SSTG
安全产品技术部

滴滴出行

滴滴SDL体系建设

--滴滴SDL从0-1建设历程

范世强

共建安全新生态
2020滴滴网络安全峰会

2020.12.17

目录

01 个人介绍

10余年安全从业经历：

- 国舜科技-安全服务
- CNCERT-渗透测试
- 阿里云-云产品安全
- 滴滴出行-SDL负责人

2017年加入滴滴，参与了整个滴滴SDL从0-1的建设过程。

02

滴滴SDL建设历程概览

01 滴滴SDL建设历程概览

SDL：Security Development Lifecycle 安全开发生命周期

开发生命周期	需求	设计	开发	测试	准入	上线	运营
滴滴SDL 2017	安全开发技术咨询	设计方案评估			代码安全评估		SRC漏洞运营
滴滴SDL 2018			提供安全开发规范	黑盒扫描 三方组件扫描	安全评估平台化 代码审计手册	商用代码扫描 黑盒扫描	漏洞月报
滴滴SDL 2019					安全评估自动化 自研代码扫描		资产库建设
滴滴SDL 2020	线上安全开发培训		自研代码扫描 提供安全SDK				漏洞月报自动化

03

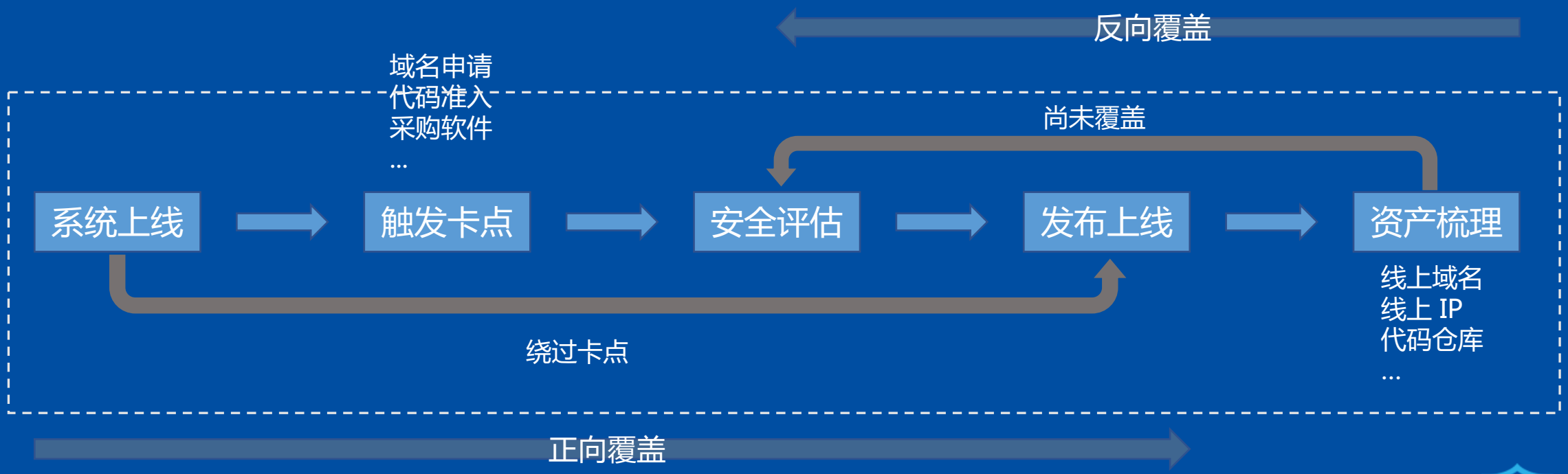
滴滴SDL建设历程详解

01 滴滴SDL 2017

背景：研发自由上线，SDL无感知；SRC安全漏洞多。

重点建设方向：

- 建立流程卡点
- 制定上线规范

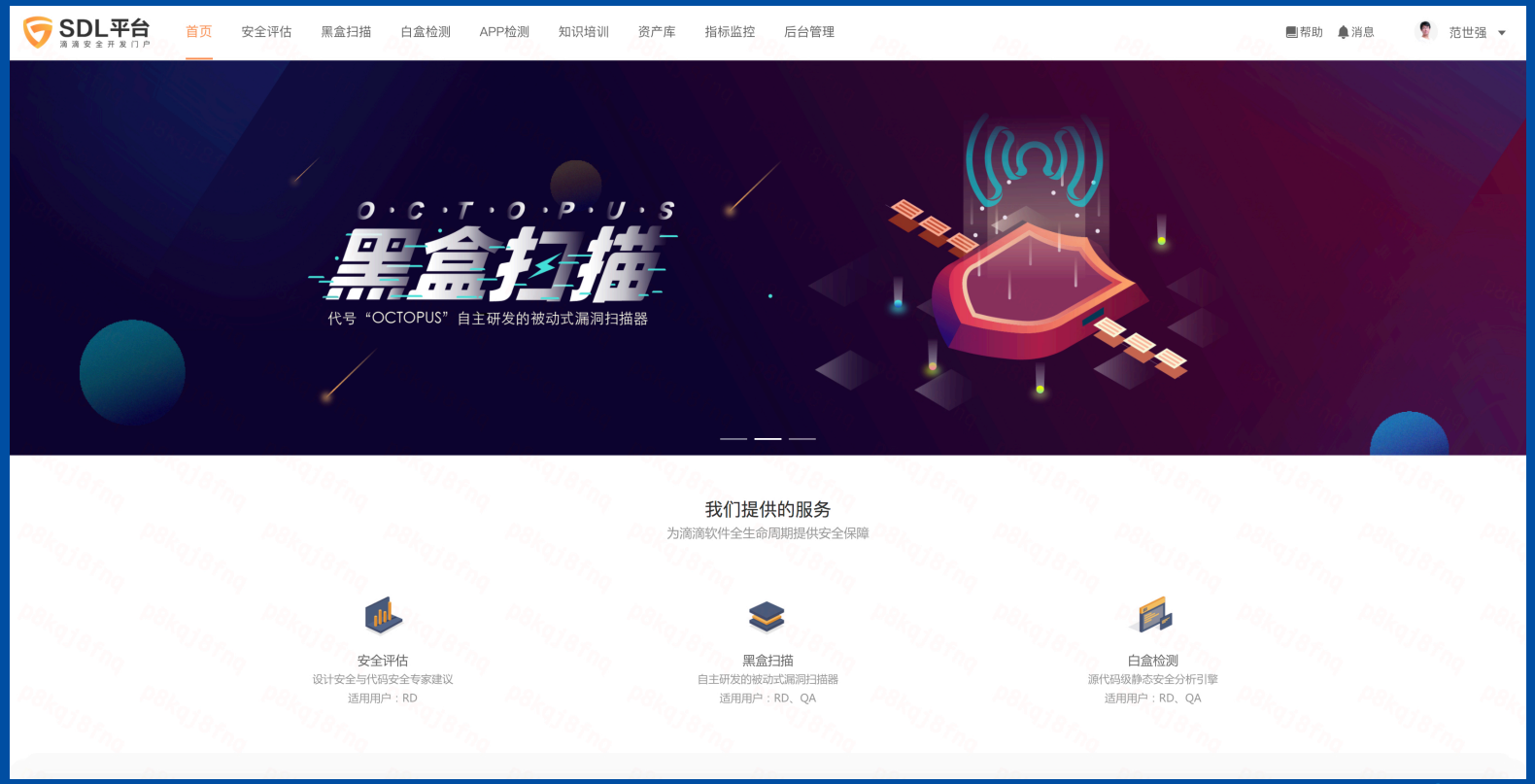


02 滴滴SDL 2018

背景：各项工作通过人肉开展、自动化程度低；过程依赖邮件、钉钉等方式，知识不能沉淀、各项工作无流程闭环。

重点建设方向：

- SDL一站式工作平台上线
  --数据沉淀、流程线上闭环
  --建设漏洞知识库及方案库
- 自研黑盒与测试环境打通
  --多渠道流量采集进行扫描
- 商用白盒与部署系统打通
  --自研检测规则
- 三方组件检测上线
  --打通构建平台拉取组件依赖

