GIAC

全球互联网架构大会

GLOBAL INTERNET ARCHITECTURE CONFERENCE

数美实时反欺诈架构实践
——构建智能欺诈账号识别体系

梁堃　数美科技　　CTO

提纲

- 背景介绍
- 风控引擎
- 实施

背景介绍：欺诈无处不在

随着移动互联网的发展，网络欺诈愈演愈烈，造成的损失触目惊心

通用欺诈问题

- 机器注册
- 账号安全
- 渠道流量欺诈

行业欺诈问题

金融

- 借贷欺诈
- 盗卡交易
- 洗钱套现
- 营销活动欺诈

社交/社区

- 淫秽色情发帖
- 欺诈广告信息
- 虚假好友请求
- 僵尸粉

电商

- 刷榜
- 促销活动欺诈
- 恶意下单
- 广告导流评论

游戏

- 黑卡
- 聊天室广告内容
- 挂机

视频/直播

- 刷榜
- 薅虚拟币
- 违规弹幕
- 涉黄/政/暴恐

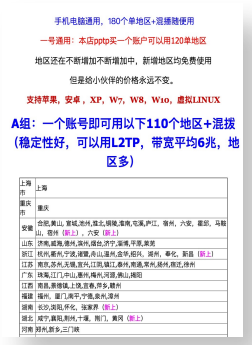
网络欺诈损失占GDP比例多达**0.63%**约**4000多亿**人民币。

—Experian《欺诈经济学：规避快速增长和创新中的风险》

背景介绍：发达的灰色产业链

灰色产业专业化程度越来越高，呈现出团伙化、高科技化、产业化的趋势

身份资料	养号包装	软硬件提供商	口子探测者	实施
拖库、购买、钓鱼	通话记录、工资、消费	VPN、肉鸡、设备农场	探测风控漏洞	广告、羊毛，...



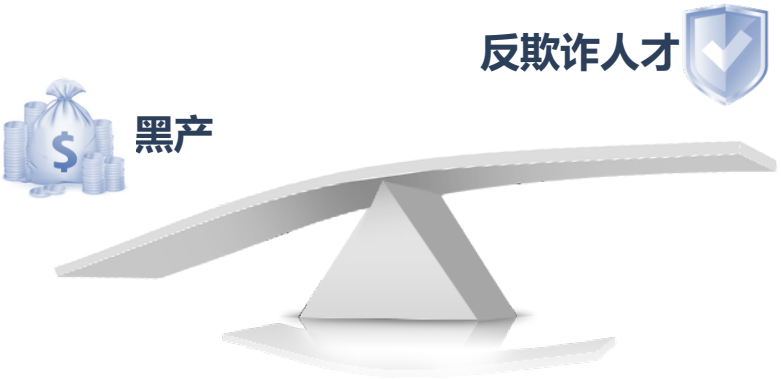
据测算，黑产从业人数超过**150万**人，掌握了**数十亿**的账号。

——《电子商务生态安全白皮书》

背景介绍：现有方案的不足

背景介绍：目标与挑战

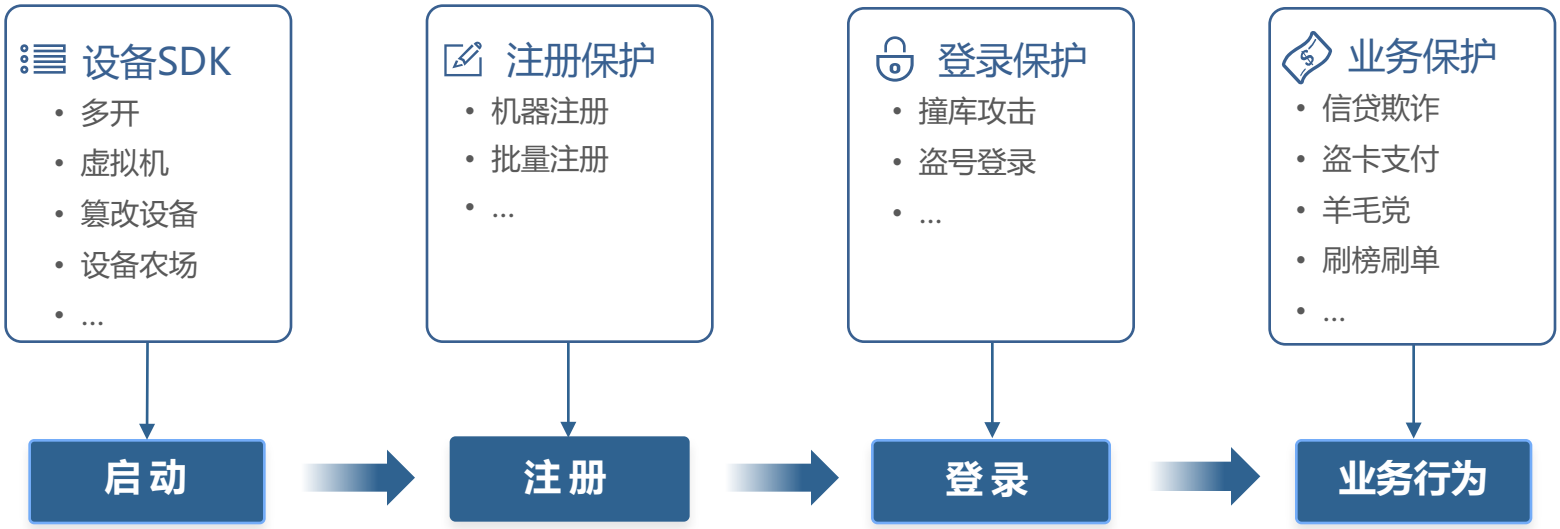
- 目标
  - 准确率：正常用户无感知
  - 召回率：实时、准确地识别欺诈行为
- 挑战
  - 业务发生的时间、地点多样化
  - 灰产技术水平与专业程度不断提高
  - 缺乏全局的风险数据支撑
  - 专业的反欺诈人才团队不足
  - 两个目标似乎是矛盾的
    - 简单的模型或策略很难同时做到高召回率与低误杀率



