唯品会安全建设及风控杂谈

目录

01

唯品会安全发展历程

Wooyun id： 小胖胖要减肥
Weibo: 小胖胖_要减肥

2013年3月加入唯品会

当时安全团队3人，信息安全管理2人

我主要负责web安全及业务安全及应急响应

2013年底

安全团队6人，信息安全管理2人，安全技术4人

2015年7月

安全35人：

总监1人

监控与响应6人----soc平台，应急，预警，src等
内部产品安全9人----主要在安全测试，黑白盒及安全研究
外部产品安全6人----主要在运维安全涉及网络，设备，软件服务等

信息安全与管理培训8人----流程规章制度指定，等保，招标，安全培训等

业务安全5人----异常业务跟踪分析，风控产品及运营，业务数据监控等

2015年底计划：安全人员50+

直接转变:
满站漏洞->相对安全?

形式转变:
救火->控制->建设

当前团队覆盖:
安全审计
安全管理
安全培训
运维安全
Web安全
App安全
产品需求安全
安全产品
日志监控平台
应急响应
Src建设
业务安全
风控策略
风控运营
。。。

02

唯品会风控杂谈

1元看电影，1分钱买午餐，低价购物靠什么?

什么是（电商）风控?

----通过技术手段对恶意行为的控制和识别，保护网站正常运营和提供账户安全保护

为什么需要做（电商）风控?

扫号撞库?
资金安全?
用户信息?
刷单?
恶意攻击?
。。。

每天各种业务上的问题。。。

用户投诉账号被盗啦
又被wooyun发漏洞被撞库拉
某接口又被攻击啦
做活动又被刷了
。。。

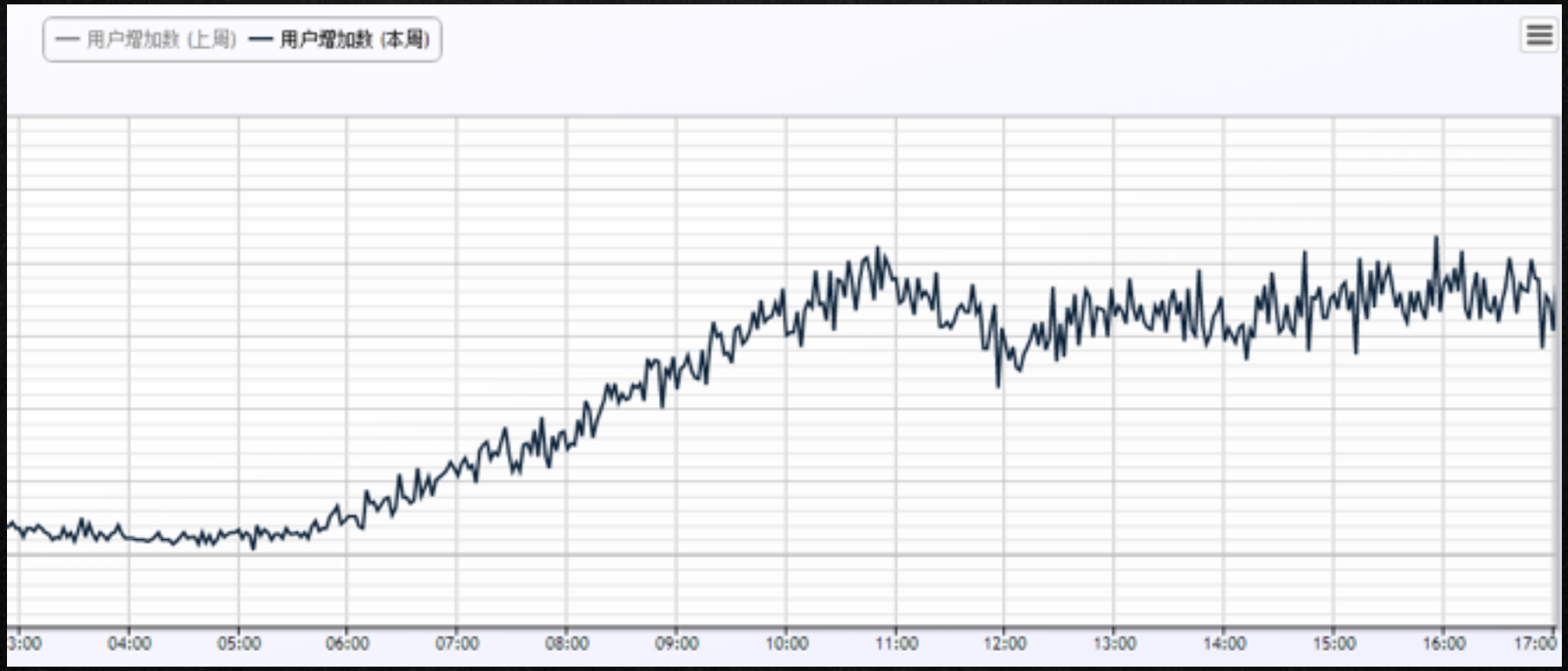
如何解决上述业务问题?

