QCon 全球软件开发大会
INTERNATIONAL SOFTWARE DEVELOPMENT CONFERENCE

BEIJING 2017

Building Security In Maturity Model (BSIMM)-构筑坚若磐石的安全软件

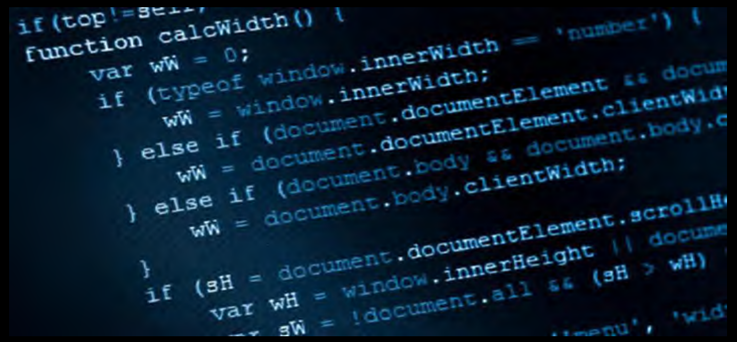
韩葆

主办方 Geekbang. 极客邦科技 InfoQ

Agenda

- 软件安全的现状
- 什么是BSIMM?
- 如何构建BSIMM?
- 典型实例

软件安全的趋势



漏洞深深隐藏

- 即使采用先进的工具和方法也很难发现
- 代码或配置很小的改动会产生新的安全漏洞

远程攻击

- 网络访问可从世界任何地点随意发起攻击
- 很难跟踪
- 无法指控

自动攻击

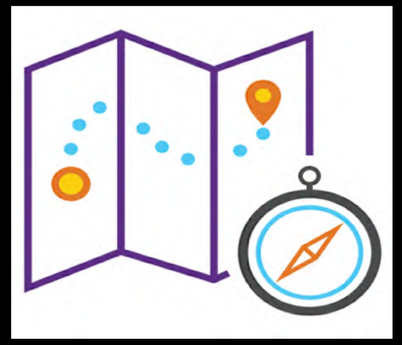
- 广泛共享软件中的一个漏洞可在同一时间随处被用来自动进行攻击
- 示例 – 城市中所有交通信号灯同时失效

任何时间 – 永久风险

任何人 – 独狼或国家

大范围 – 大规模攻击

不断演变的软件安全环境



不断演变发展的环境
需要新方法

新的技术堆栈
和攻击面

嵌入式设备

云服务（私有云、
混合云、公有云）

语言和框架

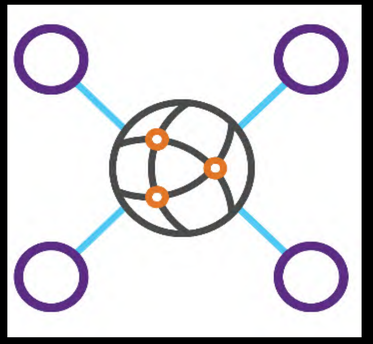
新的开发理念
和方法

敏捷

开发运维

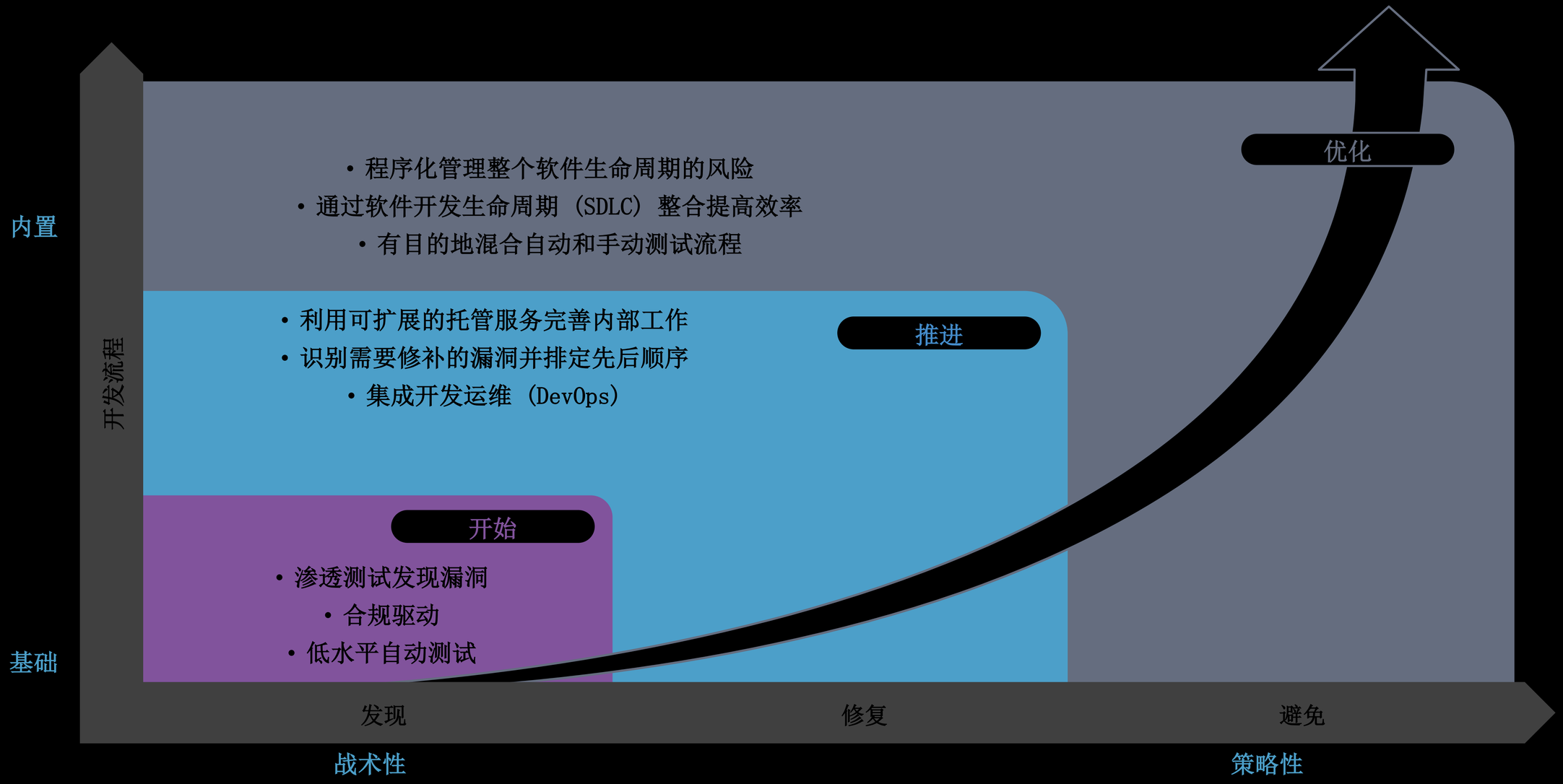
CI/CD

开源



不断变化的部署环境
改变了测试需求

软件安全计划是一种演进过程



最佳资源和适用资源

计划设计与开发-BSIMM

- 在成熟的模型中构建安全

工具

- 静态代码分析-Coverity
- 软件组成分析-ProteCode
- 智能模糊测试-Defensics
- 交互式应用安全测试（IAST）
- 远程教学与培训

