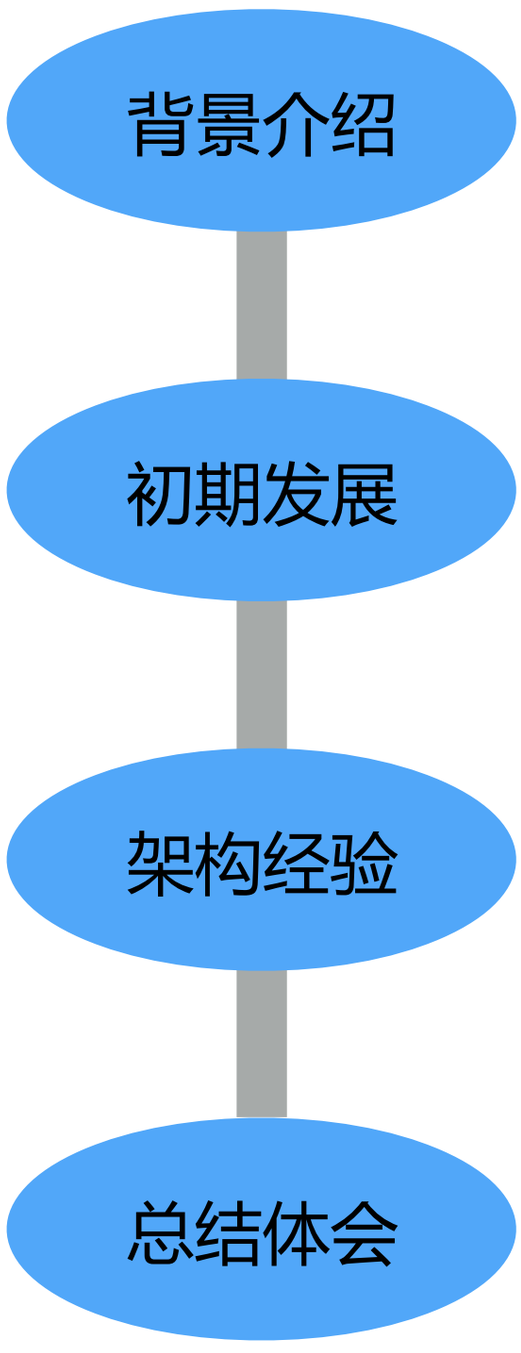
美团业务风控系统构建经验

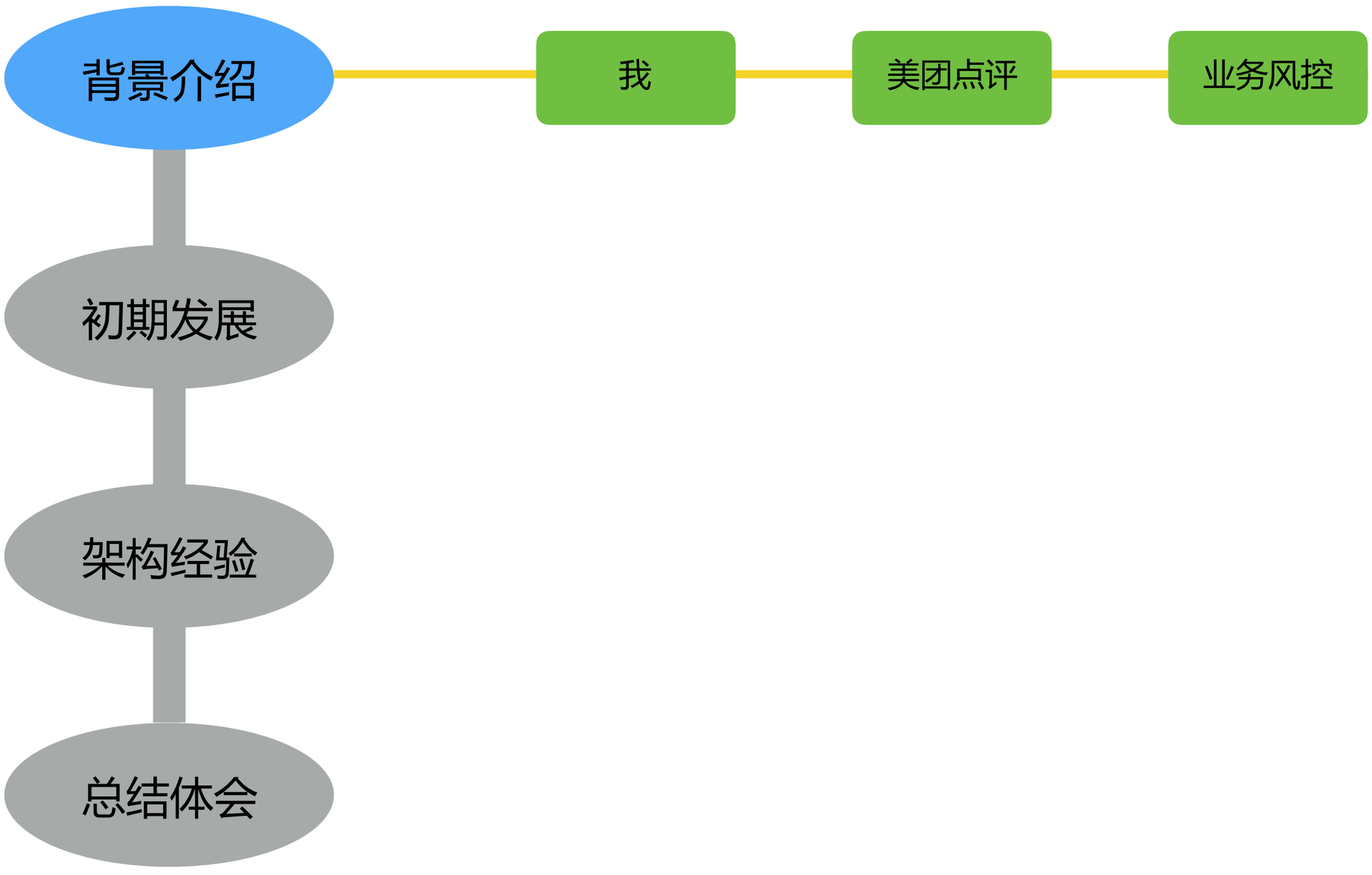
唐义哲
美团点评 风控

2016-10

目录



目录



我

2014中 美团 O2O 电商

业务风险控制 技术负责人

全业务线反作弊、反刷单、资金账户安全、反爬取

