



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

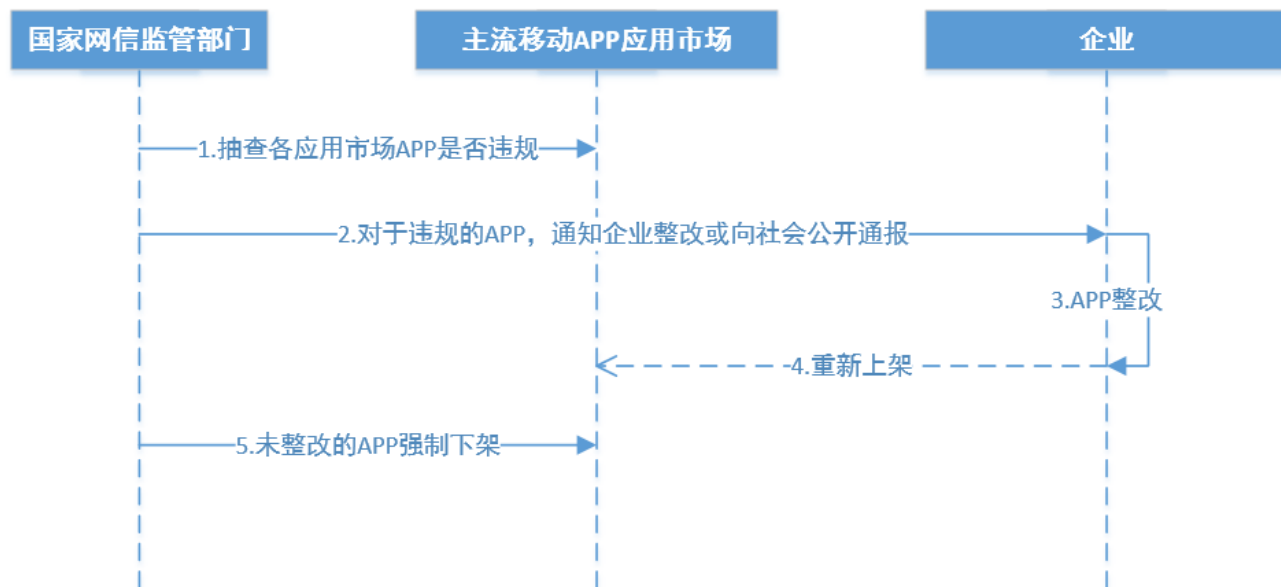
网络运营者收集、使用个人信息，应当遵循合法、正当、必要的原则，公开收集、使用规则，明示收集、使用信息的目的、方式和范围，并经被收集者同意。网络运营者不得收集与其提供的服务无关的个人信息，不得违反法律、行政法规的规定和双方的约定收集、使用个人信息，并应当依照法律、行政法规的规定和与用户的约定，处理其保存的个人信息。

《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

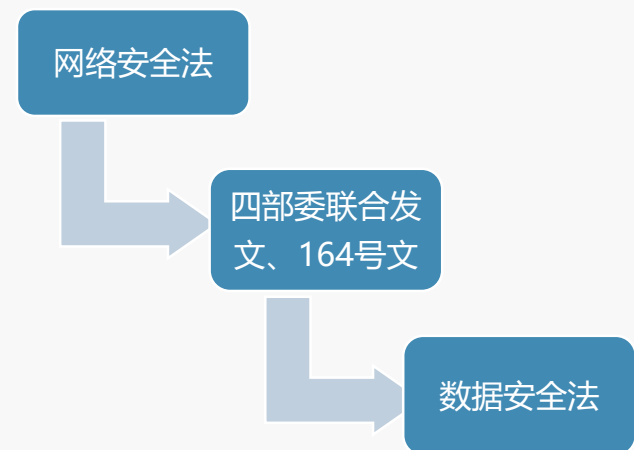
- 1.未公开收集使用规则
- 2.未明示收集使用个人信息的目的、方式和范围
- 3.未经用户同意收集使用个人信息
- 4.违反必要原则，收集与其提供的服务无关的个人信息
- 5.未经同意向他人提供个人信息
- 6.未按法律规定提供删除或更正个人信息功能 或 未公布投诉、举报方式等信息

