
HCL&安世加
企业网络安全沙龙
8月6日 / 周五下午 / 线上

安世加

基于DevSecOps平台的移动APP隐私合规实践

钱君生 安全架构师

移动APP隐私合规背景介绍

健全合规治理体系，培育企业合规文化，建立长效管理机制

——7.30《工业和信息化部信息通信管理局召开互联网行业专项整治行动企业宣贯部署会》

国信办秘字[2019]191号

《 App违法违规收集使用个人信息行为认定方法》

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

工信部信管函〔2020〕164号

《工业和信息化部关于开展纵深推进APP侵害用户权益专项整治行动的通知》

整治对象

（一）APP服务提供者，即互联网信息服务提供者提供的可以下载、安装、升级的应用软件,包括快应用和小程序等新应用形态。

（二）软件工具开发包（SDK）提供者，即集成在手机APP里的第三方工具集合。

（三）应用分发平台，包括网站、应用商店、APP等承担下载、安装、升级等分发服务的各类平台。

《工业和信息化部启动互联网行业专项整治行动》

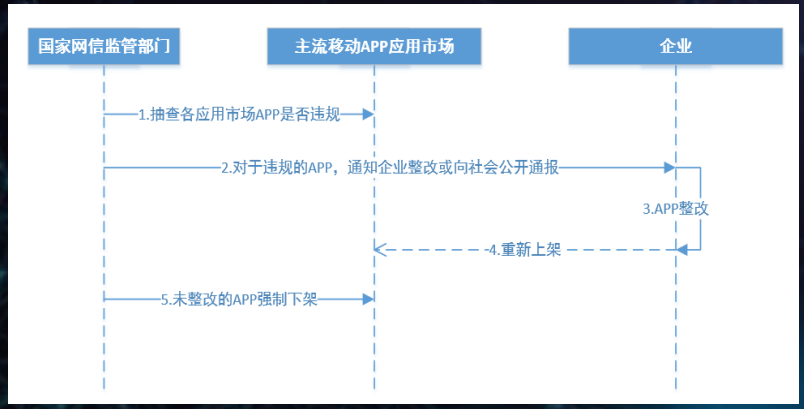
8类问题22个场景

重点整治恶意屏蔽网址链接和干扰其他企业产品或服务运行等问题

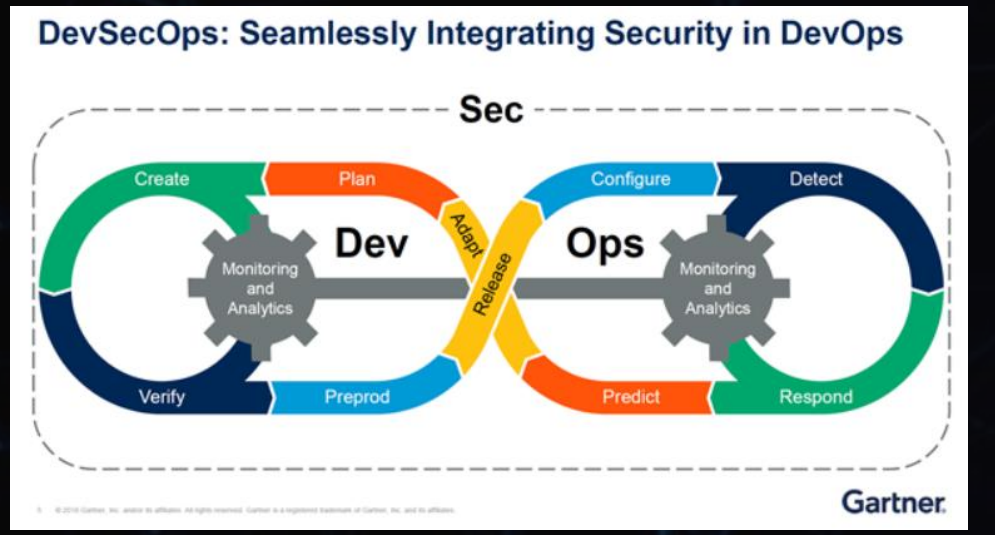
重点整治应用软件启动弹窗欺骗误导用户、强制提供个性化服务等问题

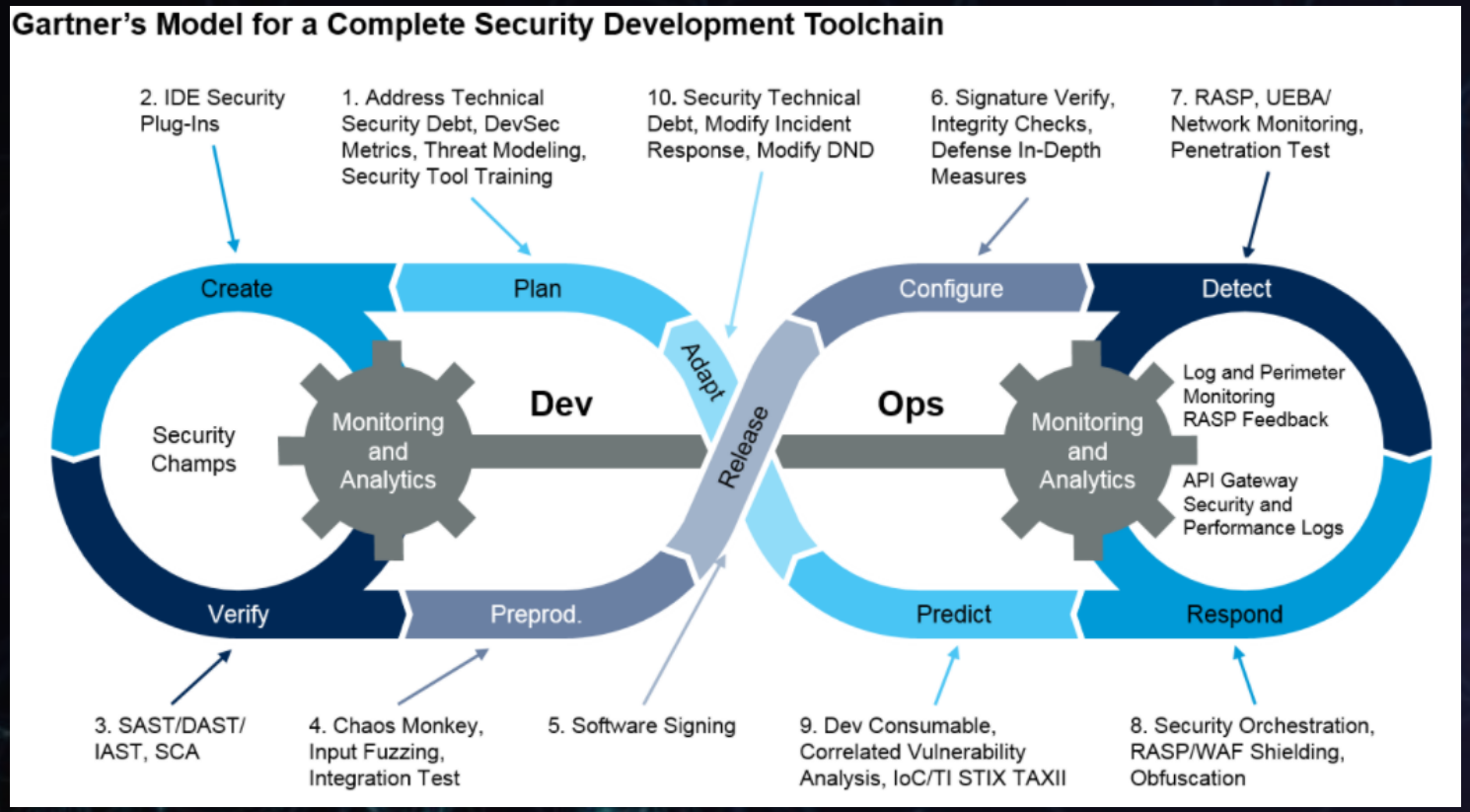
重点整治企业在数据收集、传输、存储及对外提供等环节，未按要求采取必要的管理和技术措施等问题

重点整治“黑宽带”和未履行网站备案手续等问题



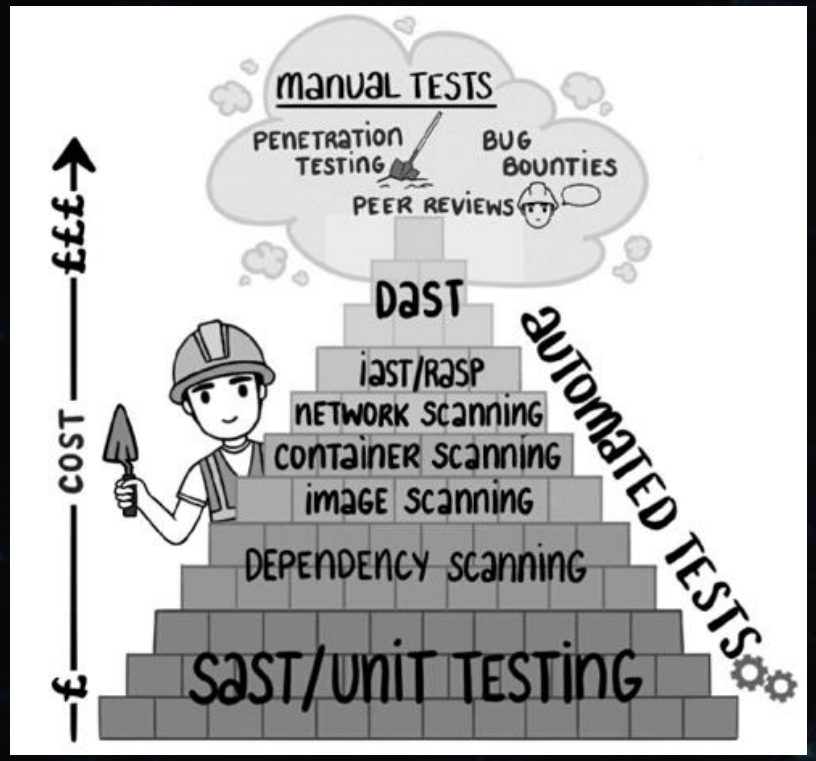
DevSecOps背景介绍





PPTR=人+流程+技术+资源

DevSecOps背景介绍



安全工具链金字塔

来源：**DevSecOps: A leader's guide to producing secure software without compromising flow, feedback and continuous improvement**