提纲

- 背景介绍
- 风控引擎
  - 防御体系
  - 策略体系
  - 功能架构
- 实施

风控引擎：全栈式防御体系



风控引擎：策略体系

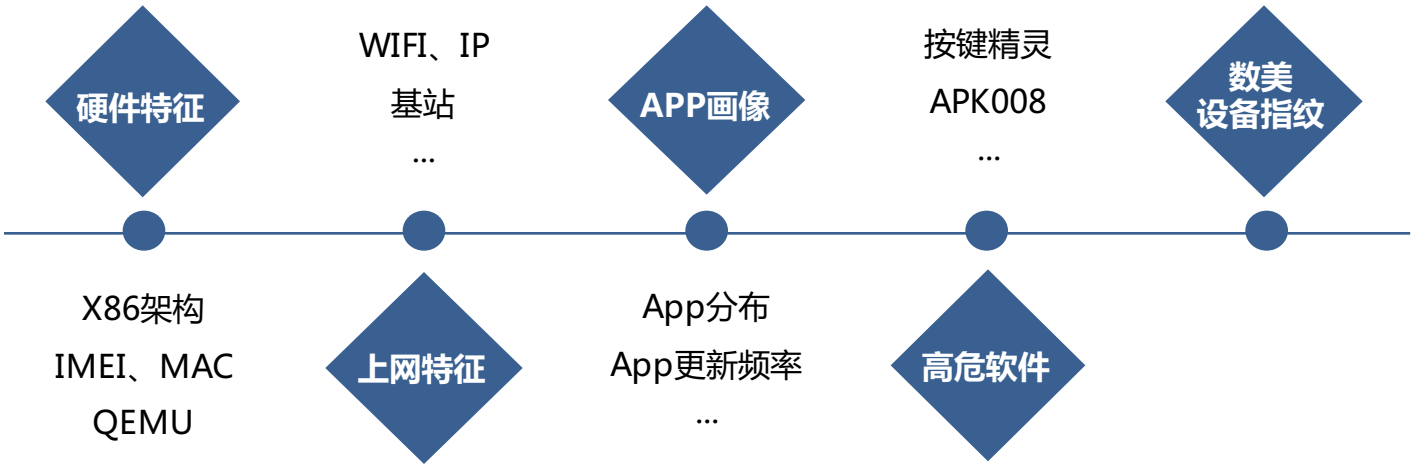
对虚拟机 、设备农场等，等风险设备进行识别

对机器注册 、撞库攻击、异常活跃等风险行为进行识别

对欺诈团伙，高危群体进行识别

策略体系：设备风险识别

基于软硬件特征、上网环境、设备指纹等**100+**基础维度、**11亿+**的样本库，采用**聚类分析、GBM**等技术构建风险设备识别模型，有效识别**虚拟机、篡改设备**和**设备农场**等高风险设备。