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。

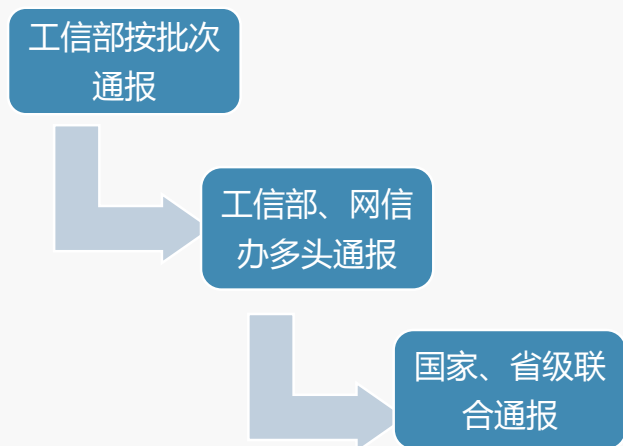


外部监管力度持续加码下通报频发，内部常态化管理机制尚未形成

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；

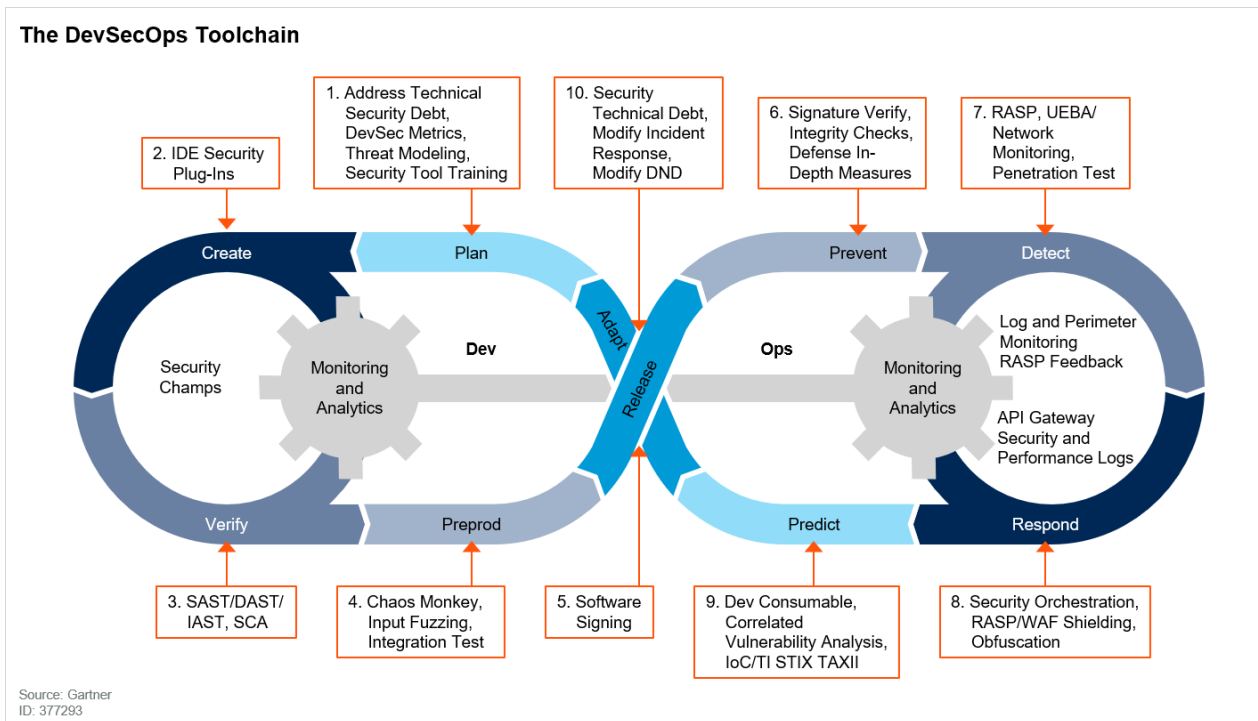
业务不想做如何去管控？

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。



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

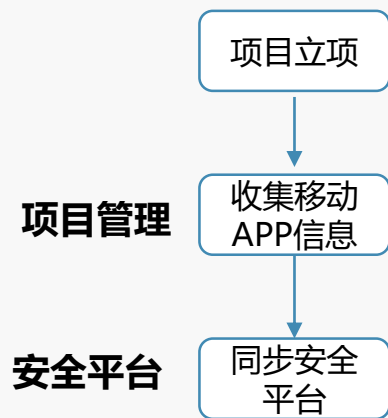
基于DevSecOps平台的APP隐私合规解决方案

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

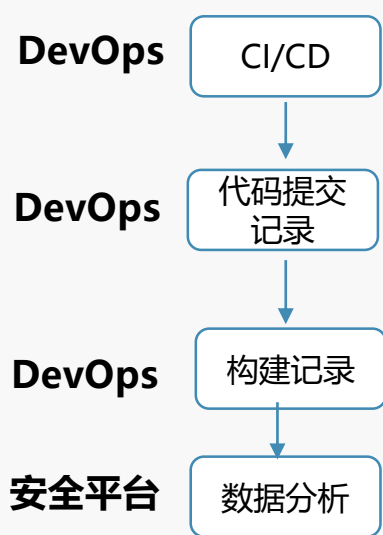
以立项流程为抓手，从源头管控移动APP的开发



开发阶段

02 解决“哪些版本做过合规检测”的问题

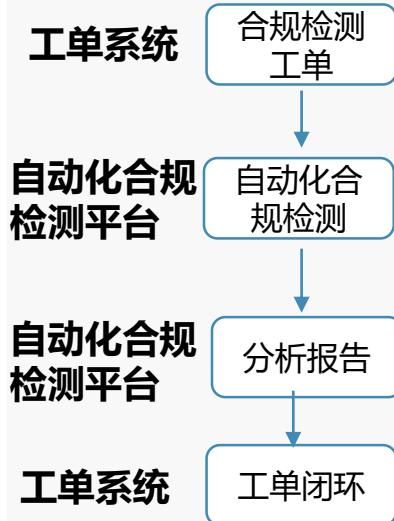
结合CI/CD数据，跟踪移动APP开发版本迭代信息



发布阶段

03 解决“缺少自动化合规检测工具”的问题

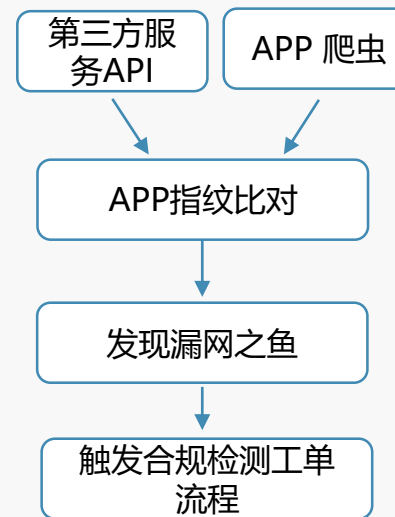
根据数据分析结果，触发自动化合规检测工单，跟踪流程闭环；对于重点APP设置卡点



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



平台功能介绍



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

产品信息

* 产品类型：请选择产品类型

* 是否包含APP： 是 否

初始项目编码：请输入产品首次立项的项目编码

* 是否能复用现有CBB： 是 否

AIZhiBo

构建历史 流程 基础配置 渠道

状态：全部 构建类型：全部 模糊搜索：构建号、分支名、触发者等 时间段：选择日期 查询 重置

| 构建号 | 版本号 | 源码版本 | 提交信息 | 时间 | 触发 | 来源系统 | 状态 | 操作 |
