饿了么

美好生活 共享安全

饿了么第一届信息安全峰会

内部威胁防护实践

拉扎斯网络科技（上海）有限公司
Rajax Network & Tehnology Co

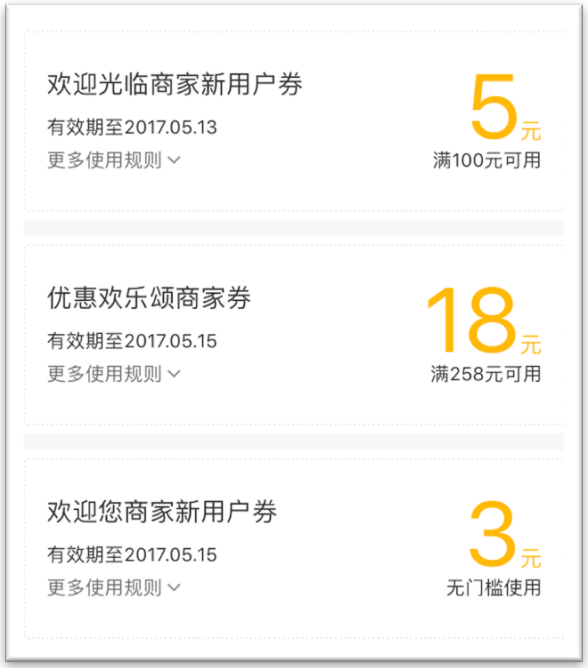
个人介绍

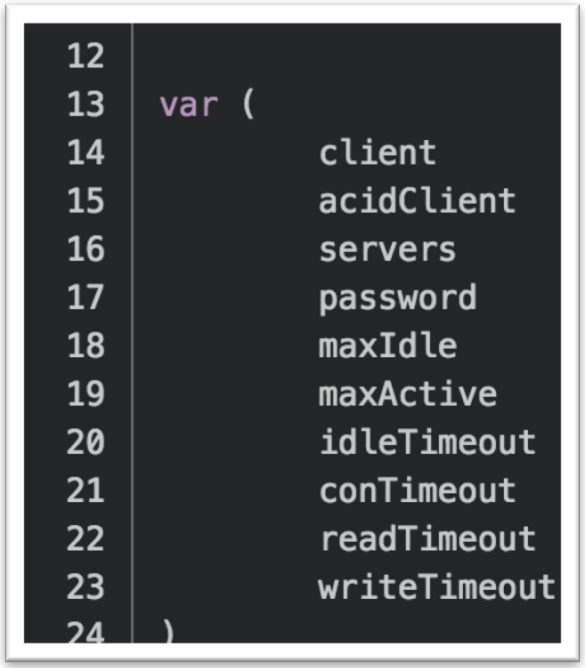
顾孔希/鸡子

滴滴信息安全部下系统安全部负责人

主要负责反入侵、防攻击等安全技术能力建设

今天我们说的内部威胁





```
12
13  var (
14          client
15          acidClient
16          servers
17          password
18          maxIdle
19          maxActive
20          idleTimeout
21          conTimeout
22          readTimeout
23          writeTimeout
24  )
```

No Hack !

非技术手段造成的关键权限的滥用，关键信息的外泄

这类内部威胁有什么特点

攻击场景1、

原始请求：http://foo/rss.aspx?keyword=lucky

SQLi http://foo/rss.aspx?keyword=lucky'));SELECT%20SERVERPROPERTY%20('edition');--

XSS http://foo/rss.aspx?keyword=lucky"/><script>alert(document.cookie)</script><!-

攻击场景2、{"timestamp":"2017-03-17T22:28:16.770537+0800","flow_id":,"in_iface":"em3","event_type":"alert","src_ip":"172.","src_port":53956,"dest_ip":"35.","dest_port":3389,"proto":"TCP","alert":{"action":"allowed","gid":1,"signature_id":2803564,"rev":2,"signature":"ETPRO WORM Worm.Win32.Morto.A Propagating via Windows Remote Desktop Protocol","category":"A Network Trojan was detected","severity":1}}

外部攻击：

1、有特征/Signature

2、Code/Tools

1、小A负责了商家入驻审核，在审核商家B时，明知道B不合格，但在某些特殊驱使下故意放过B

2、小C认识了美女D，为查到美女D住处，偷偷在后台上查了D的常用收快递地址

内部威胁：

1、可能无需技术

2、可能在授权范围内

3、可能无技术特征

挑战是什么

1、小A负责了商家入驻审核，在审核商家B时，明知道B不合格，但在某些特殊驱使下故意放过B

犯错失误还是主观作恶?

