K-Meetup

快手技术沙龙 · 攻防无界安全专场

快手应用安全演进之路

快手中学 KUAISHOU SCHOOL | 快手安全 KUAISHOU SECURITY

讲师介绍

- 廖新喜

- 大连理工大学毕业
- 快手Web安全负责人，原绿盟科技安全研究经理，8年安全攻防经验和2年甲方安全建设经验
- 2011-2014，三年安全开发经验，担任绿盟科技极光扫描器开发
- 2014-2019，五年安全攻防经验，国内各大安全峰会演讲嘉宾；专注于Web漏洞挖掘，尤其是Java反序列化漏洞，曾向RedHat、Apache、Amazon，Weblogic和阿里提交10余份RCE级别漏洞报告，被誉为国内Weblogic漏洞挖掘和反序列化漏洞挖掘的领导者
- 2019-现在，快手Web安全负责人，专注于甲方应用安全建设，对于漏洞收敛有独到的见解，所带领的项目《Java代码安全漏洞治理》获得了研发线质效提升奖

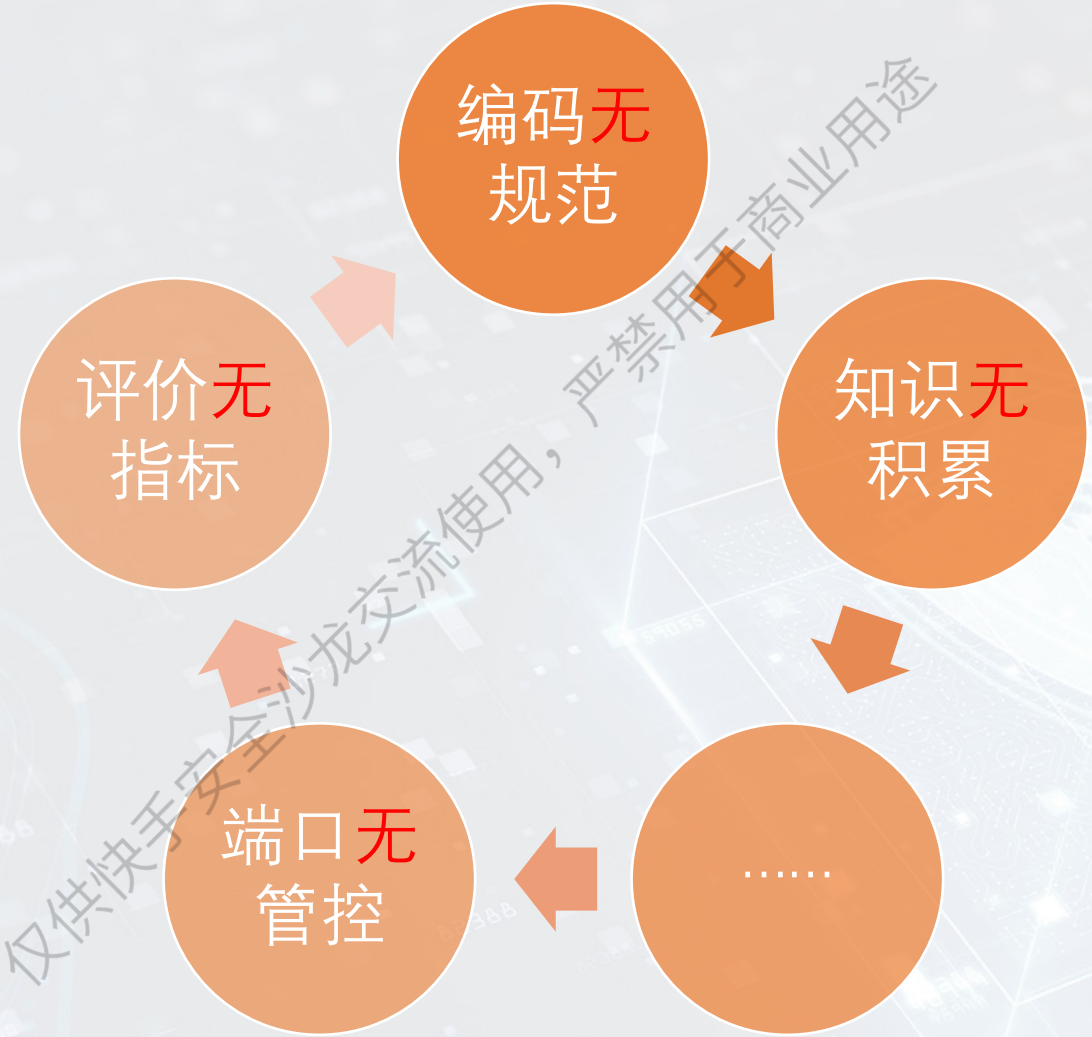
目录

一、作坊阶段

应用安全-作坊阶段

K-Meetup

2019年及以前



应用安全-作坊阶段

K-Meetup

2019年及以前

开发安全编码规范

建设外部SRC

建设内部SOC

建设黑盒扫描能力

