安世加

AFSS-亚太金融安全峰会

护驾金融，安定民生

上海站|2021年7月23日

刘顺，广发银行研发中心安全专家。10多年网络安全从业经验，曾先后就职于宇通、唯品会、华为等企业。目前就职于广发银行研发中心，在安全规划、安全架构设计、终端安全、应用安全、数据安全与隐私保护等多个领域，具有丰富的管理与实践经验。

安世加

金融企业SDL建设实践

刘顺　广发银行研发中心

安世加

目录

CONTENTS

安世加

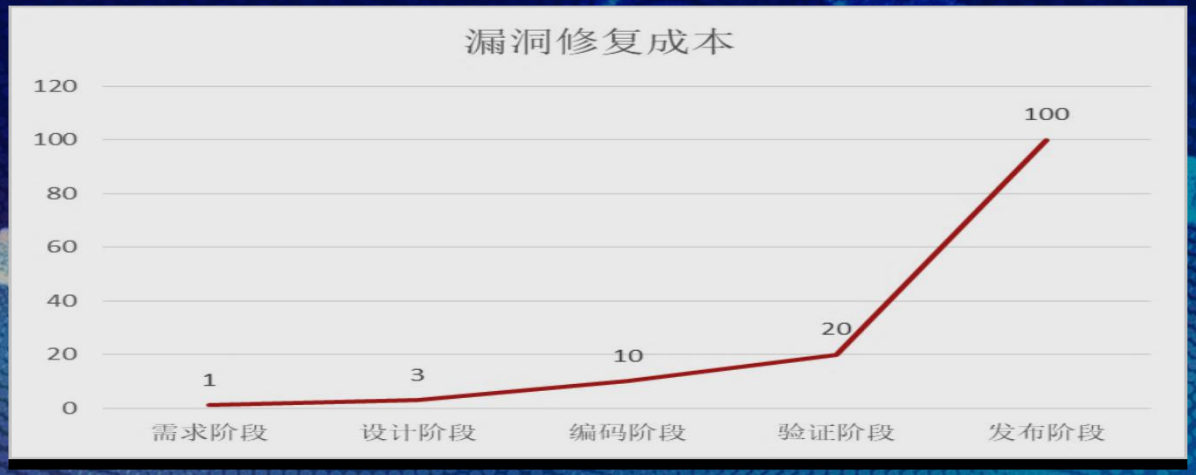
金融企业应用安全现状

监管要求严、行业法规标准多

应用安全是入侵企业的重要突破口

应用数量多、功能复杂、漏洞层出不穷

修复漏洞成本高



金融企业应用安全现状

解决之道：建立基于软件开发全生命周期的安全管控体系！

Security Development Lifecycle

安世加

目录

CONTENTS

安世加

SDL落地面临的困难

改变现有意识

人世间最难的事情莫过于改变所有人的意识与习惯

专业人员不足

安全专业人员配备不足，无法覆盖所有需求

能力要求高

威胁建模、安全编码对需求分析与设计人员、开发人员的能力要求高

合规条文多

合规条文多，无法把所有合规要求有效融入内部管理

安世加

目录

CONTENTS

安世加

SDL体系建设实践|前期准备