2008-2014 hulu 在线视频

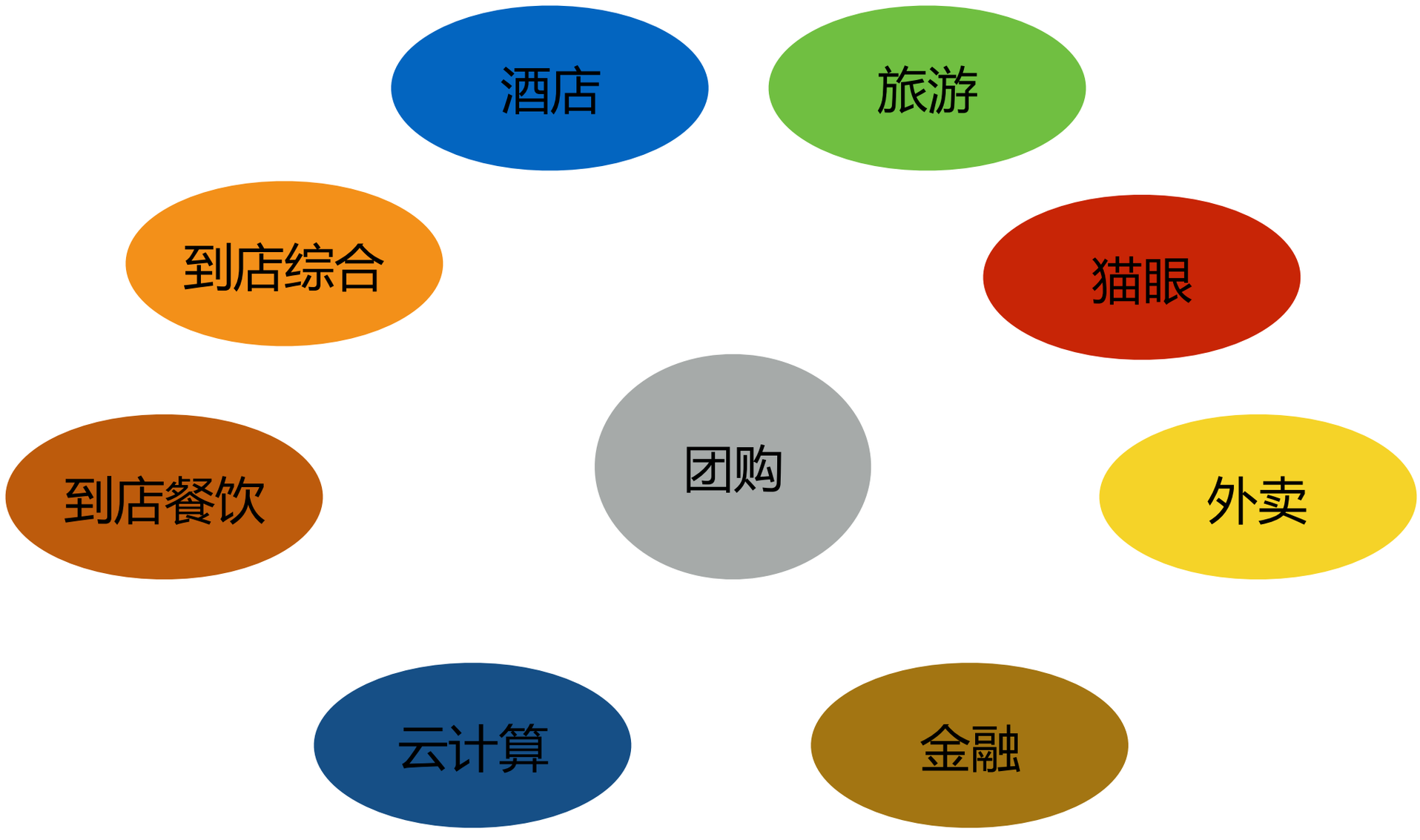
搜索

推荐

广告

用户定向平台

美团



业务风控

品类覆盖面广

用户多

商户多

高频交易

用户作弊

“薅羊毛”，促销、优惠

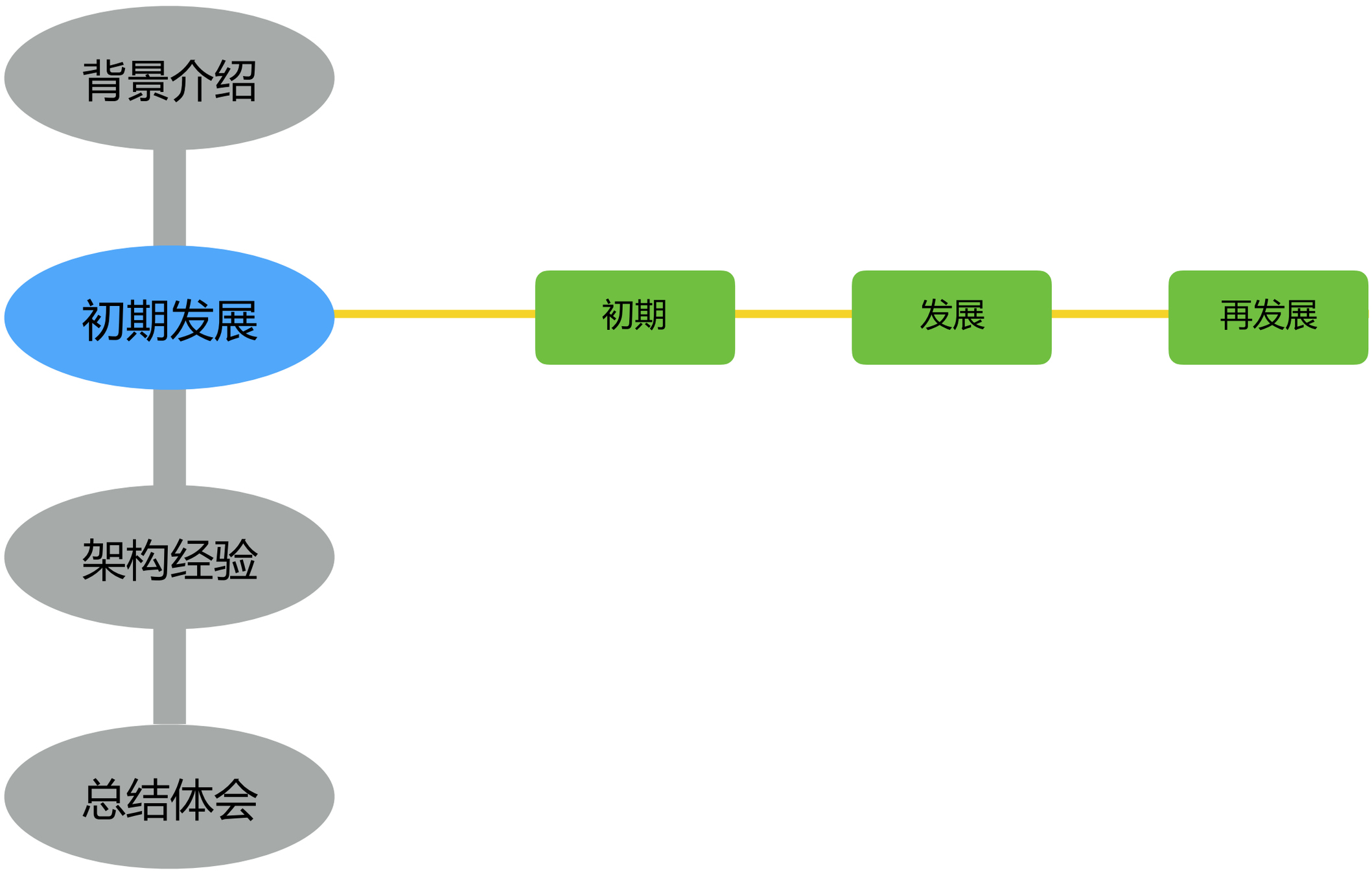
商家刷单

刷销量、排名、好评、...

