"Face the challenge,Embrace the best practice"

EISS－2019
企业信息安全峰会
之深圳站

2019.8.16

业务安全建设经验分享

李广林

个人简介

- 李广林 - 马蜂窝 现任 信息安全负责人
- 百度杀毒 - 威胁情报 - 业务风控 - 甲方安全从业者

马蜂窝

安全+

CONTENTS

1 业务风险概况

知己知彼，百战不殆

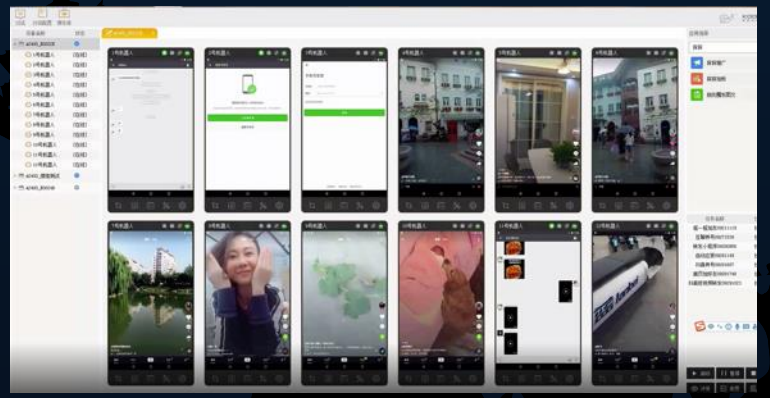
常见业务风险

黑产工具箱

工欲善其事，必先利其器

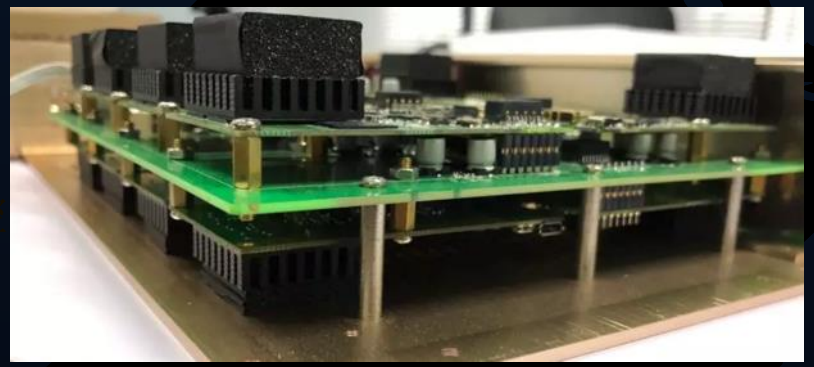
猫池

云控



手机群控

箱式群控



2 业务安全能力

善攻者，动于九天之上

甲方没有能力VS 乙方不懂业务

业务安全建设阶段

资源整合

梳理数据资源
链路打通
威胁情报

基础能力建设

端防护
链路防护
边界丰富的反制能力
大数据分析平台

话语权

SDLC
业务支持
逻辑漏洞测试
逻辑评审
一票否决权

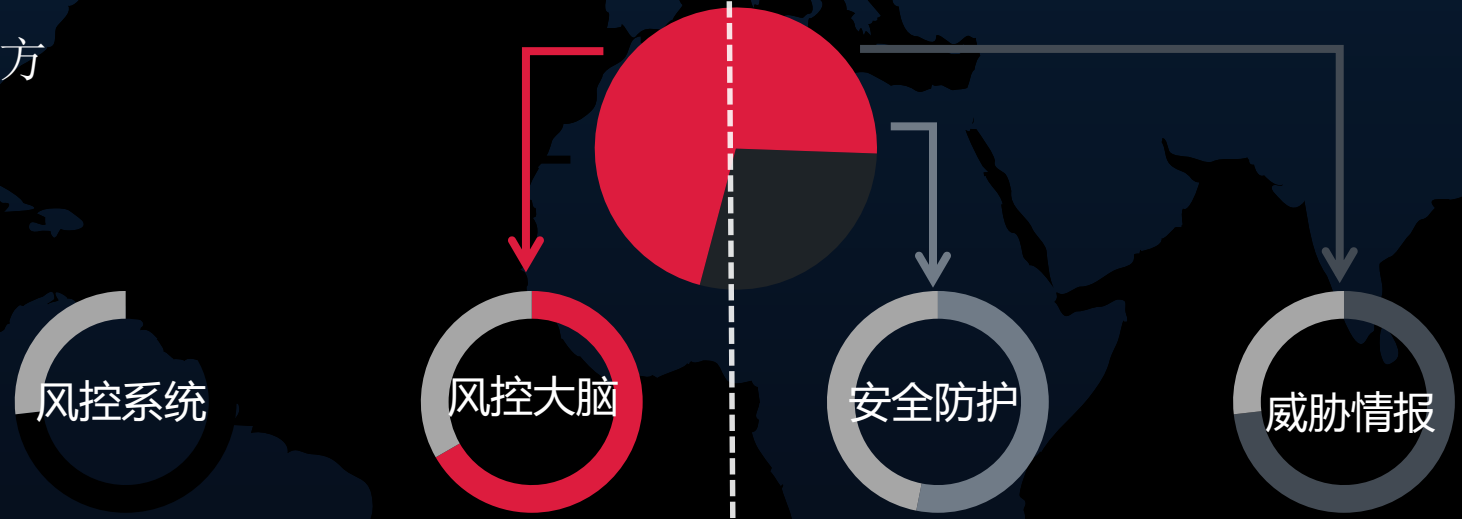
风控系统

实时模型
离线计算
风控规则
规则引擎

业务安全能力拆解