明确目标、统一信念、获得支持！

目标是什么？

提升应用安全质量、满足监管合规要求、保障企业经营发展

要获得谁的支持？

Boss、研发领导

为什么SDL是有效的？

最佳实践、他山之石

为什么SDL是有价值的？

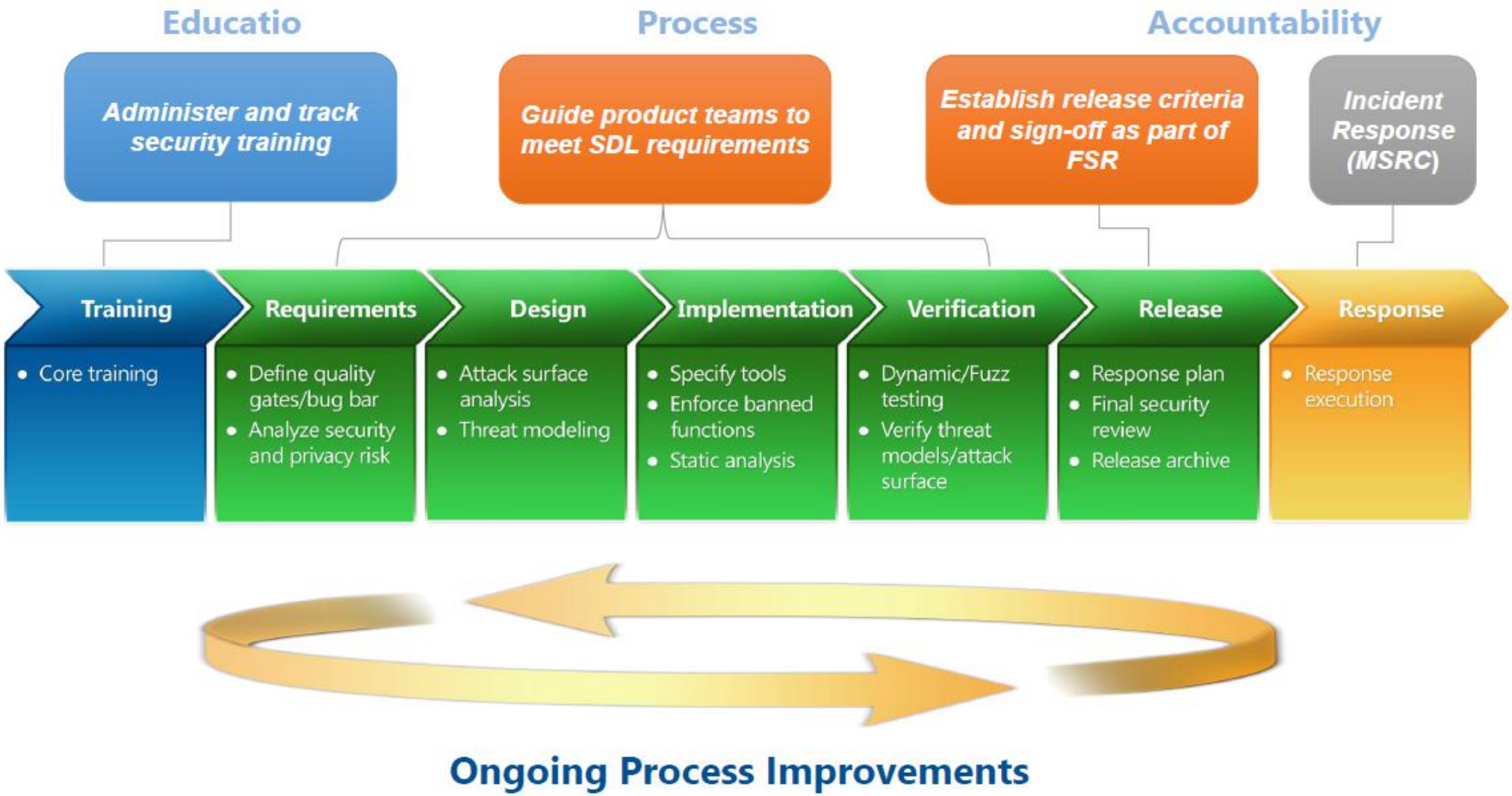
成本与收益

风险

合规

安世加

SDL体系建设实践|微软SDL



SDL体系建设实践|建设框架

目标导向

提升应用安全质量、满足监管合规要求、保障企业经营发展

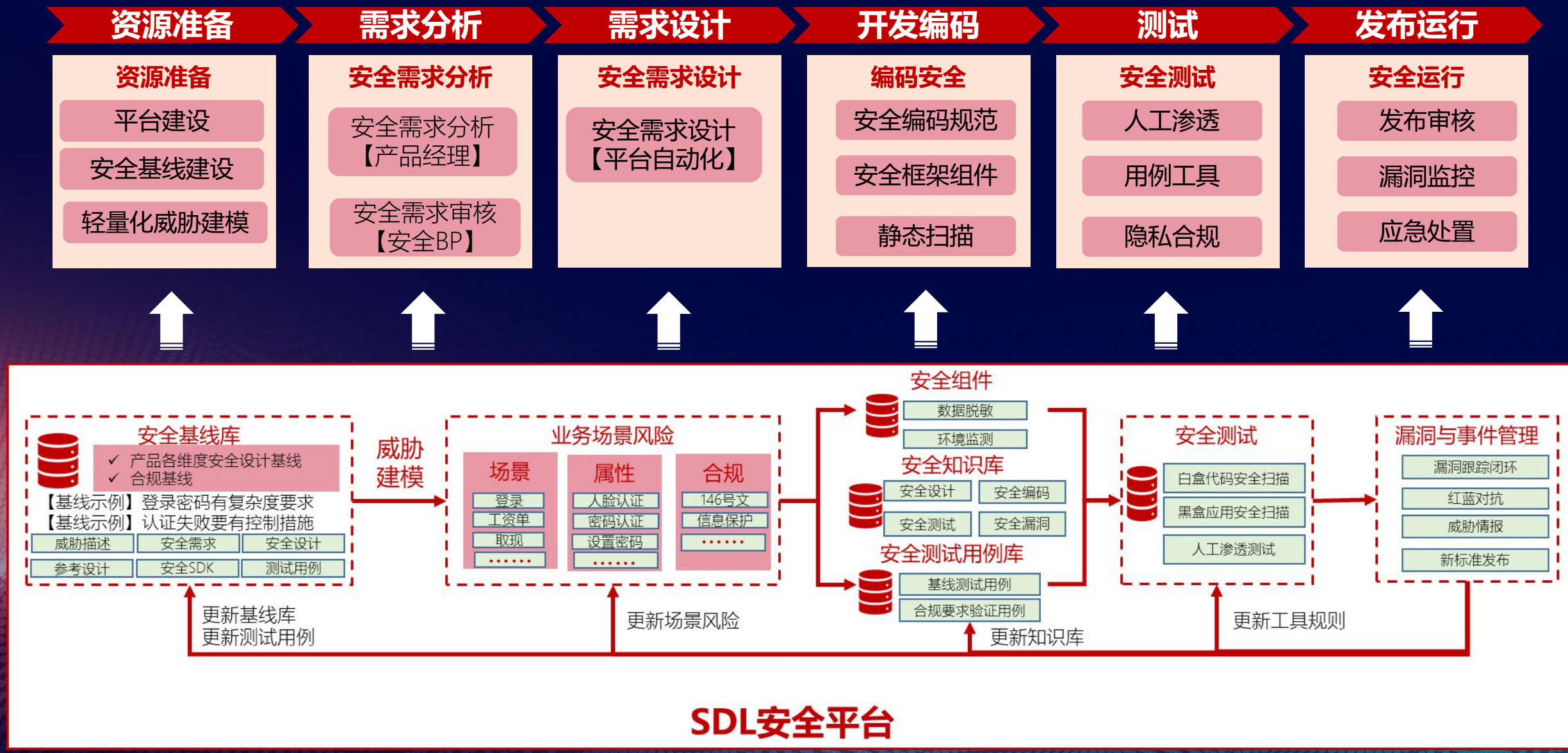
建设举措

- 通过制度流程的建设，建立全面的SDL体系，确保研发过程中各项安全举措有章可循、有据可依，确保举措有效落地执行
- 通过培训、知识库、能力考核举措，从安全职责、安全能力两个方面，建立覆盖产品、开发、测试不同岗位的人才体系，为SDL体系的落地执行提供必要条件
- 通过平台、组件、测试工具的建设，提供流程化、自动化能力，提升人员的工作效率、降低对人员安全能力的依赖，为研发安全管控体系的有效执行提供支撑

效果体现

- 通过内生合规举措，把重要的监管标准、合规规范中的研发相关要求，转成内部安全基线，在SDLC执行流程中实现这些要求，实现内生合规。
- 把监管标准、合规规范的原生要求录入安全基线库，借助安全管控平台，可生成合规排查任务。
- 有节奏逐步推广