策略体系：行为风险识别

基于**机器操作、异常操作识别**等技术，识别机器注册、机器养号、撞库攻击、账号盗用、问题渠道、薅羊毛等风险操作与风险行为。

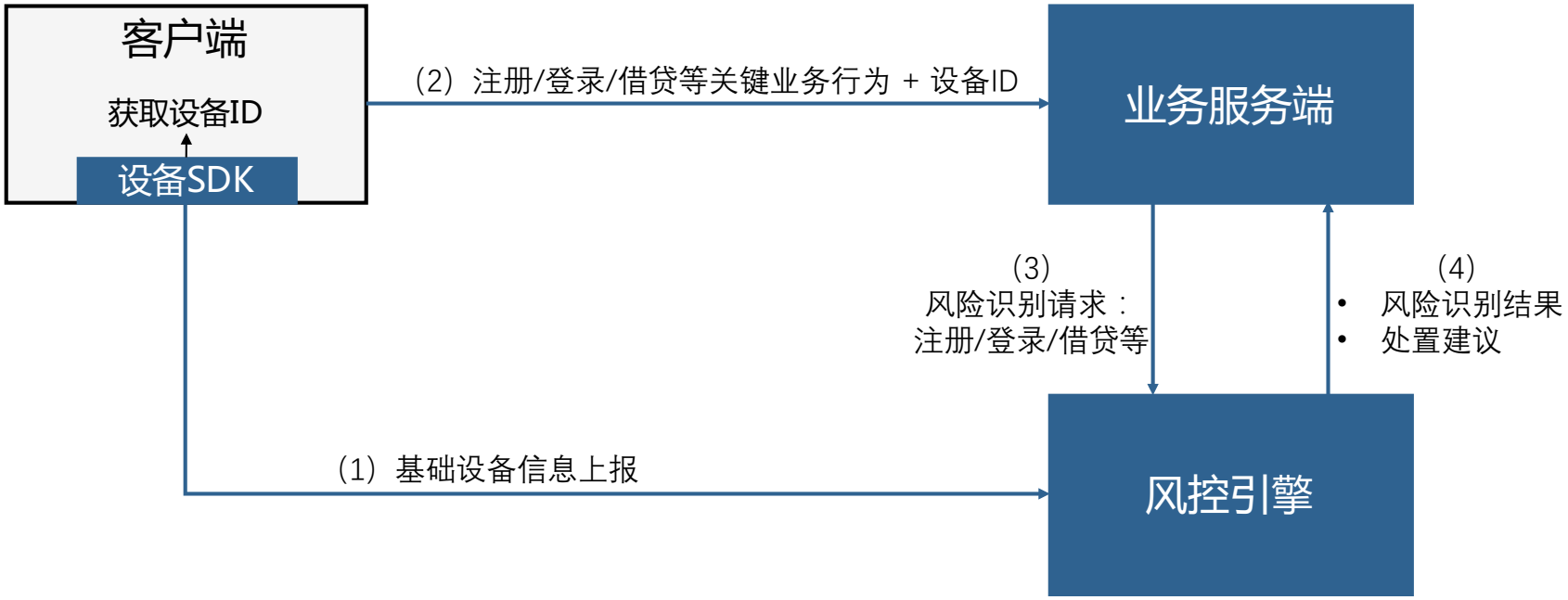
策略体系：关联风险挖掘

基于手机号、设备、IP等实体，采用**连通图挖掘、频繁子图挖掘、PageRank风险传播**等关联分析技术进行**欺诈团伙挖掘**等**多种潜在或新型欺诈风险识别**。

