OWASP
Open Web Application
Security Project

基于DevSecOps平台的移动APP隐私合规实践

章亮

移动APP隐私合规背景介绍

《网络安全法》

第四十一条

网络运营者收集、使用个人信息，应当遵循合法、正当、必要的原则，公开收集、使用规则，明示收集、使用信息的目的、方式和范围，并经被收集者同意。网络运营者不得收集与其提供的服务无关的个人信息，不得违反法律、行政法规的规定和双方的约定收集、使用个人信息，并应当依照法律、行政法规的规定和与用户的约定，处理其保存的个人信息。

《 App违法违规收集使用个人信息行为认定方法》国信办秘字[2019]191号

共六大类，三十一条

1.未公开收集使用规则

2.未明示收集使用个人信息的目的、方式和范围

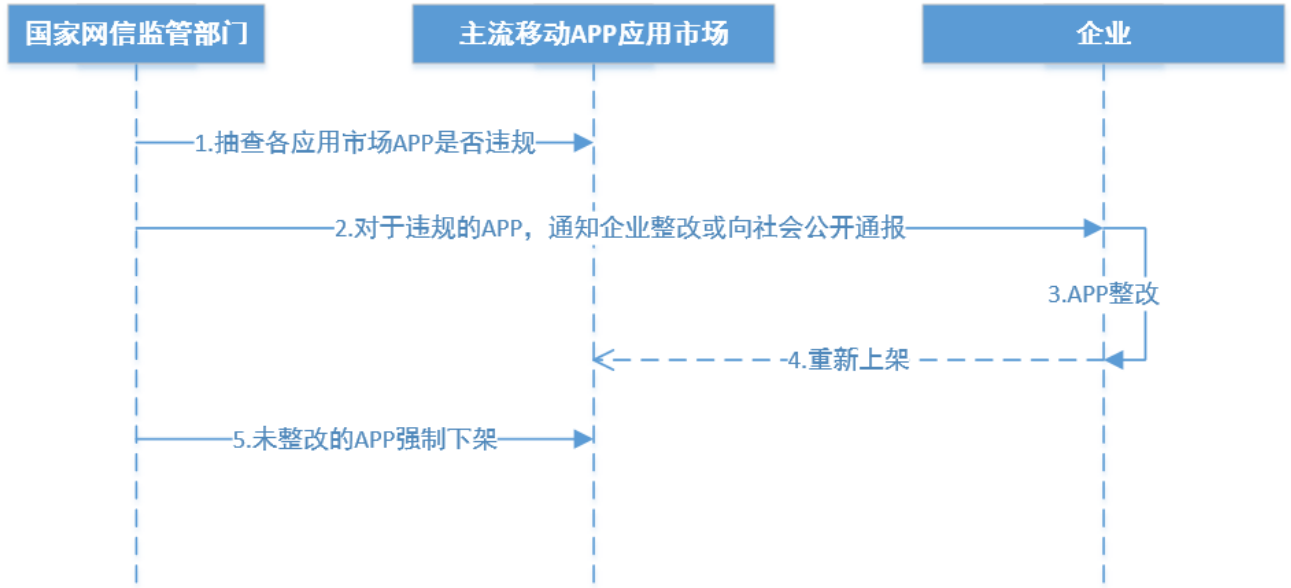
3.未经用户同意收集使用个人信息

4.违反必要原则，收集与其提供的服务无关的个人信息

5.未经同意向他人提供个人信息

6.未按法律规定提供删除或更正个人信息功能 或 未公布投诉、举报方式等信息

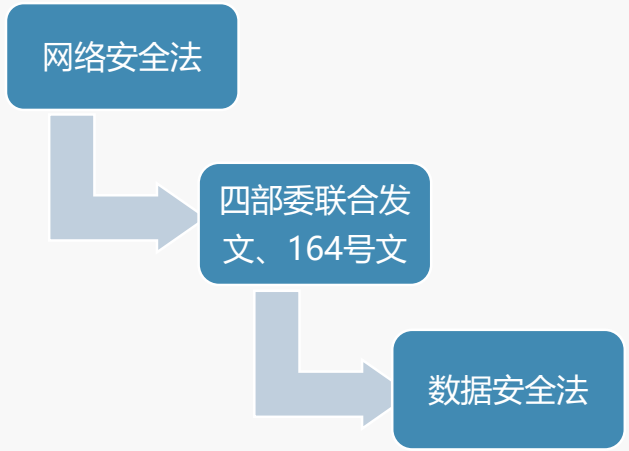
国家网信监管部门，依据《网络安全法》和《 App违法违规收集使用个人信息行为认定方法》，在全国范围内，开展移动APP个人信息保护专项治理行动，**重点整治《App违法违规收集使用个人信息行为认定方法》中明确要求的六大类问题**，为了满足监管要求，企业需要在合规的前提下开展业务活动，这就是移动APP隐私合规的含义。