- 成熟行动计划
- 指标开发

托管

- Web应用测试
- 手机应用测试
- 网络渗透测试
- 源代码检查

- 整体软件安全计划

订制

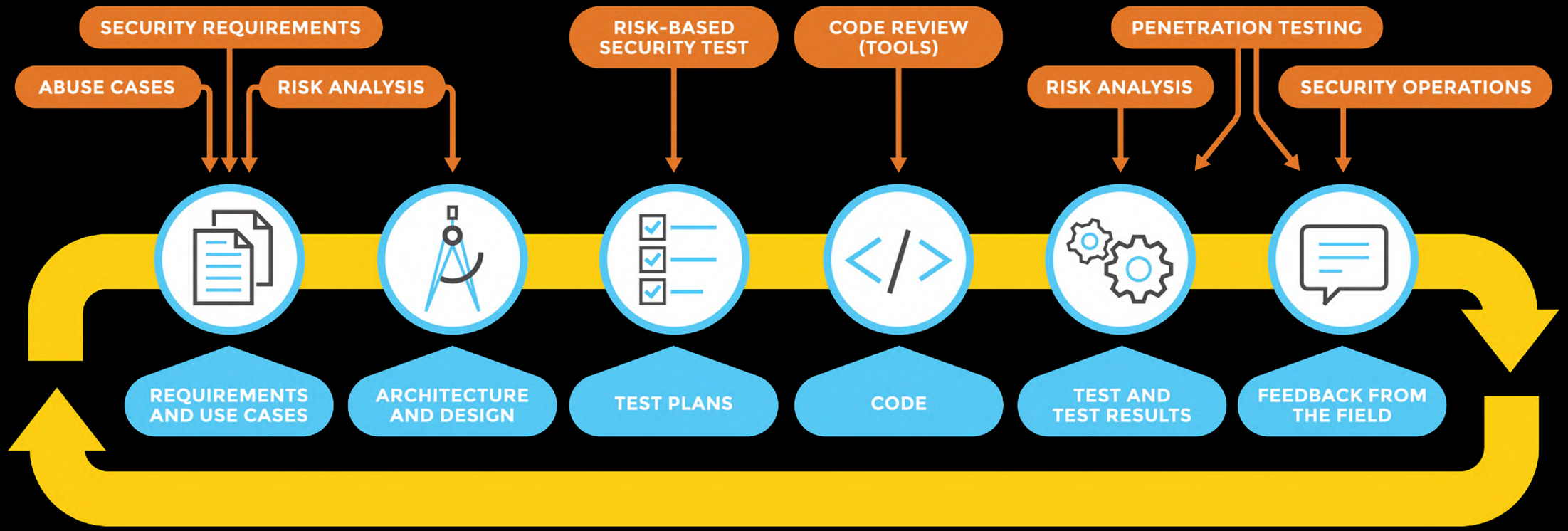
- 架构与设计
- 安全编码规范
- 嵌入式软件测试
- 内部威胁检测
- 红队测试
- 胖客户端测试

计划设计与开发

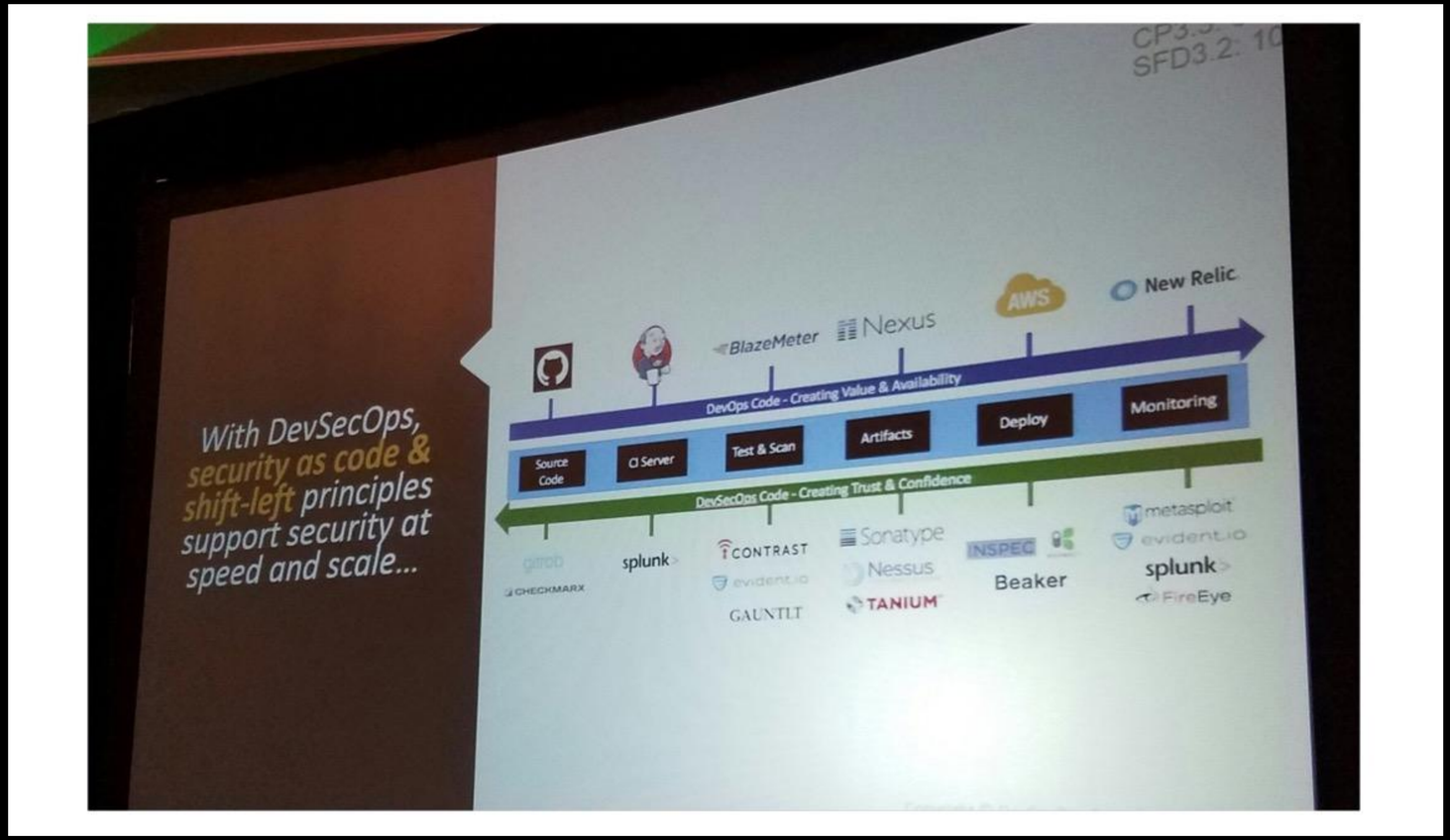
在成熟模型中构建安全（BSIMM）	通过评估现状测评软件安全计划（SSI）有效性。
成熟行动计划（MAP）	明确建立软件安全计划或趋于成熟的方向。
指标制定	帮助针对风险状况和业务流程选择定义明确可实现的指标。
整体软件安全计划（SSIB）	涵盖发布软件安全计划的一切条件。

定义、实施和测评SSSI，以反映不断演变的开发部署环境。

Co’s 们的安全视角


SECURITY REQUIREMENTS
ABUSE CASES
RISK ANALYSIS
RISK-BASED SECURITY TEST
CODE REVIEW (TOOLS)
PENETRATION TESTING
RISK ANALYSIS
SECURITY OPERATIONS
REQUIREMENTS AND USE CASES
ARCHITECTURE AND DESIGN
TEST PLANS
CODE
TEST AND TEST RESULTS
FEEDBACK FROM THE FIELD