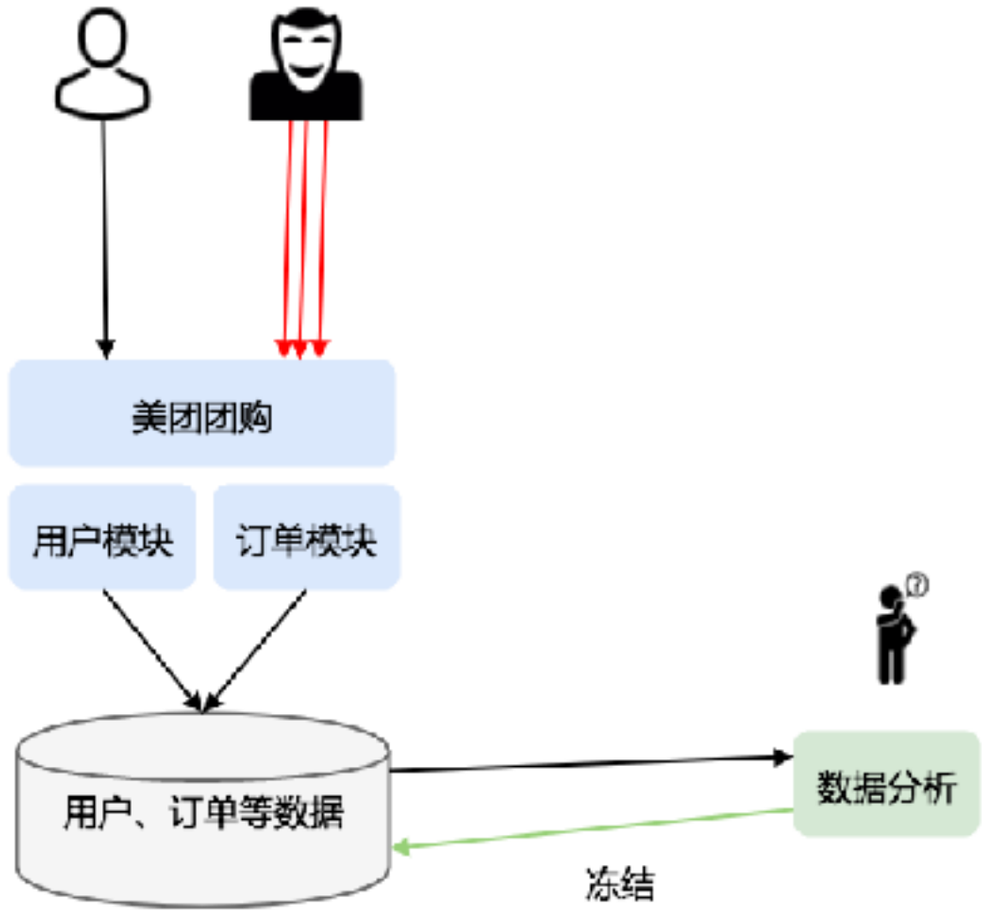
账户和支付安全

信息、余额、支付盗用

目录



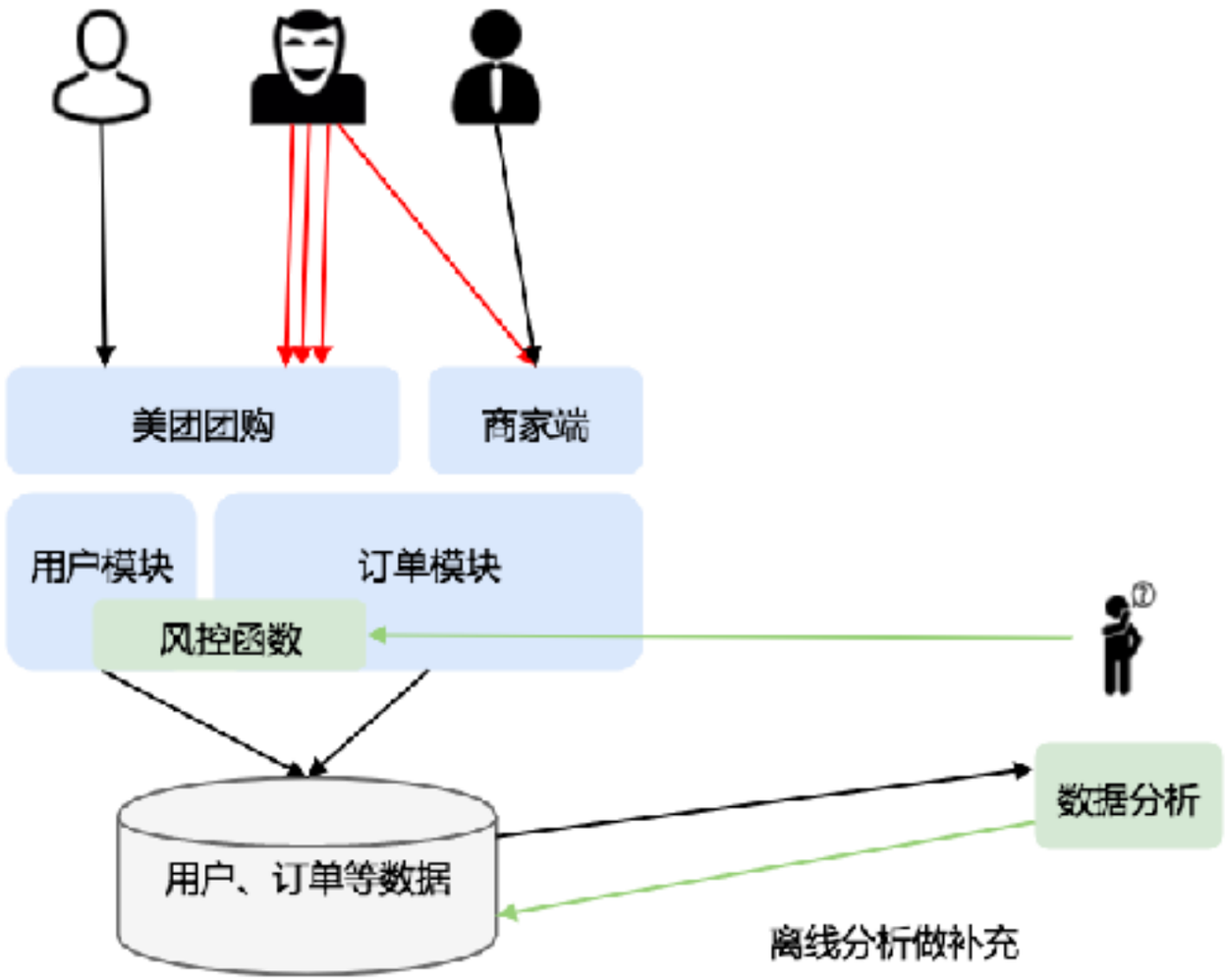
初期



单一团购，频繁注册、购买骗取优惠

数据分析，异步冻结

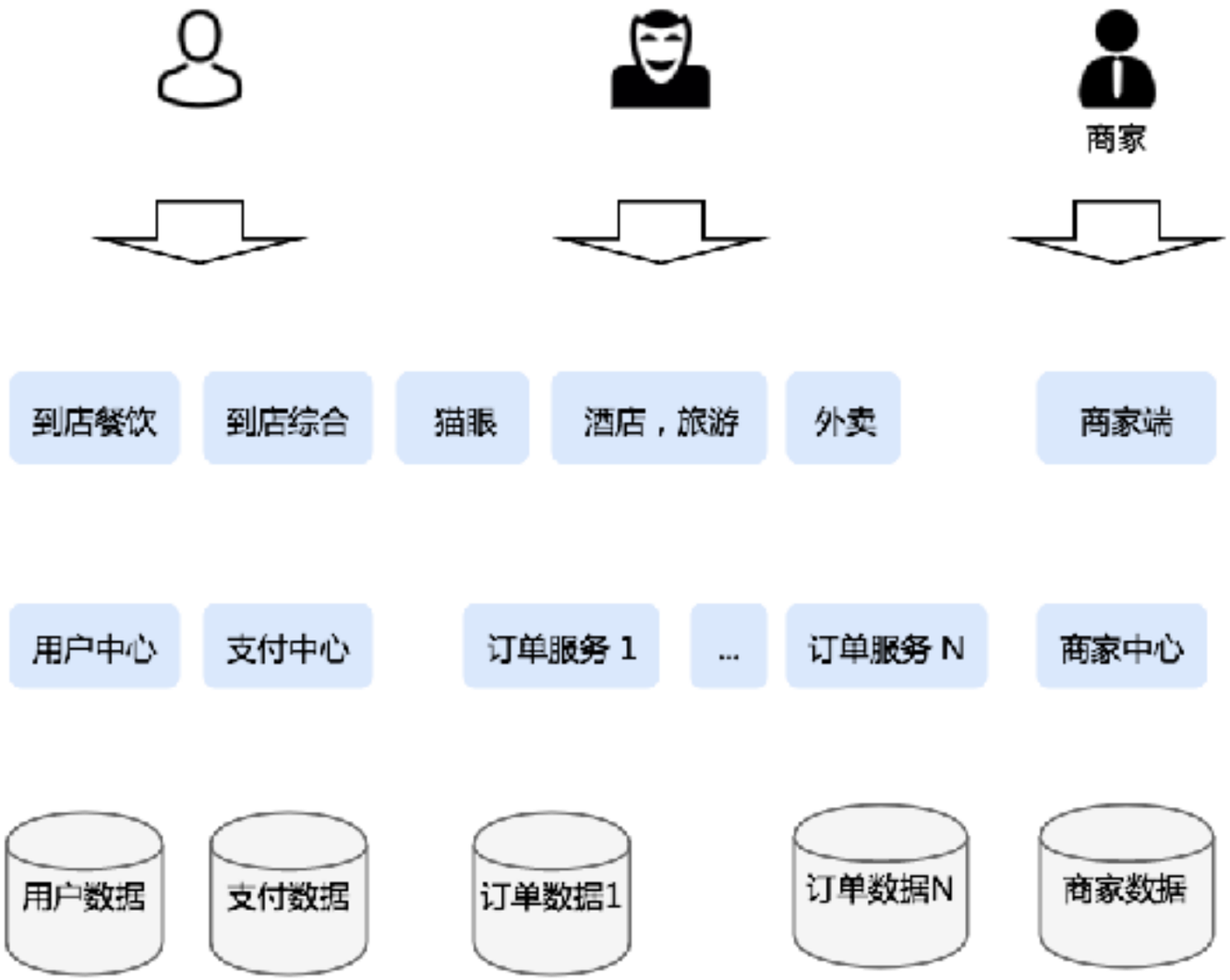
发展



快速销赃，联合商家

实时防御，离线分析补充

再发展



① 内部职责耦合
工程/策略
② 与业务方耦合
决策处理？

风险升级，业务扩张

独立团队，独立服务，加速迭代

挑战

① 业务多带来风险点多

购买、支付流程

用户操作

商家操作等

② 变化快

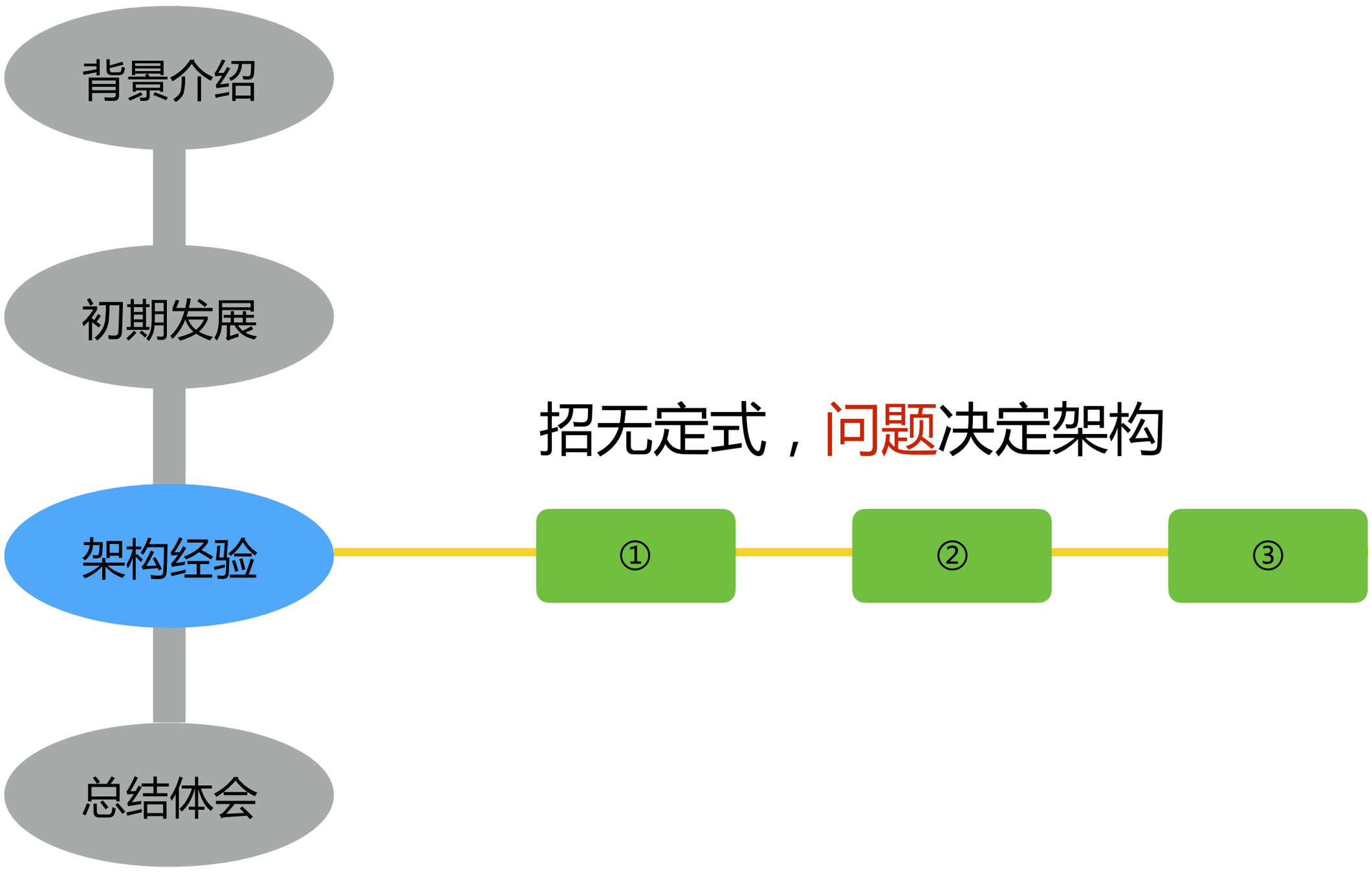
黑产升级

业务发展

环境变化

③ 我在明，敌在暗

目录



问题一

风险在哪，怎么控制？

对接

目标

感知风险 + 控制风险

感知什么？

- 谁
- 时间
- 环境
- 方式
- 对象
- 动作

控制什么？

站在坏人的角度想——利益

从利益找关联场景，思考控制点

促销优惠 -> 促销的下单、支付、...

销量、排名 -> 购买、创建活动、...

用户余额 -> 下单、支付、退款、...

对接

现实

业务多

X

前台多
后台多

X

场景多

近100个细分业务

iPhone, Android
i版, PC
移动后台, 订单中心
用户中心, 促销工具
商家后台, ...

购买流程

下单、支付、支付成功、配送成功等

用户操作

注册、登录、找回密码、换绑手机等

商家端操作

验券、新建促销、退款等

对接

关键

业务

V.S.