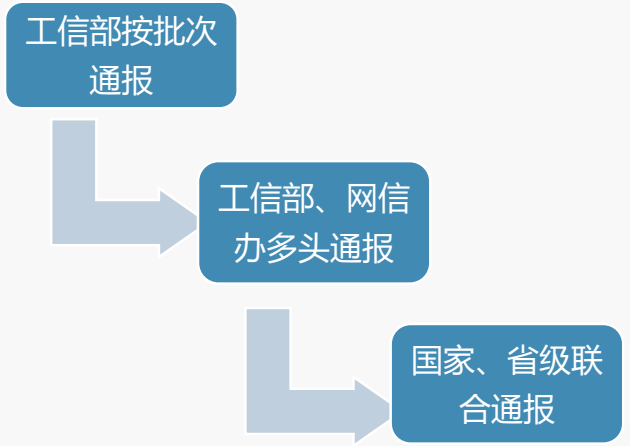
移动APP隐私合规背景介绍

外部监管力度持续加码下通报频发，内部常态化管理机制尚未形成

国家层面的网络安全立法不断推进



监管部门通报和处罚力度不断加大



当前主要问题

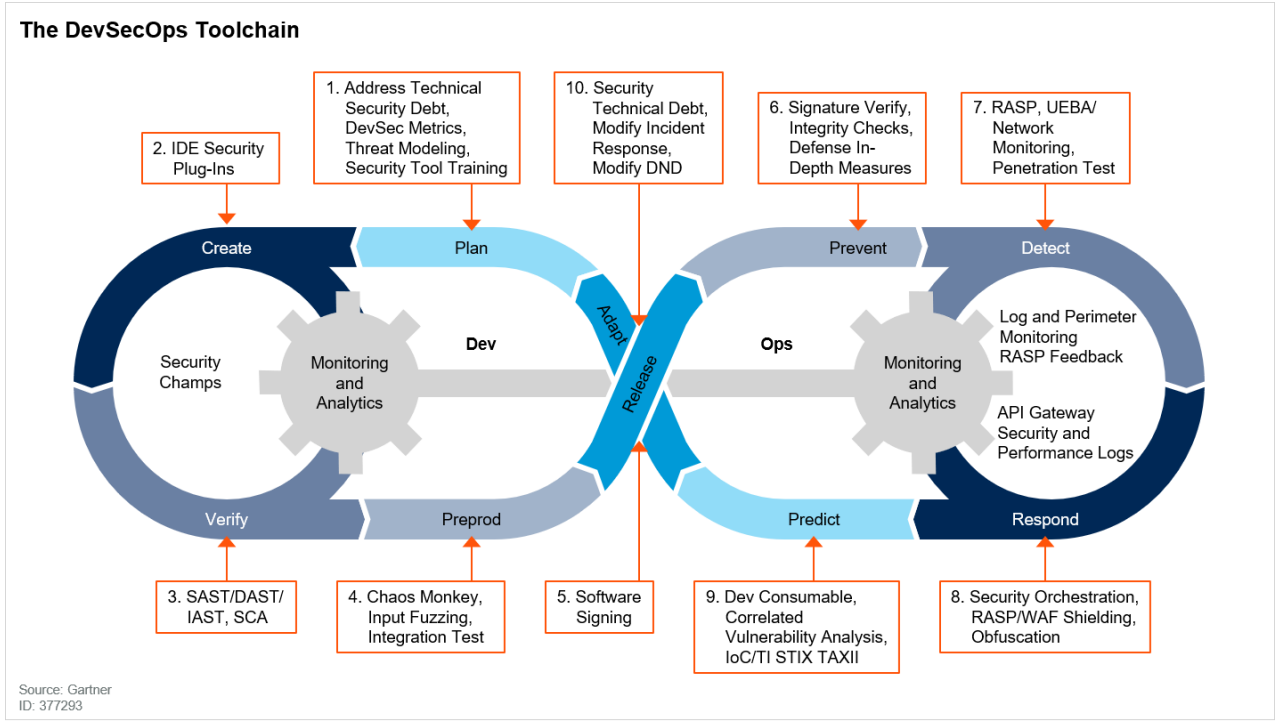
业务视角： 业务侧想做但不知道该怎么做？比如管理卡点如何设置、合规检测、自动化工具等；
业务不想做如何去管控?