软件安全是一个集成的过程



测试并不能保证软件安全

67% Discovery on re-test

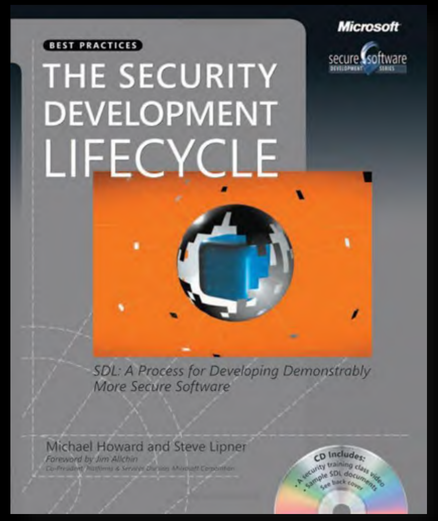
98% Re-exploit rate

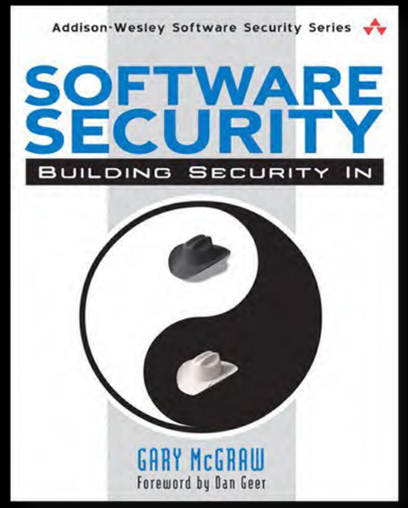
软件安全：技术+流程

- 软件安全不仅仅是安全功能与需求
- 50%技术保障+50%管控流程
- 安全是整体的属性
- SDLC的集成是软件安全非常必须的一步

理论到实际应用

- SSDL 集成 – 最佳实践
  - BSIMM
  - Microsoft’s SDL
  - OWASP CLASP





规定 vs. 描述模式

规定模式

- 规定你必须做的：
  - SAFECode
  - SAMM
  - SDL
  - Touchpoints
- 每个团队都有一个需要遵循的规定

描述模式

- 描述正在发生的
- BSIMM就是一个衡量SSDL的描述性模型

BSIMM：软件安全度量

- 129 个团队已经被评估过（data freshness）
- BSIMM7 = 95个真实场景的数据
- 290 独立衡量模型
- McGraw, Migues, and West

Cigital

NETSUITE

创建BSIMM（2008）

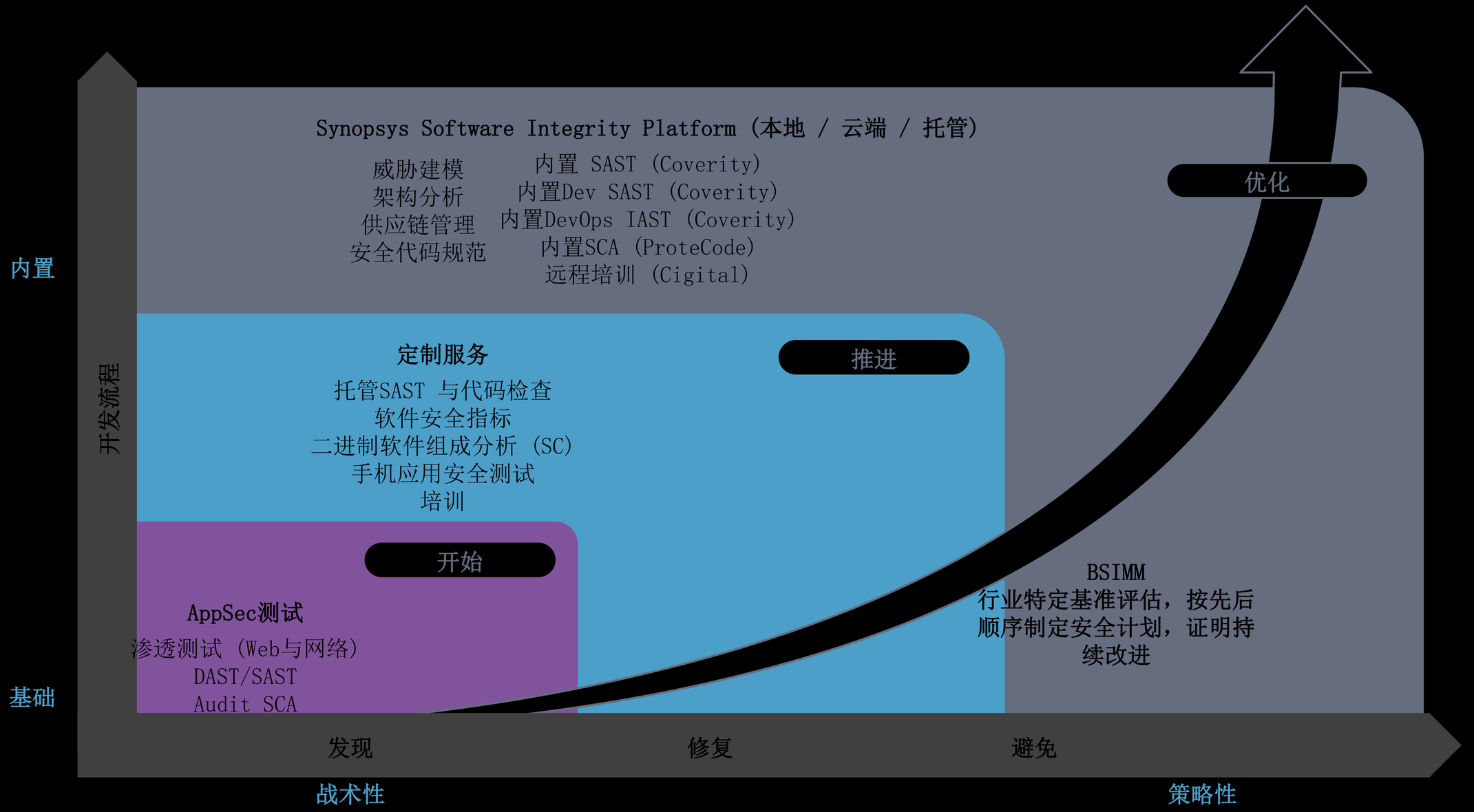
- 全球第一个提出了“Build Security In” 概念，建立成熟度模型（ Maturity Model ）
- 初始目标：创建一个成熟度模型（从9个知名的大型软件安全实体中收集到的真实数据模型）.
  - 创建一个软件安全架构
  - 9个企业一对一的人力资讯
  - 发现 110 活动 (1 removed, 4 added later).
  - 将所有的活动分为三个等级
  - 创建 scorecard.
- 该模型已经被129个企业验证过 (95 BSIMM7).