1 层级防御
2 需求风控介入，风险控制
3 风控平台支持
4 风控运营（站在第一线）

用户登陆成功数监控图


登录成功次数 (上周)
登录成功次数 (本周)
03:00
04:00
05:00
06:00
07:00
08:00
09:00
10:00
11:00
12:00
13:00
14:00
15:00
16:00

用户注册成功数监控图


用户增加数 (上周)
用户增加数 (本周)
3:00
04:00
05:00
06:00
07:00
08:00
09:00
10:00
11:00
12:00
13:00
14:00
15:00
16:00
17:00

Storm动态查询页面

首页 规则页面 概览页面 HIVE CDN节点查询

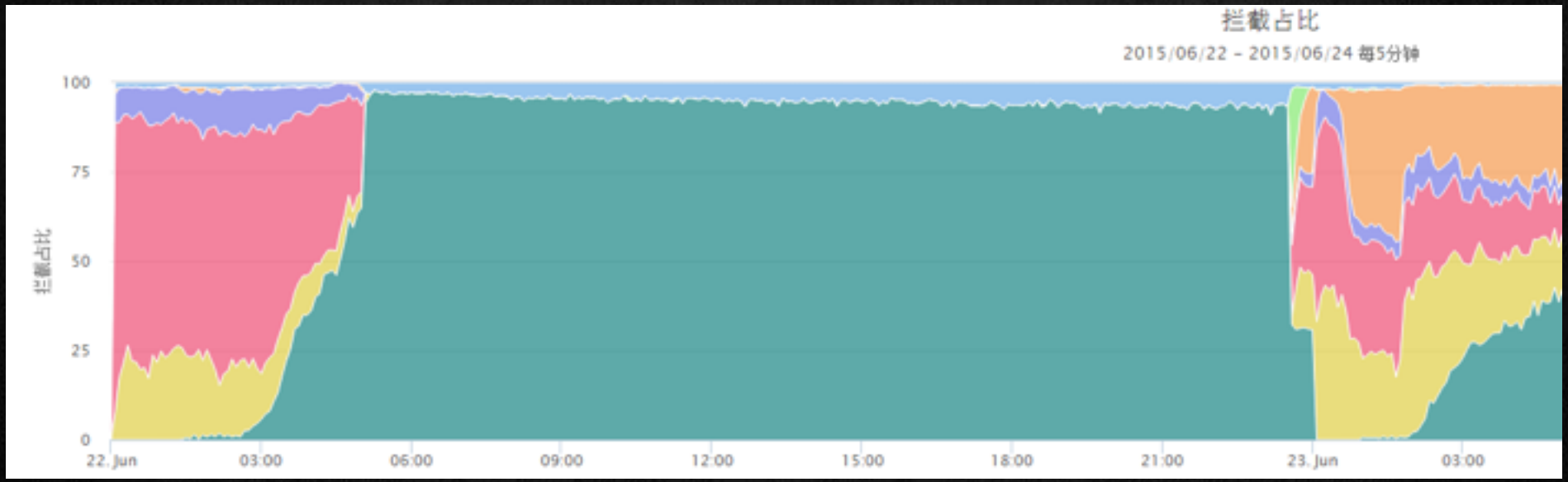
From,格式HHii To,格式HHii

06-23 16:35 ~ 06-23 17:05

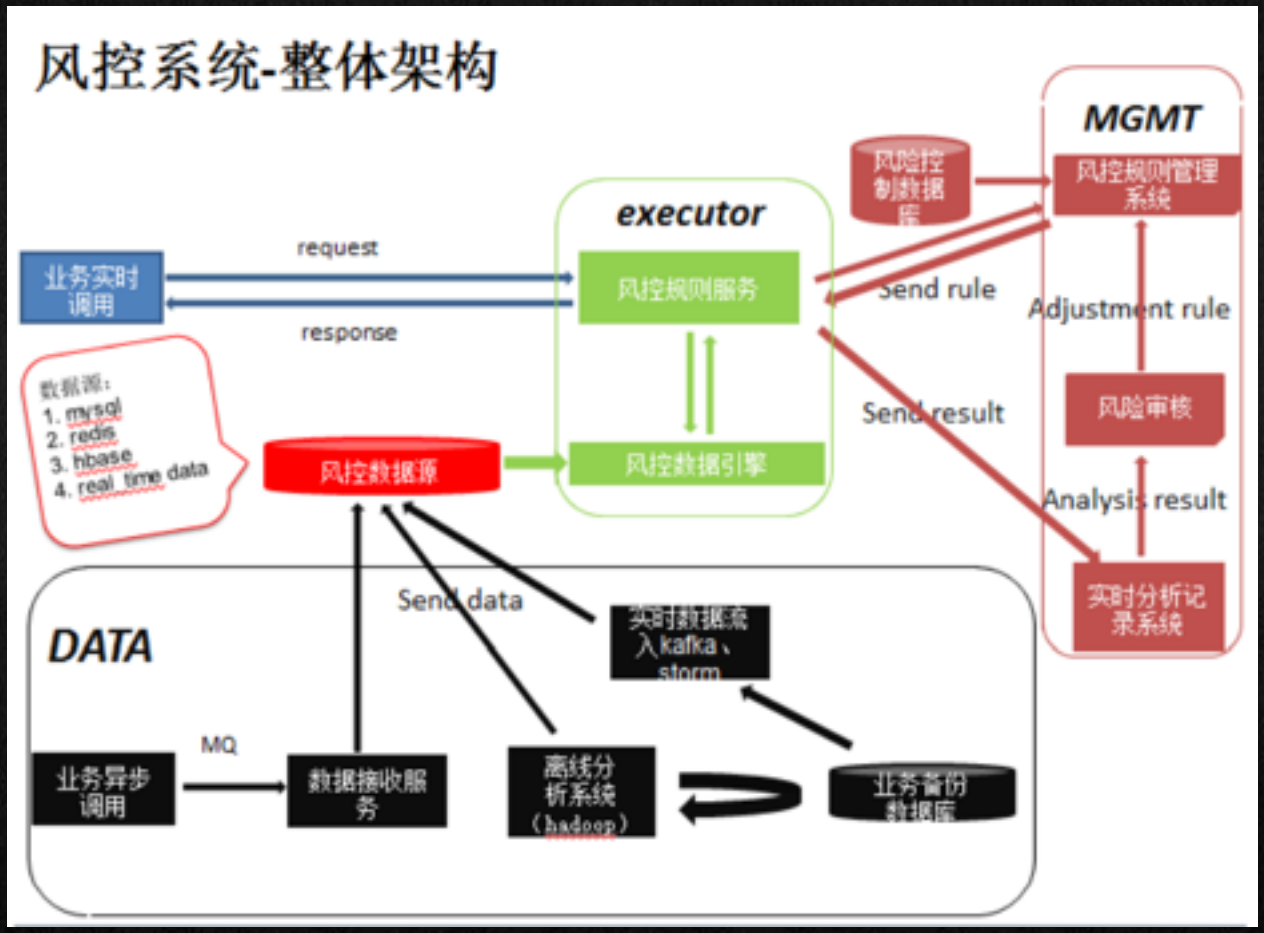
IP_ABC段		次数	IP段		标签	访问次数	日志
112.	.0	1607	218.	165	history_available	1002	日志
60.	.0	1382	125.	248	-	252	日志
112.	.0	1346	183.	170	-	223	日志

