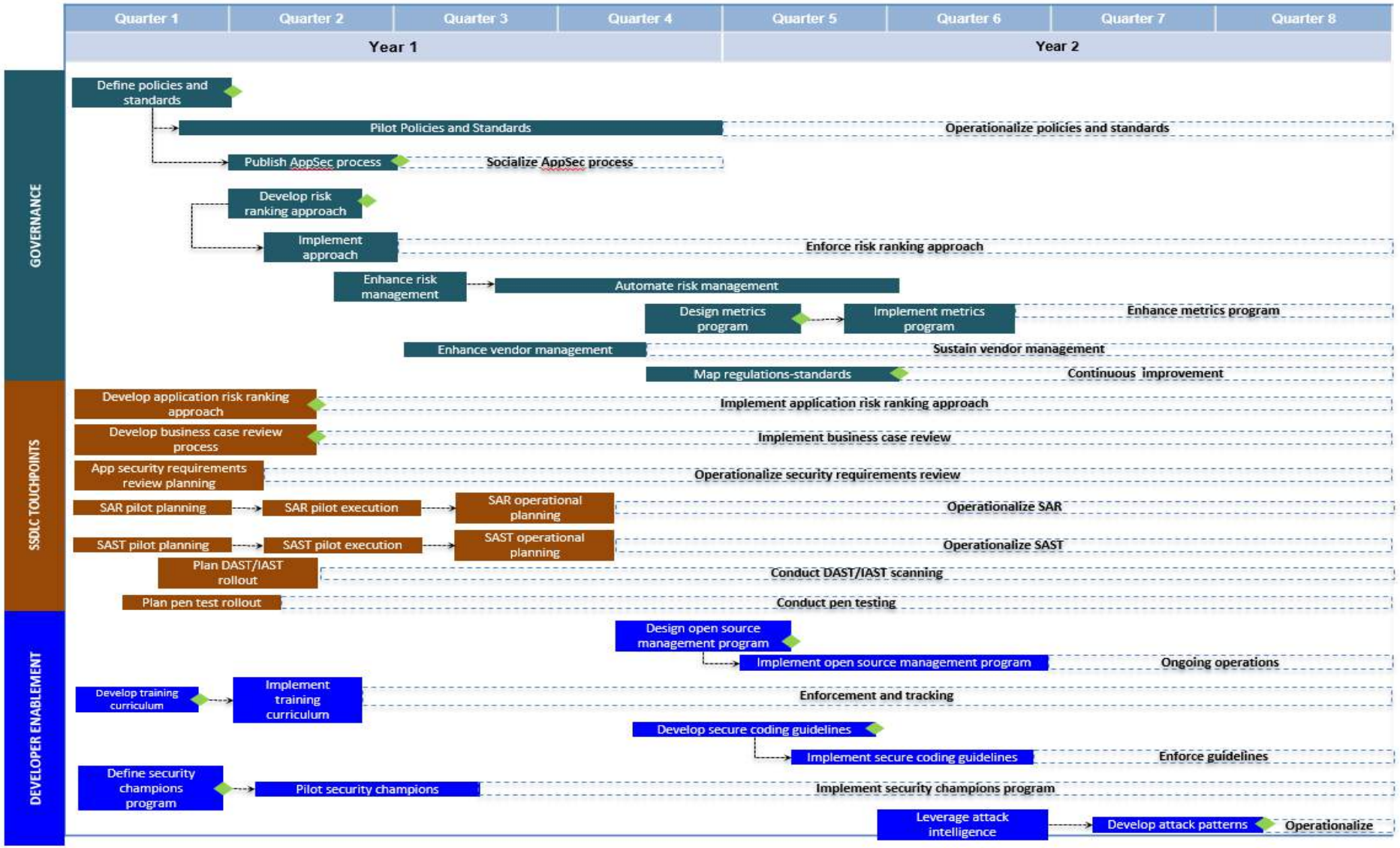
Key Stakeholders

- SSG to help develop the role-based training curriculum focused on application security
- CISO-governance to implement and enforce the training program
- Developers, EA, QA to complete their assigned courses

Activity milestone using internal resources
Activity milestone using external providers
Activity Progress
Ongoing Refinement
Full-time resource

SYNOPSYS®

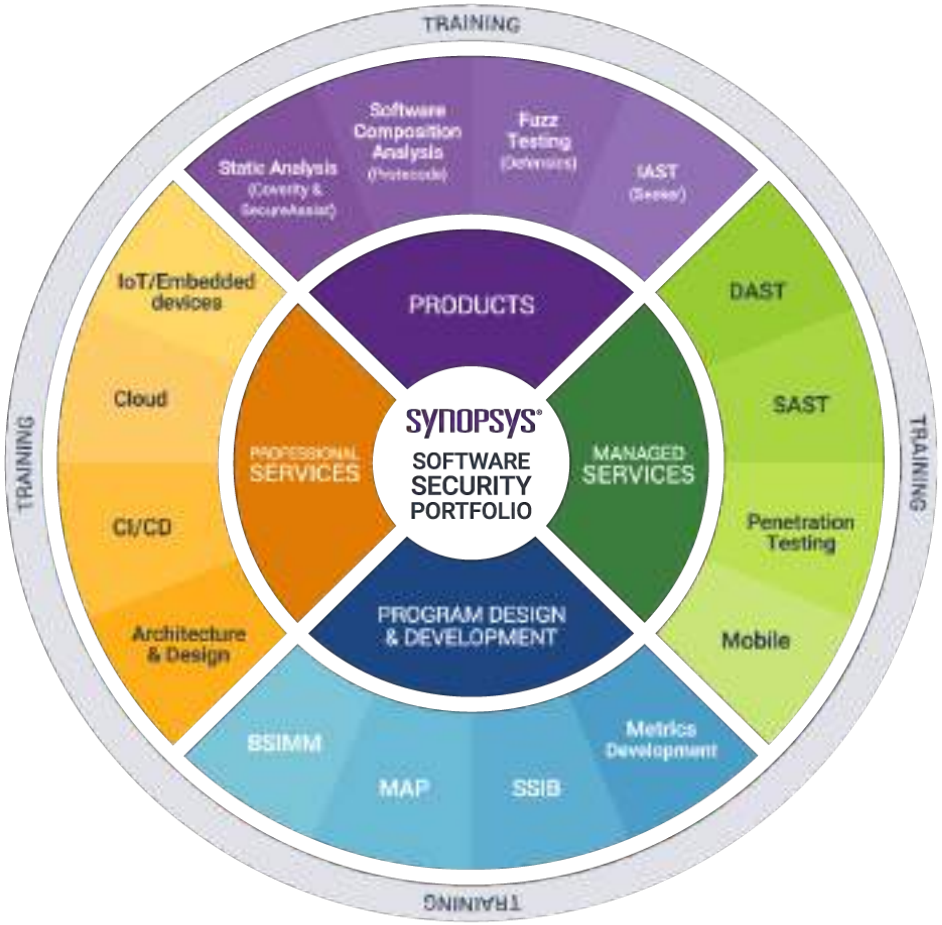
Sample Deliverables – 2 Year Roadmap



SYNOPSYS®

Synopsys Software Integrity Portfolio

Gartner应用安全测试魔力象限



BSIMM8

Thank You!

SYNOPSYS®