合规视角： 如何审视当前APP隐私合规管理现状？比如哪些项目里有APP、哪些版本做过合规、应用市场上架情况如何等

DevSecOps背景介绍

最早由Gartner在2012年首次提出，它是一种糅合了开发、安全及运营理念的全新安全管理模式。

- **协作共识**：每一个项目都不是纯安全部门的事，是安全和产品、研发、测试、运维等部门一起参与的项目，每一个人皆为安全负责
- **安全工作左移（Shift Left）**：通过在软件开发早期融入安全环节来降低解决问题的成本
- **柔和嵌入现有开发流程体系**：并将安全工作导入现有的开发工作流程和工具中，借助“黄金管道”将高度自动化的安全工具链融入其中。



移动APP隐私合规落地挑战

业务方难点

01

- 想做但不知道该怎么做?
- 什么时候开始做?
- 如何衡量做的效果?
- 是否有工具支持合规检测等

管理方难点

02

- 业务方不想做我怎么知道?
- 如何审视当前APP隐私合规管理现状？
- 哪些项目里有APP?
- 哪些版本做过合规检测?
- 哪些应用市场上架了APP等

基于DevSecOps平台的APP隐私合规解决方案

打通上下游管控流程，依托平台运营驱动业务隐私合规

立项阶段

01 解决“哪些项目里有移动APP”的问题

- 以立项流程为抓手，从源头管控移动APP的开发

项目管理：项目立项 → 收集移动APP信息

安全平台：同步安全平台

开发阶段

02 解决“哪些版本做过合规检测”的问题

- 结合CI/CD数据，跟踪移动APP开发版本迭代信息

DevOps：CI/CD

DevOps：代码提交记录

DevOps：构建记录

安全平台：数据分析

发布阶段

03 解决“缺少自动化合规检测工具”的问题

- 根据数据分析结果，触发自动化合规检测工单，跟踪流程闭环；对于重点APP设置卡点

