OWASP

Open Web Application Security Project

Build Security In Maturity Model

构筑坚若磐石的安全软件

韩葆

Agenda

- 软件安全的现状
- BSIMM （Build Security In Maturity Model）起源
- BSIMM 的执行与落地
- 基于BSIMM的SDLC全生命周期软件安全管控

软件安全的现状

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

任何时间 – 永久风险

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

任何人 – 独狼或国家

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

大范围 – 大规模攻击

不断演变的软件质量与安全环境

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

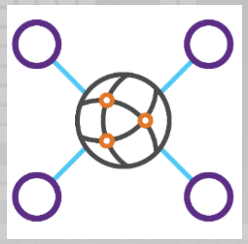
**新的开发理念
和方法**

敏捷

开发运维

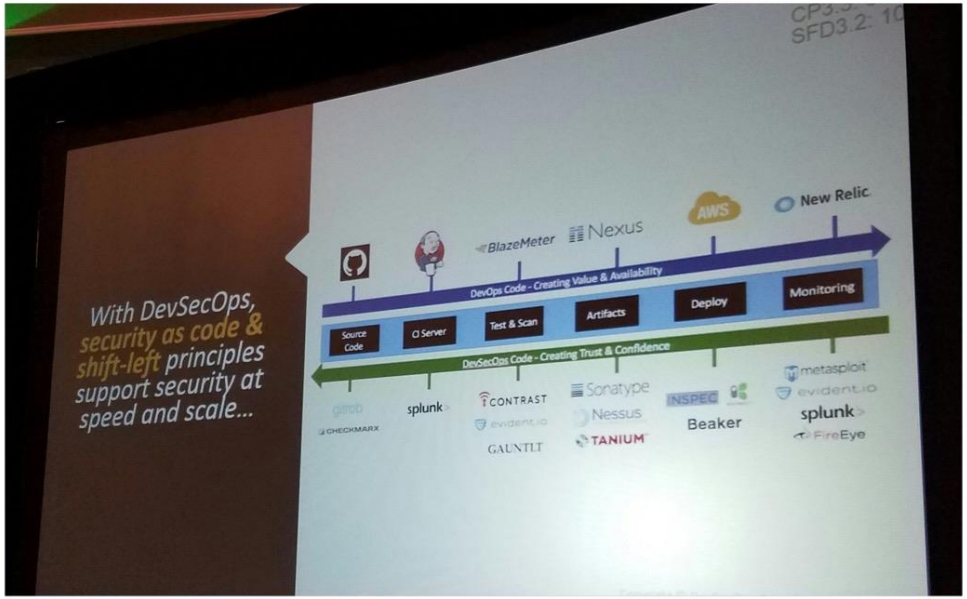
CI/CD

开源



不断变化的部署环境
改变了安全需求

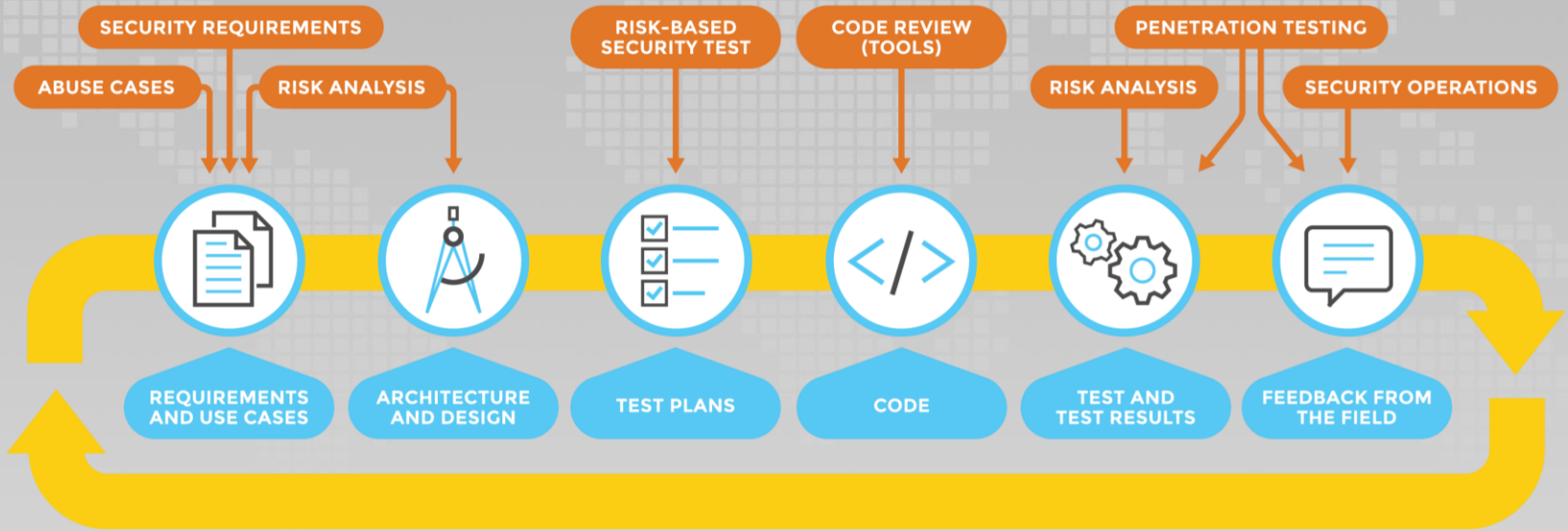
软件安全是一个集成的过程



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