2、小C认识了美女D，为查到美女D住处，偷偷在后台上查了D的常用收快递地址

能不能查？该不该查?

除了上述这些行为，还有什么行为有问题?

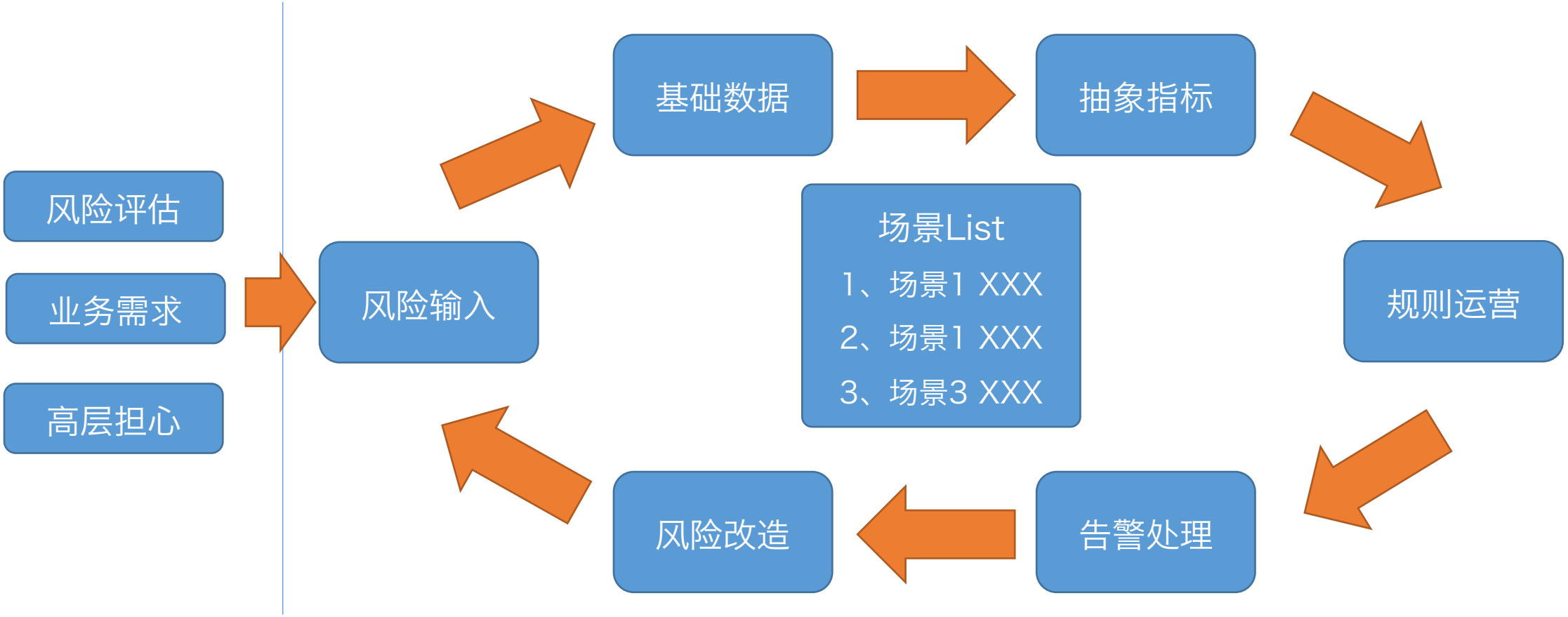
总结:

1、什么样叫异常，到底要找什么?