软件安全架构

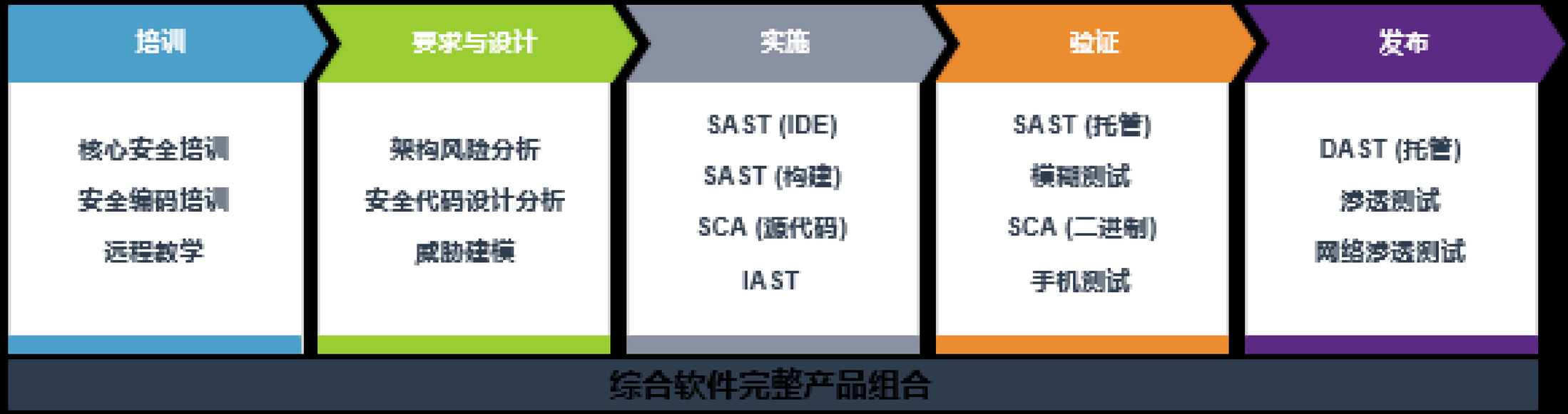
4 区域　　12 实践手段

Governance	1. Strategy & Metrics (SM) 2. Compliance & Policy (CP) 3. Training (T)
Intelligence	4. Attack Models (AM) 5. Security Features & Design (SFD) 6. Standards & Requirements (SR)
SSDL Touchpoints	7. Architecture Analysis (AA) 8. Code Review (CR) 9. Security Testing (ST)
Deployment	10. Penetration Testing (PT) 11. Software Environment (SE) 12. Configuration Management & Vulnerability Management (CMVM)

BSIMM的详细实施过程…



SDLC中的关键技术点



BSIMM7 评估流程

安全措施融入SDLC

如果制造商和开发人员在开发过程中重视安全和隐私保护措施，最近报告的物联网漏洞100%可以被轻松避免。

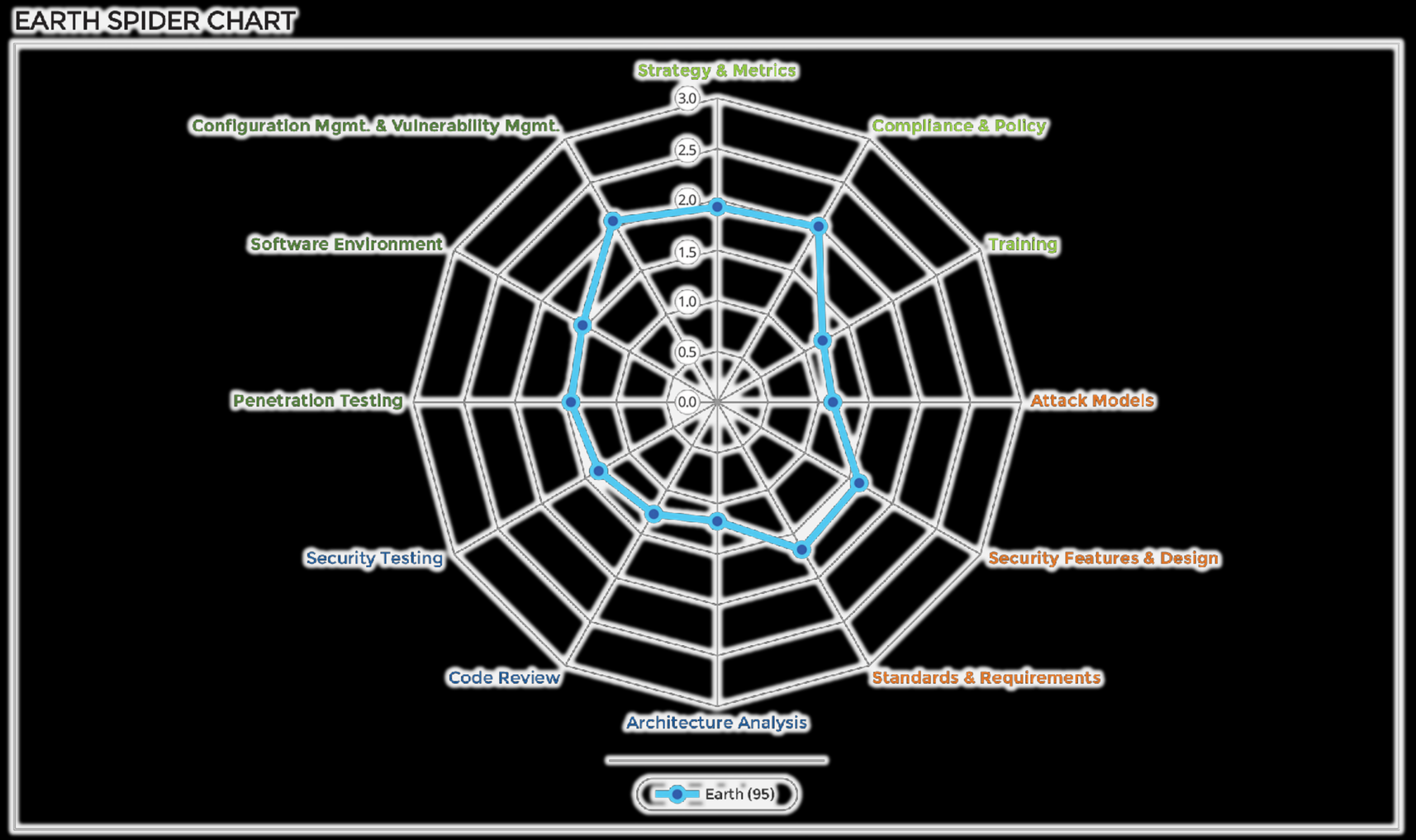
将安全整合在当前开发流程中

开发团队需要一种方法将完整的应用安全测试融入现有技术堆栈和语言中，而不会降低开发速度。

持续扫描开源代码

采用高级分析工具持续扫描第三方代码，确保符合安全和法律标准，从而降低风险保证合规。

BSIMM 示例 Earth (95)