SDL体系建设实践|建设成果

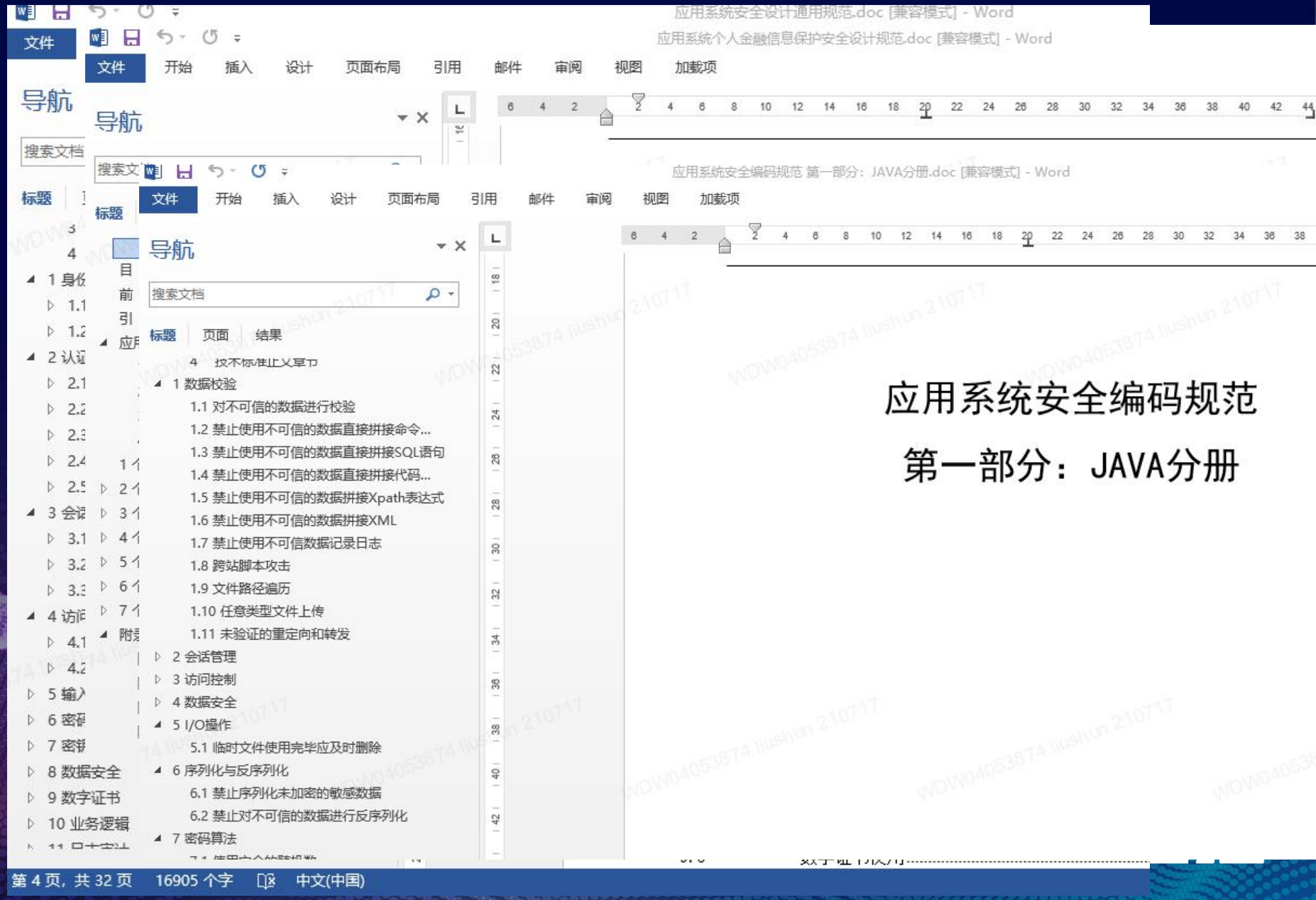


SDL体系建设实践|流程建设

安世加

SDL体系建设实践|制度建设

体系管理类
《软件安全开发管理细则》
《安全基线管理细则》
安全设计类
《应用系统安全设计通用规范》
《应用安全客户信息保护设计规范》
《API接口应用安全设计规范》
安全编码类
《Java语言安全编码规范》
《PHP语言安全编码规范》
《Python语言安全编码规范》
《JavaScript语言安全编码规范》
《C++/C语言安全编码规范》
平台安全类
《Android平台安全开发规范》
《IOS平台安全开发规范》
安全测试类
《安全测试管理细则》



