业务安全与反欺诈

全链路治理总结与探索

华泰证券 信息安全中心 丁安安

业务安全-场景与类型

对日常业务的运营和增长进行保障

全链路治理体系

问题

- 安全意识低
- 信息泄露
- 信息流转/买卖

- 盗卡/盗账户
- 垃圾注册
- 营销作弊
- ……

- 黑产持续攻击
- 风控效能退化

事前

事中

事后

治理

- 情报建设
- 安全教育
- 实时风控
- 离线分析
- 线下打击
- 风控生命周期管理

丰富数据维度

- 身份
- 行为
- 关系
- 环境
- 设备
- 标签

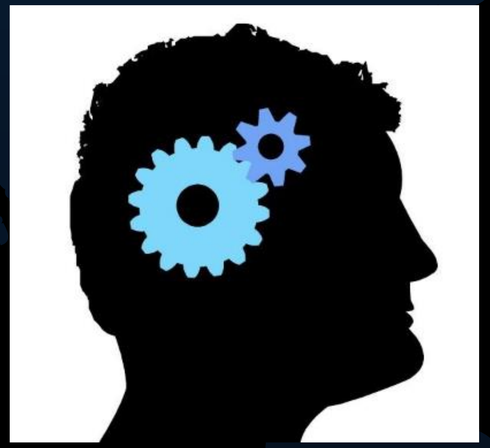
完善平台建设

- 风控引擎
- 变量计算
- 机器学习

多职能联动

- 公安
- 业务
- 审理

事前：将风险扼杀在摇篮



提高用户安全意识

- 抖音：反诈者集合
- 支付宝：反诈侦探
- 各地的官方反诈中心

内部规范和监控建设

- 钓鱼邮件演练
- 数据安全监控和全周期管理
- 法律规范和定期的宣讲

黑产情报获取

- 团伙情报与攻击倾向
- 产业链与行业研究

事中：风险防控体系总结

快速判断

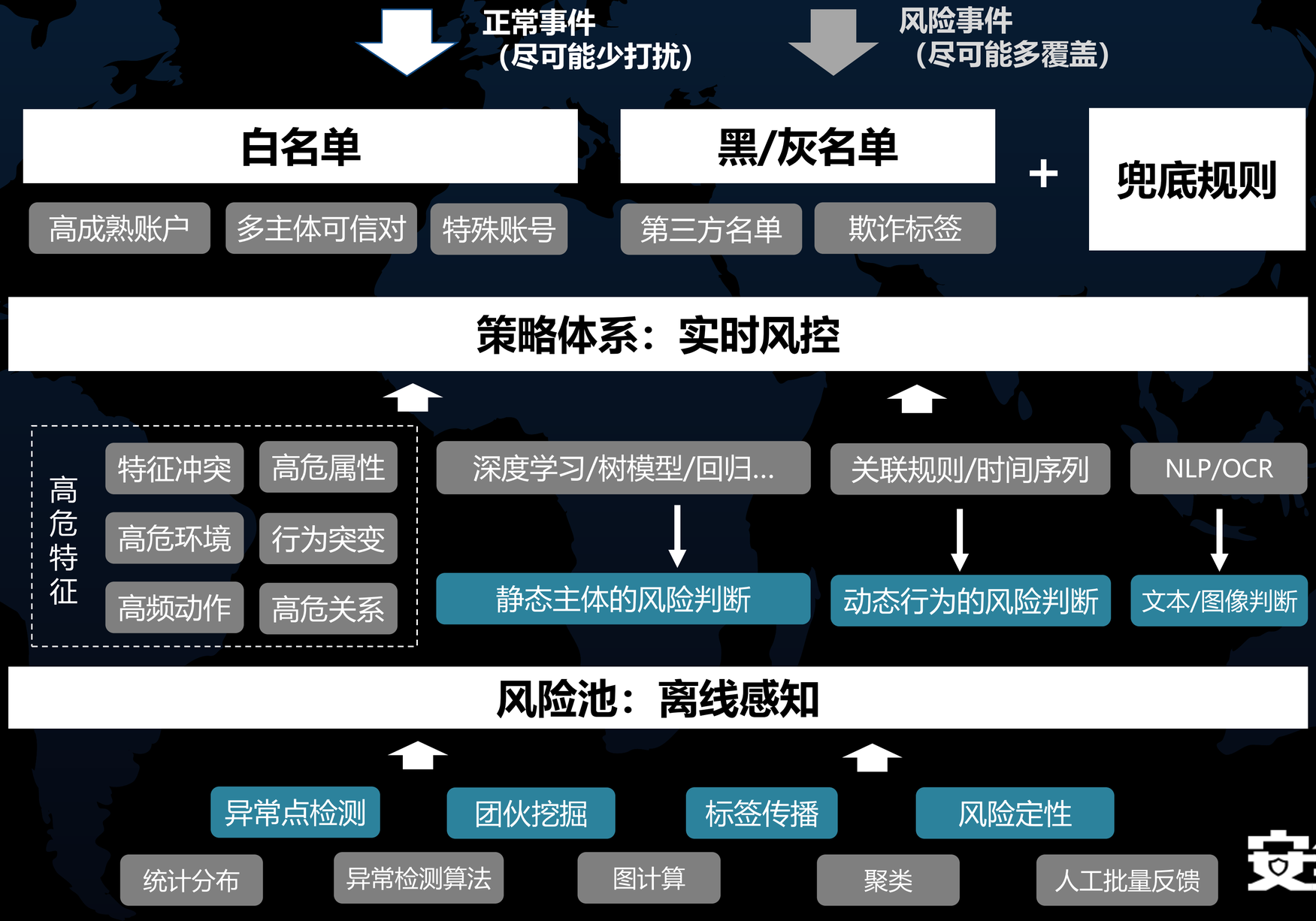
- 高准确率快速判断

实时分析

- 并行深度分析

离线挖掘

- 事中快速感知



事中：风险防控体系总结

快速判断

白名单

高成熟账户　多主体可信对　特殊账号

黑/灰名单

第三方名单　欺诈标签

\+

兜底规则

目的

- 减少风控引擎的压力
- 减少误稽核

要求：

- 准确率高、逻辑简单