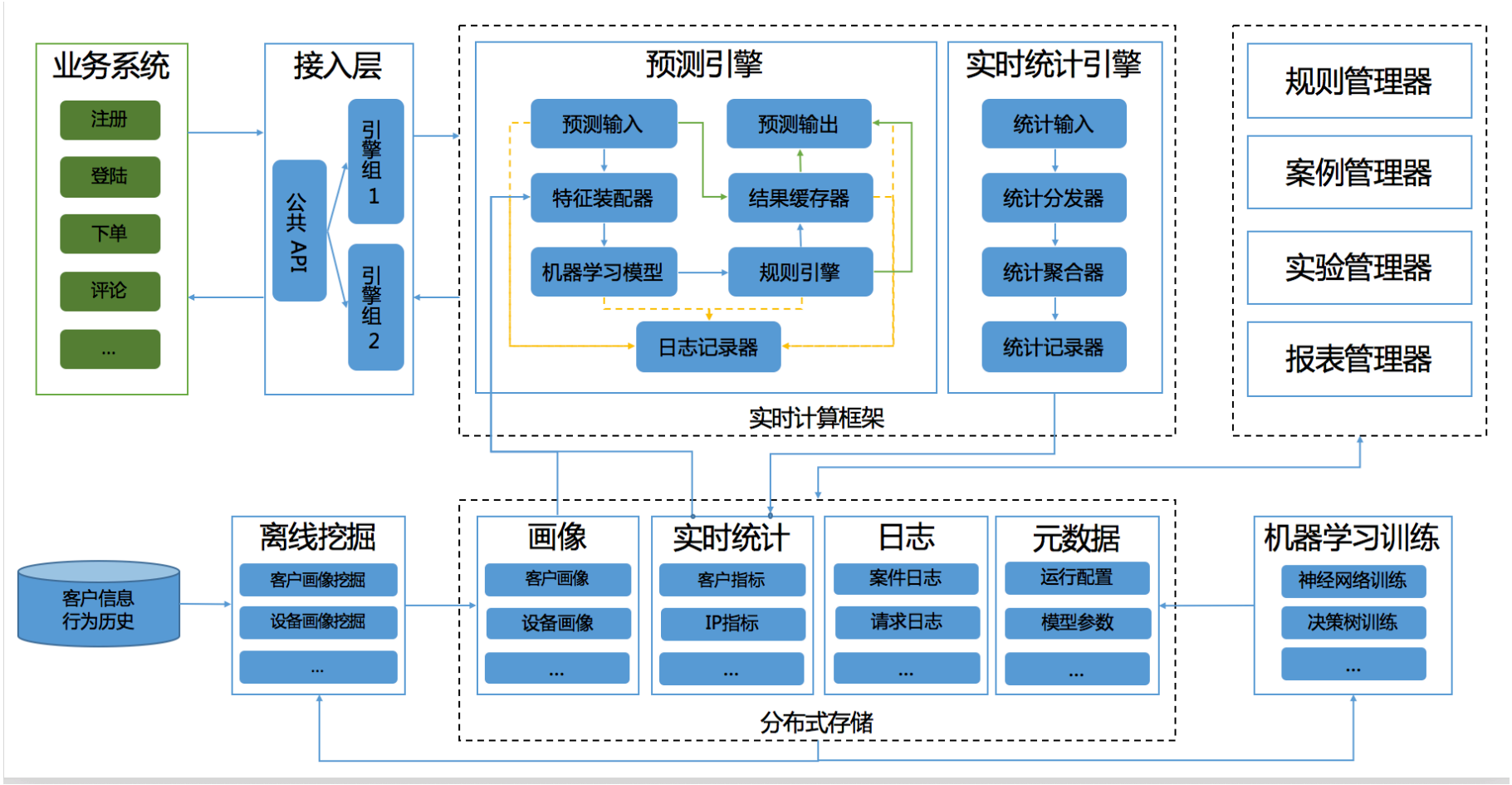
- 同IP关联设备、手机风险
- 同设备关联手机、IP风险
- 同手机关联设备、IP风险
- 同WIFI IP、设备、手机风险
- 紧急联系人风险
- 同紧急联系人关联风险

…

风控引擎：功能架构


客户端
获取设备ID
设备SDK
（2）注册/登录/借贷等关键业务行为 + 设备ID
业务服务端
（3）
风险识别请求：
注册/登录/借贷等
（4）
• 风险识别结果
• 处置建议
（1）基础设备信息上报
风控引擎

风控引擎：引擎架构


业务系统
注册
登陆
下单
评论
...
接入层
公共 API
引擎组 1
引擎组 2
预测引擎
预测输入
预测输出
特征装配器
结果缓存器
机器学习模型
规则引擎
日志记录器
实时统计引擎
统计输入
统计分发器
统计聚合器
统计记录器
实时计算框架
规则管理器
案例管理器
实验管理器
报表管理器
客户信息
行为历史
离线挖掘
客户画像挖掘
设备画像挖掘
...
画像
客户画像
设备画像
...
实时统计
客户指标
IP指标
...
日志
案件日志
请求日志
...
元数据
运行配置
模型参数
...
分布式存储
机器学习训练
神经网络训练
决策树训练
...

提纲

- 背景介绍
- 风控引擎
- 实施

实施步骤：持续对抗

- 针对业务场景建模、制定策略

- 业务风险点梳理
- 黑产路径分析
- 制定反欺诈方案

- **持续运营、监控、迭代**

实施：感想

- 策略
  - 持续运营，构建体系
  - 核心策略特征保密
  - 全局风险画像
  - 寻找“团伙”
- 架构
  - 微服务
  - 便捷的规则配置
  - 在线镜像/分流实验
  - 多维可扩展实时统计引擎

谢谢

www.ishumei.com

400-610-3866

GIAC 全球互联网架构大会

GLOBAL INTERNET ARCHITECTURE CONFERENCE

关注公众号获得
更多案例实践