OWASP
Open Web Application
Security Project

基于虚拟安全团队的S-SDLC在跨国团队的实践

主讲人：肖文棣
Mendick Xiao
2017-07-08

MORNINGSTAR

33 周年

15 周年

27 国家与地区

2000 亿美元资产

目录

- 安全落地的最佳实践
- 安全评级-高层会的更新
- 流程、工具和培训

安全落地的最佳实践

我们的挑战

我们的应对之道

OWASP
Open Web Application Security Project

我们的挑战

区域挑战

资源挑战

落地挑战

美国 vs 全球 - 需要代言人


10 VS 1000
需要帮手

落地

我们的应对

双赢模式

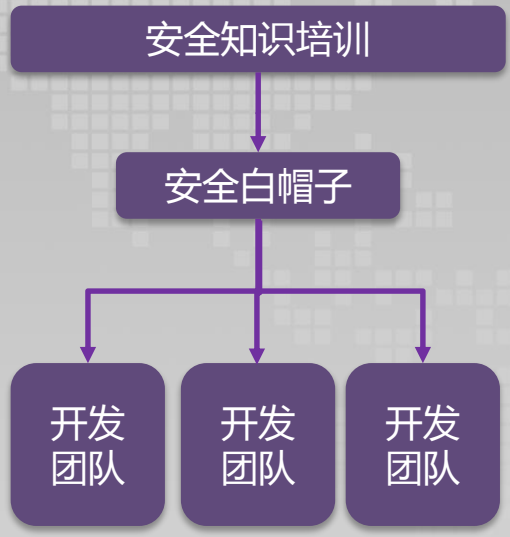
数据驱动

OWASP
Open Web Application Security Project

三大使命

桥梁

守卫者



导师

安全白帽子的全球分布

安全白帽子的文化


SC
Security Champion
Guard
Mentor
Protect
SC
Security Champion
安全白帽子，共筑防护墙

数据驱动

5星

★★★★★

1000+

项目

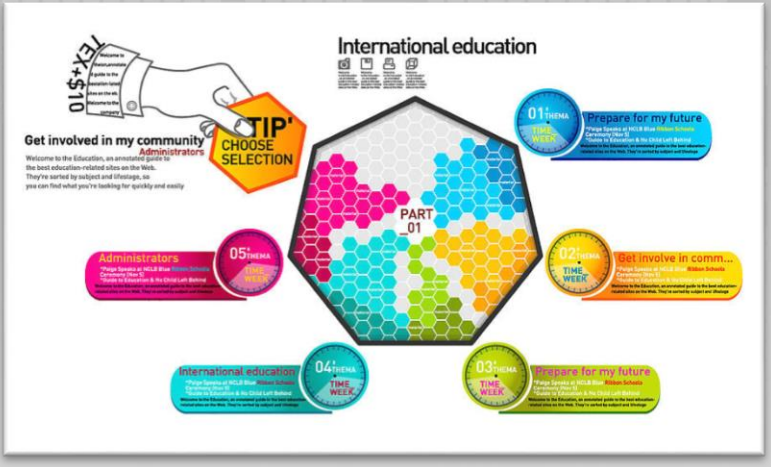
2.2亿

行代码

22万

漏洞

安全评级-高层会的更新


International education
Get involved in my community
Administrators
TIP
CHOOSE SELECTION
PART _01
01 THEMA
Prepare for my future
02 THEMA
Get involve in comm...
03 THEMA
Prepare for my future
04 THEMA
International education
05 THEMA
Administrators

安全星等级

应用名称	严重	高	中	低	总数	安全星等级	趋势	数据密级	等级评级
APP 1	0	0	0	1	1	★★★★	平	敏感	2
APP 2	0	0	11	3	14	★★★★	向上	敏感	1
APP 3	0	0	0	1	1	★★★★	平	受限	1

数据密级分类

密级	描述
公开	公开信息，如公开刊物的信息、外部IP地址、网站地址，金融财报公开信息等
敏感	敏感信息，如一般个人信息，包括用户姓名、地址、电话号码、邮箱地址；金融账号信息，如银行卡账号；公司业务算法和公式等
受限	严格受限的信息，包括身份证号，税务登记号，信用卡号和PIN码