风控

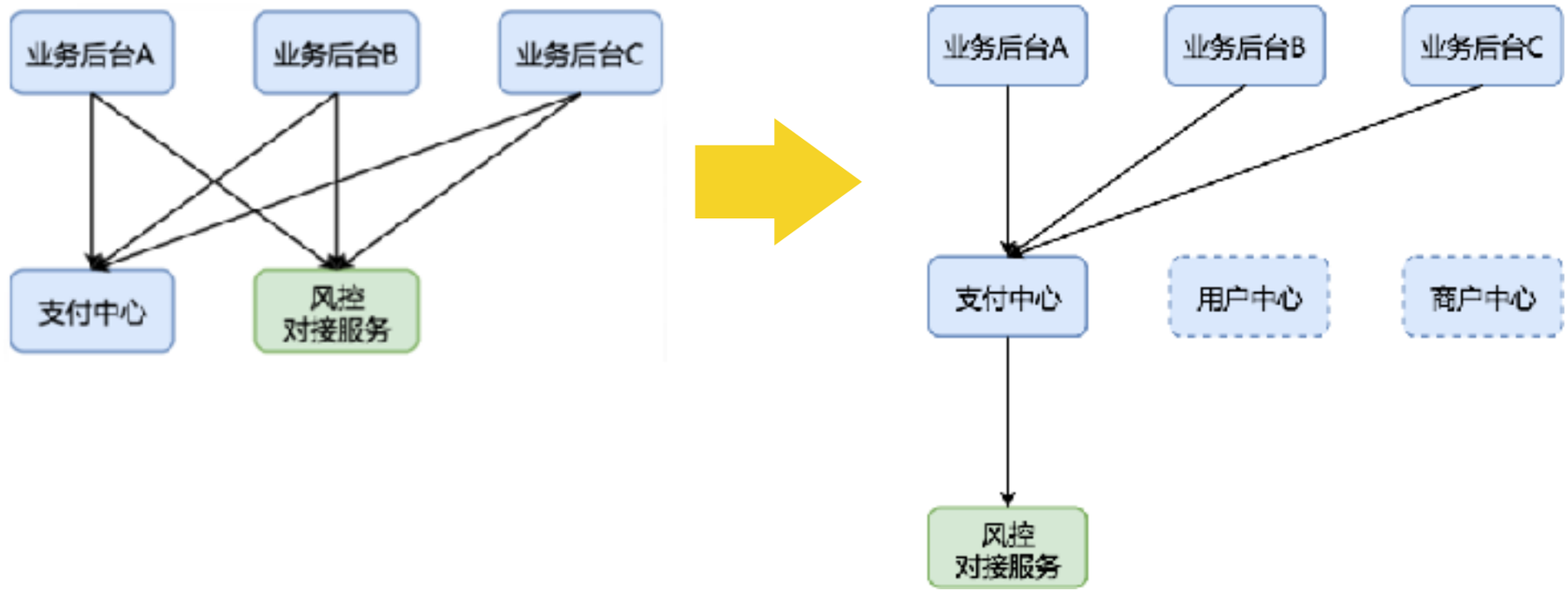
风控工作原则一

风控是业务产品的必要属性

做好服务者，把业务痛点降到最低

对接

对接成本



业务保证安全

使用风控工具

中间件保证安全

使用风控服务

对接

运行成本

稳定性 + 性能 + 善后

路径优先级

隔离 + 调优

外部依赖、组件依赖

降级

攻击

限流

同步接口、异步接口

迁移规则平台——并行

报表、客诉、

核查、赔付

2亿请求/日，90%响应时间36ms，稳定性5个9

问题二

黑衣服的是坏人 —— 但坏人会换上其他颜色

对抗

风控工作原则二 —— 持续对抗过程

策略

增加要素

模型+规则

减少强依赖

黑衣服 + 黑帽子的是坏人

策略网

模型问题？

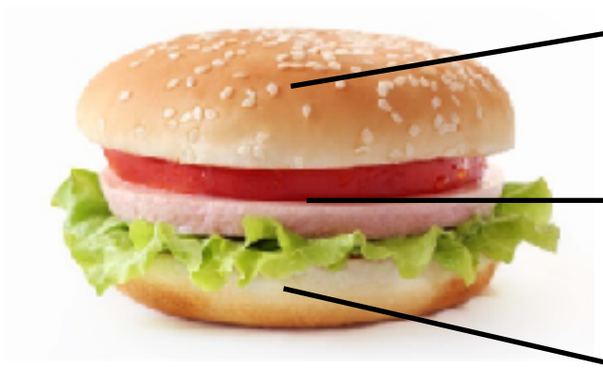
不稳定的算法问题

结合使用

对抗

效率

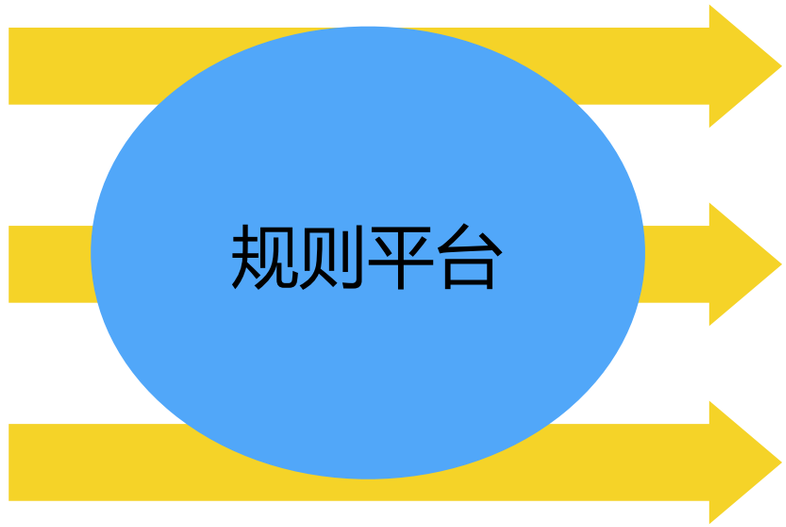
持久战的决定因素



产品：策略应用

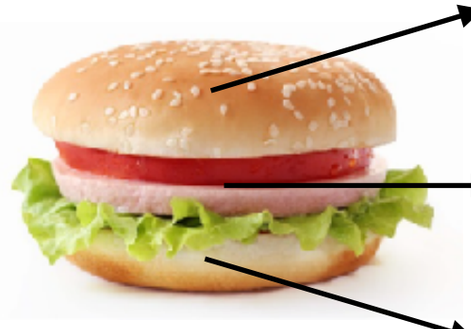
策略：策略开发

开发：系统开发



并行

对抗



策略应用

策略开发

系统开发

规则平台
标准化执行

请求

场景：规则集

仅计算一次+并行

合并决策

m x n

规则：决策单元

仅计算一次+并行

m x n

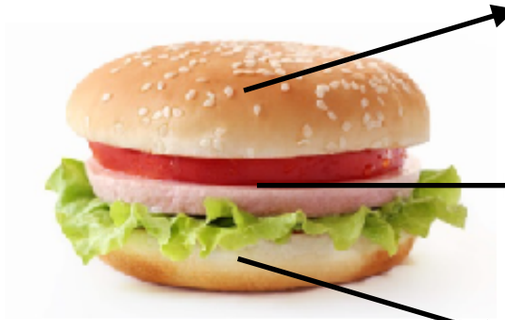
因子：逻辑单元

仅计算一次+并行

复用配置

动态执行提高性能

对抗



策略应用

策略开发

系统开发

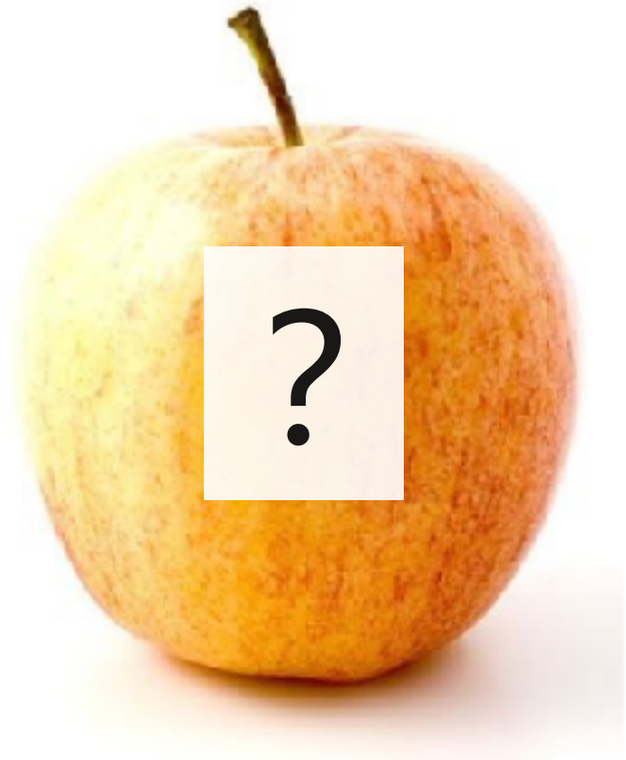
决策

松耦合：可配置

策略

对抗

决策

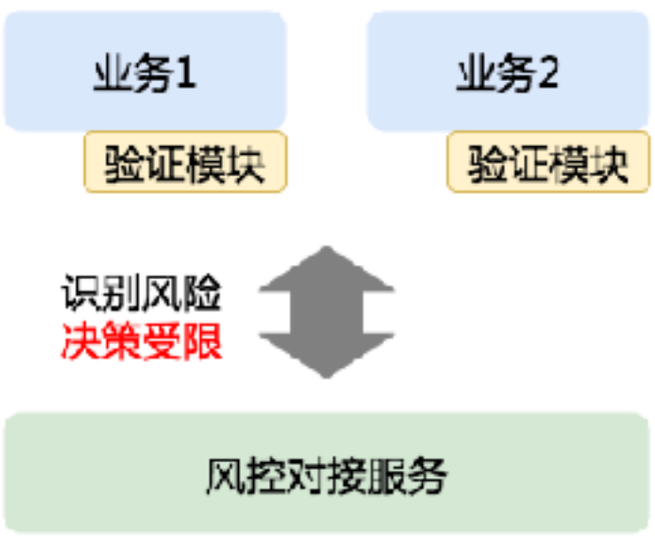


验证

对抗

验证

早期



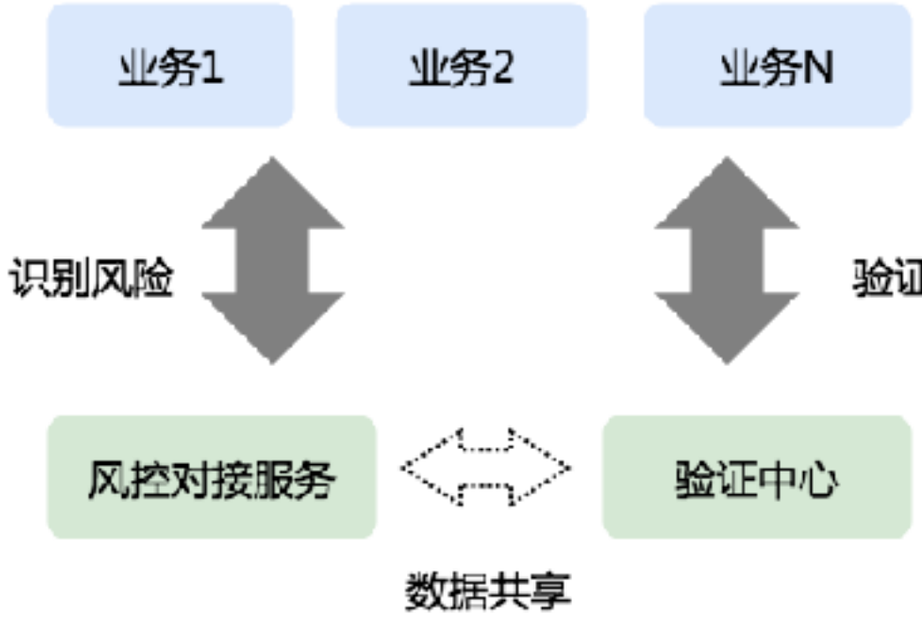
业务验证

业务开发负担

验证决策受限

“只管杀，不管埋”

改进



独立服务

身份+图灵

接入体验

“杀埋一条龙服务”