- 命中后直接放过或者拒绝
- 兜底防悲剧

事中：风险防控体系总结

不同的场景

（登陆/注册/业务活动...）

＋

不同的风险敞口

账户　设备　环境　行为　模型　...

＋

不同的管控

（接受/拒绝/强校验/观察）

低耦合、上线下线互不影响

- 不同风险类型分级管控
- 策略便于维护管理

实时分析

策略体系：实时风控

高危特征：属性冲突　高危属性　高危环境　行为突变　高频动作　高危关系

深度学习/树模型/回归...　关联规则/时间序列　NLP/OCR

静态主体的风险判断　动态行为的风险判断　文本/图像判断

登陆风险　注册风险　领券风险　支付风险　校验风险

账户风险　设备风险　.....

事中：风险防控体系总结

不同的场景（登陆/注册/业务活动...）

＋

不同的风险敞口

账户 | 设备 | 环境 | 行为 | 模型 | ...

＋

不同的管控（接受/拒绝/强校验/观察）

低耦合、上线下线互不影响

- 不同风险类型分级管控
- 策略便于维护管理

实时分析

策略体系：实时风控

高危特征：属性冲突、高危属性、高危环境、行为突变、高频动作、高危关系

深度学习/树模型/回归... → 静态主体的风险判断

关联规则/时间序列 → 动态行为的风险判断

NLP/OCR → 文本/图像判断

活动作弊：注册 → 登陆 → 领券/红包 → 解绑

账号被盗：登陆 → 浏览1 → 浏览2 → 浏览3 → 换绑 → 改密

事中：风险防控体系总结

不同的场景（登陆/注册/业务活动...）

＋

不同的风险敞口

账户 | 设备 | 环境 | 行为 | 模型 | ...