漏洞等级

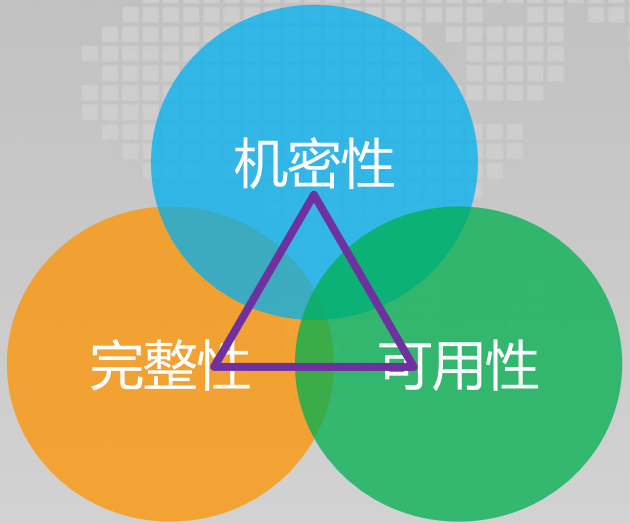
漏洞等级	描述
严重 Critical	自定义，导致敏感信息被窃取和系统不可用的漏洞
高 High	CVSS评级在7和10之间的漏洞
中 Medium	CVSS评级在3和6之间的漏洞
低 Low	CVSS评级在1和2之间的漏洞

安全星等级的标准

星级/数据密级分类	受限数据	敏感数据	公开数据
★★★★★	All = 0	All = 0	Low > 0
★★★★	Low > 0	Low > 0	Medium > 0
★★★	Medium > 0	N/A	High > 0
★★	Critical = 0 AND High < 6	High > 0	N/A
★	Critical > 0 OR High >= 6	Critical > 0	Critical > 0