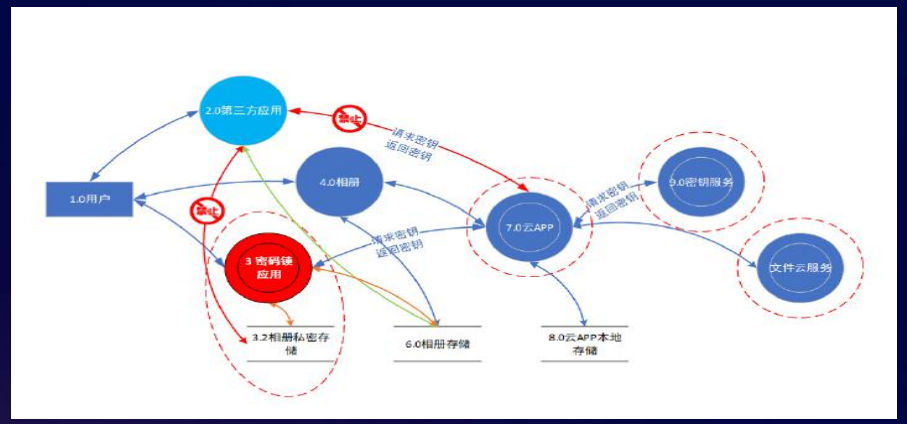
SDL体系建设实践|培训考试知识库

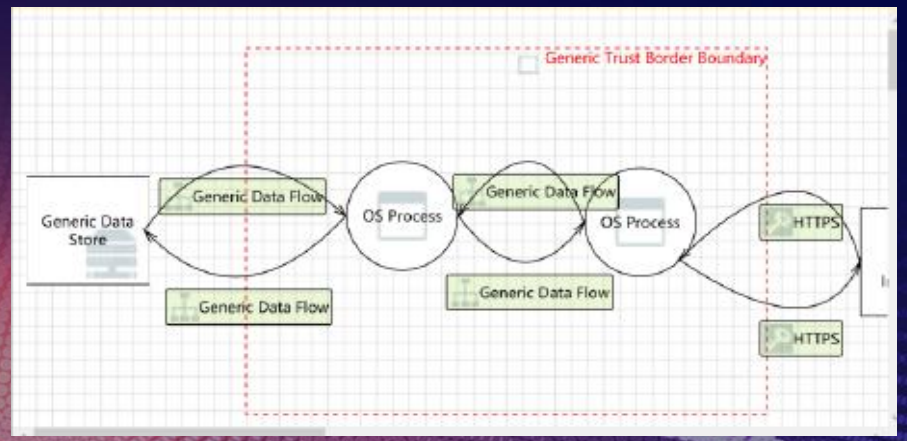
培训类别		考试类别	面向人群
SDLC管理体系类	《SDLC安全基础知识培训》	《安全意识》 《安全设计》 《Java安全编码》 《Android安全编码》 《IOS安全编码》 《安全测试》	安全团队、安全BP
安全设计类	《威胁建模培训》		产品、安全BP
	《安全需求分析与设计培训课件》		产品、安全BP
	《安全平台使用操作培训》		产品、安全BP
安全编码类	《Java安全编码培训》		开发、安全BP
	《移动应用开发安全培训》		开发、安全BP
安全测试类	安全测试技能培训		安全团队及其他
安全合规类	《安全合规培训》		安全团队、安全BP
研发中心入职网络安全培训	———		所有入职人员

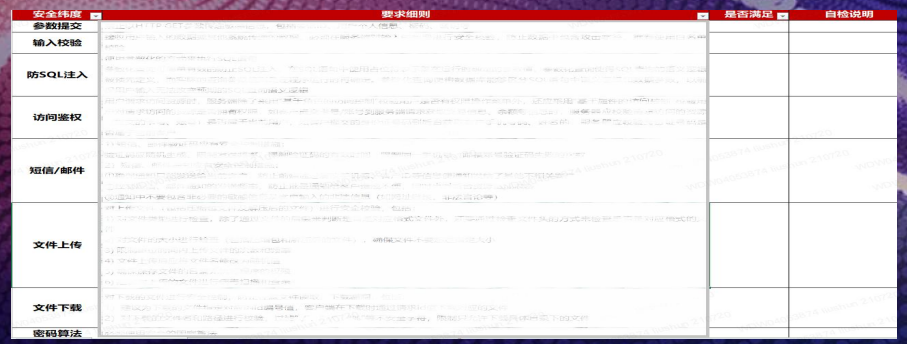
序号	标题	登记时间	登记人	状态
1	移动互联网应用程序（App）系统权限申请使用指引（征求意见稿）	2020-10-23 15:12:09		正常
2	中国金融移动支付 检测规范 第3部分：客户端软件	2020-10-23 15:13:05		正常
3	商业银行应用程序接口安全管理规范	2020-10-23 15:14:22		正常
4	金融分布式账本技术安全规范	2020-10-23 15:15:02		正常
5	个人金融信息保护技术规范	2020-10-23 15:16:16		正常
6	移动金融客户端应用软件安全管理规范	2020-10-23 15:16:58		正常
7	移动终端支付可信环境技术规范	2020-10-23 15:19:05		正常
8	网上银行系统信息安全通用规范	2020-10-23 15:20:00		正常
9	移动互联网应用程序（App）收集使用个人信息自评估指南（征集意见稿）	2020-10-23 15:22:17		正常
10	App违法违规收集使用个人信息行为认定方法	2020-10-26 10:56:13		正常