甲方

乙方



风控系统

业务逻辑评审
逻辑漏洞测试
大数据计算平台
风控运营

风控大脑

基于业务场景的
威胁情报
实时模型
离线模型
风控引擎

安全防护

WEB端防护
客户端防护
私有协议
环境检测
设备指纹
客户端加固
代码混淆

威胁情报

通用的
IP
手机号
黑产工具
黑产手段

业务安全能力-威胁情报

战略情报

预警重大安全风险，指导主动防御和应急响应

潜在损失巨大，实效性至关重要

0day APT 数据泄露

战术情报

格式化攻击特征 ip情报 设备情报，实时监控

基础类情报，标准格式，可读/自动化

检测各类攻击，如撞库 盗号等

运营情报

高级情报攻击技术，工具 团伙身份

协助应急止损、取证溯源 和线下打击

重点关注以及成功的攻击

- 安全金字塔
- IP画像建设经验

业务安全-逻辑漏洞测试

支付业务

- 并发提现
- 并发支付
- 并发转账
- 负数提现
- 负数转账
- 替换订单
- 商品突破整形限制
- 直接修改数量

电商平台

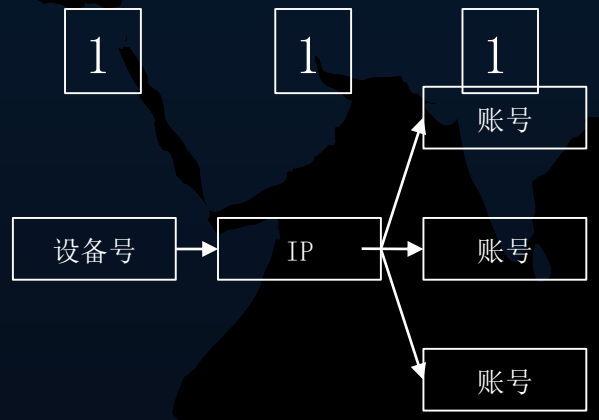
- 购买数量：0，小数，负数，正负值
- 优惠券：并发领取，遍历领取，重复使用，测试环境上生产
- 越权：操作订单，修改资料