Storm监控规则配置

Passport域名检查风控接口规则拦截占比

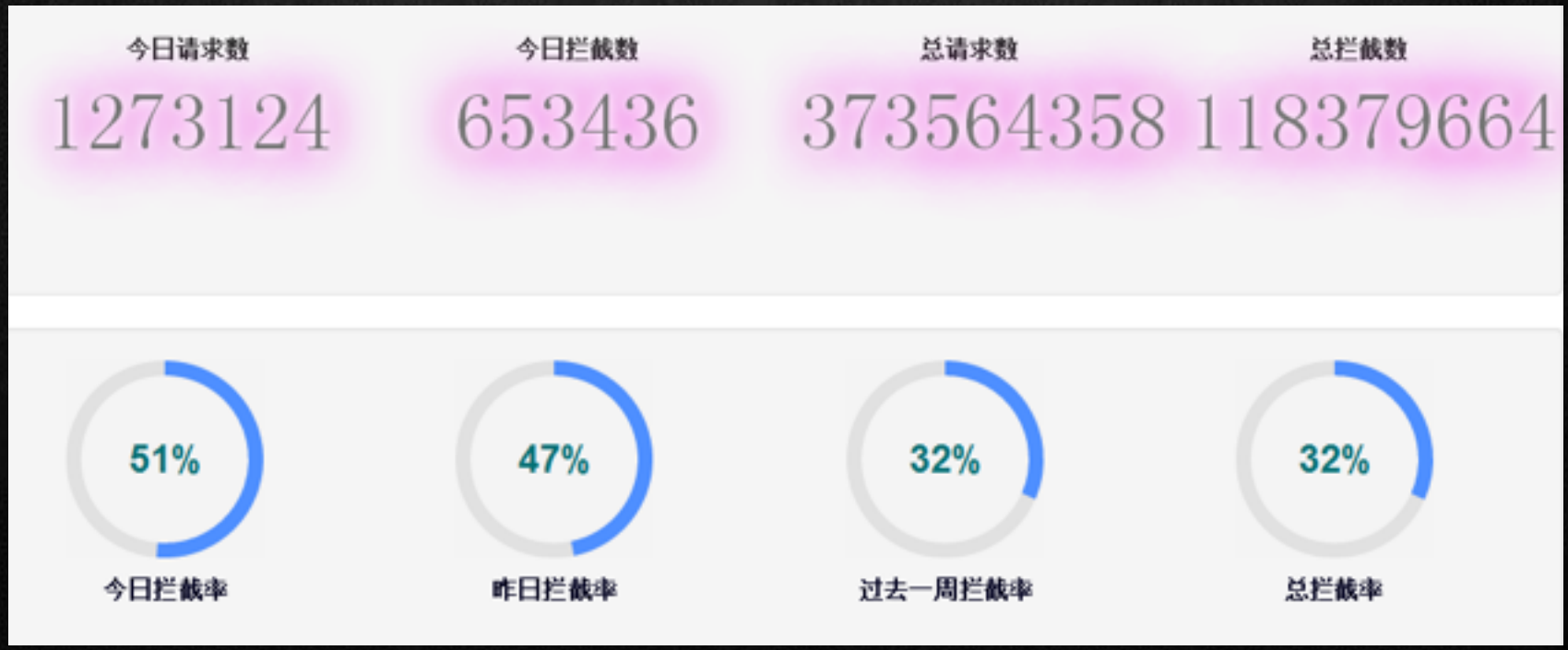


风控系统-整体架构

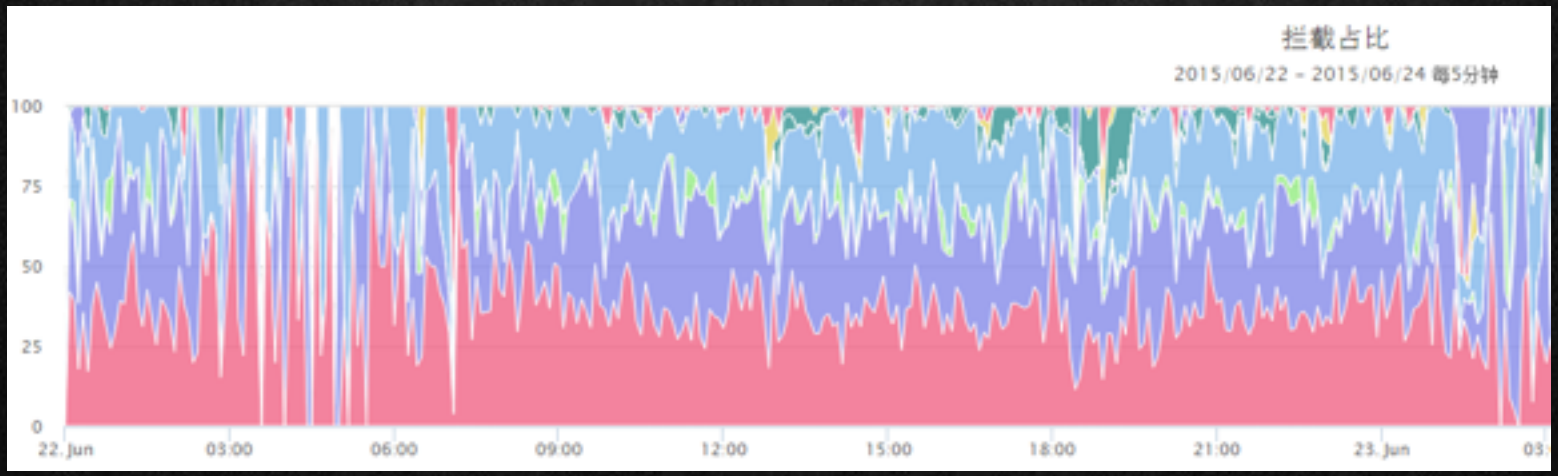

MGMT
风险控制数据库
风控规则管理系统
executor
request
业务实时调用
response
风控规则服务
Send rule
Adjustment rule
数据源：
1. mysql
2. redis
3. hbase
4. real_time data
风控数据源
风控数据引擎
Send result
风险审核
Analysis result
实时分析记录系统
DATA
Send data
实时数据流入kafka、storm
MQ
业务异步调用
数据接收服务
离线分析系统（hadoop）
业务备份数据库

