CAICT 中国信通院　中国通信标准化协会 China Communications Standards Association

软件开发的安全痛点及IAST技术浅析

开源网安 裴伟伟

2021 可信云大会
2021 TRUSTED CLOUD SUMMIT
数字裂变 可信发展

开发人员对安全工作的误解

- 口若悬河
- 袖手旁观
- 阴魂不散
- 小题大做
- 无能为力

安全人员做开发安全的误区

- 势不两立
- 罪大滔天
- 怨声载道
- 独善其身
- 飞黄腾达

SDL的落地难和难落地

- 人微言轻
- 艺高胆大
- 不谙世事
- 按部就班
- 举步维艰

SDL的实践价值与效果

- 有的放矢
- 寸光寸金
- 一本十利
- 对精不贵多

安全开发痛点一：茫然无措

- 各自为政
- 毫不知情
- 蒙在鼓中
- 盛名难副

安全开发痛点二：不知所措

- 千里之堤毁于蚁穴
- 差之毫厘谬以千里
- 尽人事，知天命

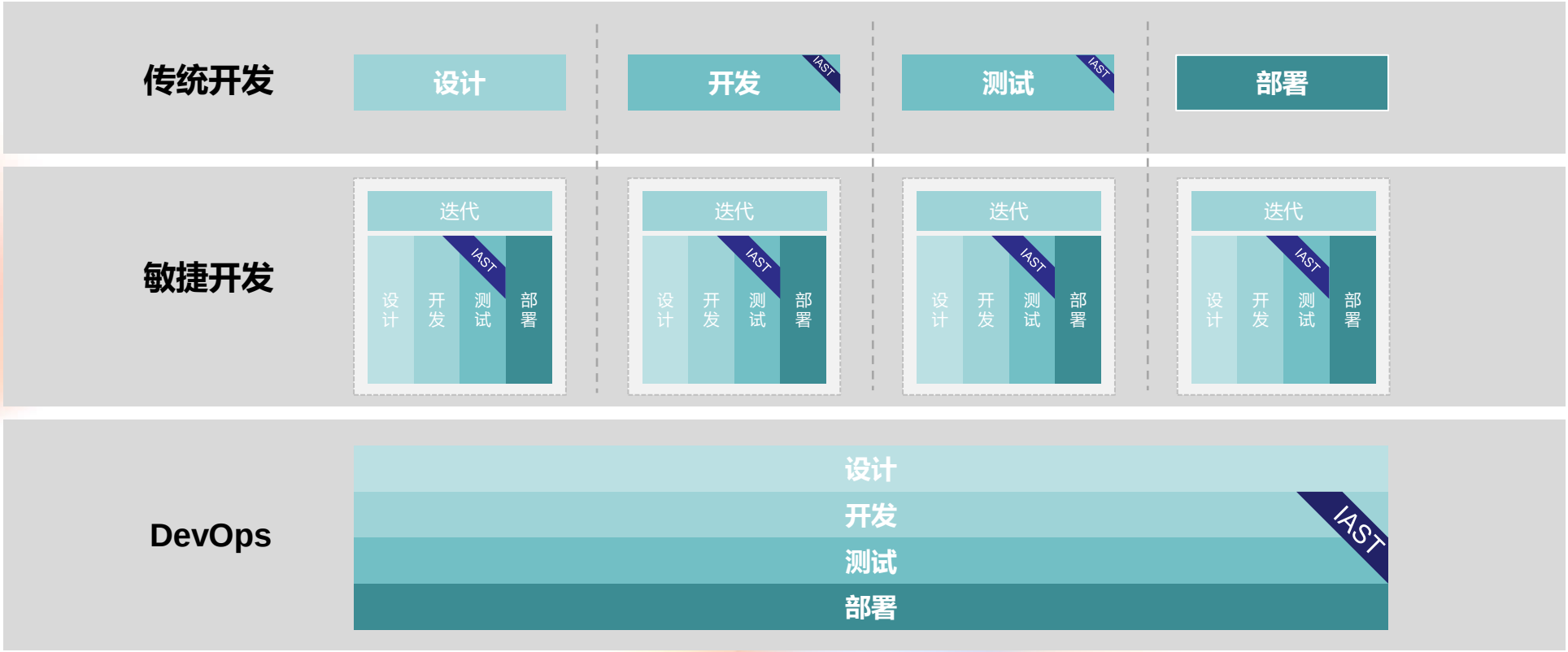
安全开发痛点三：仓皇失措

- 压力山大
- 杯水车薪
- 周而复始

欲善其事，必利其器

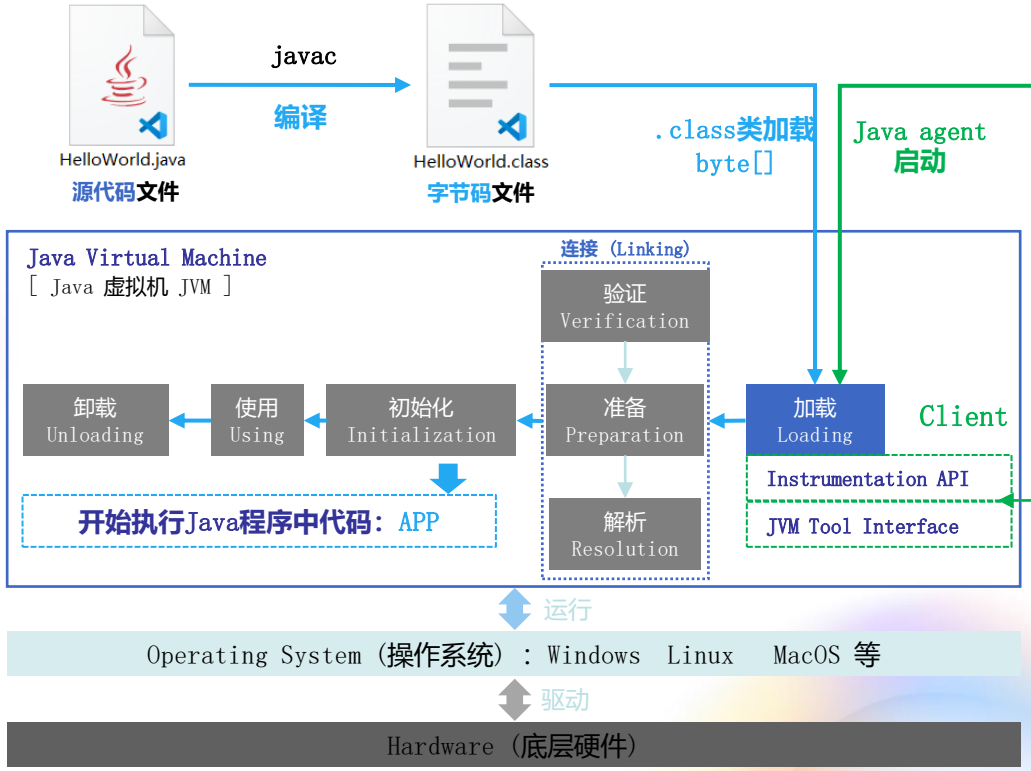
- SAST
- IAST
- DAST
- SCA