＋

不同的管控（接受/拒绝/强校验/观察）

低耦合、上线下线互不影响
- 不同风险类型分级管控
- 策略便于维护管理

实时分析

策略体系：实时风控

高危特征：属性冲突 | 高危属性 | 高危环境 | 行为突变 | 高频动作 | 高危关系

深度学习/树模型/回归... → 静态主体的风险判断

关联规则/时间序列 → 动态行为的风险判断

NLP/OCR → 文本/图像判断

行为埋点数据（浏览、点击、停留...）

行为A 行为B 行为A 行为D → 欺诈

行为A 行为B 行为D → 欺诈

行为A 行为E 行为R 行为D → 欺诈

→ 行为A 行为D → 高危行为

事中：风险防控体系总结

不同的场景（登陆/注册/业务活动...）

＋

不同的风险敞口

账户　设备　环境　行为　模型　...

＋

不同的管控（接受/拒绝/强校验/观察）

低耦合、上线下线互不影响

- 不同风险类型分级管控
- 策略便于维护管理

实时分析

策略体系：实时风控

高危特征：属性冲突　高危属性　高危环境　行为突变　高频动作　高危关系

深度学习/树模型/回归... → 静态主体的风险判断

关联规则/时间序列 → 动态行为的风险判断

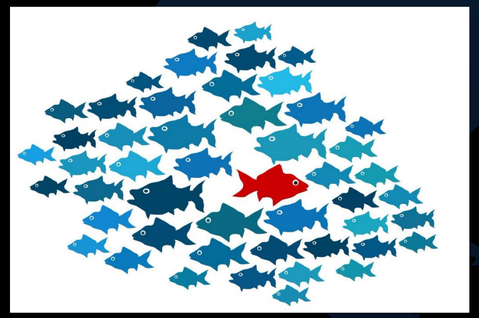
NLP/OCR → 文本/图像判断

Embedding

相似度计算

.....