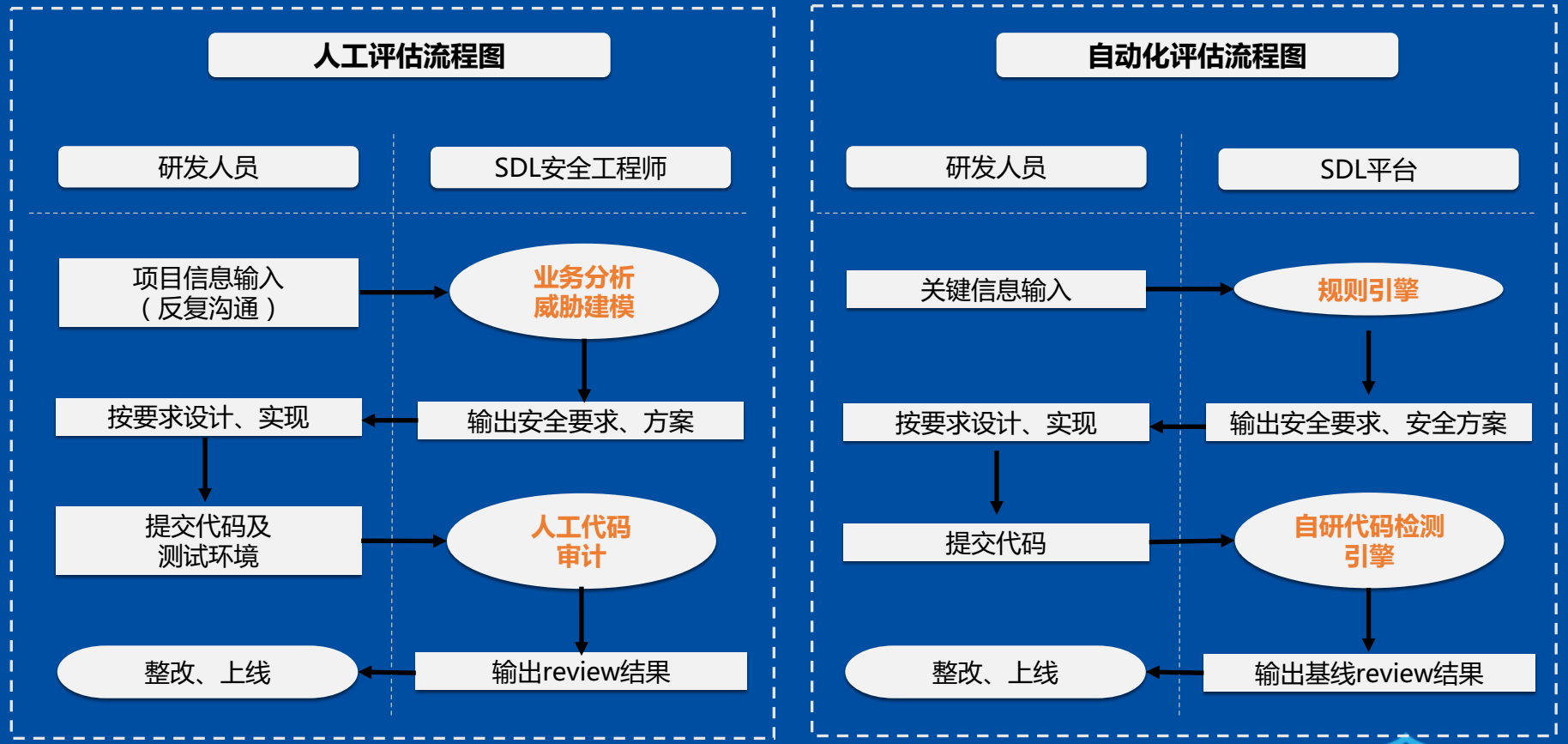


03 滴滴SDL 2019

背景：安全评估数量巨大，人效明显不足。

重点建设方向：

- 安全评估自动化
  --将各个场景的风险提炼成规则引擎
- 自研白盒扫描工具
  --基于图搜索技术
- 重新制定开发规范



04 滴滴SDL 2020

背景：线上漏洞下降，以逻辑漏洞为主；工具成熟度低、流程体验不足；研发安全意识仍有较大提升空间。

白盒+基线左移

■ 目的：
提升覆盖、降低后期修复成本

■ 方法：
① 自研白盒在CI/CD流水线中左移至构建阶段；
② 开发/测试阶段自助检测/修复；

研发安全教育

■ 目的：
提升研发安全编码

■ 方法：
① 将安全开发录制成系列短视频；
② 短视频按需组成课程包，推送给新研发；
③ 将短视频形式嵌入知识库；

安全SDK

■ 目的：
降低研发修复成本

■ 方法：
① 常用安全功能及漏洞修复标准化
② 提供安全SDK给研发使用

上线指标大盘

■ 目的：
提升运营效率

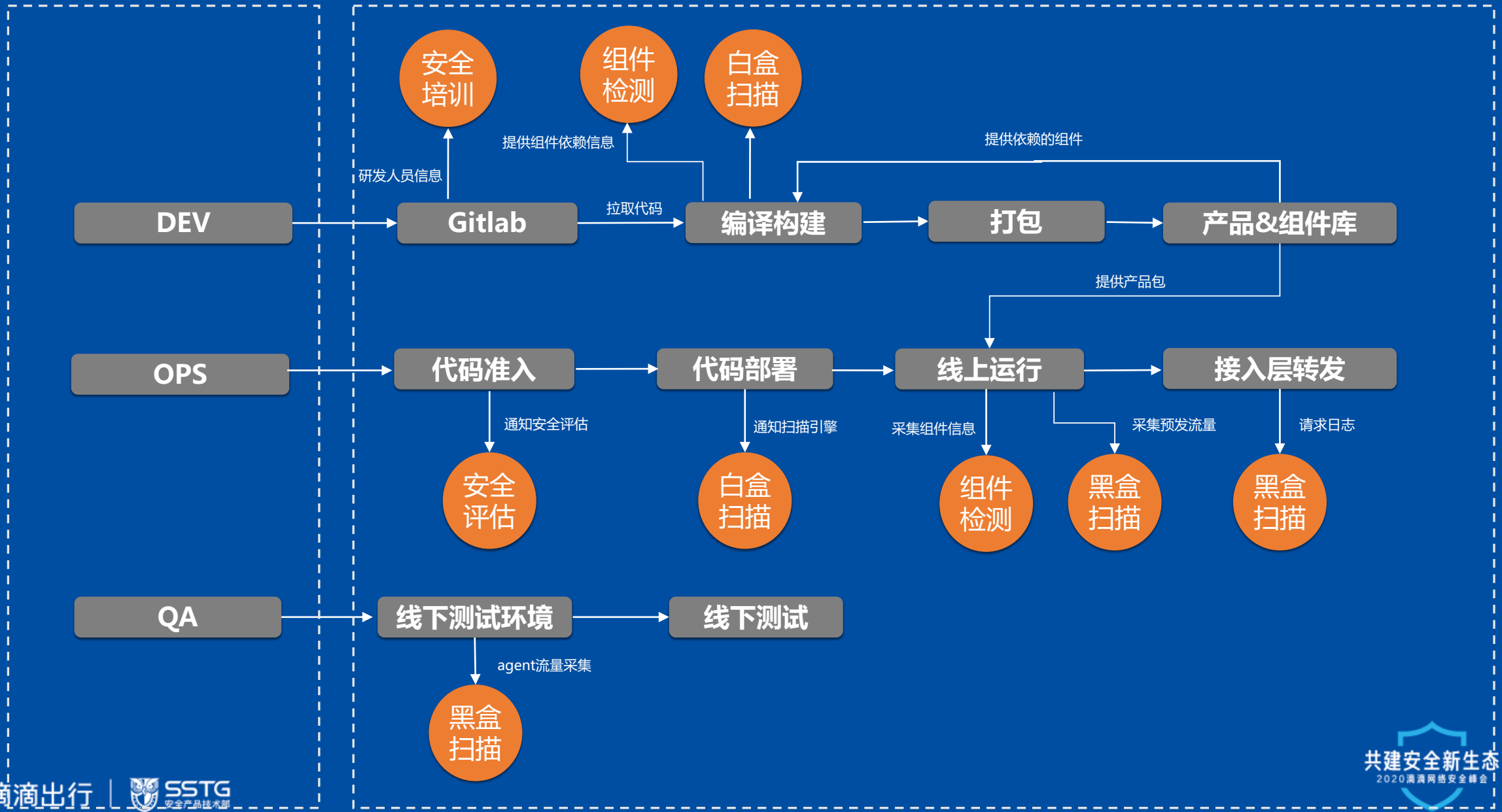
■ 方法：
① 将覆盖率、检出率修复率、漏洞分布、扫描时长、NPS等各项指标自动化计算
② 在SDL平台提供指标大盘

05 关于如何做好SDL我的几个观点

- 一开始不要研究多么牛逼的技术和工具，先把覆盖率搞上去。
- 做好资产建设，资产不清楚是很多问题的根源。
- 工具不在多、技术不需要多牛，对标问题是关键。
- 建立有效的指标评价体系，保证运营的有效性。
- 做好漏洞和事件的持续复盘、改进，发生事件不一定是坏事。
- 技术栈的复杂度、代码来源的多样性、互联网业务高频迭代给SDL带来了极大的挑战，把漏洞不是唯一的手段，也要多依赖安全培训、网络隔离、内外部蓝军、白帽子等其他手段。

04 滴滴SDL的现在与未来

02 滴滴SDL自动化能力部署



03 滴滴SDL的未来

降发生：

逻辑漏洞检测自动化

工具链+资产库打通

…

安全感：

Devsecops体系建设

赋能研发提升效率体验

…

招贤纳士：

欢迎对SDL有兴趣的同学加入我们，共建滴滴SDL…

微信：fsqsec

谢谢观看

THANK YOU