建立评价体系

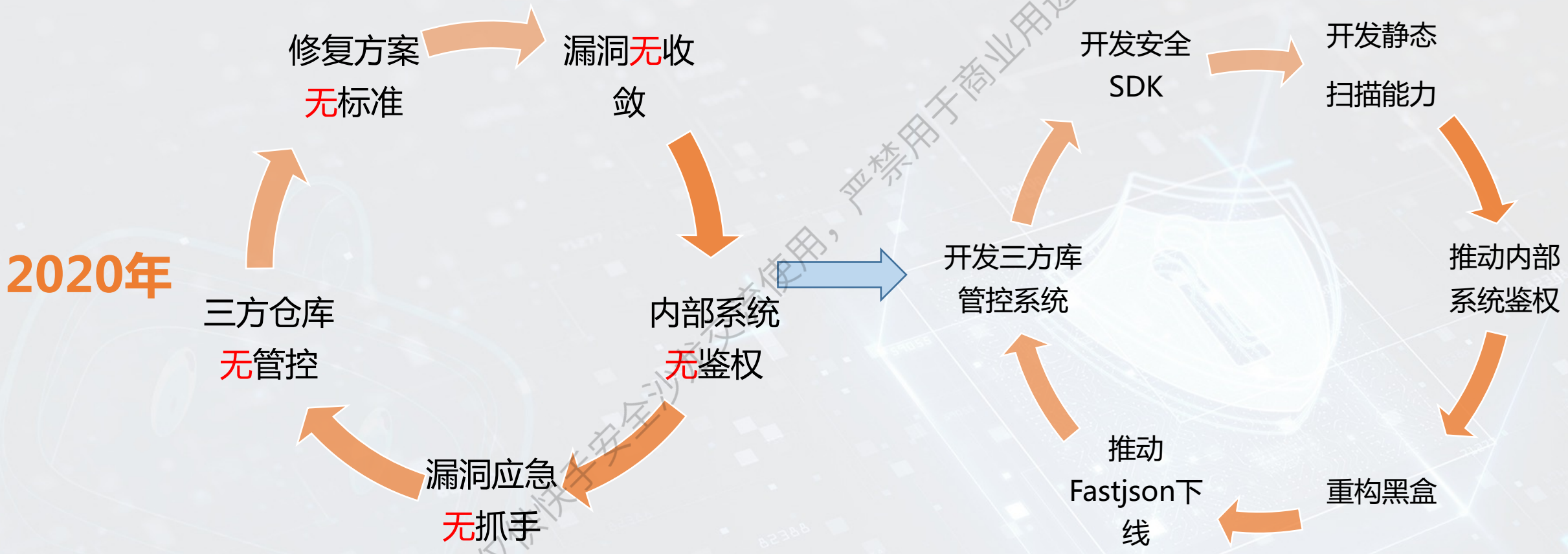
开展核心业务安全专项

保障重大活动

指标体系建设

二、自动化阶段

应用安全-自动化阶段



静态代码扫描能力建设

需求分析

- 核心业务Java
- Java后端占比46%
- 历史漏洞基础类型占比高
- DevOps快速发版，人工无法完成覆盖

规则迭代运营

- 编写自定义规则
- 覆盖历史漏洞，提升精准度
- 离线分析所有Java项目
- 优化规则

推动修复

- 开发自动化扫描系统
- 发送高层邮件，推动修复
- 自动化运营
- 接入代码Review平台

三方库漏洞收敛

供应链攻击日趋频繁

缺乏统一的管控机制

高危漏洞频发应急

Fastjson频频告急

Fastjson痛点

近三年漏洞指之王，3 次无任何限制RCE

安全意识差，测试代码泄露Poc

漏洞通报机制差，RCE漏洞不通报

全局安全风险

代码质量差

全司 3 次Fastjson应急

调研替代方案，形成Jackson和gson方案

增量

CheckStyle禁用

静态扫描规则扫描

存量

应急过程中完成主站替代

对外/对内业务收敛

第三方库漏洞管理平台

三、BP阶段

应用安全-BP阶段

K-Meetup