Co's 们的安全视角 – 怎么办?



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).

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

BSIMM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)

BSIMM7 的执行与落地

指标权重

BSIMM7 SCORECARD

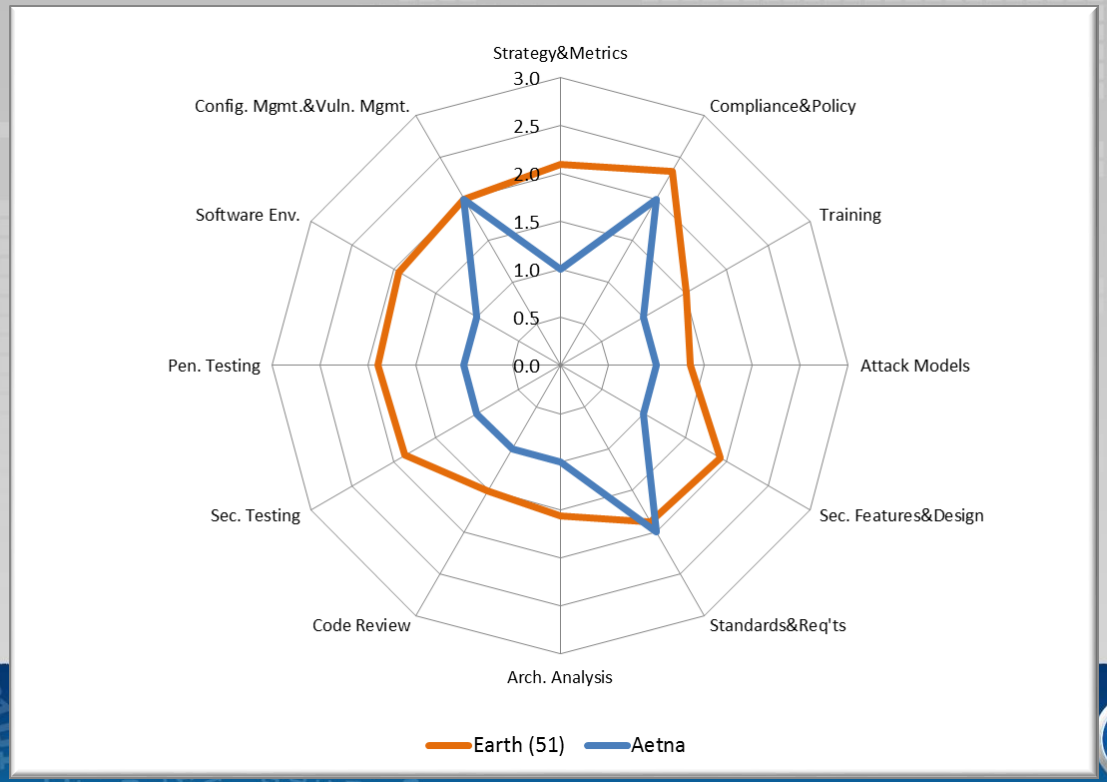
GOVERNANCE		INTELLIGENCE		SSDL TOUCHPOINTS		DEPLOYMENT	
ACTIVITY	OBSERVED	ACTIVITY	OBSERVED	ACTIVITY	OBSERVED	ACTIVITY	OBSERVED
[SM1.1]	47	[AM1.2]	63	[AA1.1]	81	[PT1.1]	82
[SM1.2]	48	[AM1.3]	34	[AA1.2]	29	[PT1.2]	58
[SM1.3]	46	[AM1.5]	48	[AA1.3]	23	[PT1.3]	54
[SM1.4]	81	[AM2.1]	8	[AA1.4]	47	[PT2.2]	21
[SM2.1]	41	[AM2.2]	8	[AA2.1]	15	[PT2.3]	16
[SM2.2]	35	[AM2.5]	13	[AA2.2]	12	[PT3.1]	10
[SM2.3]	33	[AM2.6]	9	[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						
[CP1.1]	56	[SFD1.1]	74	[CR1.2]	58	[SE1.1]	46
[CP1.2]	84	[SFD1.2]	65	[CR1.4]	63	[SE1.2]	78
[CP1.3]	50	[SFD2.1]	27	[CR1.5]	28	[SE2.2]	27
[CP2.1]	24	[SFD2.2]	40	[CR1.6]	34	[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			[CR3.2]	3		
[CP3.1]	19			[CR3.3]	2		
[CP3.2]	13			[CR3.4]	3		
[CP3.3]	5			[CR3.5]	5		
[T1.1]	69	[SR1.1]	60	[ST1.1]	78	[CMVM1.1]	82
[T1.5]	27	[SR1.2]	66	[ST1.3]	72	[CMVM1.2]	84
[T1.6]	17	[SR1.3]	64	[ST2.1]	22	[CMVM2.1]	69
[T1.7]	37	[SR2.2]	28	[ST2.4]	10	[CMVM2.2]	74
[T2.5]	13	[SR2.3]	22	[ST2.5]	7	[CMVM2.3]	41
[T2.6]	14	[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	[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						