内容/社交业务

- 验证码：绕过发帖
- 越权 ：发消息，加好友，禁言
- 信息泄露，临时链接
- 非会员使用会员功能
- 代币控制，任务控制

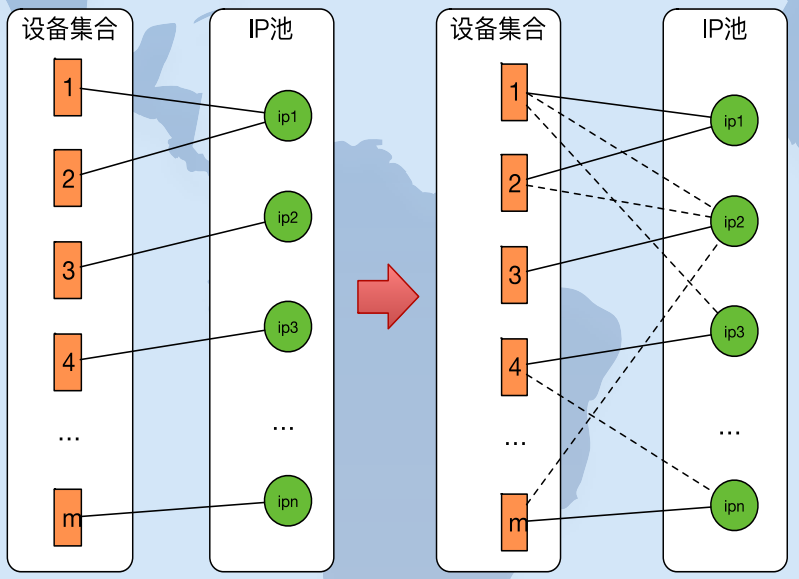
业务风控数据分析方法-基础分析

- 打码平台与注册时IP比对
- IMEI-IDFA-设备指纹-PASSID-IP
- 同一设备不间断访问
- 访问路径判断
- 周期性行为分析
- 团伙行为分析 群控设备
- 刷流量类行为
- 低频持续访问
- 设备信息 是否ROOT 是否越狱，是否有风险APP
- 正常用户数据与异常数据
- 作弊残留率



