

互联网业务安全实践浅谈



方超（习林）



SFDC

SegmentFault
Developer Conference



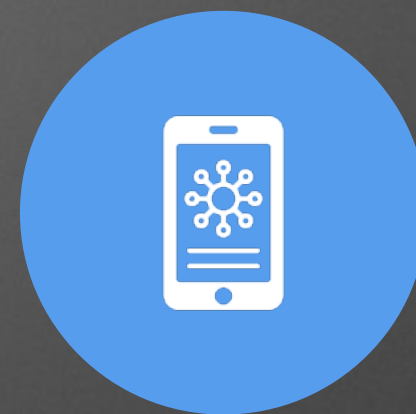
PC



Network



DC/Cloud



?

安全环境演变趋势



SFDC

SegmentFault
Developer Conference



黑灰产业链已完善



国内黑产从业人员**150万+**

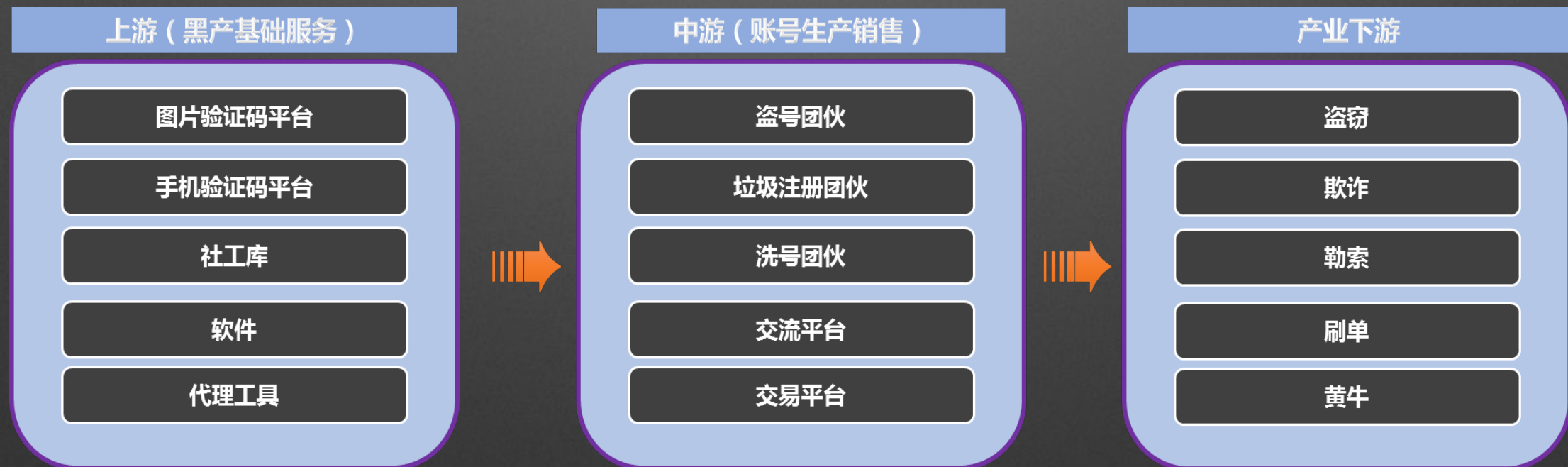


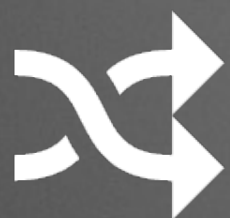
黑产市场规模**1000亿+**

产业链的上游是一个基础性的行业；

中游是网络账号提供商及信息交易交流平台；

下游主要是利用非正常渠道的网络账号进行欺诈、盗窃、刷单等犯罪和不道德行为的团伙。





实时要求高



黑产专业化



业务种类多



平台限制大



新手段层出不穷