问题三

全面防守 V.S. 攻击弱点

对称

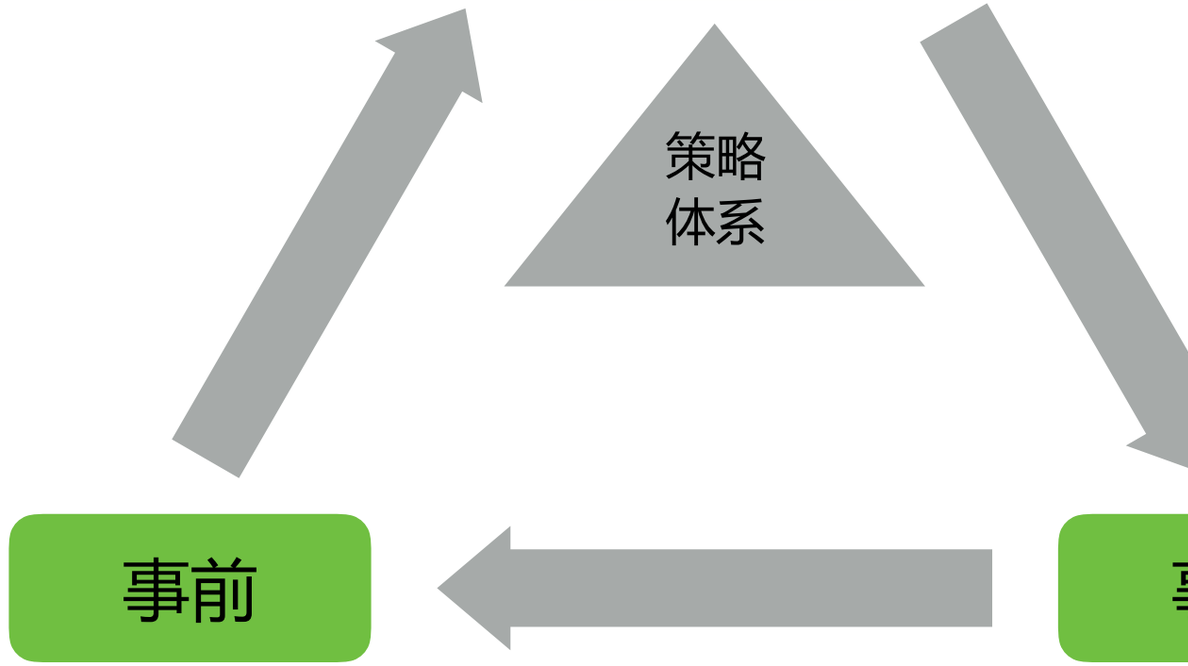
风控原则三

立体闭环防御

攻击

批量注册
接码平台
盗取银行卡
身份证
公民信息

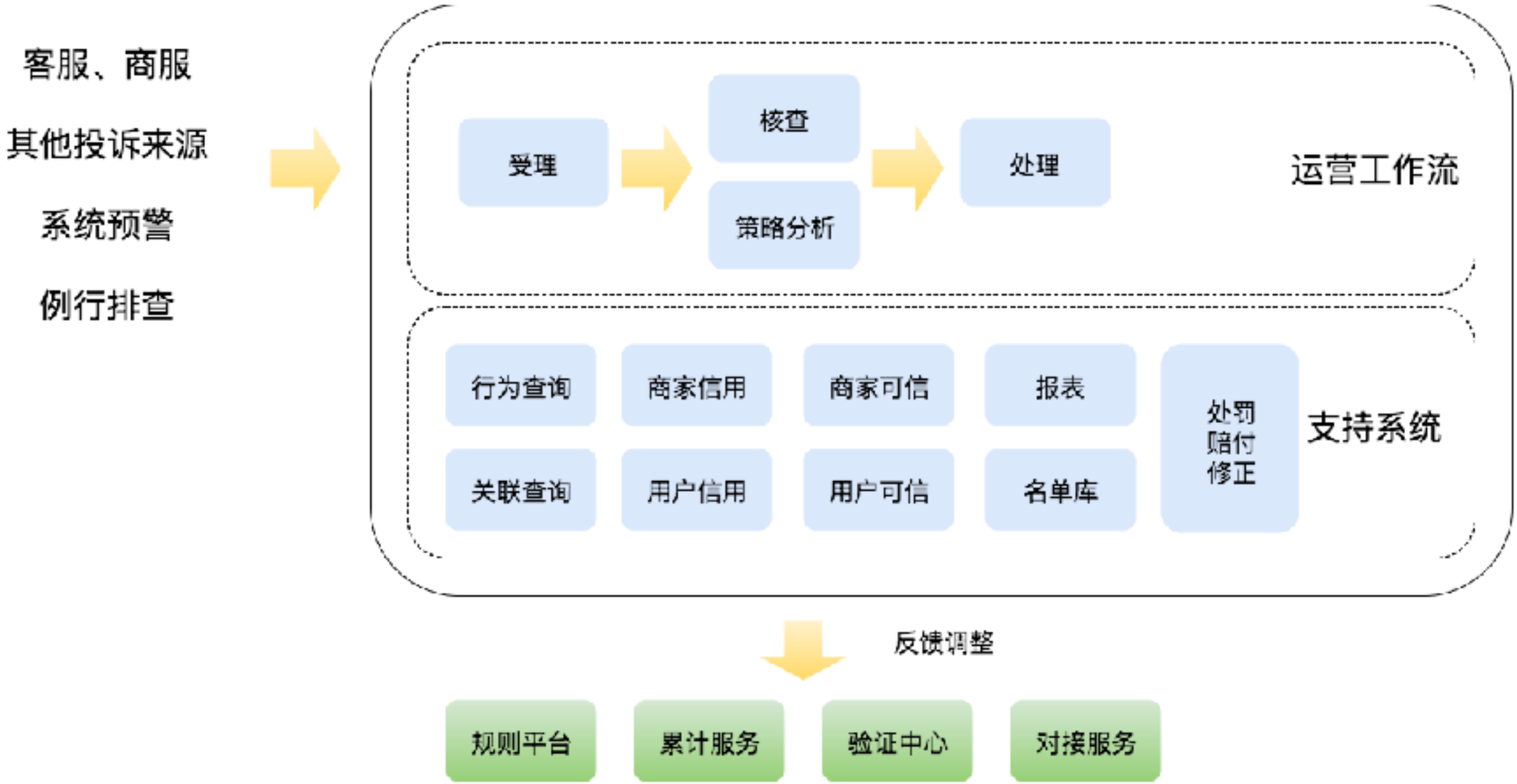
木马
伪基站
猫池
…



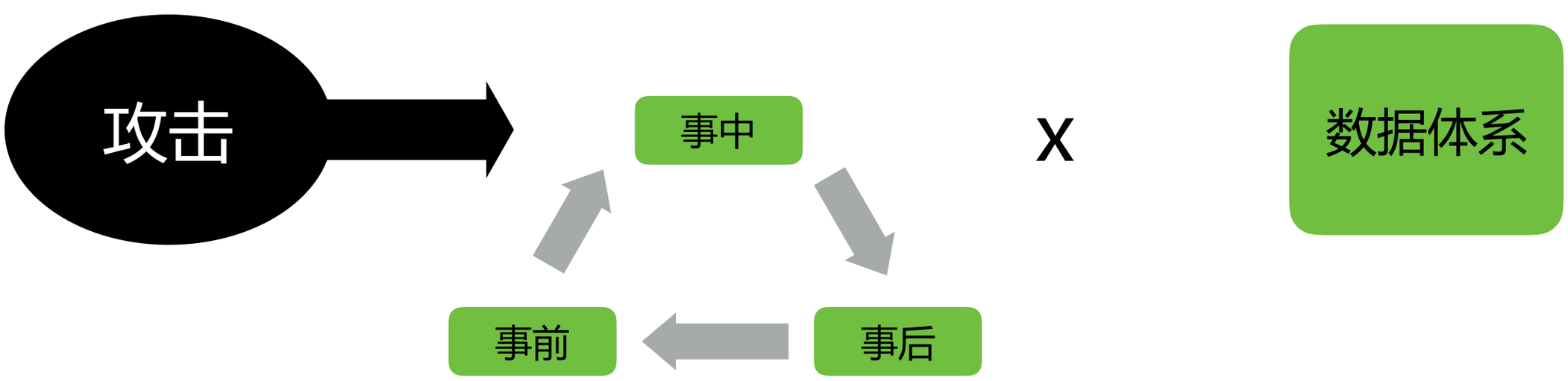
风险教育