安世加

SDL体系建设实践|传统威胁建模





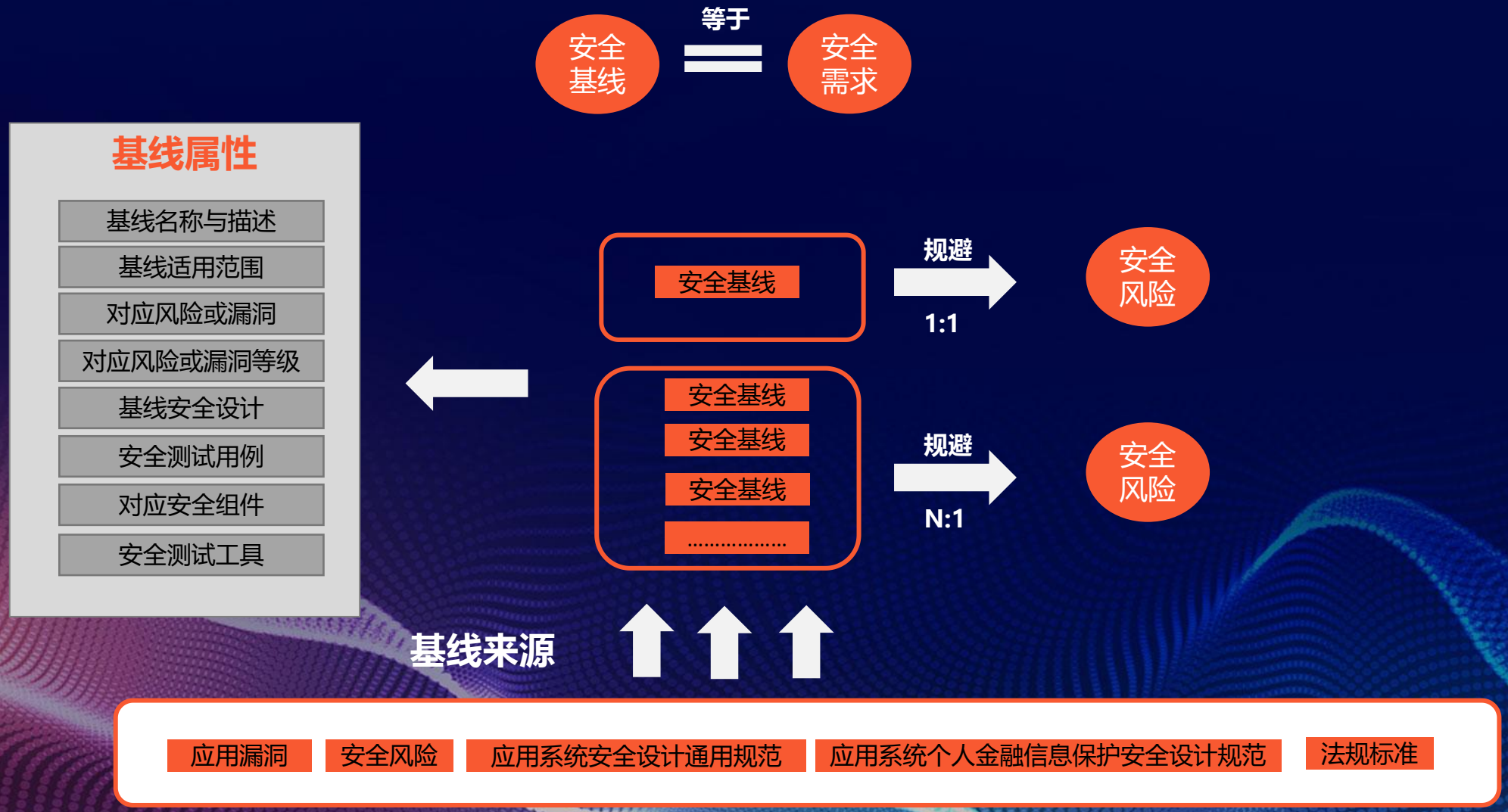


面临问题

- 模型复杂
- 专业能力要求高
- 花费时间长
- Checklist多研发团队不愿意执行
- Checklist少安全团队担心有风险

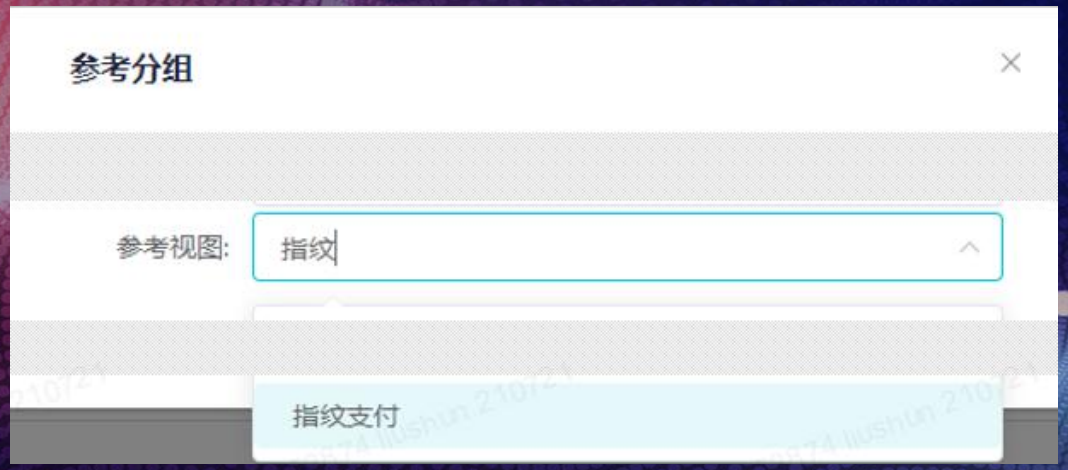
安世加

SDL体系建设实践|基于业务场景的轻量化威胁建模

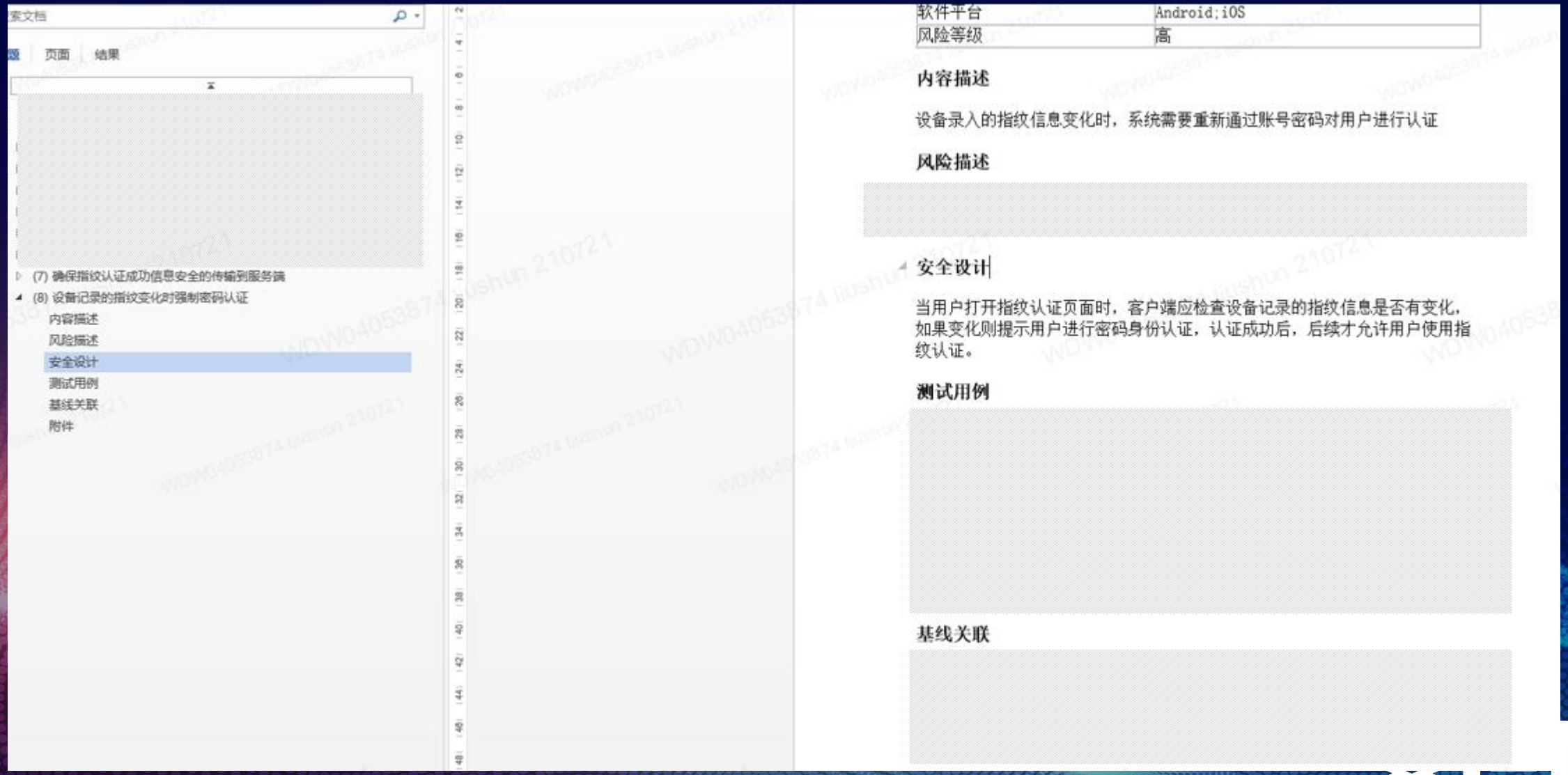


SDL体系建设实践|基于业务场景的轻量化威胁建模

SDL体系建设实践|基于业务场景的轻量化威胁建模



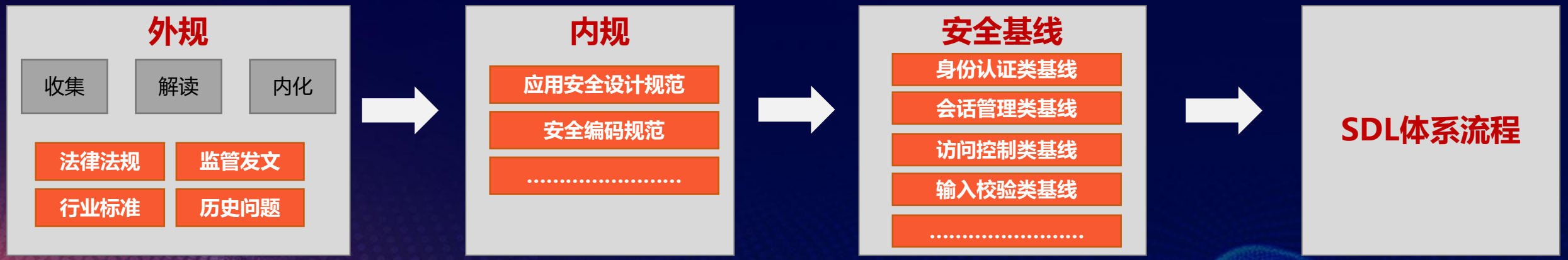
SDL体系建设实践|自动化安全概要设计



SDL体系建设实践|基于业务场景的轻量化威胁建模

安世加

SDL体系建设实践|内生合规



外规转内规、内规转基线，基线融入SDL流程！

安世加