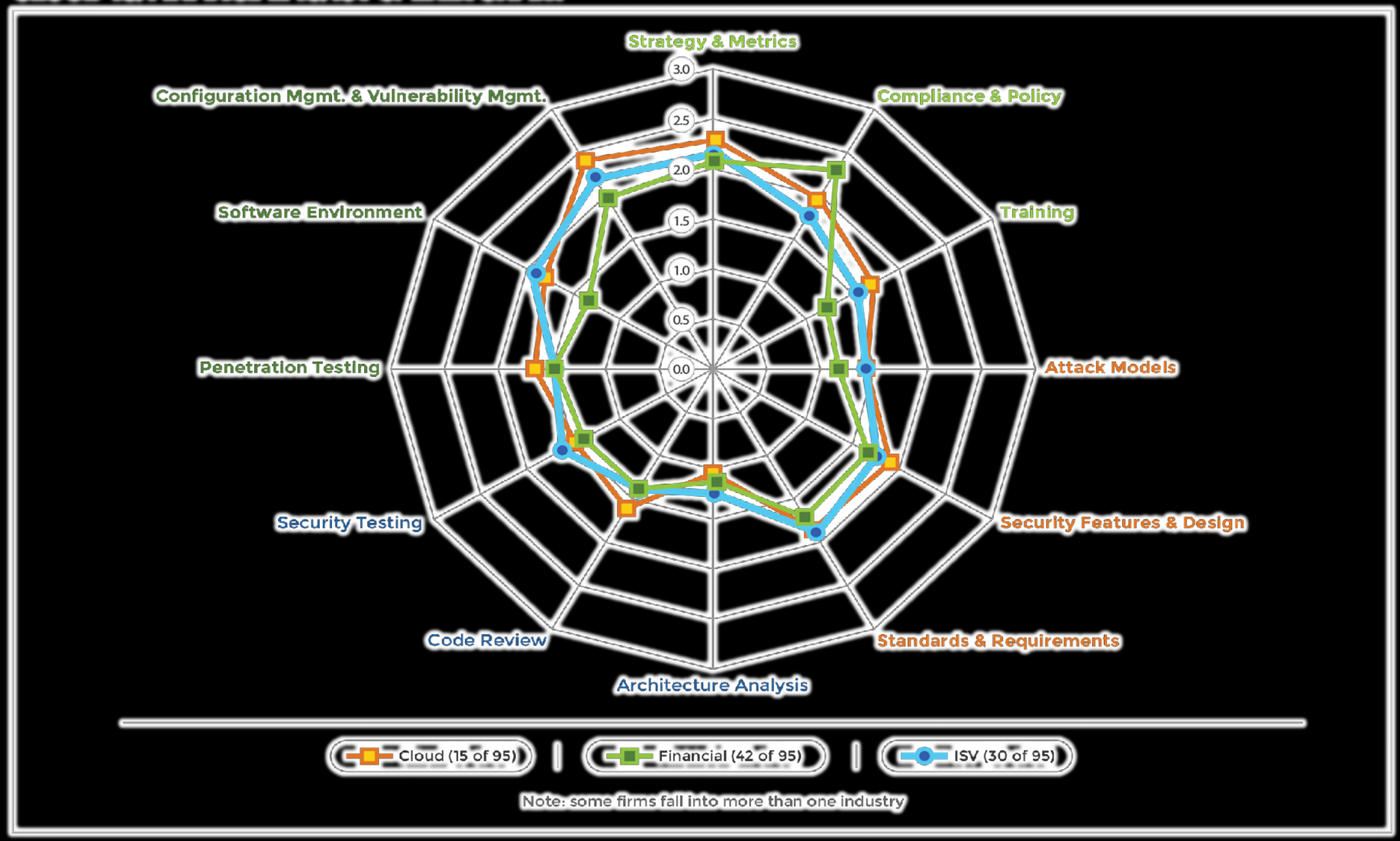
BSIMM7 结果报告

BSIMM7 SCORECARD FOR: FAKEFIRM | OBSERVATIONS: 37

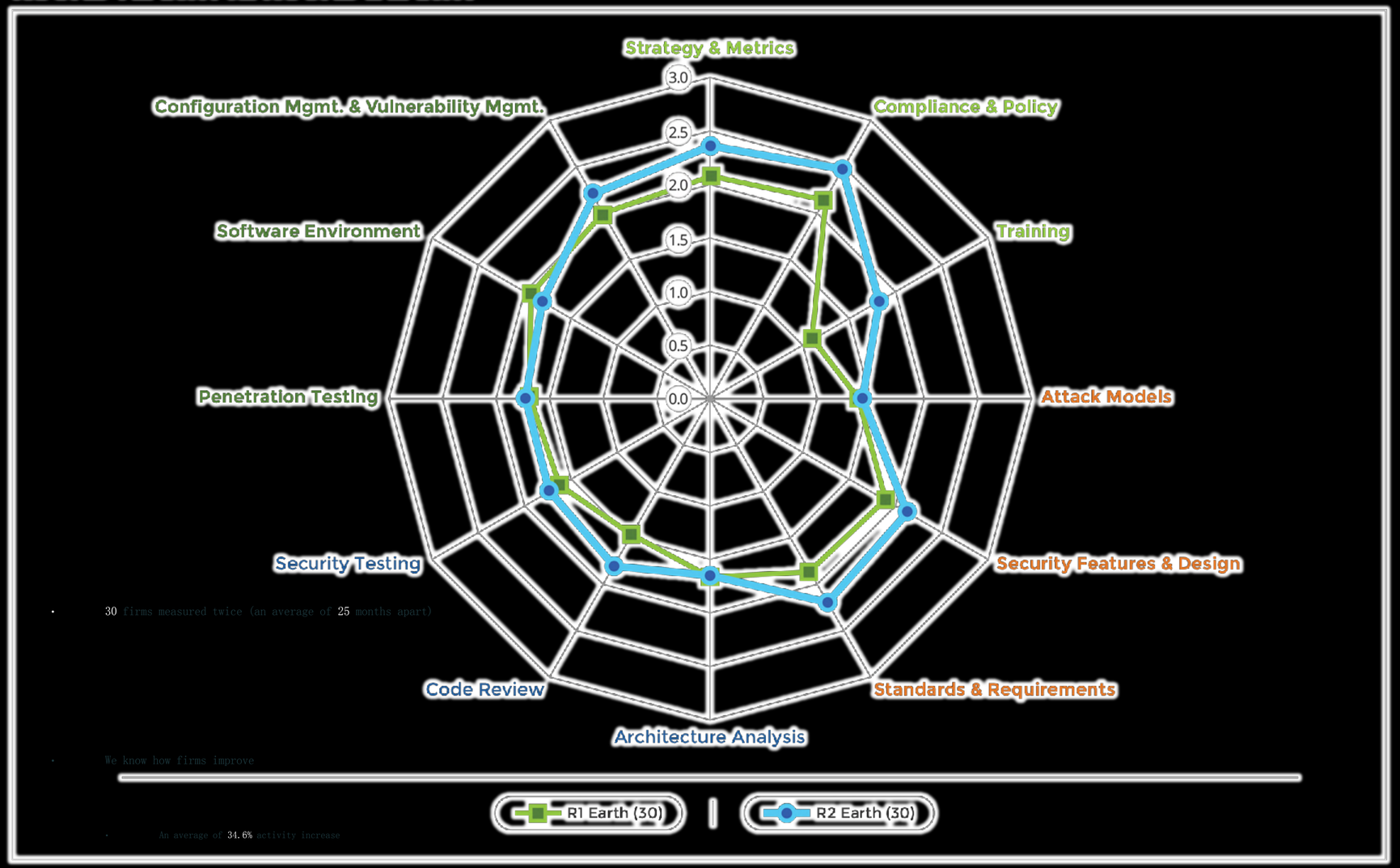
GOVERNANCE			INTELLIGENCE			SSDL TOUCHPOINTS			DEPLOYMENT		
ACTIVITY	BSIMM7 FIRMS (95)	FAKEFIRM	ACTIVITY	BSIMM7 FIRMS (95)	FAKEFIRM	ACTIVITY	BSIMM7 FIRMS (95)	FAKEFIRM	ACTIVITY	BSIMM7 FIRMS (95)	FAKEFIRM
STRATEGY & METRICS			ATTACK MODELS			ARCHITECTURE ANALYSIS			PENETRATION TESTING		
[SM1.1]	47	1	[AM1.2]	63		[AA1.1]	81	1	[PT1.1]	82	1
[SM1.2]	48		[AM1.3]	34		[AA1.2]	29	1	[PT1.2]	58	1
[SM1.3]	46	1	[AM1.5]	48	1	[AA1.3]	23	1	[PT1.3]	54	
[SM1.4]	81	1	[AM2.1]	8		[AA1.4]	47		[PT2.2]	21	1
[SM2.1]	41		[AM2.2]	8	1	[AA2.1]	15		[PT2.3]	16	
[SM2.2]	35		[AM2.5]	13	1	[AA2.2]	12	1	[PT3.1]	10	1
[SM2.3]	33		[AM2.6]	9	1	[AA2.3]	5		[PT3.2]	6	
[SM2.5]	19		[AM2.7]	9		[AA3.1]	4				
[SM2.6]	33		[AM3.1]	4		[AA3.2]	0				
[SM3.1]	14		[AM3.2]	2							
[SM3.2]	9										
COMPLIANCE & POLICY			SECURITY FEATURES & DESIGN			CODE REVIEW			SOFTWARE ENVIRONMENT		
[CP1.1]	56	1	[SFD1.1]	74		[CR1.2]	58	1	[SE1.1]	46	
[CP1.2]	84		[SFD1.2]	65	1	[CR1.4]	63	1	[SE1.2]	78	1
[CP1.3]	50	1	[SFD2.1]	27		[CR1.5]	28		[SE2.2]	27	1
[CP2.1]	24		[SFD2.2]	40		[CR1.6]	34	1	[SE2.4]	24	
[CP2.2]	31		[SFD3.1]	6		[CR2.5]	22		[SE3.2]	12	
[CP2.3]	34		[SFD3.2]	10		[CR2.6]	15		[SE3.3]	3	
[CP2.4]	36		[SFD3.3]	1		[CR2.7]	19		[SE3.4]	0	
[CP2.5]	38	1				[CR3.2]	3	1			
[CP3.1]	19					[CR3.3]	2				
[CP3.2]	13					[CR3.4]	3				
[CP3.3]	5					[CR3.5]	5				
TRAINING			STANDARDS & REQUIREMENTS			SECURITY TESTING			CONFIG. MGMT & VULN. MGMT		
[T1.1]	69	1	[SR1.1]	60	1	[ST1.1]	78	1	[CMVM1.1]	82	1
[T1.5]	27		[SR1.2]	66		[ST1.3]	72	1	[CMVM1.2]	84	
[T1.6]	17	1	[SR1.3]	64	1	[ST2.1]	22	1	[CMVM2.1]	69	1
[T1.7]	37		[SR2.2]	28	1	[ST2.4]	10		[CMVM2.2]	74	
[T2.5]	13		[SR2.3]	22		[ST2.5]	7		[CMVM2.3]	41	
[T2.6]	14	1	[SR2.4]	21		[ST2.6]	9		[CMVM3.1]	3	
[T2.7]	5		[SR2.5]	22		[ST3.3]	4		[CMVM3.2]	5	
[T3.1]	3		[SR2.6]	17	1	[ST3.4]	2		[CMVM3.3]	8	
[T3.2]	5		[SR3.1]	8		[ST3.5]	4		[CMVM3.4]	6	
[T3.3]	2		[SR3.2]	11							
[T3.4]	7										
[T3.5]	2										