参与业务
数据准备
主动防护

善后：客诉、核查、赔付
回归：监控、预警、优化

运营平台

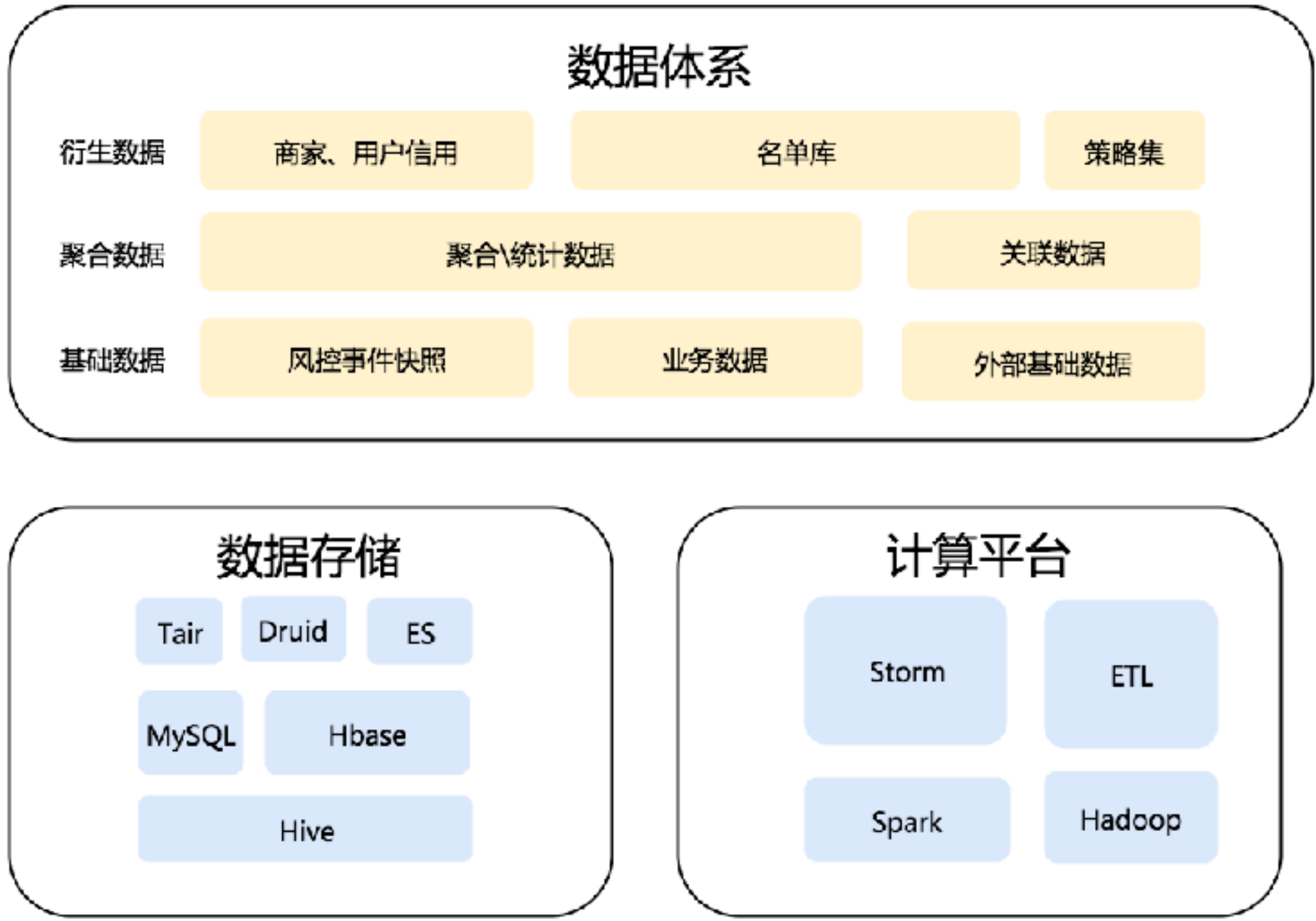

客服、商服
其他投诉来源
系统预警
例行排查
受理
核查
策略分析
处理
运营工作流
行为查询
商家信用
商家可信
报表
关联查询
用户信用
用户可信
名单库
处罚
赔付
修正
支持系统
反馈调整
规则平台
累计服务
验证中心
对接服务