IAST的应用场景


传统开发
设计
开发
IAST
测试
IAST
部署
敏捷开发
迭代
设计
开发
测试
IAST
部署
DevOps
设计
开发
测试
部署
IAST

IAST的技术原理

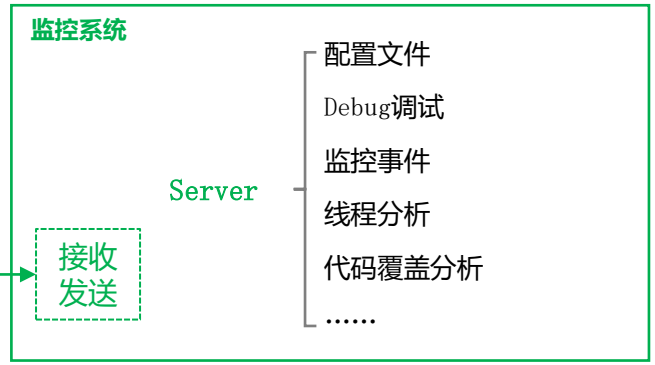
Java 编写的APP从编译到执行



Java Instrumentation 插桩技术

Java agent
启动

独立于应用程序之外的代理（agent）程序，
可监测和协助运行在JVM上的应用程序APP，
无侵入性，即不会改变源代码结构。

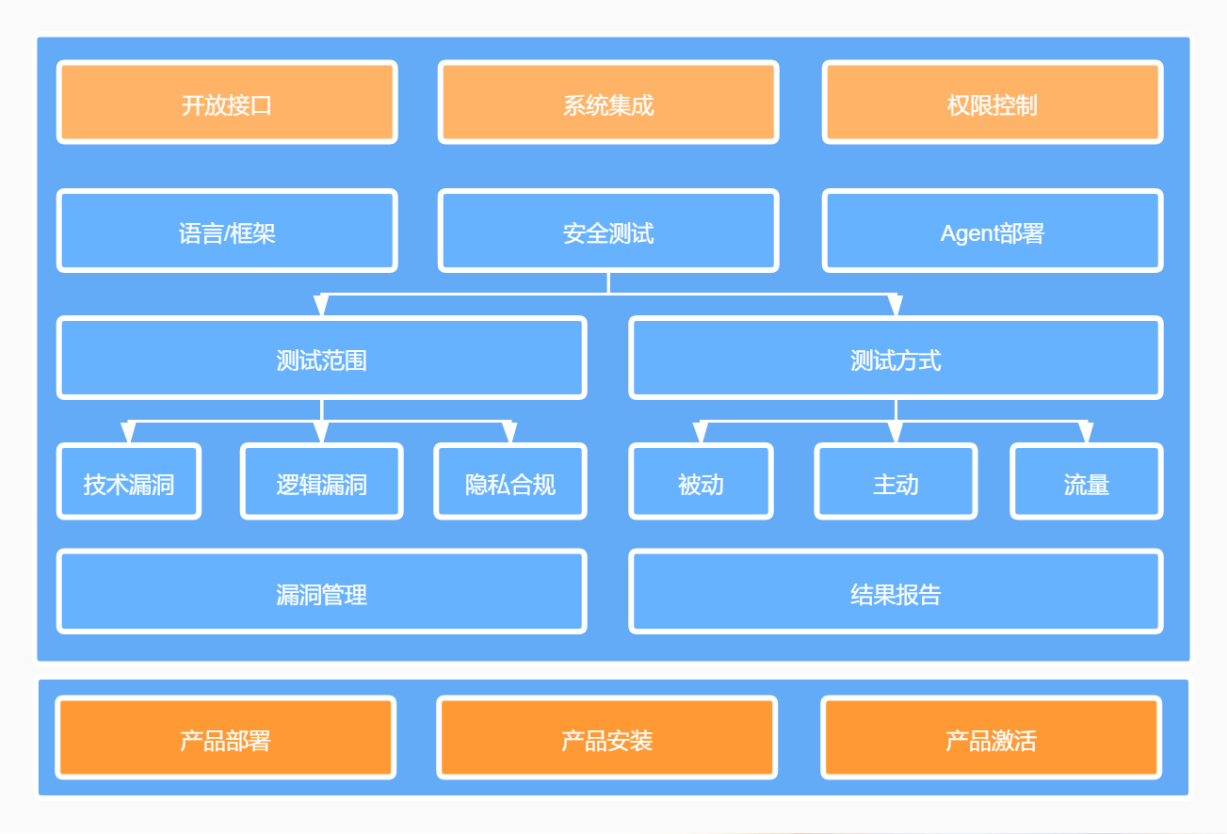