伪造设备号
IMEI 000000000
IDFA
DEVICEID

业务风控数据分析方法-图关联



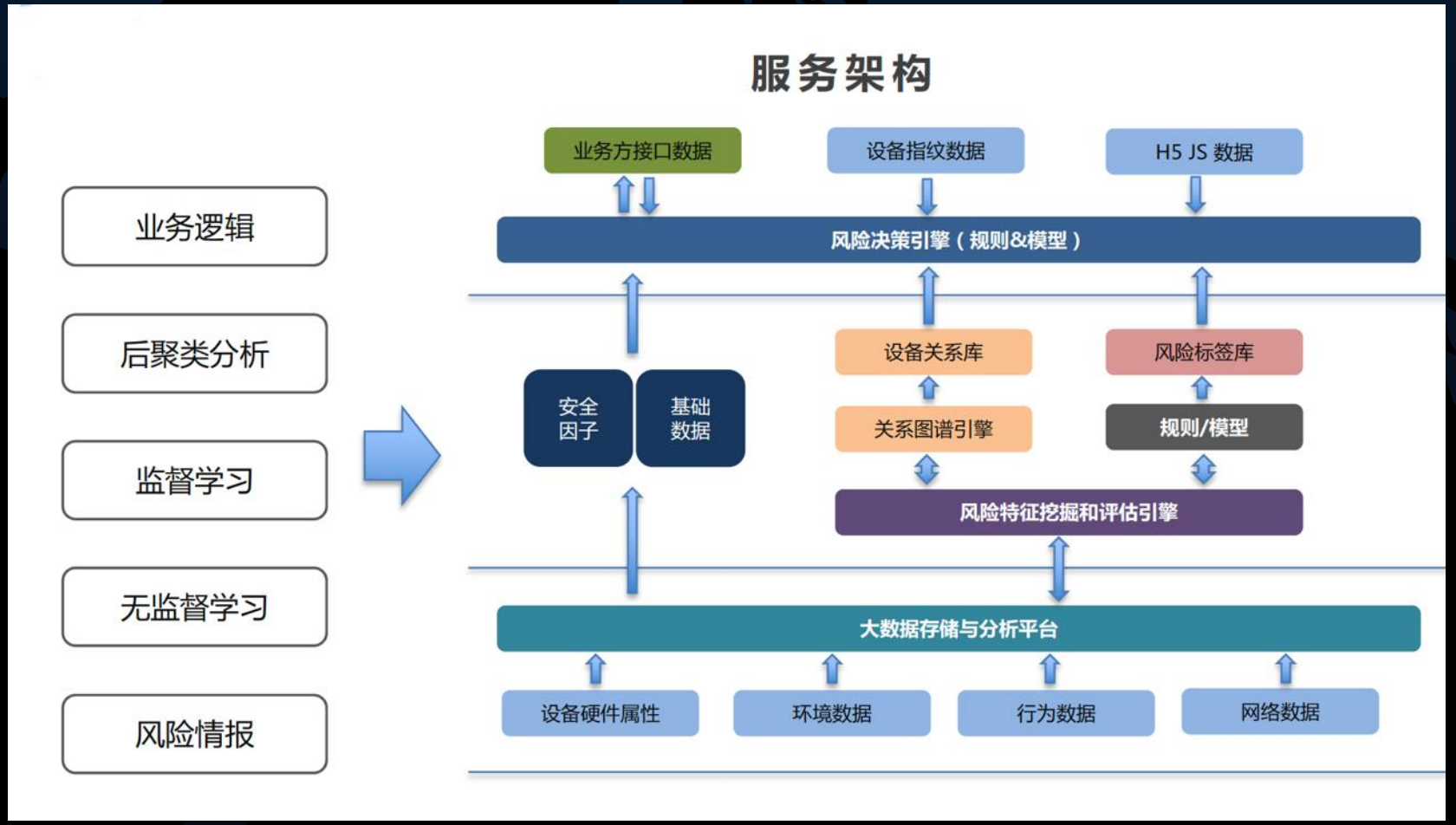
子图id	vertex数量	设备指纹数量	ip数量
0	15557314	1101786	14455528
78711	22	16	6
17179940251	62	5	57
25769812261	67	5	62
25769841379	114	5	109
8589969108	114	5	109
8590012376	6	5	1
120259137126	12	4	8
137439006032	11	4	7
146028965899	12	4	8