对称



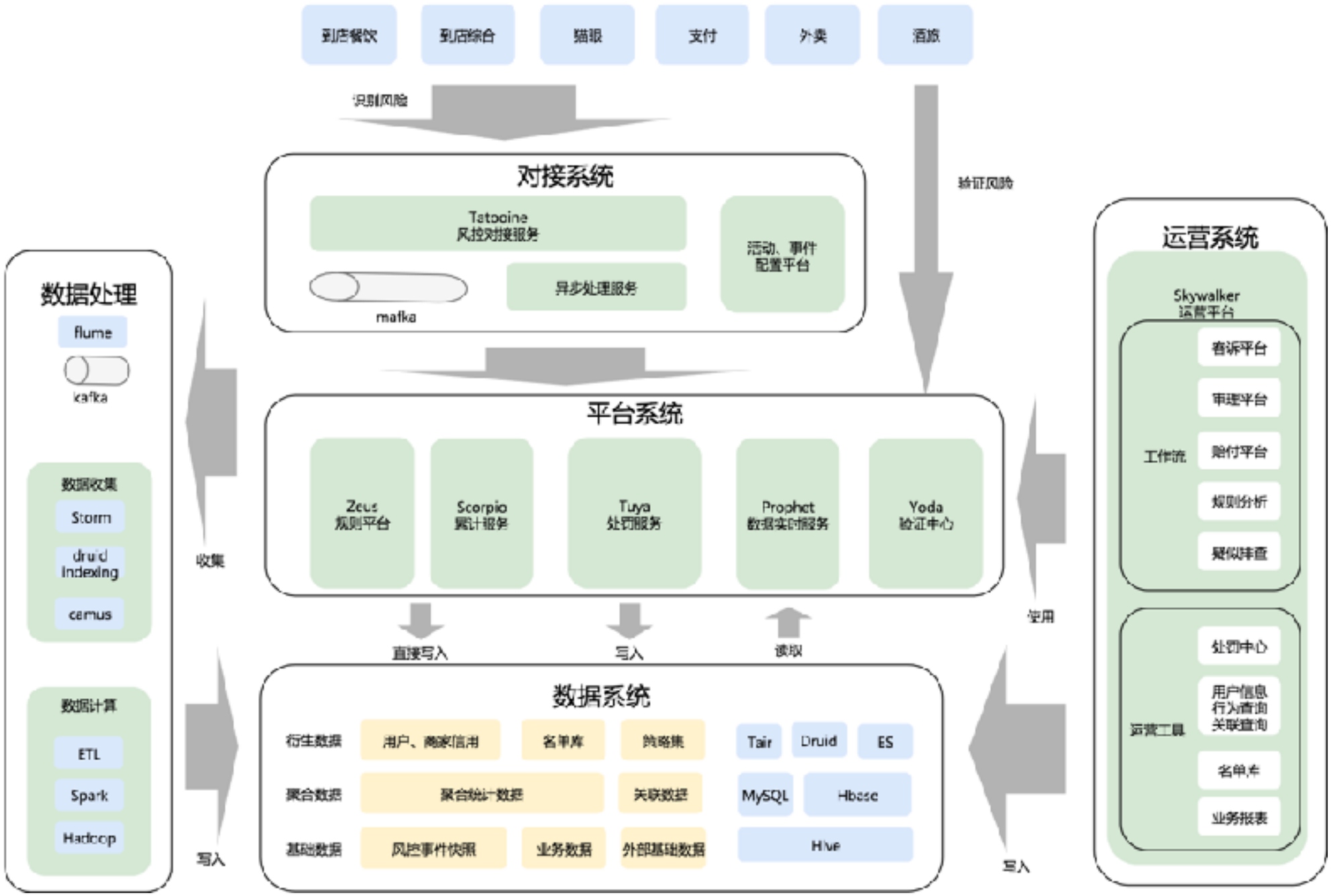
数据平台

数据收集

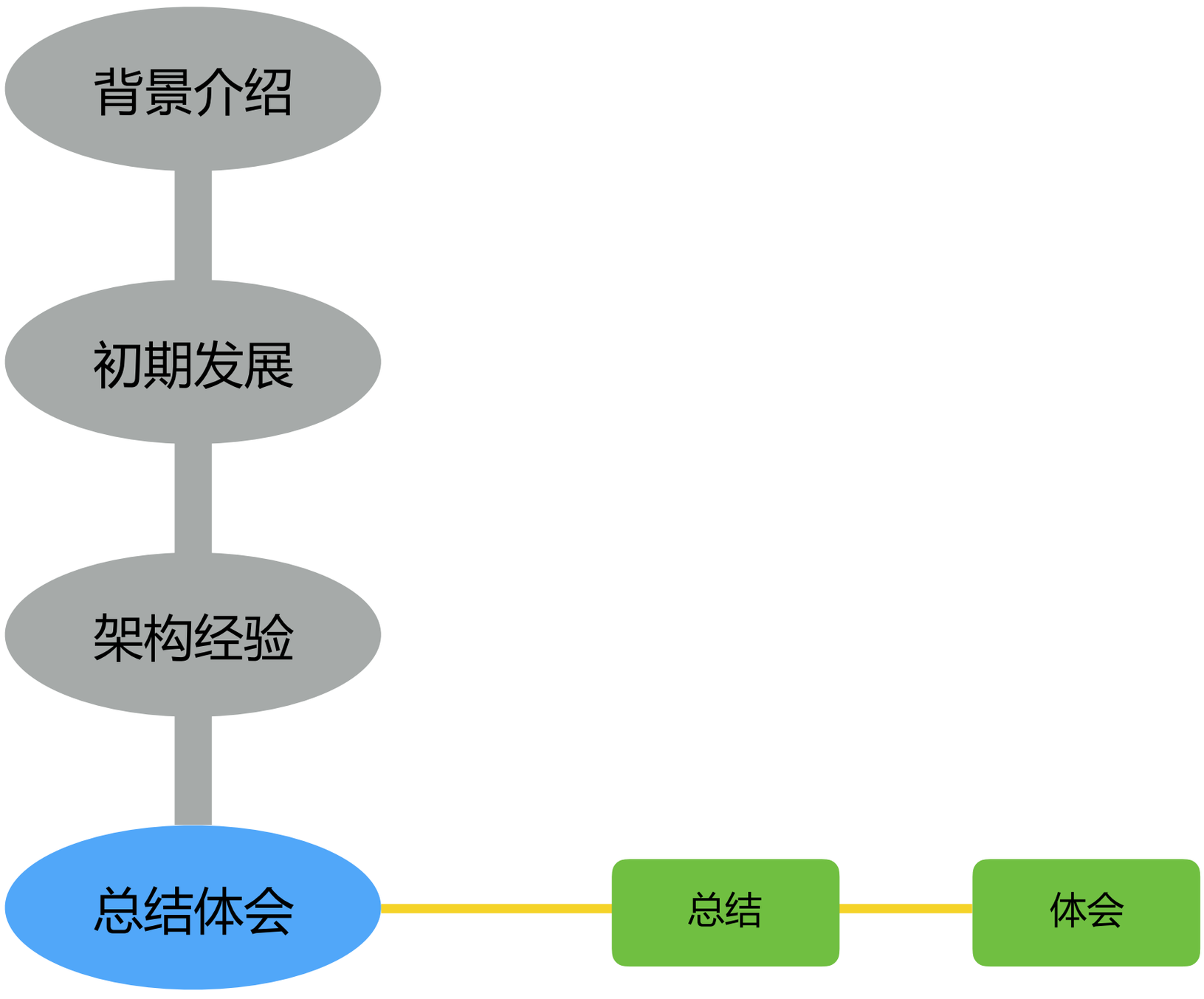

数据体系
衍生数据
商家、用户信用
名单库
策略集
聚合数据
聚合\统计数据
关联数据
基础数据
风控事件快照
业务数据
外部基础数据
数据存储
Tair
Druid
ES
MySQL
Hbase
Hive
计算平台
Storm
ETL
Spark
Hadoop

风控系统

招无定式，问题决定系统架构



目录



总结

原则

① 业务需要风控，风控做好服务

② 持续对抗过程，效率决定成败

③ 立体闭环防御，逆转信息劣势

体会——必经被动挨打的过程

①服务　　②效率　　③立体闭环

未来如何发展？

体会——从对手学习

- 恶意程序开发
- 散播木马
- 收集身份证、办银行卡
- 接码平台、猫池、IP代理、伪基站
- 验证码破解
- 批量注册
- 脱库
- 洗号
- 电信诈骗、社会工程学
- 众包：刷单、验证码、差评师
- 销赃

回到原则二：风控是持久战

资源拆分 → 服务化模块

对利益的嗅觉 → 对风险敏感

体会——从军事学习

故知胜有五

知可以战与不可以战者胜；

识寡众之用者胜；

上下同欲者胜；

以虞待不虞者胜；

将能而君不御者胜。

故曰：知彼知己，百战不殆

——《孙子兵法·谋攻篇》

现不现实

人够不够

团队价值观

准备得当

老板支持

体会

回到原则一：业务需要风控，风控做好服务

THANKS

SequeMedia 盛拓传媒 | IT168.com 专注导购16年 | ChinaUnix.net | ITPUB www.itpub.net