对比企业中不同的团队

Special Snowflake (NOT)



BSIMM长线-持续修复



BSIMM 指标权重

BSIMM NUMBERS OVER TIME

	BSIMM7	BSIMM6	BSIMM-V	BSIMM4	BSIMM3	BSIMM2	BSIMM1
	95	78	67	51	42	30	9
MEASUREMENTS	237	202	161	95	81	49	9
	30	26	21	13	11	0	0
3RD MEASURES	15	10	4	1	0	0	0
		1,084	976	978	786	635	370
SATELLITE MEMBERS	3,595	2,111	1,954	2,039	1,750	1,150	710
		287,006	272,358	218,286	185,316	141,175	67,950
APPLICATIONS	87,244	69,750	69,039	58,739	41,157	28,243	3,970
		3.98	4.28	4.13	4.32	4.49	5.32
SSG AVG. OF AVGS	1.61/100	1.51/100	1.4/100	1.95/100	1.99/100	1.02/100	1.13/100
	42	33	26	19	17	12	4
ISVS	30	27	25	19	15	7	4
	15	10					
INTERNET OF THINGS	12	13					
INSURANCE	10						

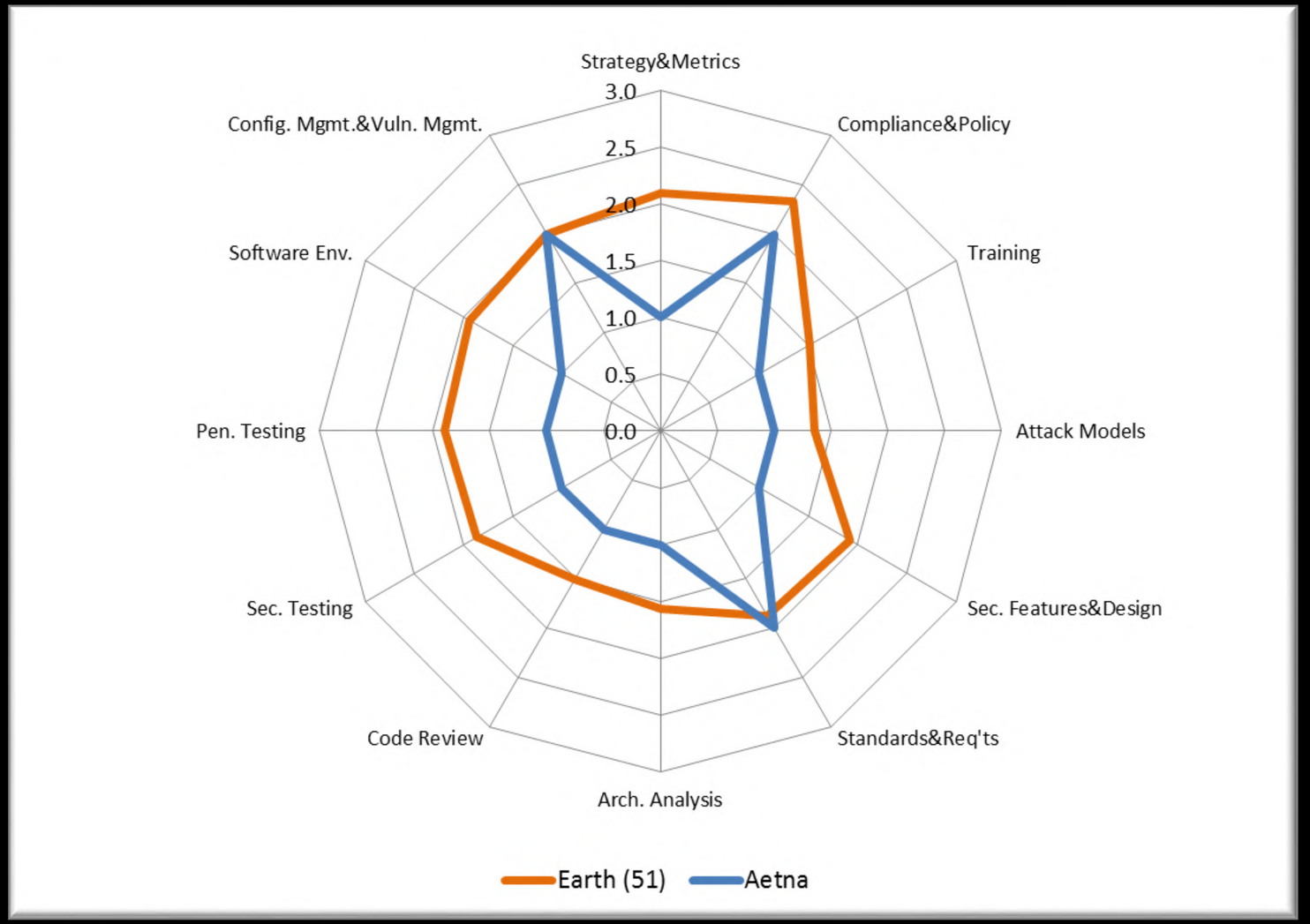
95 企业 - BSIMM7 社区

SYNOPSYS®
Silicon to Software™

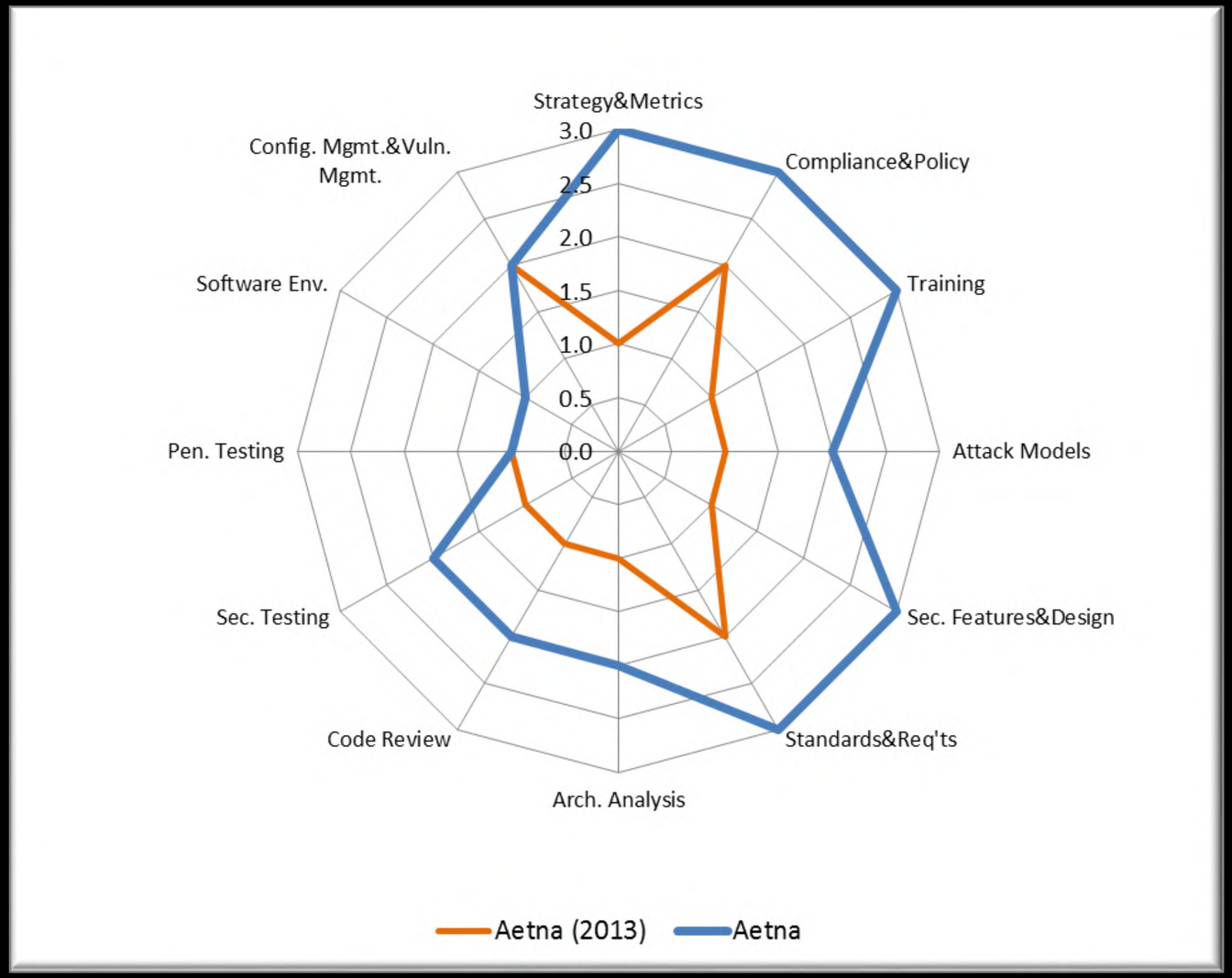
Aetna

典型BSIMM案例

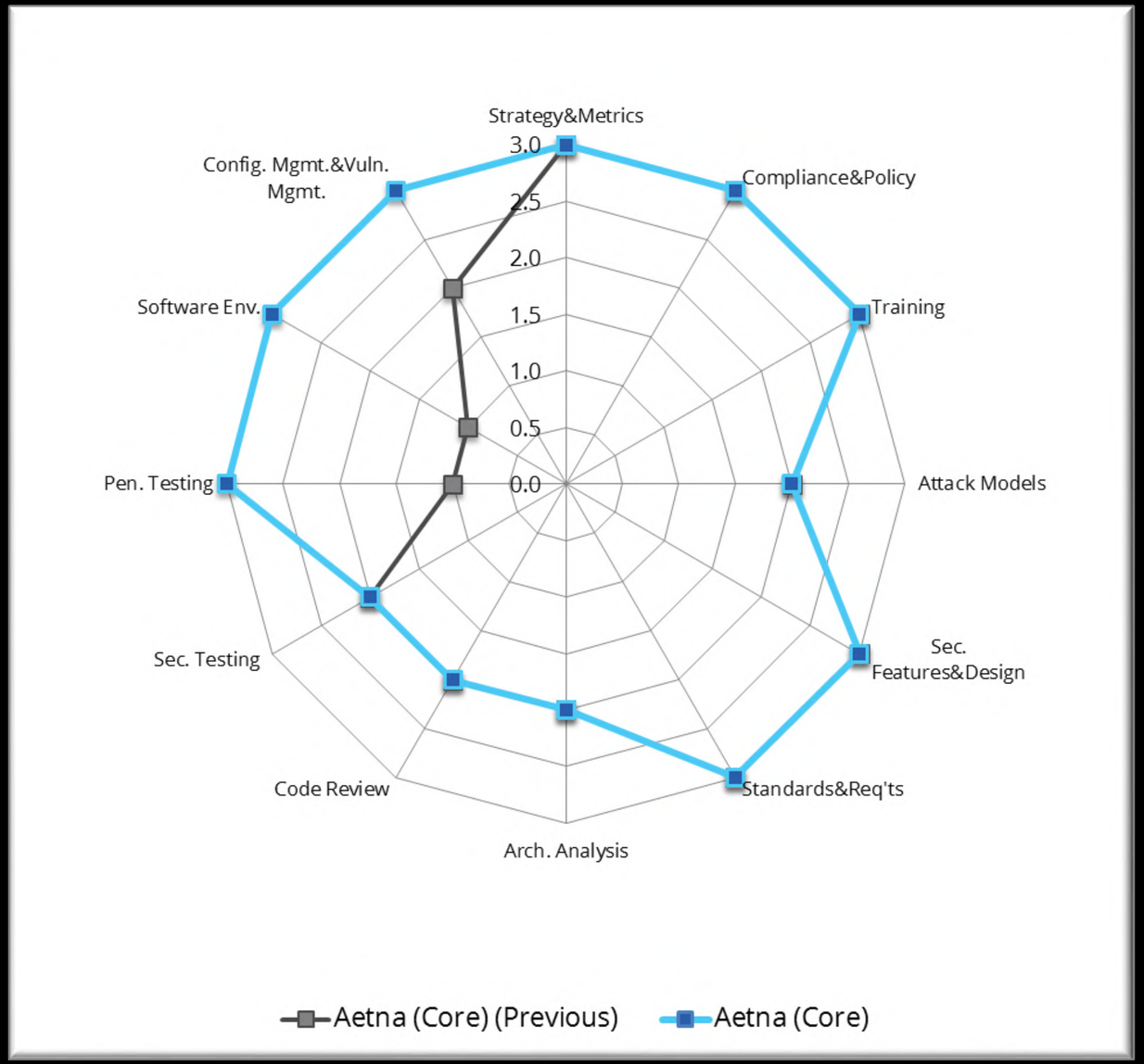
2013 BSIMM Results



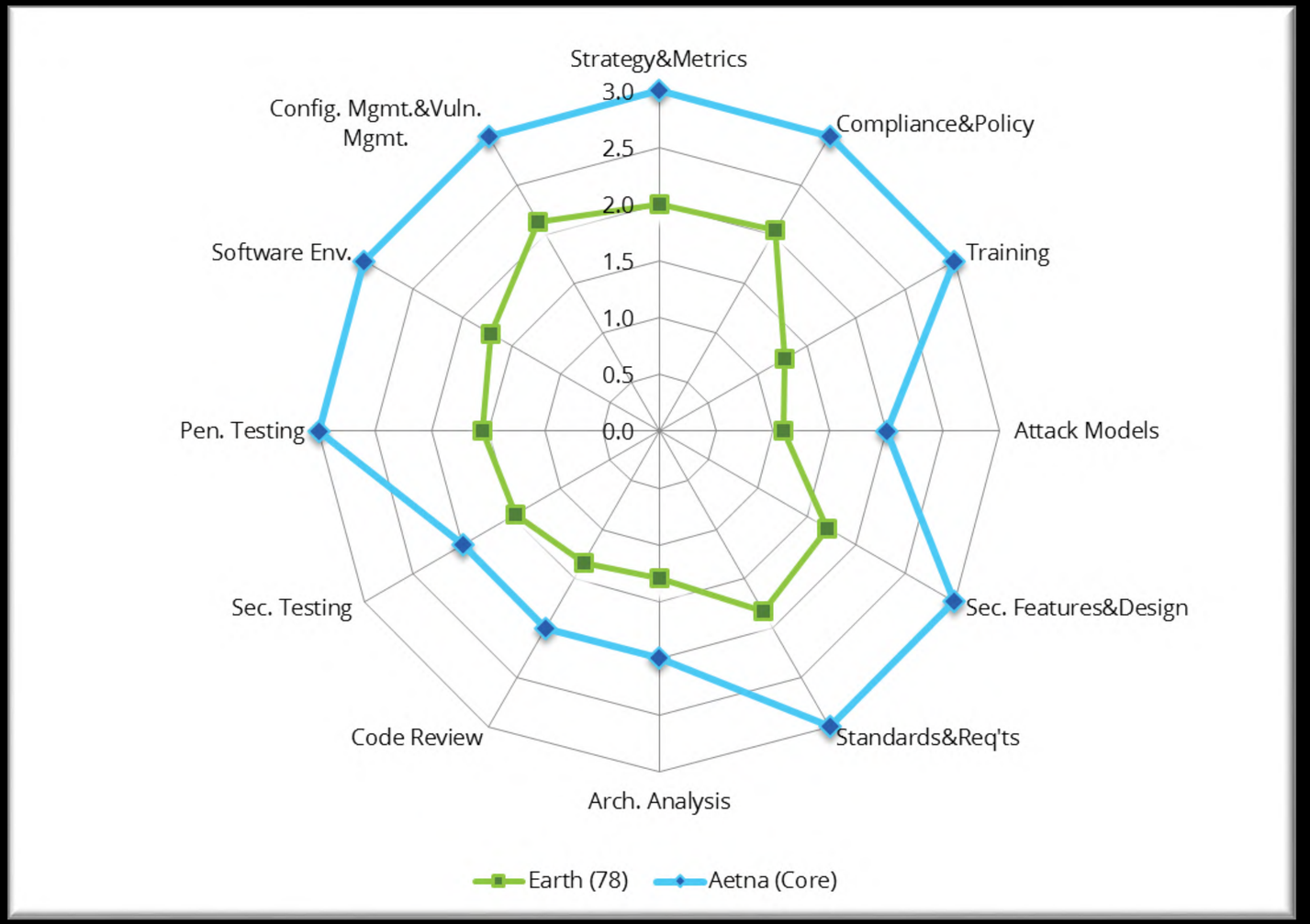
BSIMM Re-measurement (2014)