工单系统：合规检测工单

自动化合规检测平台：自动化合规检测

自动化合规检测平台：分析报告

工单系统：工单闭环

运营阶段

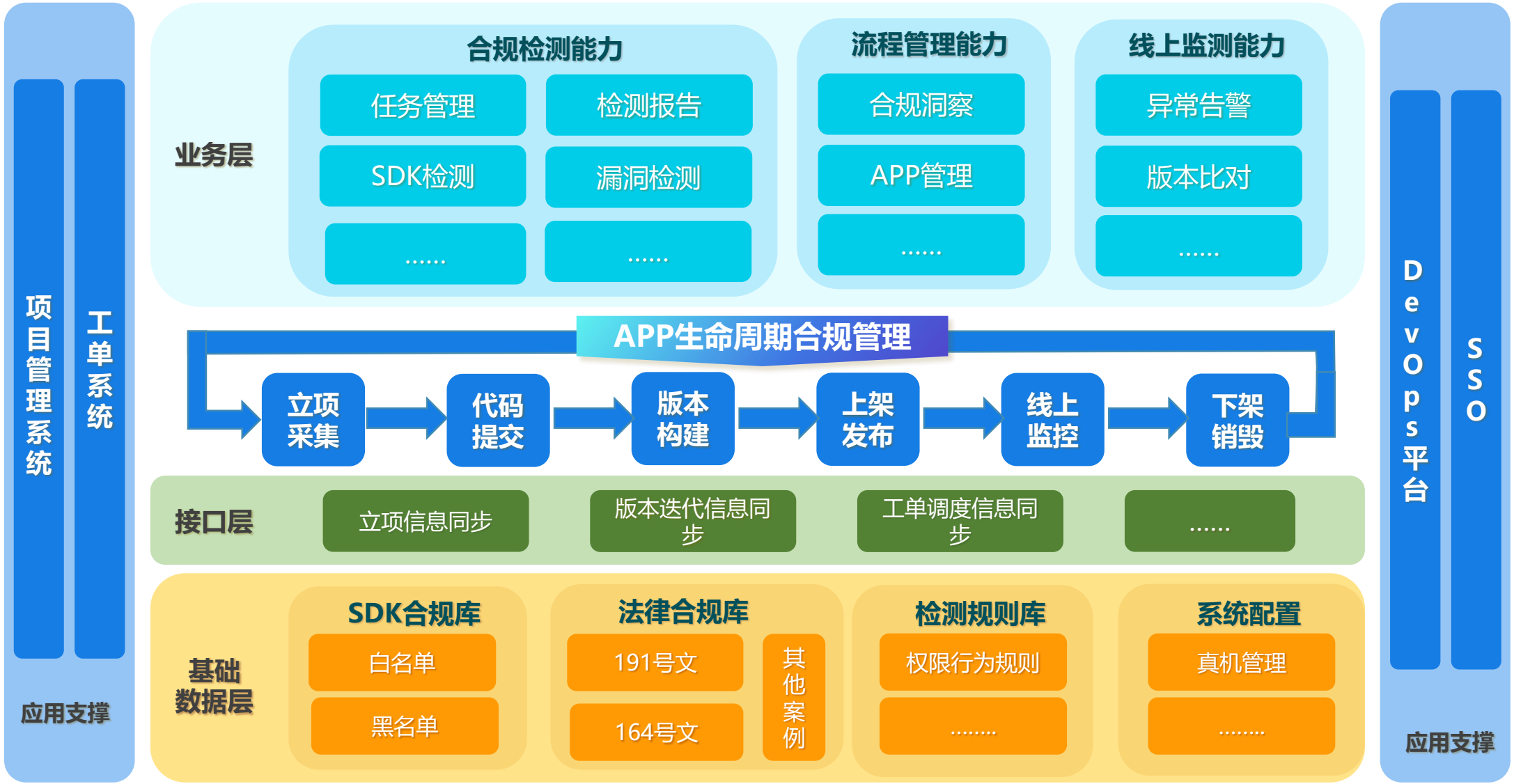
04 解决“应用市场上架后监控和发现”的问题

- 监控应用市场发布情况，发现漏网之鱼并预警，触发工单流程，跟踪流程闭环

第三方服务API、APP 爬虫 → APP指纹比对 → 发现漏网之鱼 → 触发合规检测工单流程

APP合规监测平台

平台功能介绍


项目管理系统
工单系统
应用支撑
业务层
合规检测能力
任务管理
检测报告
SDK检测
漏洞检测
……
……
流程管理能力
合规洞察
APP管理
……
线上监测能力
异常告警
版本比对
……
APP生命周期合规管理
立项采集
代码提交
版本构建
上架发布
线上监控
下架销毁
接口层
立项信息同步
版本迭代信息同步
工单调度信息同步
……
基础数据层
SDK合规库
白名单
黑名单
法律合规库
191号文
164号文
其他案例
检测规则库
权限行为规则
……
系统配置
真机管理
……
DevOps平台
SSO
应用支撑

实际落地情况

将产品的生命周期分为**立项**、**编码**、**测试**、**发布**、**运营**阶段。

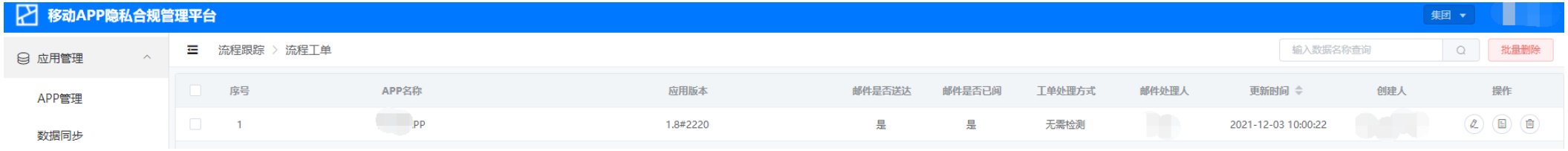
- **立项阶段**：打通集团立项流程，收集包含APP的项目信息至隐私合规平台
- **编码阶段**：打通集团DevOps流程，收集APP的构建版本信息

实际落地情况

- **测试阶段**：将安全活动融入到CI/CD流水线中，以后端流水线为例，上线之前会进行安全评测，包括隐私合规测试。同时流水线可编辑、配置，后续可以按需加入更多的自动化扫描或者其他安全活动。