BSIMM 指标权重

BSIMM NUMBERS OVER TIME

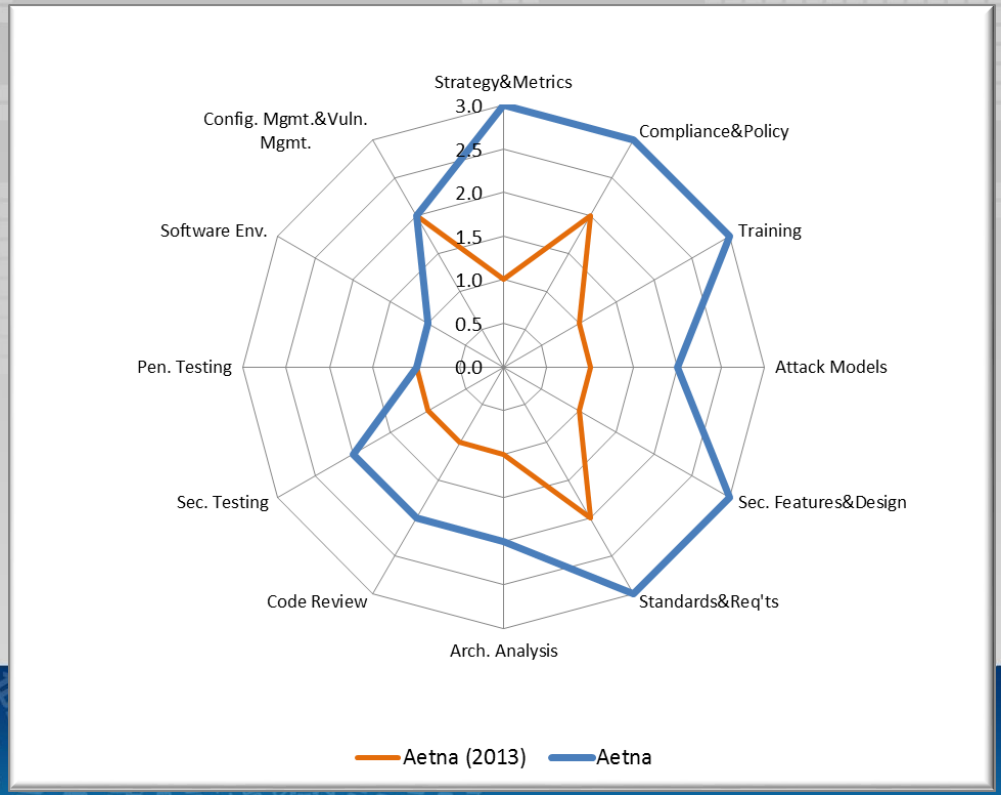
	BSIMM7	BSIMM6	BSIMM-V	BSIMM4	BSIMM3	BSIMM2	BSIMM1
FIRMS	95	78	67	51	42	30	9
MEASUREMENTS	237	202	161	95	81	49	9
2ND MEASURES	30	26	21	13	11	0	0
3RD MEASURES	15	10	4	1	0	0	0
SSG MEMBERS	1,111	1,084	976	978	786	635	370
SATELLITE MEMBERS	3,595	2,111	1,954	2,039	1,750	1,150	710
DEVELOPERS	272,782	287,006	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
AVG. SSG AGE (IN YRS.)	3.94	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
FINANCIAL SERVICES	42	33	26	19	17	12	4
ISVS	30	27	25	19	15	7	4
HEALTHCARE	15	10					
INTERNET OF THINGS	12	13					
CLOUD	15						
INSURANCE	10						

Example - 2013 BSIMM Results



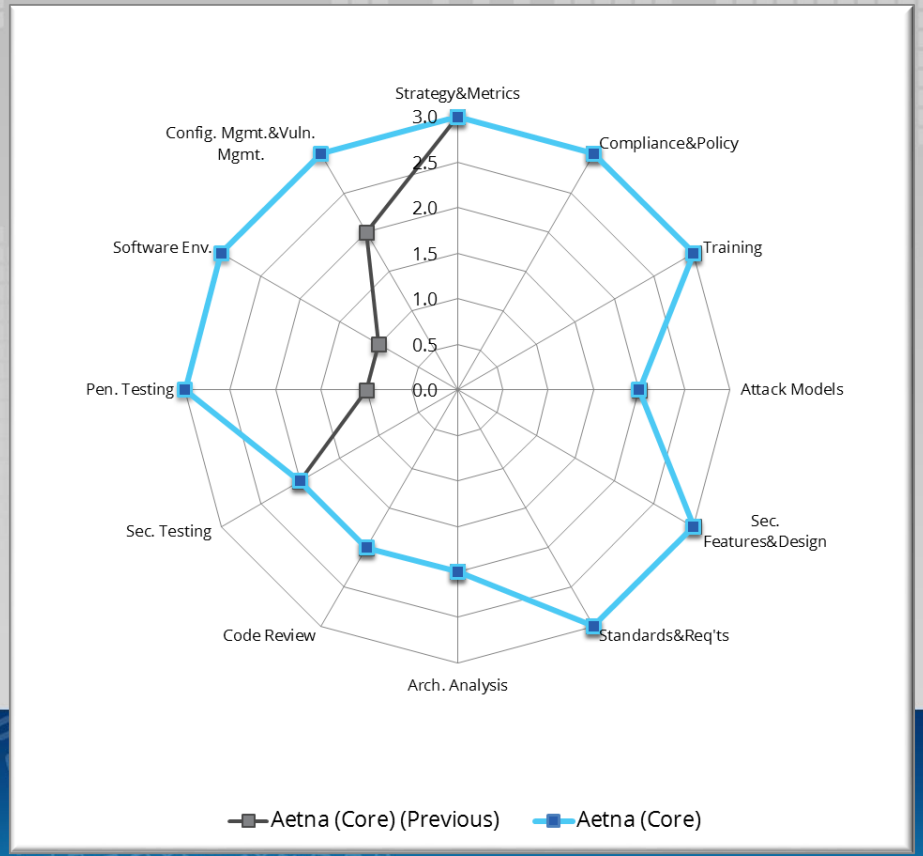
OWASP
Open Web Application Security Project