|------|----------|------------------------|---------------------|------------------------------------|------|--------|----|----|
| 1529 | 2.0#1529 | dbc10779 aizhibo... | 1、 song2,202... | 耗时 24分58秒 2021-12-03 15:31:45开始 | 手动执行 | iBuild | 成功 | |
| 1528 | 2.0#1528 | 687b5b68 aizhibo... | - | 耗时 25分44秒 2021-12-02 17:57:45开始 | 手动执行 | iBuild | 成功 | |
| 1527 | 2.0#1527 | 687b5b68 aizhibo... | 1、 2021-12-02... | 耗时 16分51秒 2021-12-02 17:29:14开始 | 手动执行 | iBuild | 成功 | |
| 1526 | 2.0#1526 | 03de3cfb aizhibo... | 21-1 | 耗时 23分26秒 2021-12-02 16:55:41开始 | 手动执行 | iBuild | 成功 | |
| 1525 | 2.0#1525 | e32d668f aizhibo... | 15.36... | 耗时 24分14秒 2021-12-02 16:09:41开始 | 手动执行 | iBuild | 成功 | |

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。

流水线列表

应用流水线 项目流水线

应用名称: 标签: 查询 重置

| 应用流水线 | 最新构建号 | 上次执行 | 流程 | 状态 | 操作 |
|--------|-------|---------------------|------------------|----|--|
| center | 1342 | 2021-12-03 16:18:45 | 构建 > 开发阶段 > 测试阶段 | 成功 | ▶ 📄 ⋮ |
| veb | 1110 | 2021-12-03 10:01:10 | 构建 > 开发阶段 > 测试阶段 | 成功 | ▶ 📄 ⋮ |

移动APP隐私合规管理平台

应用管理 合规检测 > 任务管理 + 创建任务

| 业务单元 | 序号 | 任务状态 | 静态检测状态 | 动态检测状态 | 更新时间 | 创建人 | 操作 |