事中：风险防控体系总结



风险漏过的可能

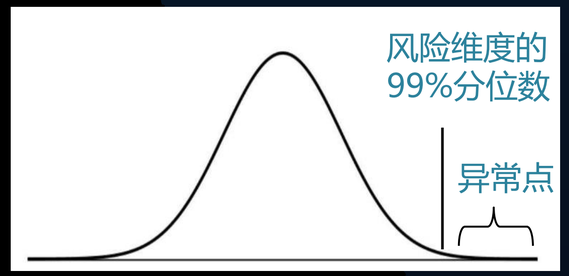
1）冷启动时，无标签或者少标签

2）新生风险发生时

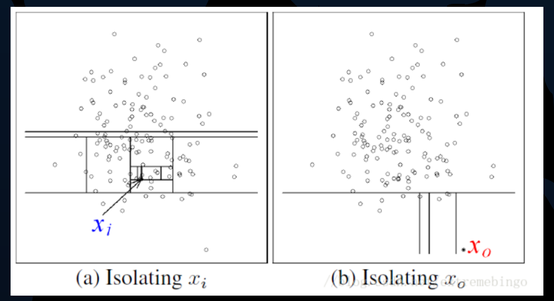
3）风险程度不确定，待观察

1. 通过风险“离群”和“异常”的特性，进行异常检测，适用于风控冷启动时，对风控进行兜底

统计分布



Isolation Forest



- ✓ 多元分布
- ✓ One Class SVM
- ✓ PCA
- ✓ LOF

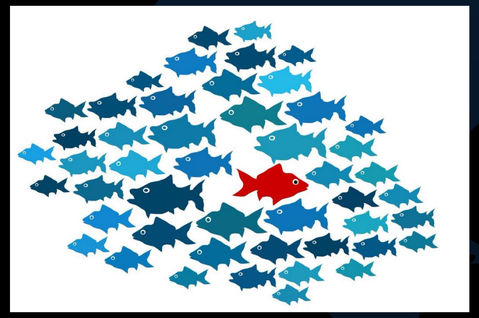
离线挖掘

风险池：离线感知

异常点检测 | 团伙挖掘 | 标签传播 | 风险定性

统计分布 | 异常检测算法 | 图计算 | 聚类 | 人工批量反馈

事中：风险防控体系总结



风险漏过的可能

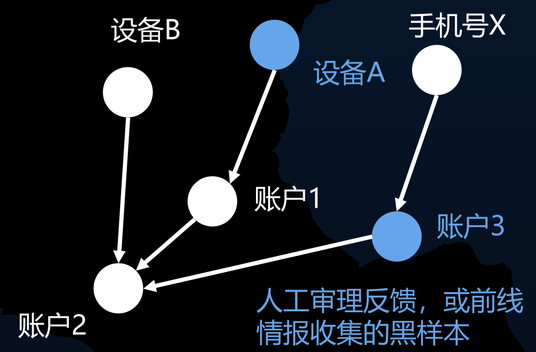
1）冷启动时，无标签或者少标签

2）新生风险发生时

3）风险程度不确定，待观察

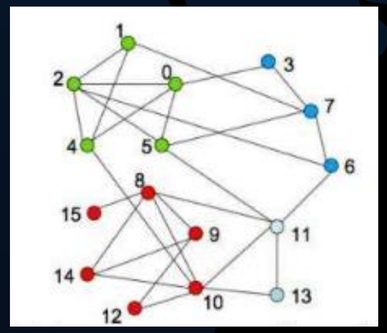
2. 通过风险团伙“关联”或“相似”的特性，进行标签传播和关系聚类，适用新生批量风险/团伙的快速发现感知

标签传播



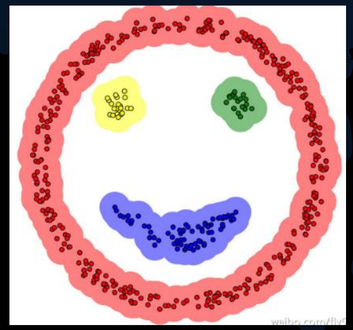
通过N度邻居的风险标签，对每个点进行风险标签进行传播

社区发现-fast unfolding



对划分出来的社区，结合风险统计指标进行风险团伙发现

特征聚类-DBSCAN



对账户的风险特征、手法进行聚类，发现新的团伙或者批量手法

加我v信 12345
加 我 v 信 1 2 3 4 5
加-v-x 1-2-3-4-5
加.我vx 12345
+VX 123.45

nan jing dong lu 100, USA
n a n j I n g d o n g l u 1 0 0, U S A
nan..jing..dong..lu..100……USA