DevOps 基础底座

OA系统　SSO系统　项目管理系统

工单系统　IM系统　运维管理系统

周边生态环境

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

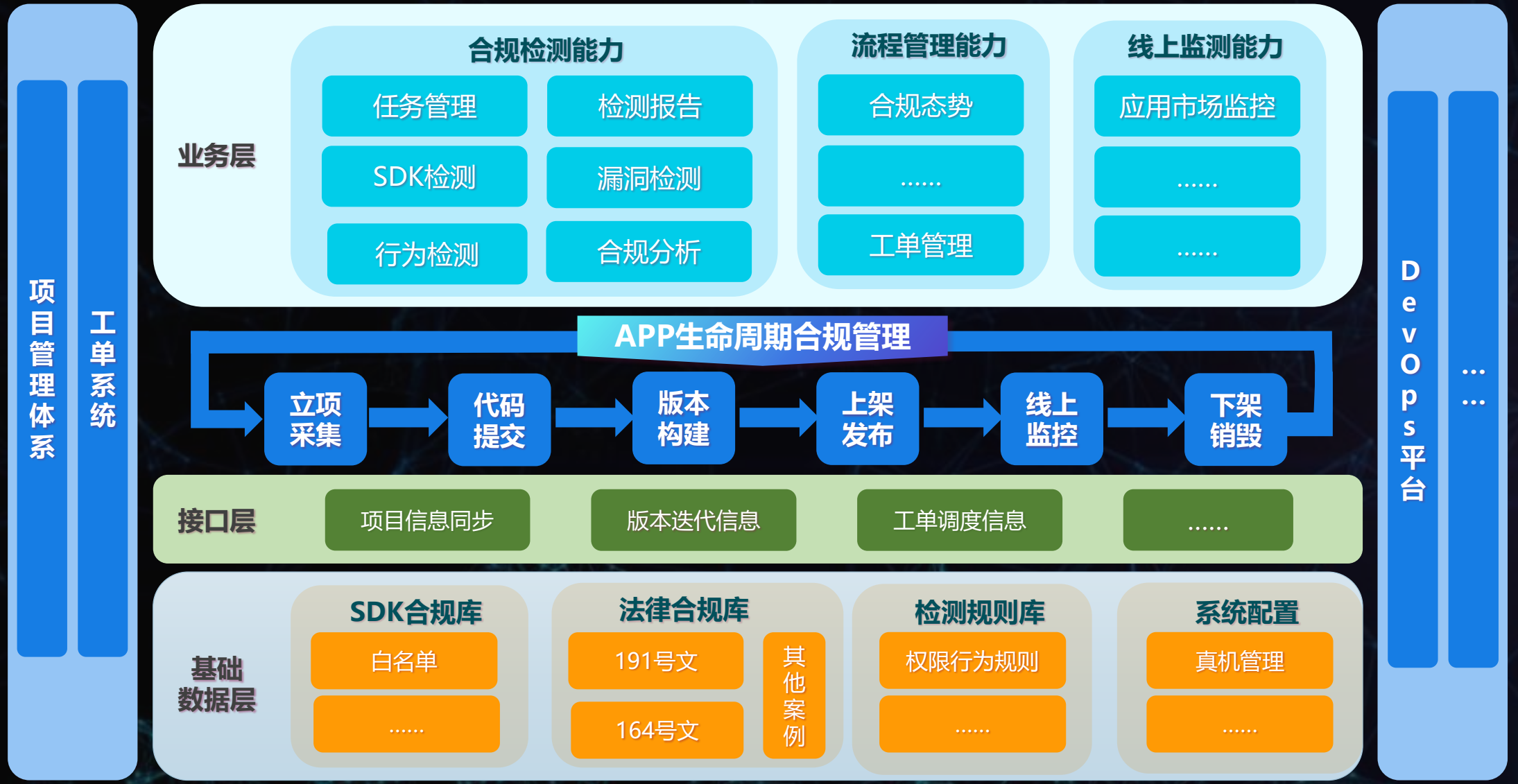
02

- 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

平台功能介绍


项目管理体系
工单系统
业务层
合规检测能力
任务管理
检测报告
SDK检测
漏洞检测
行为检测
合规分析
流程管理能力
合规态势
.....
工单管理
线上监测能力
应用市场监控
.....
.....
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
项目信息同步
版本迭代信息
工单调度信息
.....
基础数据层
SDK合规库
白名单
.....
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
...

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

结束语

HCL&安世加 企业网络安全沙龙

安世加专注于网络安全行业，通过互联网平台、线下沙龙、峰会、人才招聘等多种形式，致力于创建亚太地区最好的甲乙双方交流、学习的平台，培养安全人才，提升行业整体素质，助推安全生态圈的健康发展。

官方网站：
https://www.anshijia.net.cn
微信公众号：asjeiss

安世加