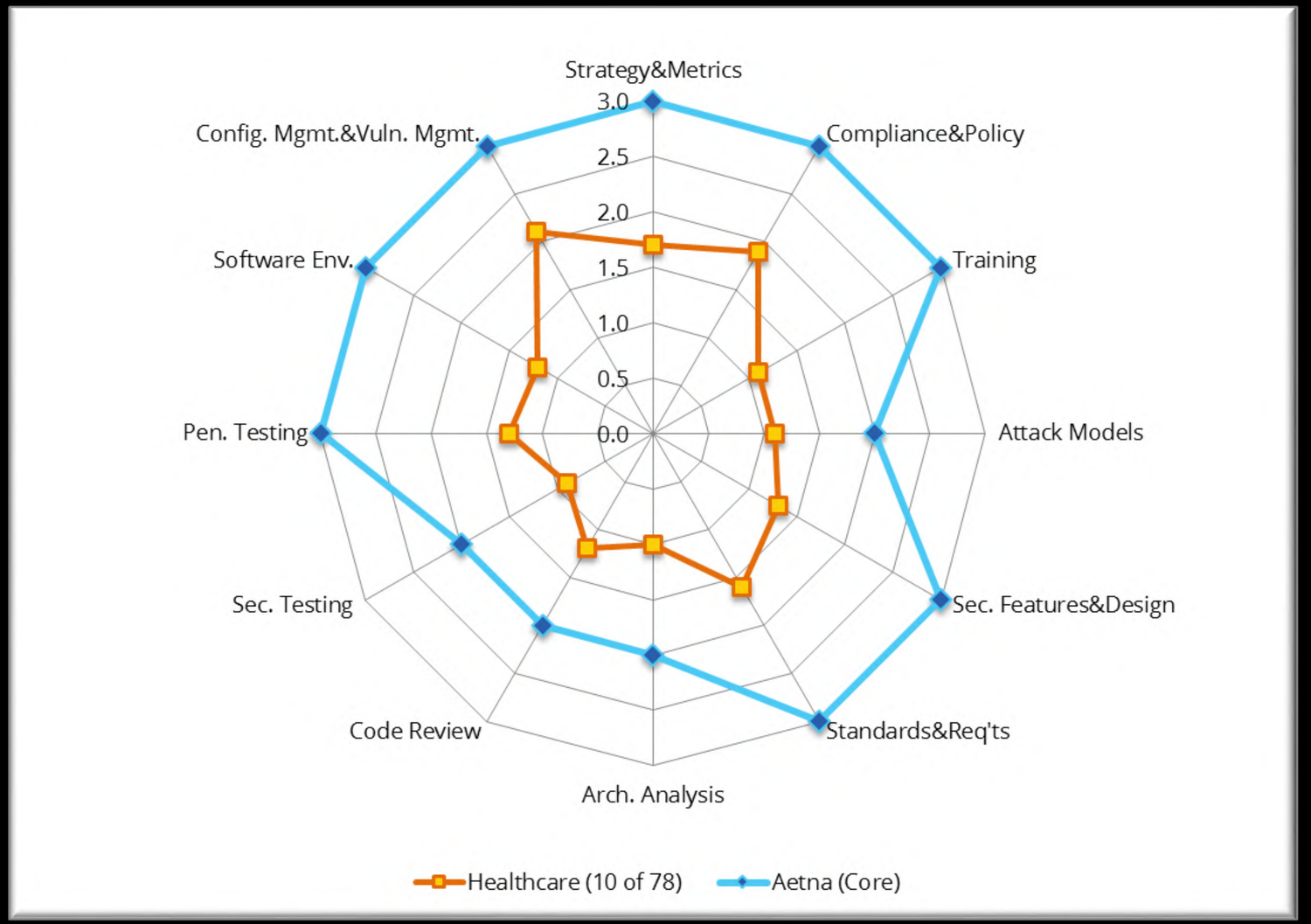
BSIMM (2015)


Strategy&Metrics
Compliance&Policy
Training
Attack Models
Sec. Features&Design
Standards&Req'ts
Arch. Analysis
Code Review
Sec. Testing
Pen. Testing
Software Env.
Config. Mgmt.&Vuln. Mgmt.
3.0
2.5
2.0
1.5
1.0
0.5
0.0
Aetna (Core) (Previous)
Aetna (Core)

2015 BSIMM Results: Aetna vs. Earth



2015 BSIMM Results: Aetna vs. Healthcare



关注QCon微信公众号，
获得更多干货！

Thanks!

INTERNATIONAL SOFTWARE DEVELOPMENT CONFERENCE

主办方 Geekbang. 极客邦科技 InfoQ