攻防要求高



SFDC

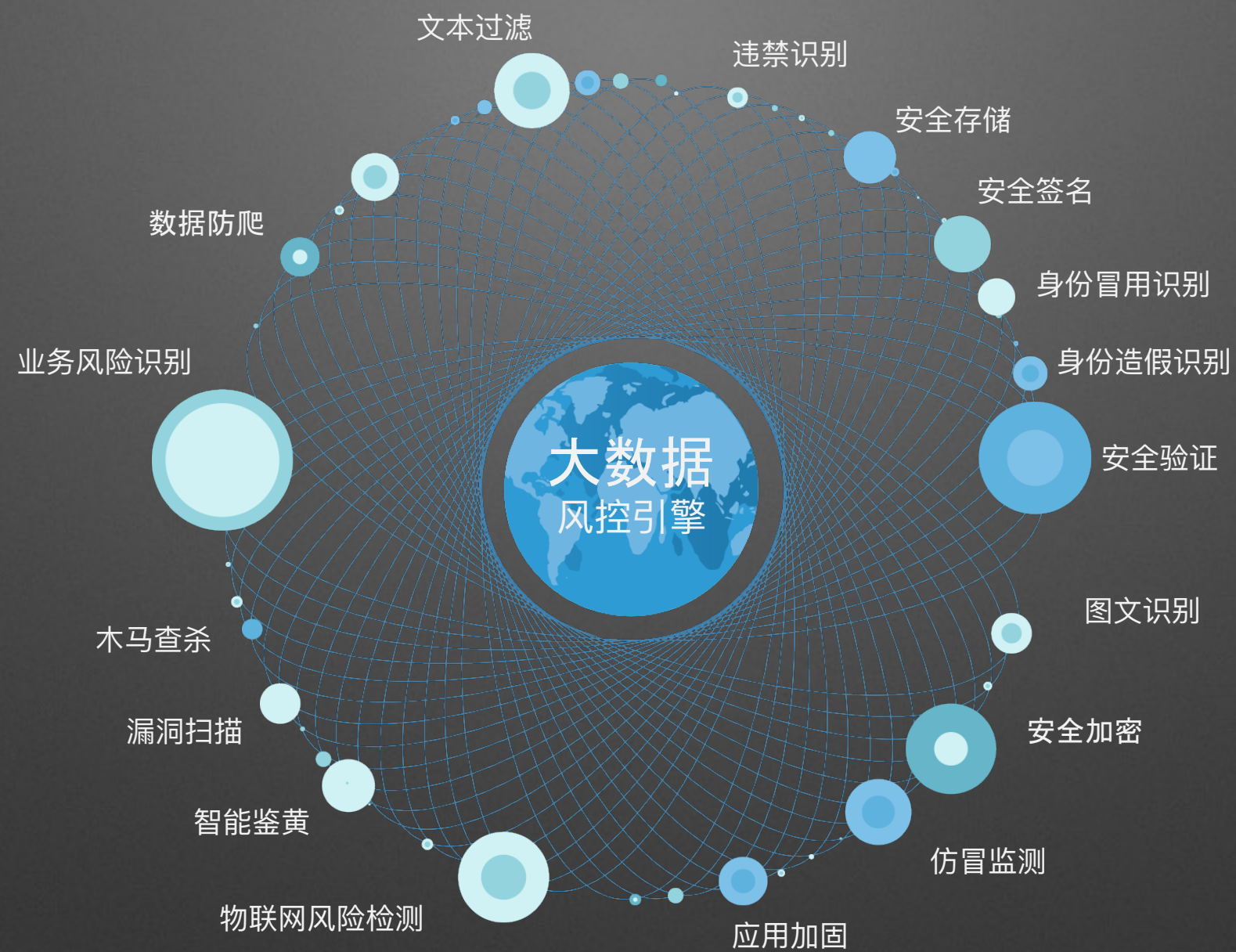
SegmentFault
Developer Conference

互联网业务的层次



互联网业务的安全模型





SFDC

SegmentFault
Developer Conference

97%移动应用自身存在大量的漏洞



某金融P2P系统

日均垃圾账号申请量超过申请总量的50%



某O2O平台2015年单次活动，
现金券被刷最高达到70%



超过5亿网民的身份信息曾被泄露



如何搭建自己的业务安全体系



业务安全的角色演变

传统企业

封闭的环境
有限的账号
可控的终端

以系统为中心的安全

通过保护主机、网络、终端来构建安全体系

业务的支撑者



互联网业务

开放的环境
海量的账号
不可控的终端

以业务为中心的安全

围绕业务来构建安全体系

业务的不可分割部分



基础安全



主机安全



WAF



抗DDos



漏洞检测

.....