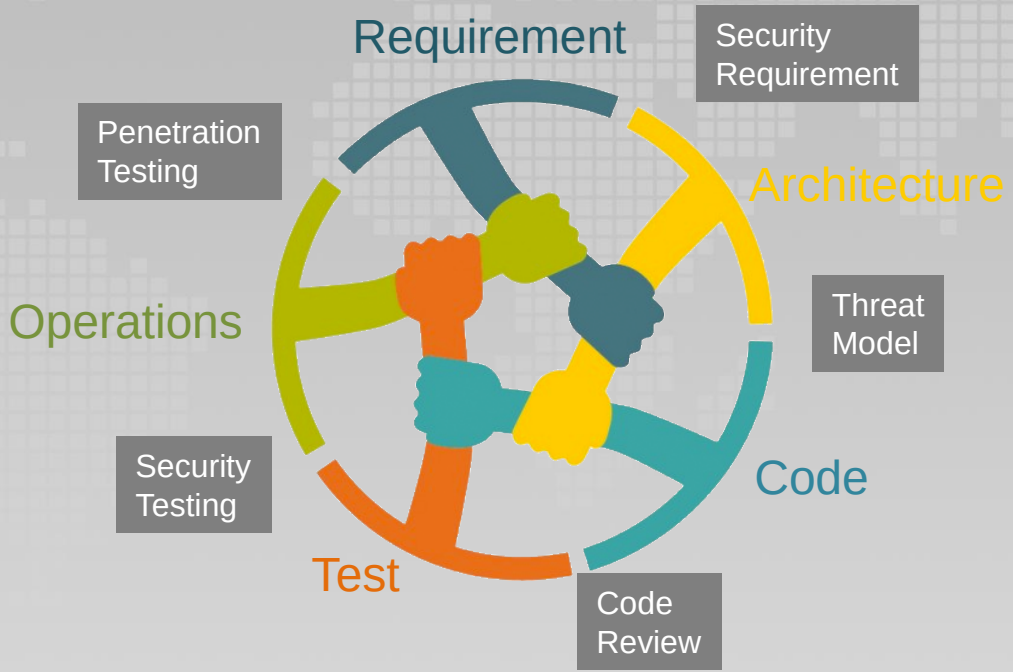

流程
工具
培训

安全铁三角

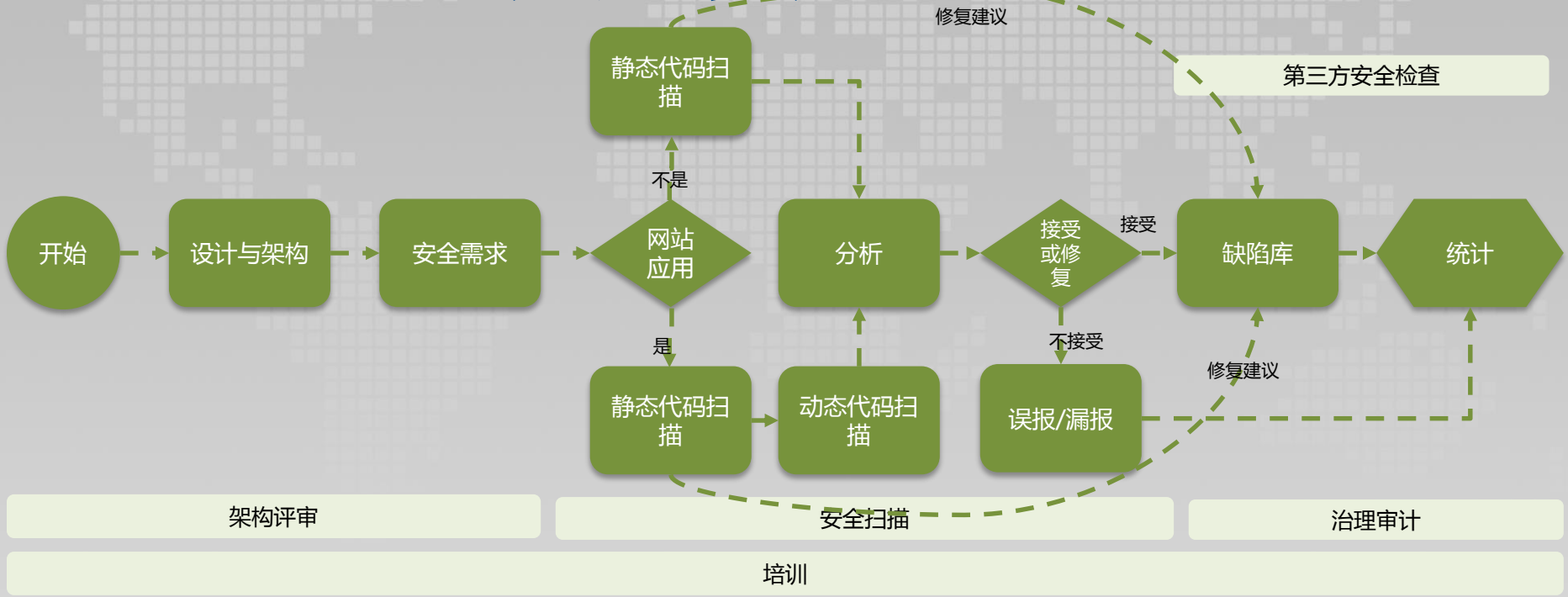


安全白帽子与S-SDLC

S-SDLC的具体实践


Requirement
Security Requirement
Penetration Testing
Architecture
Operations
Threat Model
Security Testing
Code
Test
Code Review