新特性：

Instrumentation API
Java SE 5.0 JDK1.5 2004-09-29 发布

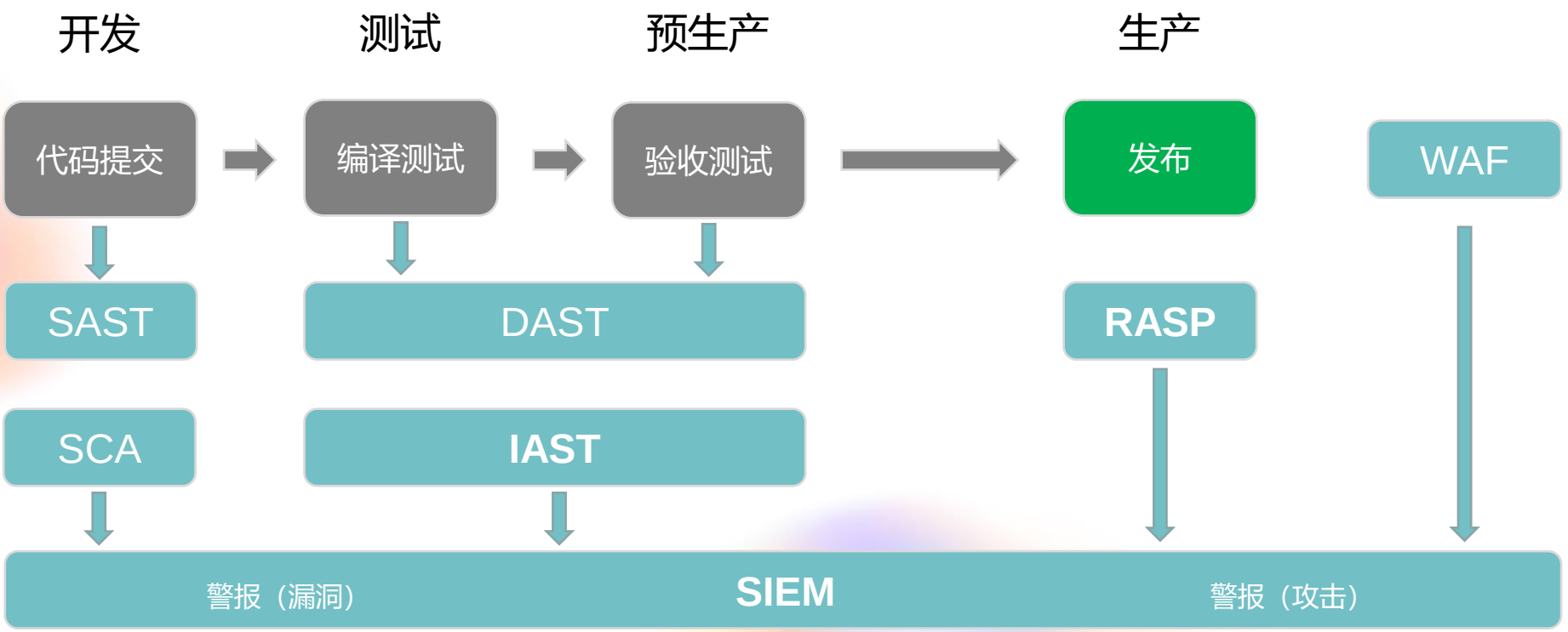
JVM Tool Interface（JVMTI）
Java SE 6.0 JDK1.6 2006-12-11 发布
JVM 暴露给用户扩展使用的接口集合

IAST技术的局限性



- 语言相关
- 性能影响
- 环境约束
- 部署成本

IAST与RASP的差别



THANKS!

2021
TRUSTED CLOUD
SUMMIT