SDL体系建设实践|统一开发框架

SDL体系建设实践|安全组件

APP	环境安全检查 通讯协议加密 安全软键盘 界面防劫持 加解密组件
客户端	加解密组件 密码控件

框架安全组件	
身份认证 会话管理	
漏洞防御	
加解密	
隐私保护	
文件日志	

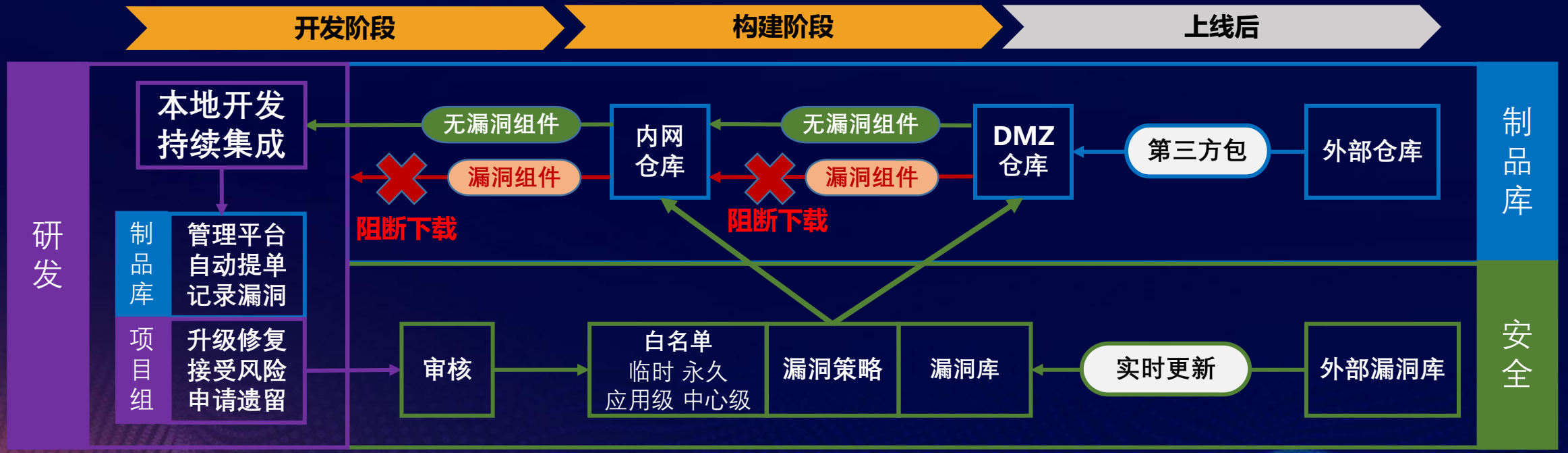
非框架安全组件	
身份认证 会话管理	
漏洞防御	
加解密	
隐私保护	
文件日志	

安世加

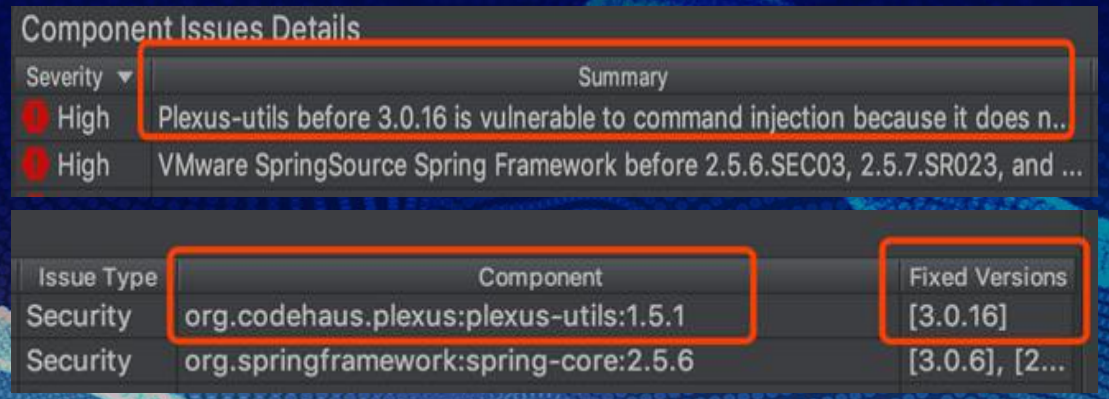
SDL体系建设实践|安全测试

为每个推广SDL应用配备固定的安全测试人员，针对每单新增需求开展以下安全测试。

SDL体系建设实践|开源安全管控



- **开发阶段：**开发人员在本地终端编译代码时，制品库根据漏洞策略禁止下载漏洞组件至本地终端。同时，IDE插件会提示漏洞信息。
- **构建阶段：**制品库根据漏洞策略禁止漏洞组件被下载，同时流水线构建失败，开发人员应根据提醒升级至修复版本。