逻辑评审

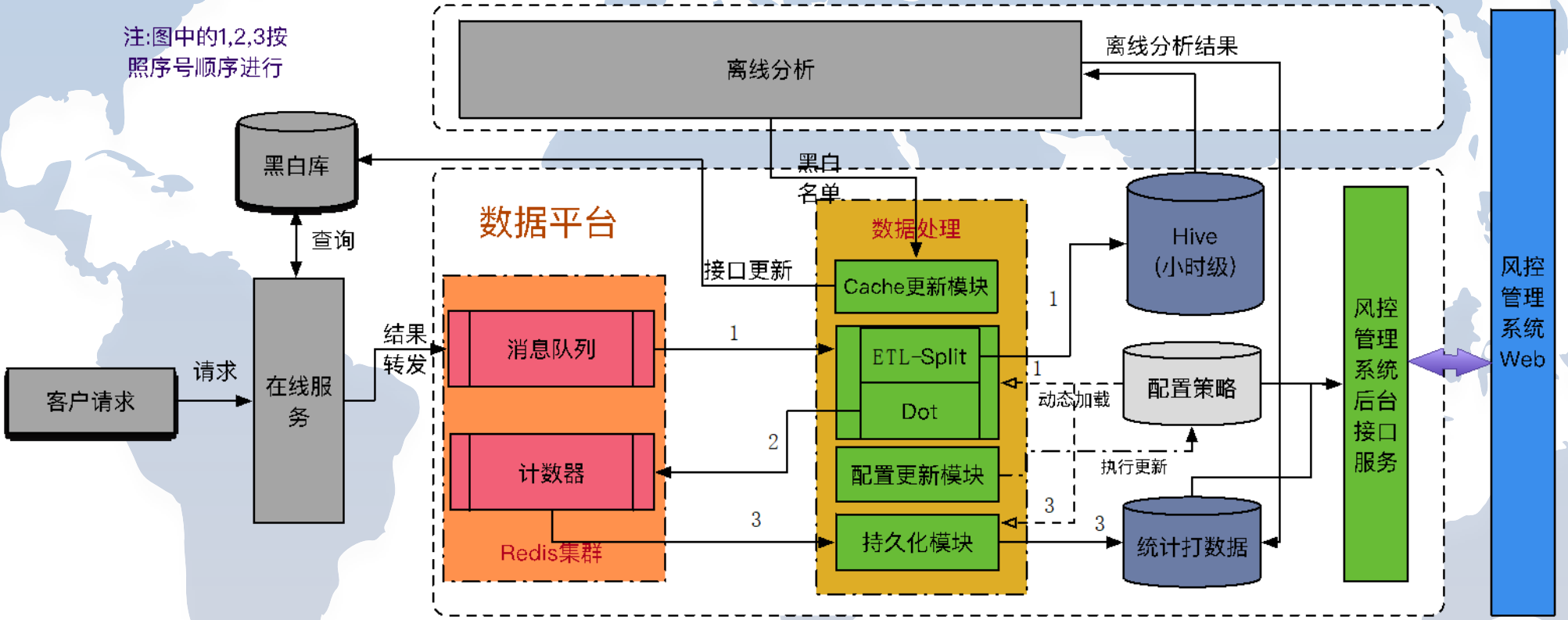
一票否决权的重要性
安全开发流程的一环
业务安全需求评审应包含内容

- 成本与收益
- 奖金支付方式
- 拉新传播风险
- 机器行为、刷单、薅羊毛风险
- 离线/在线分析，支付唯一性校验
- 攻击者模拟
- 接口健壮性
- 降级策略
- 异常监控和发现
- 应急预案

典型的风控系-百度昊天镜

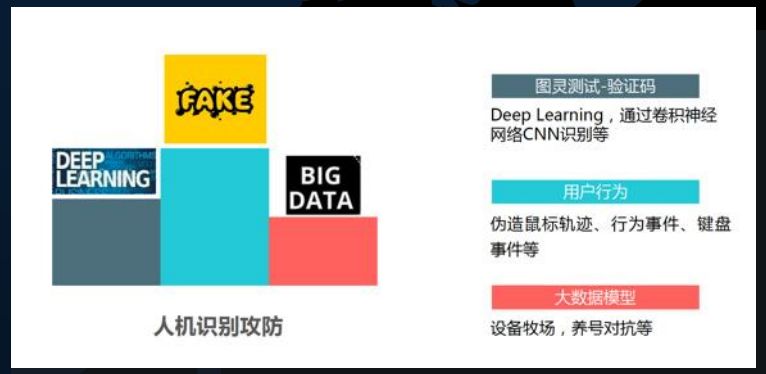


风控体系架构


注:图中的1,2,3按照序号顺序进行
离线分析
离线分析结果
黑白库
黑白名单
查询
数据平台
数据处理
接口更新
Cache更新模块
Hive(小时级)
客户请求
请求
在线服务
结果转发
消息队列
ETL-Split
Dot
配置策略
动态加载
计数器
配置更新模块
执行更新
Redis集群
持久化模块
统计打数据
风控管理系统后台接口服务
风控管理系统Web
1
2
3

3 进阶思考

善守者，敌不知其所攻



建设与对抗

01 **高质量代理IP**
对抗IP画像☺

02 **算法模型**
基于Logistic 等算法模型的对抗☺

03 **场景特有的规则**
注册频率、UA分布比例等☺

马蜂窝

安全+

THANK YOU
FOR WATCHING