2021年

业务迅速发展
安全诉求高

漏洞发现靠后
修复成本高

业务漏洞突出
发现难度高

新型漏洞突出
治理难度高

……

应用安全-BP阶段

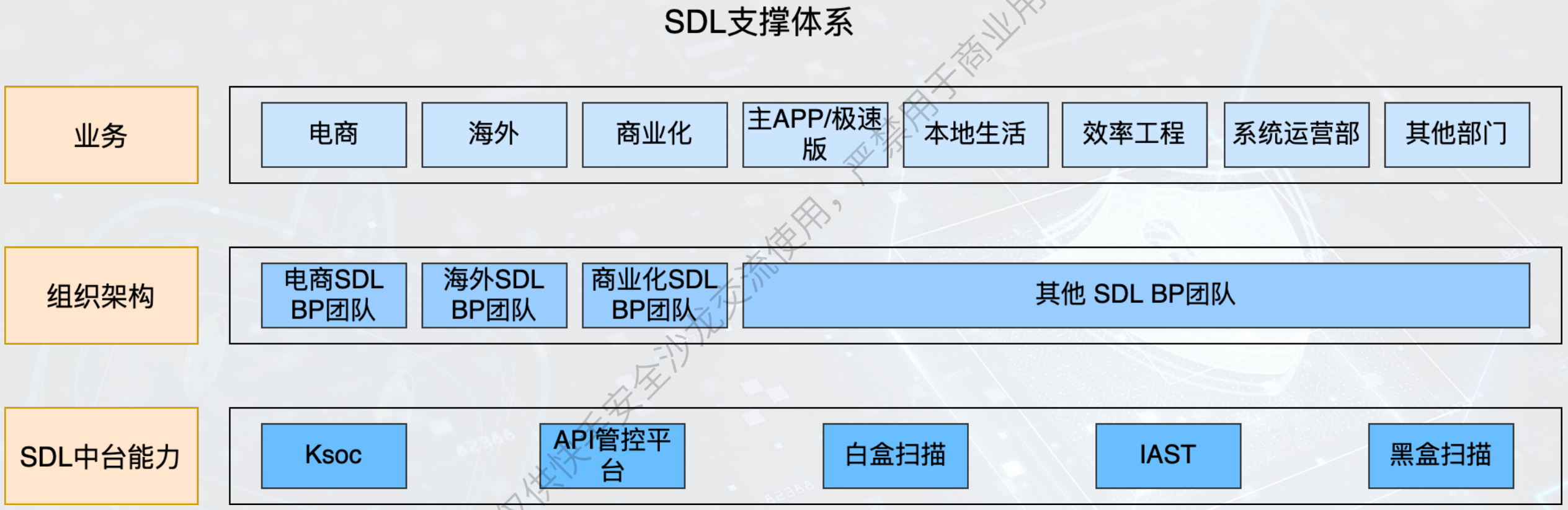
2021年

- 大搞BP机制
- 大搞通用漏洞收敛机制
- 大搞DevSecOps卡点
- 大搞IAST
- 大搞越权收敛
- 大搞应用安全三板斧迭代

漏洞收敛体系

需求/方案设计	研发	测试	上线	监控运营	
减少漏洞数		及时检出，及时修复，自动检出		复盘检验	阶段目标
万行代码漏洞率		自动化检出率 漏洞自检率&漏洞按期修复率			核心指标
培训考试强化	Java安全SDK	Java静态扫描	动态扫描	Docker扫描	动态扫描	端口扫描	DevSecOps卡点
IDE 插件	Maven 安全插件	三方依赖	IAST	域名管控	应急体系建设	质量体系打通	
设计安全建模	静态扫描赋能左移	安全测试平台	API管控平台	端口管控	SRC&安全众测		
前端漏洞收敛体系		账号漏洞收敛体系建设					专项治理
越权/资损漏洞收敛体系建设							
2021重点项目	静态扫描	动态扫描	IAST	DevSecOps			
初步建设	进一步完善&运营	已成熟运营					