数据安全



权限管理



数据分级



数据加密

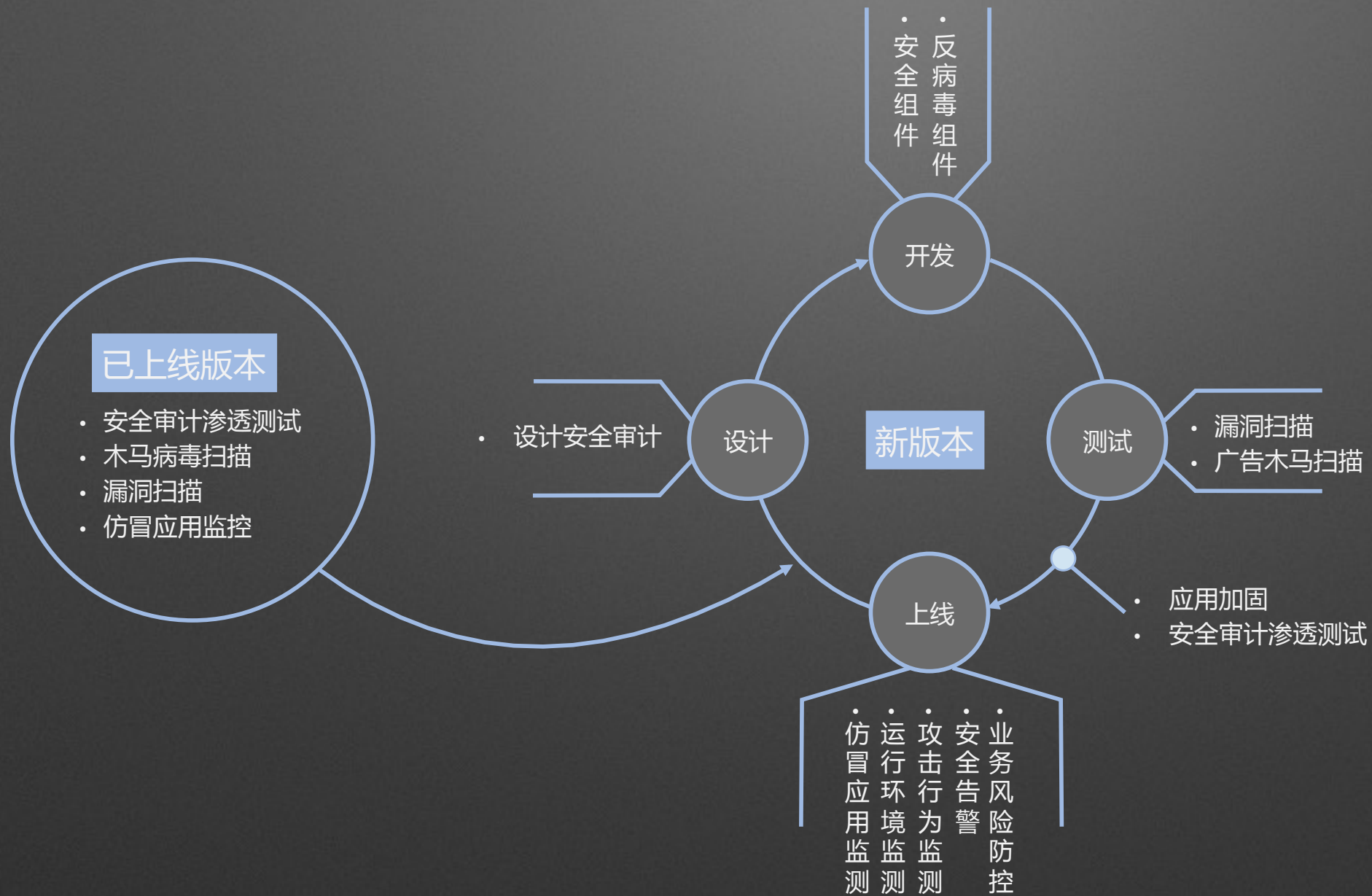
.....