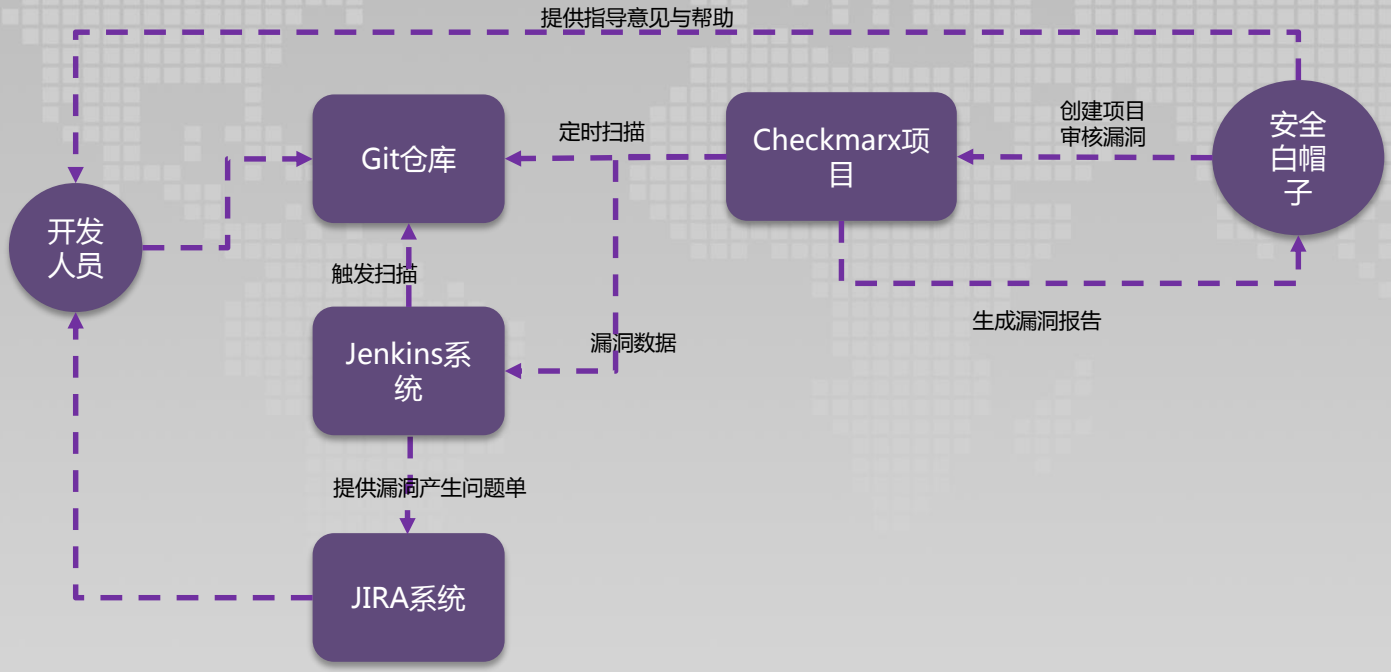
S-SDLC的具体实践



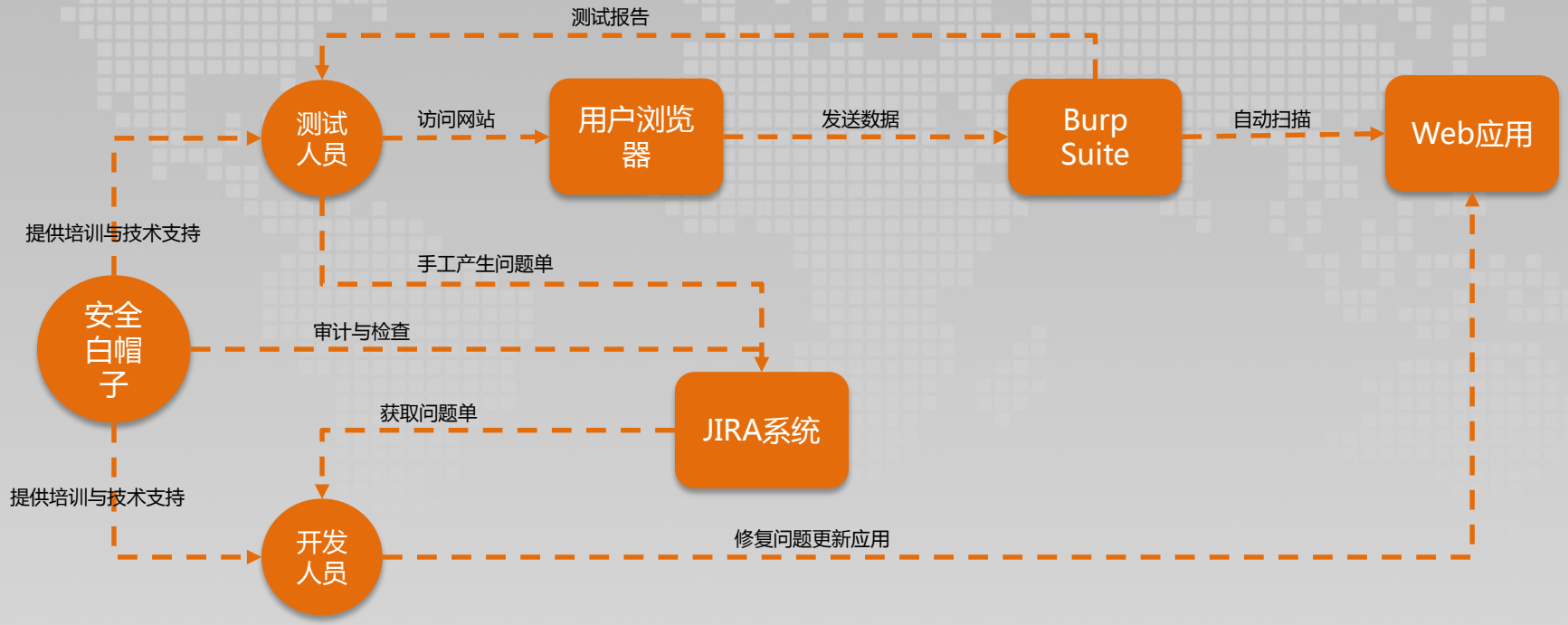
架构评审

- 数据流的信息密级
- STRIDE威胁建模
- 第三方依赖的安全性
- 身份认证、权限管理和日志审计

静态代码扫描



动态代码扫描



培训和指导

- MDP培训
- 测试人员培训/开发人员培训
- 安全白帽子内部培训
- 安全问题的通用解决方案培训

总结