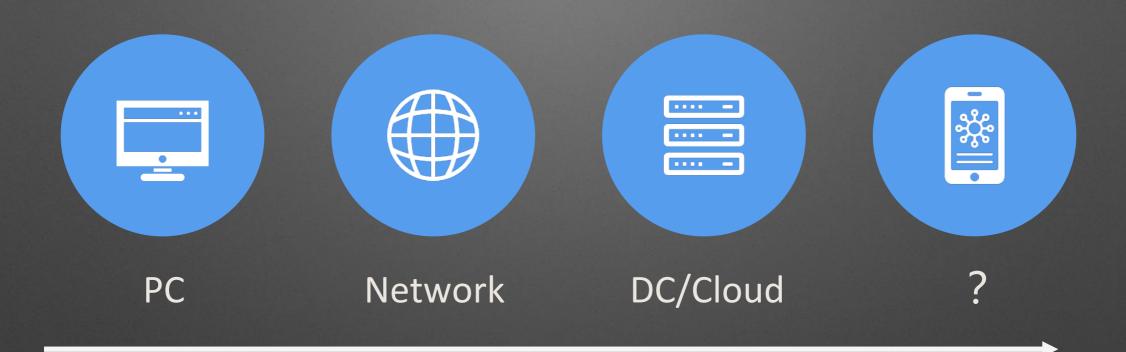
互联网业务安全实践浅谈



方超(习林)



安全环境演变趋势

 垃圾注册
 帐号盗用

 黄牛
 虚假身份

业务

黑卡刷单推广作弊炒信活动作弊

链路

数据破解 API伪造 漏洞 DDoS 提权 木 嗅探 数据泄露 选规内容 暴力破解 SQL注入

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。









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

互联网业务的层次

	电商业务	视频业务
内容	商品图片和信息	视频、互动评论
用户	买家、卖家	普通用户、会员、主播
服务	购买、促销、秒杀、抽奖	视频与直播服务
应用	电商APP	视频 APP
数据	交易数据	内容数据
传输	移动网络	移动网络
系统	操作系统	操作系统
硬件	手机	手机

互联网业务的安全模型

数据

数据窃取 数据伪造

违禁内容

垃圾账户

黄牛刷单

逻辑逆向

信息截取

系统漏洞

数据防爬 安全存储

内容

涉黄图片

智能鉴黄 文本过滤

违禁识别 图文识别

用户

虚假身份

身份造假识别

身份冒用识别

服务

活动作弊 账号盗用

风险识别

安全验证

应用

破解外挂 应用漏洞

漏洞扫描

应用加固 仿冒监测

传输

消息伪造

流量劫持

安全加密

安全签名

系统

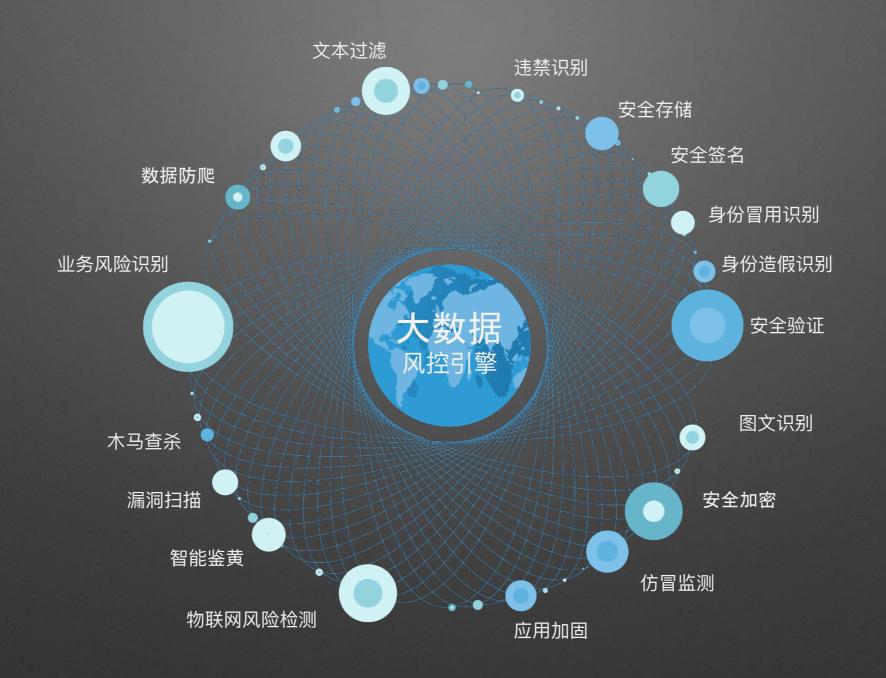
病毒木马

木马查杀

硬件

硬件漏洞 协议漏洞

IOT风险检测



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









漏洞检测

数据安全

...