BSIMM Re-measurement (2014)



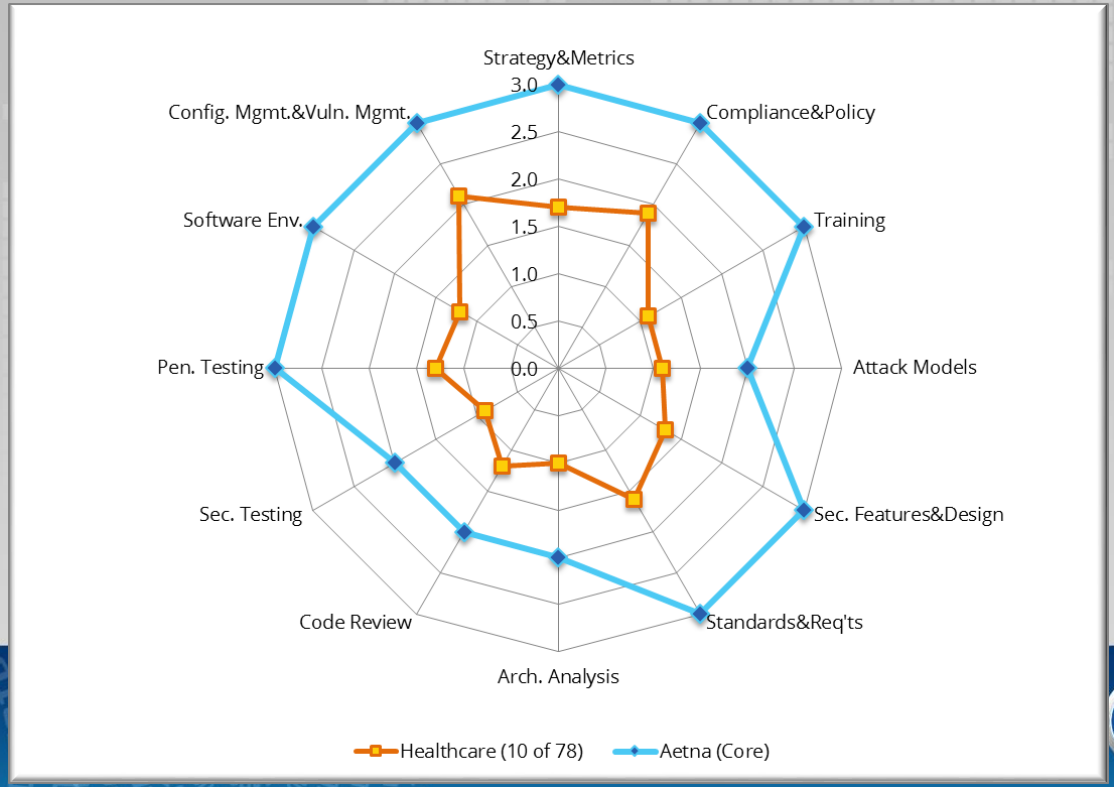
OWASP
Open Web Application Security Project

BSIMM (2015)



OWASP
Open Web Application Security Project

2015 BSIMM Results: Aetna vs. Healthcare



OWASP
Open Web Application Security Project

SDLC全生命周期软件安全管控

Cigital with SDLC

© 2017 Synopsys, Inc.

Confidential

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、实施和测评软件安全计划，以适应不断演变的开发部署环境。

管理整个SDLC风险-典型技术

SAST	编写过程中高度精确地找出代码中的缺陷和安全漏洞
SCA	发现二进制、开源和第三方代码已知漏洞
IAST	模拟应用中实际漏洞，验证结果，消除误报
eLearning	扩展软件安全意识和最佳实践

Build in security and quality at every step during development, and across the supply chain.