IDE插件提示漏洞信息

SDL体系建设实践|安全运营

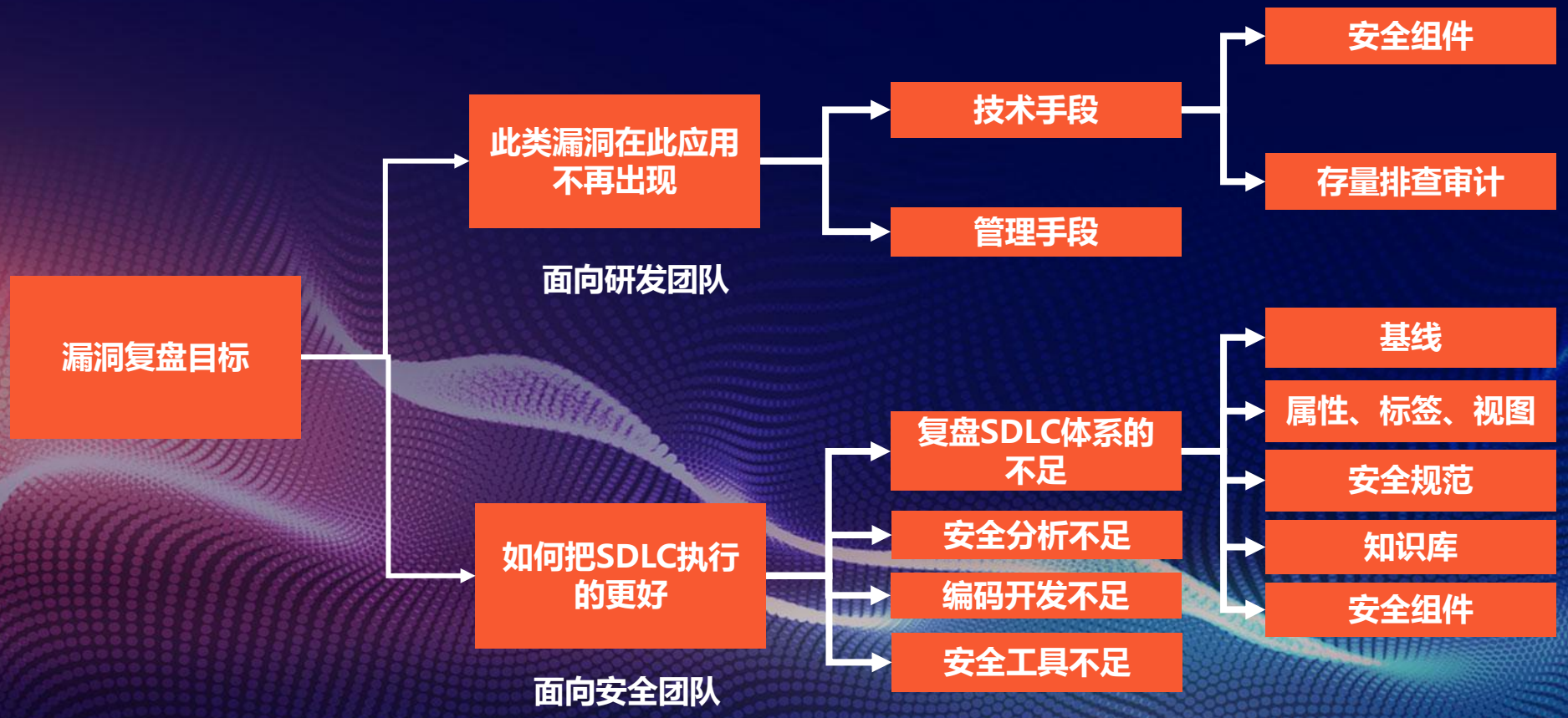
安世加

SDL体系建设实践|漏洞复盘

1 统一思想 认可价值

2 灵魂五问

3 找措施 定计划 保闭环



SDL体系建设实践|度量评价

如果你不能度量它，你就无法改进它。

度量维度

通过以下纬度评价SDLC执行效果：

- **需求覆盖度**
- **安全分析及时性**
- **安全分析准确性**
- **文档规范性**
- **代码规范性**
- **安全测试及时性**
- **安全测试准确性（漏检率）**
- **终极目标：**提升应用安全质量（生产安全漏洞降低率）★