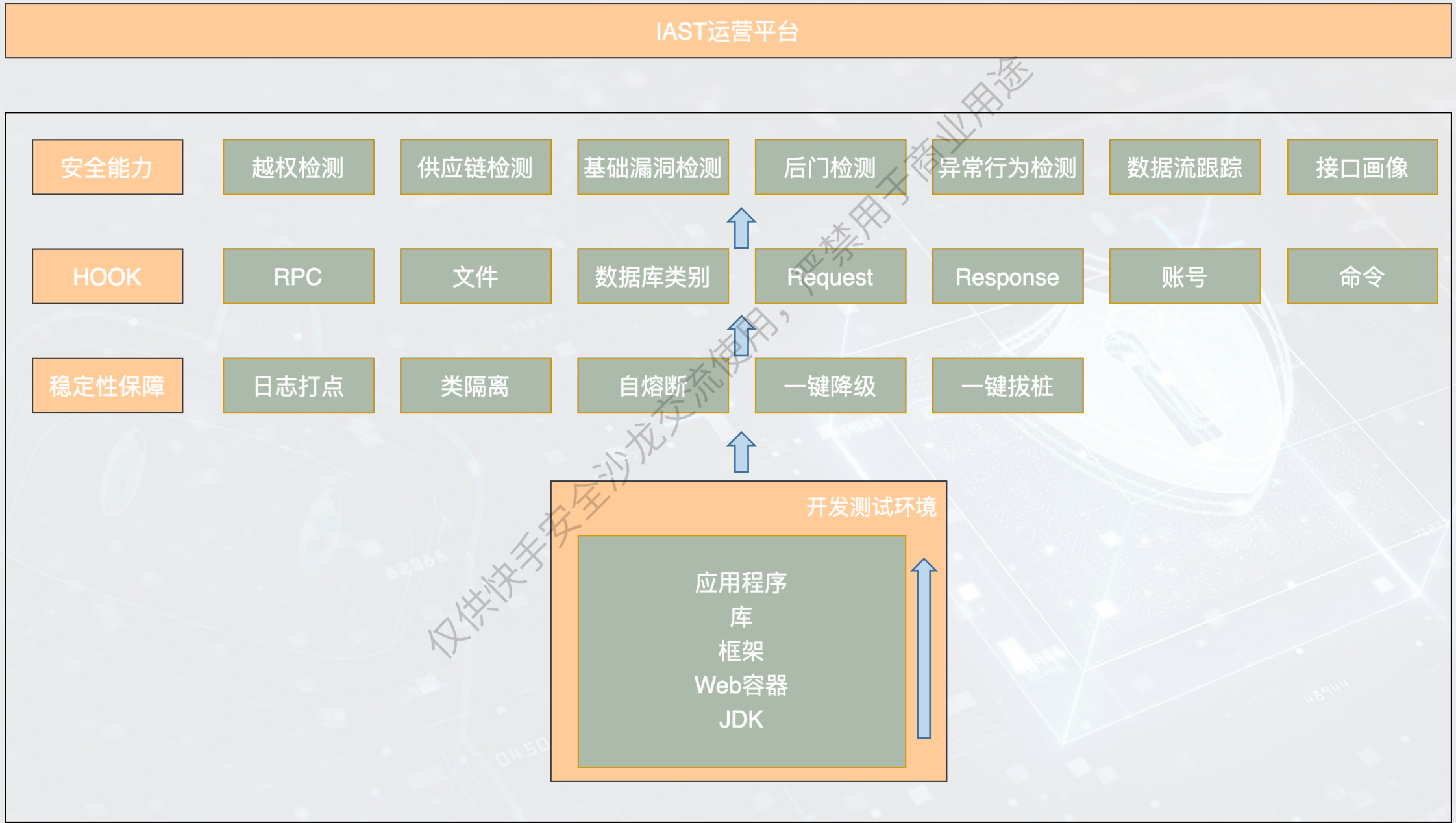
SDL BP架构



漏洞收敛漏斗

漏出5%以内，漏出数逐年降低

漏洞三板斧之IAST



快手中学 KUAISHOU SCHOOL | 快手安全 KUAISHOU SECURITY

THANKS

K-Meetup