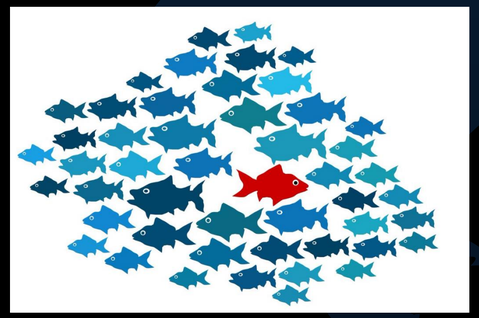
离线挖掘

风险池：离线感知

异常点检测 | 团伙挖掘 | 标签传播 | 风险定性

统计分布 | 异常检测算法 | 图计算 | 聚类 | 人工批量反馈

事中：风险防控体系总结



风险漏过的可能

1）冷启动时，无标签或者少标签

2）新生风险发生时

3）风险程度不确定，待观察

3. 对于不确定的风险，可以放入风险池进行观察、调查、处置，T+1将风险闭环处理

- 业务反馈
- 异常波动

- 风险浓度

- 归因分析
- 多维分析

- 名单/策略

批量分析 → 新生风险

离线挖掘

风险池：离线感知

异常点检测 | 团伙挖掘 | 标签传播 | 风险定性

统计分布 | 异常检测算法 | 图计算 | 聚类 | 人工批量反馈

事中：风险防控体系总结

快速判断

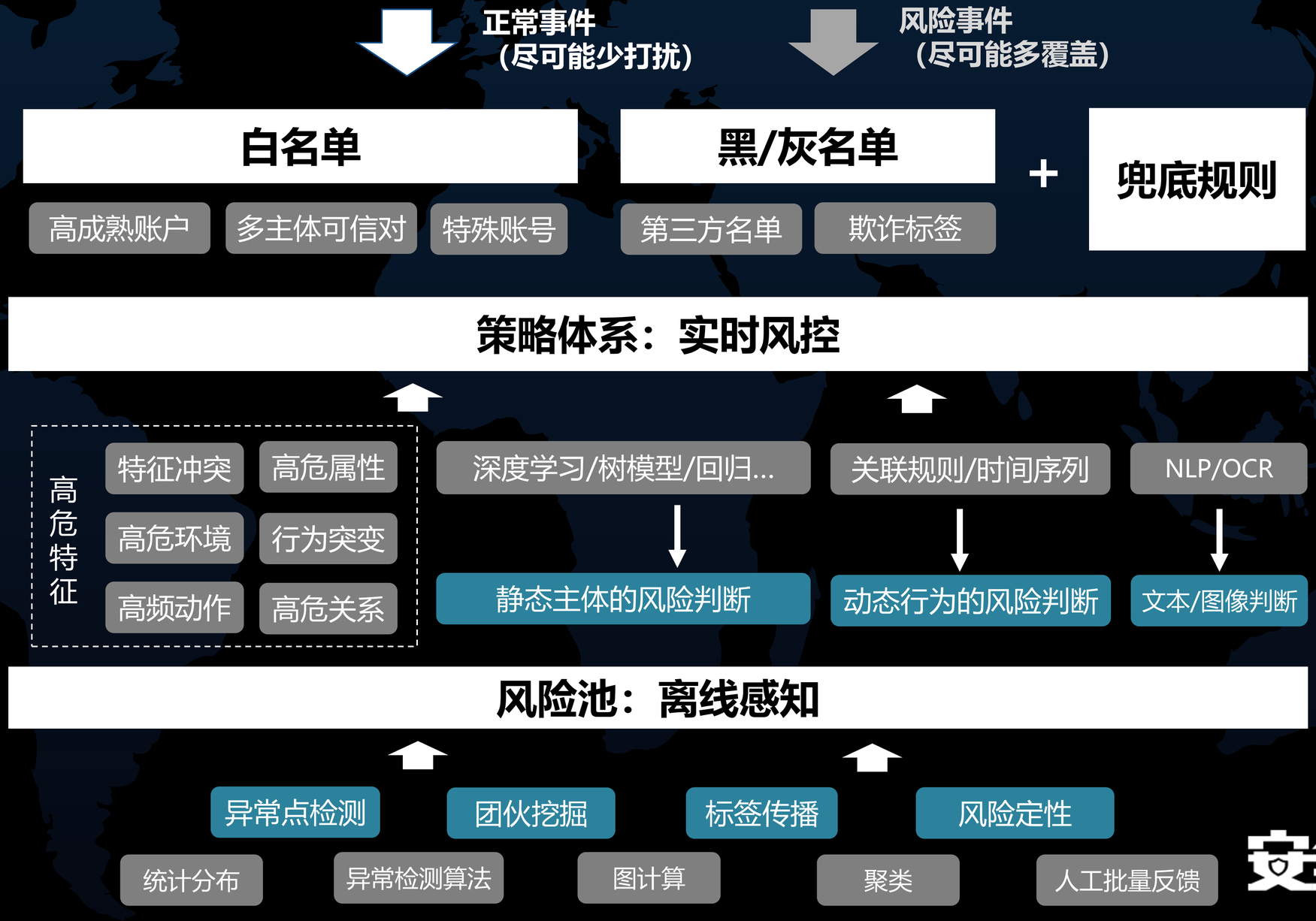
- 高准确率快速判断

实时分析

- 并行深度分析

离线挖掘

- 事中快速感知



事后：安全生态治理

黑产持续攻击

线下打击

运营商 + 媒体 + 公安 + 金融机构

羊毛/赌博/盗用/黄牛/诈骗

风控效能退化

风控生命周期管理

效能监控

名单退出

策略下线

模型迭代

策略归并

策略D

策略A

策略C

策略A

总结：全链路治理体系

问题

- 安全意识低
- 信息泄露
- 信息流转/买卖

- 盗卡/盗账户
- 垃圾注册
- 营销作弊
- ……

- 黑产持续攻击
- 风控效能退化

事前

事中

事后

治理

情报建设

安全教育

实时风控

离线分析

线下打击

风控生命周期管理

丰富数据维度

- 身份
- 环境
- 行为
- 设备
- 关系
- 标签

完善平台建设

- 风控引擎
- 变量计算
- 机器学习

多职能联动

- 公安
- 业务
- 审理


谢谢！