安全分析节点执行度量

开发编码节点执行度量

安全测试节点节点执行度量

执行过程目标度量

执行结果目标度量

软件安全成熟度模型：BSIMM、SAMM

安世加

SDL体系建设实践|度量评价

统计分析

应用

人员

工具

漏洞

绩效考核

面向研发团队

面向个人

安世加

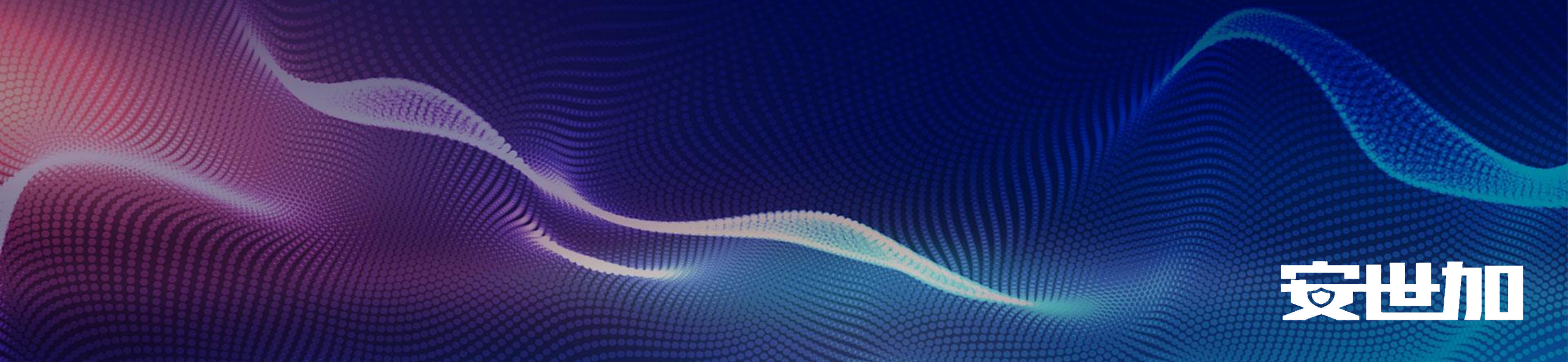
目录

CONTENTS

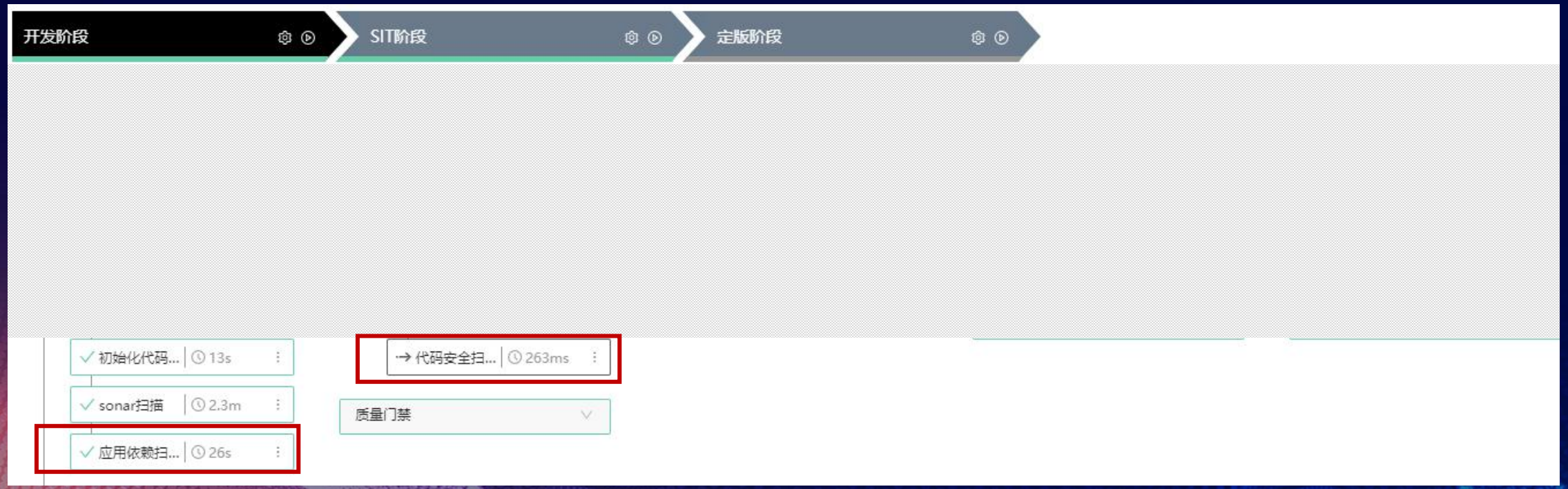
安世加

SDL持续演进

SDL or DevSecOps?



SDL持续演进

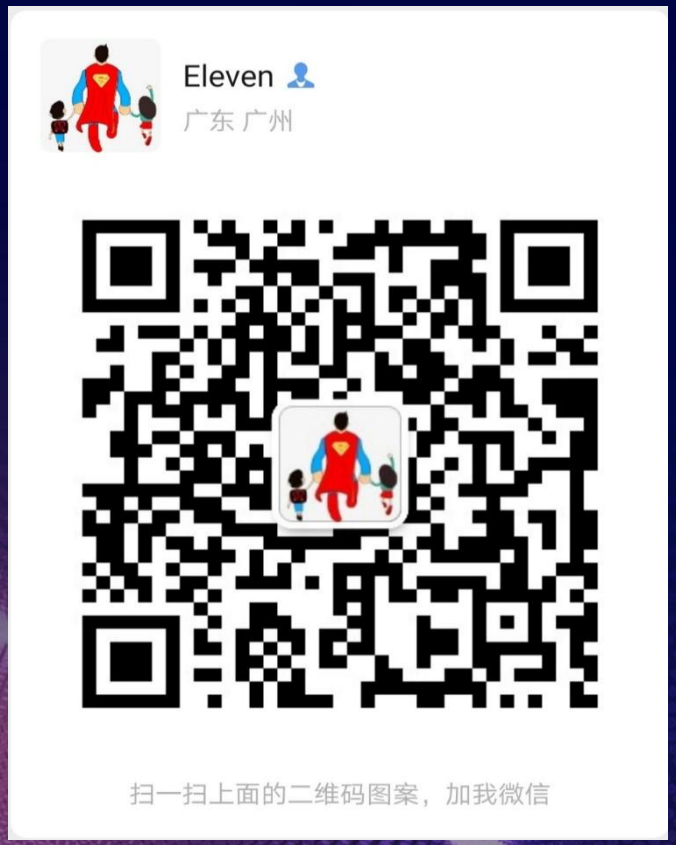

开发阶段
SIT阶段
定版阶段
初始化代码... 13s
sonar扫描 2.3m
应用依赖扫... 26s
代码安全扫... 263ms
质量门禁

SDL持续演进

支撑业务、融入业务、随业务变化而不断演进！

安世加

欢迎交流



招贤纳士

源码审计

安全开发

安全合规

安世加

安世加专注于安全行业，通过互联网平台、线下沙龙、峰会、人才招聘等多种形式，致力于创建亚太地区最好的甲乙双方交流、学习的平台，培养安全人才，提升行业整体素质，助推安全生态圈的健康发展。

官方网站：
https://www.anshijia.net.cn
微信公众号：asjeiss

安世加