某接口拦截情况，攻击比例让人惊愕

正常接口拦截情况
可见业务上的攻击比例是很高的



规则拦截占比，显示每天规则触发所占比例



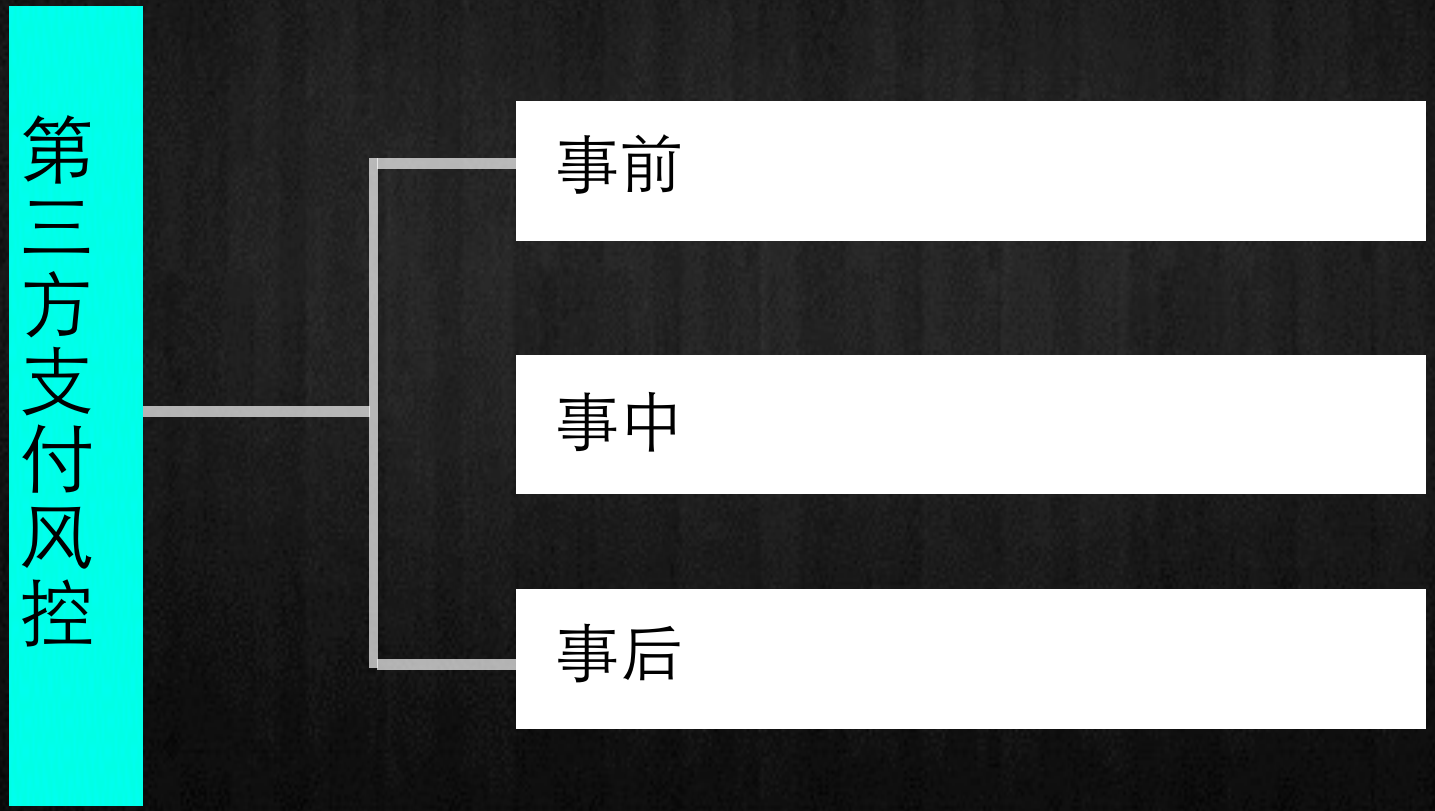
风控运营方式：

1 异常事件接入分析
2 动态规则实时调整
3 拦截数据定期分析
4 项目上线风控准入

风控等相关工作直接影响黑市数据定价

某互联网安全沙龙群聊到第三方支付风控

风险:
盗号
盗卡
欺诈
诈骗


第三方支付风控
事前
事中
事后

Q&A

Tank you !