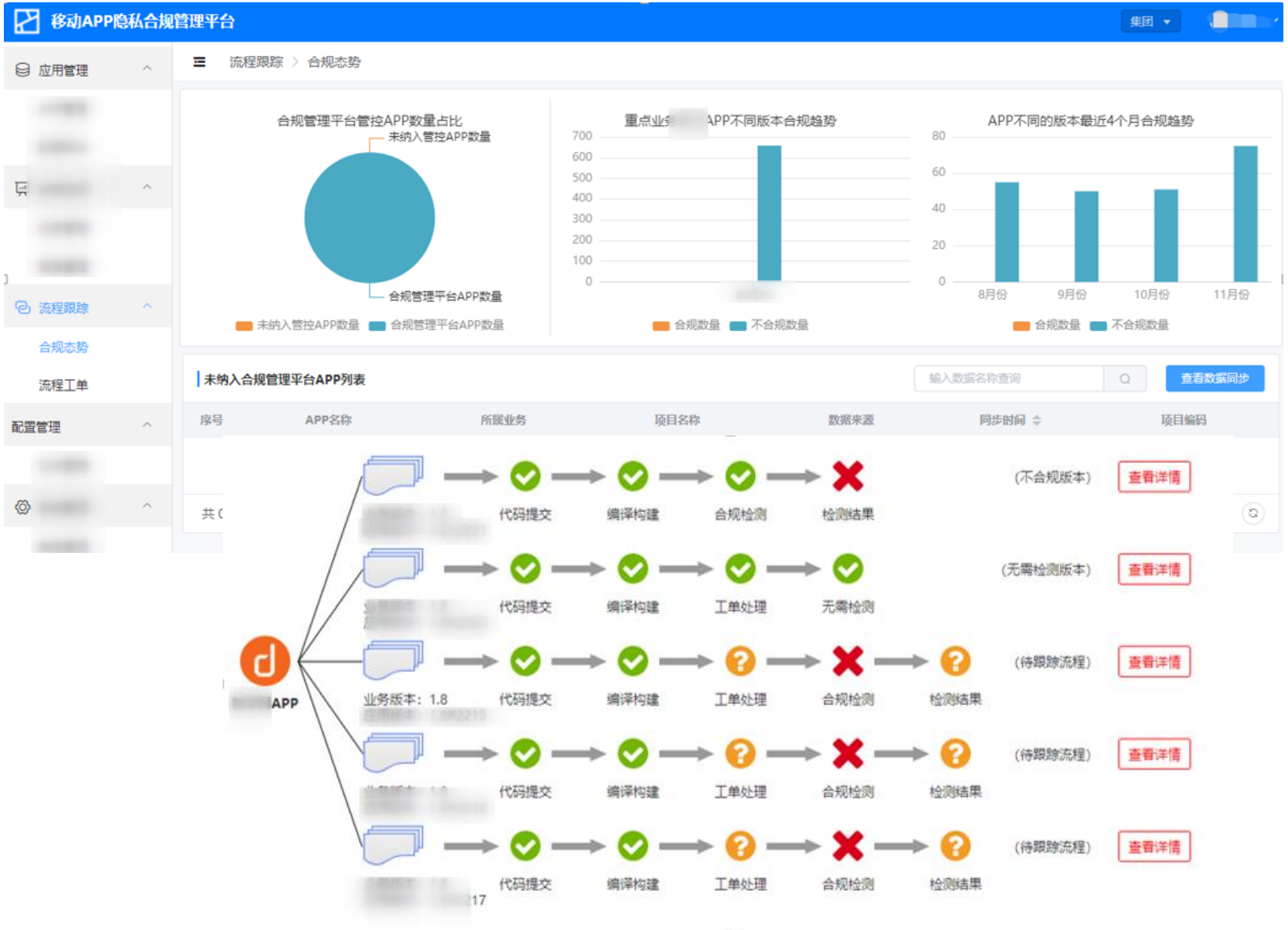
实际落地情况

- **隐私合规扫描系统**：应用行为检测、个人信息检测、第三方SDK检测、获取个人信息行为检测、明问存储行为检测、隐私政策检测、标准合规检测



实际落地情况

- **运营阶段**：合规态势分析、业务应用各构建版本感知、应用市场预警



重点解决的几个难点问题

研发过程版本迭代跟踪问题

同一版本多渠道发布问题

统一发布问题

总体合规趋势问题

OWASP

Open Web Application
Security Project

THANK