|------|----|------|--------|--------|---------------------|-----|---|
| 集团 | 1 | 已完成 | 检测完成 | 检测完成 | 2021-12-03 14:21:30 | | 📄 📄 🗑️ |
| 集团 | 2 | 已完成 | 检测完成 | 检测完成 | 2021-12-03 09:01:55 | | 📄 📄 🗑️ |
| 集团 | 3 | 已完成 | 检测完成 | 检测完成 | 2021-12-02 19:12:45 | | 📄 📄 🗑️ |

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、明文存储行为检测、隐私政策检测、标准合规检测

合规检测 > 检测报告详情

报告目录详情

基本信息

权限声明与使用分析

SDK分析

应用行为

通信行为分析

191号文分析

164号文分析

APP应用基本信息

▼ 基本信息概述

| 概述项 | 描述 |
|---------------------|--|
| SDK分析概述 | 集成SDK共1个，其中涉及1个类别，来自1个开发者 |
| 权限声明 | 在AndroidManifest.xml中声明权限共1个 |
| 漏洞分析 | 检测出3项漏洞 |
| 合规分析 ? | 总评估项为4项，其中164号文合规;191号文、授权前行为、授权后行为不合规; |
| 行为分析 | 对外通信共0次，其中涉及0个域名。 该App在检测期间共发生0次异常通信行为。 使用权限共5次，其中涉及可收集个人信息权限2次。 |

移动APP隐私合规管理平台

集团

应用管理

流程跟踪 > 流程工单

输入数据名称查询

Q

批量删除

APP管理

数据同步

| <input type="checkbox"/> | 序号 | APP名称 | 应用版本 | 邮件是否送达 | 邮件是否已阅 | 工单处理方式 | 邮件处理人 | 更新时间 | 创建人 | 操作 |
|--------------------------|----|-------|----------|--------|--------|--------|-------|---------------------|-----|---|
| <input type="checkbox"/> | 1 | PP | 1.8#2220 | 是 | 是 | 无需检测 | | 2021-12-03 10:00:22 | |    |

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