SFDC

SegmentFault
Developer Conference

移动安全



 破解风险

 接口盗刷

 应用漏洞

 仿冒盗用



构建多维度的数据与识别能力

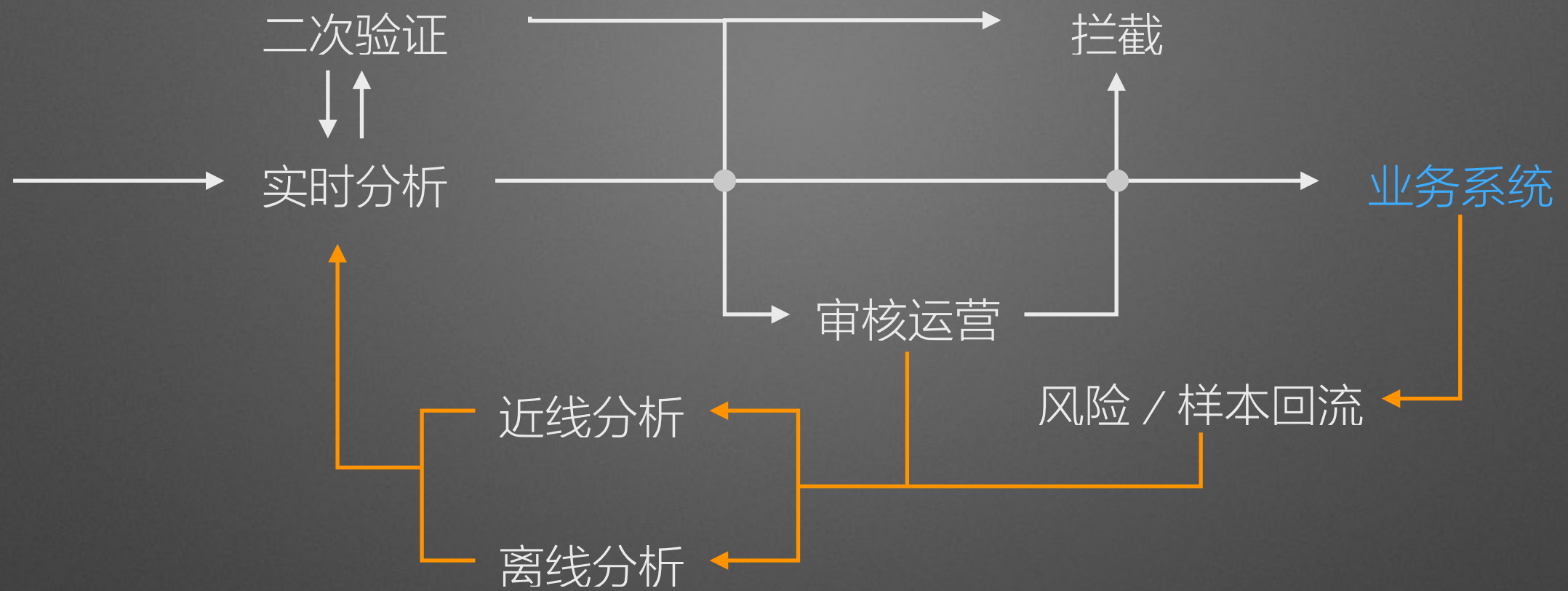
针对不同的风险将适用的能力组合起来判断



多节点综合判断

常见风险	注册	登陆	信息修改	活动/交易	发帖/弹幕	其他
反垃圾注册 (虚假 , 垃圾)	✓					
防账号盗用 (撞库 , 盗用)		✓	✓			
反活动作弊 (刷单 , 黄牛)	✓	✓		✓		
反垃圾信息 (色情、违禁)	✓	✓			✓	✓
反虚假身份 (色情、违禁)	✓	✓				✓





 技术与运营相结合

 利用反馈形成数据闭环，持续提升效果



	第三方 / 采购	定制 / 自研
数据	风险数据共享	可信数据沉淀
识别	共性风险识别	根据业务特性的识别
验证	通用方式为主	业务结合、提升体验
对抗	基础对抗	效果监控与报警
监控	互联网	业务系统



联防联控共抗黑灰产



SFDC

SegmentFault
Developer Conference