静态代码分析
Coverity

从源头保证安全

静态分析技术能够在编写代码的同时发现其中的严重安全漏洞。

Synopsys提供**Coverity**静态代码分析工具

“开发人员首先” 保证安全

- 签交前发现并修复漏洞

企业就绪

- 企业级报表和仪表板
- 超大型代码库 (10M以上LOC)

符合标准

- OWASP Top 10, CWE Top 25
- 报告包括 PCI-DSS

手机安全

- Android和 iOS Objective-C
- OWASP Mobile Top 10, JSSEC, CERT

OWASP
Open Web Application Security Project

静态代码分析
Coverity

从源头保证安全

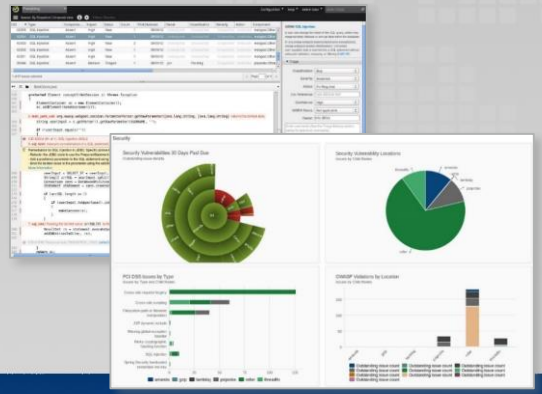
采用行业最高效、最可靠的静态分析解决方案，在编写代码的同时发现其中的严重安全漏洞。

可发现的缺陷包括

- 缓冲区溢出
- 内存损坏
- 资源泄漏
- 资源争用

OWASP10 + CWE25 覆盖范围包括

- SQL注入
- 跨站脚本
- 敏感数据误用
- 命令注入



OWASP
Open Web Application Security Project

软件成分分析
ProteCode

了解软件构成。

识别第三方软件组件中的已知漏洞并修复，避免被利用。

Synopsys提供ProteCode软件组成成分分析工具

软件组成分析包括:

- 任何软件或器件的完整物料清单
- 企业工作流集成
- 可配置CI插件的开放式API

覆盖范围包括:

- 源代码和二进制代码 (包括容器、固件和虚拟HD)
- 开源代码许可义务
- 第三方代码已知漏洞

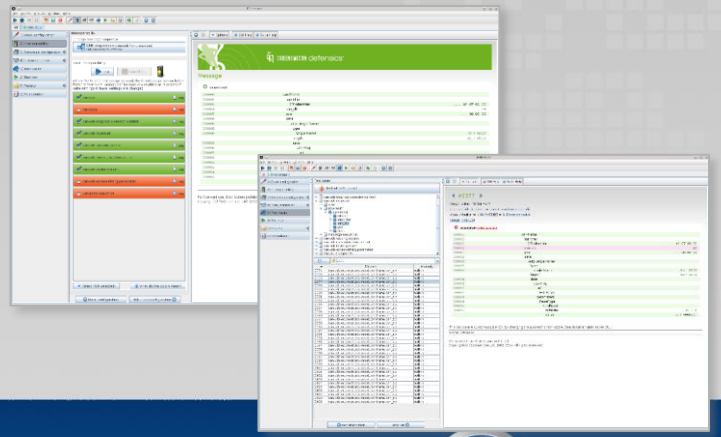
智能模糊测试

Defensics

在黑客动手前... 在软件中发现未知危险漏洞。
Synopsys提供Defensics模糊测试工具

先进的模糊测试

- 降低总体开发成本和时间
- 避免召回/修补/更新造成损失
- Heartbleed漏洞的发现原理-Defensics工具



交互式应用安全测试（Seeker）

将动态测试和运行时代码分析集成到现有开发生命周期之中，帮助开发团队发现并确认多层 web 应用中的安全漏洞

介于白盒测试与黑盒测试之间的安全漏洞检测

- 通过模拟漏洞利用和数据分析，精确评估每一个漏洞风险的影响和分类
- IAST的技术能够覆盖到每一个漏洞的源代码
- BSIMM推荐的的IAST软件工具为Seeker，来自以色列