权限管理

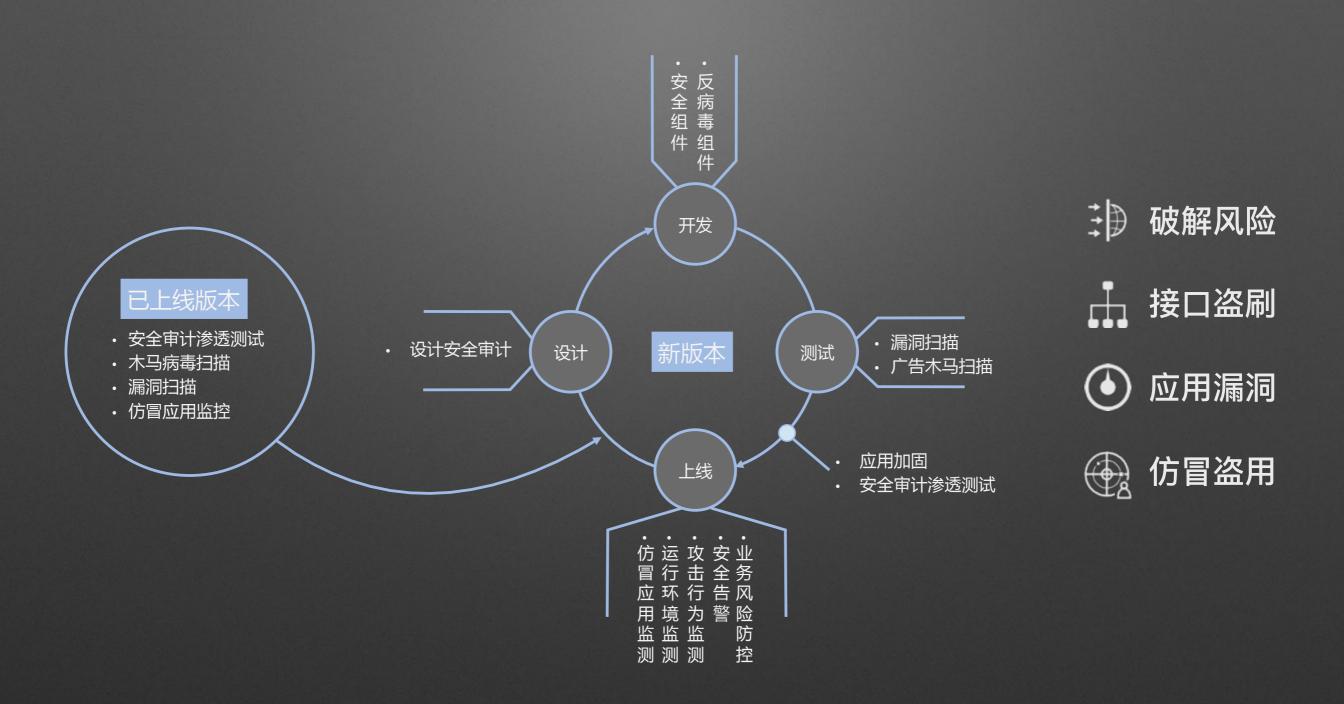


数据分级



数据加密

移动安全



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

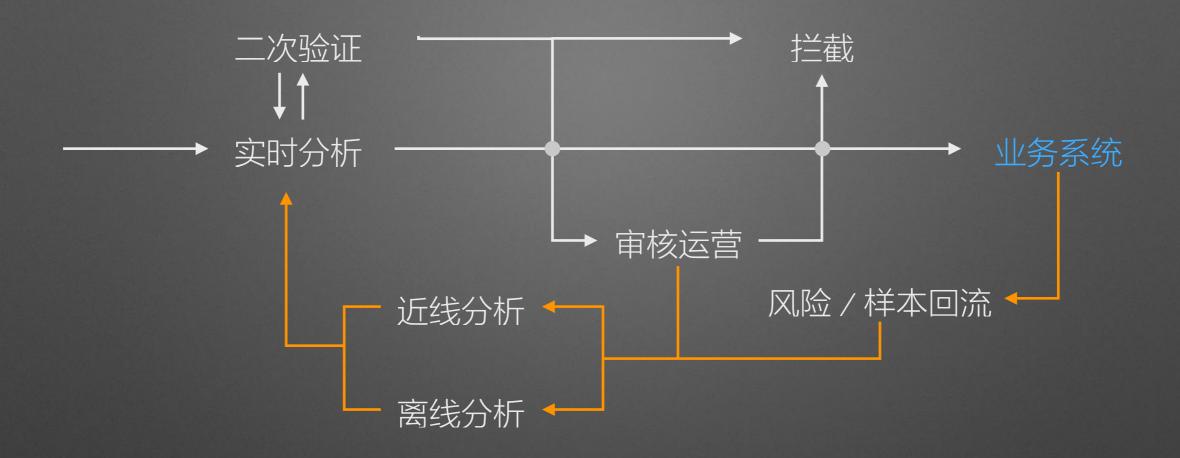


逆向数据 正向数据



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)	\odot					
防账号盗用 (撞库,盗用)		\odot	\odot			
反活动作弊 (刷单 , 黄牛)	\odot	\odot		\Diamond		
反垃圾信息 (色情、违禁)	\odot	\odot			\Diamond	\odot
反虚假身份 (色情、违禁)	\odot	\odot				\Diamond



- 团 技术与运营相结合
- (三)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