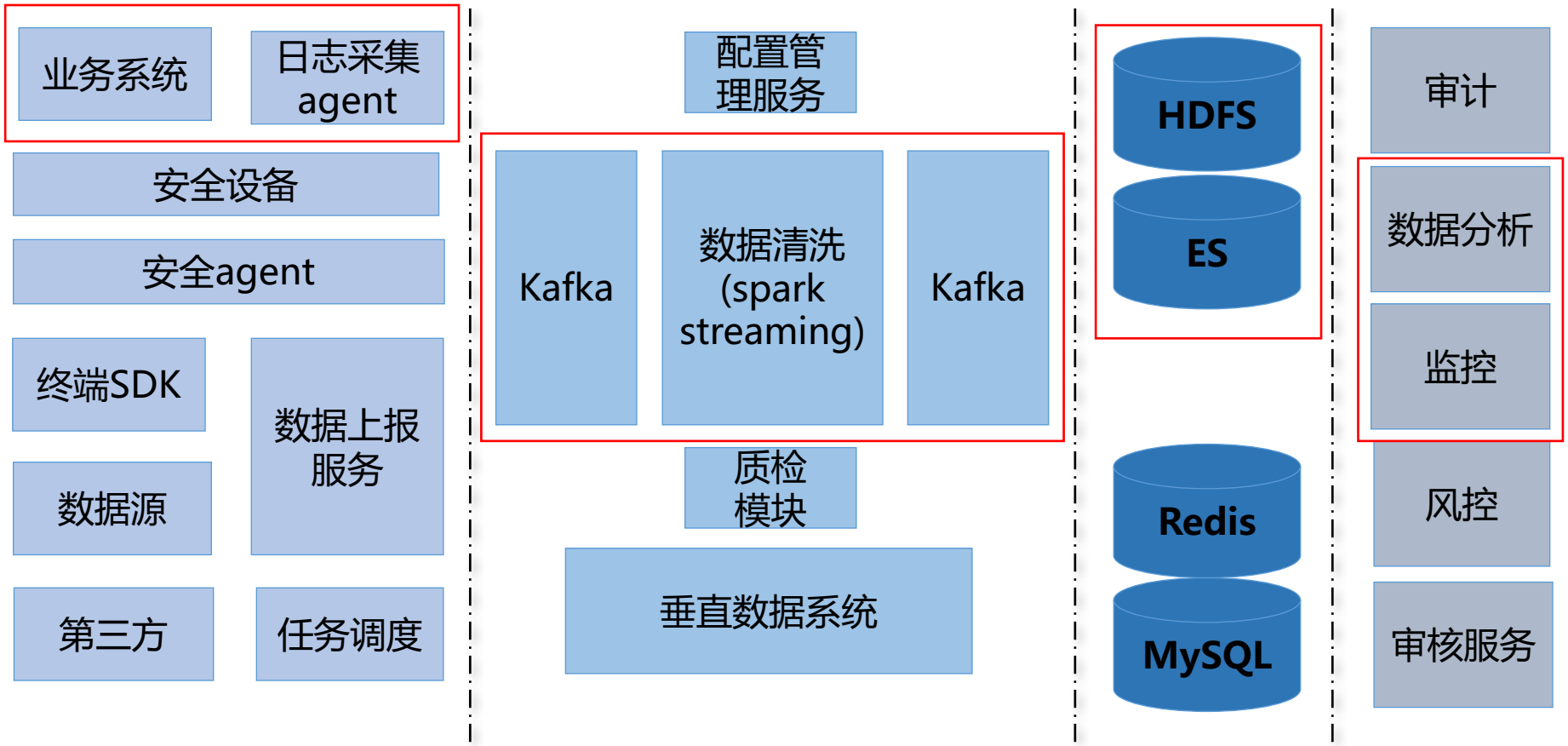
2、怎么判别异常，怎么去找出来?

3、如何确认异常，怎么去确认行为是否恶意?

整体思路


风险评估
业务需求
高层担心
风险输入
基础数据
抽象指标
规则运营
告警处理
风险改造
场景List
1、场景1 XXX
2、场景1 XXX
3、场景3 XXX

整体架构


业务系统
日志采集agent
安全设备
安全agent
终端SDK
数据源
第三方
数据上报服务
任务调度
配置管理服务
Kafka
数据清洗(spark streaming)
Kafka
质检模块
垂直数据系统
HDFS
ES
Redis
MySQL
审计
数据分析
监控
风控
审核服务

基础数据

collectTime: April 18th 2017, 16:32:17.794 cleanTime: April 18th 2017, 16:32:18.532 clientHost:
logName: sec.log appName: sinkTime: April 18th 2017, 16:32:18.799 logOffset: 71347268 logID: 11432
projectName: message: auditlog||system=mis||hostIp= ||userName=||userIp=1 |
url=http://1 ||getParams=||postParams={"params":"{\"no

collectTime: April 18th 2017, 16:32:17.794 cleanTime: April 18th 2017, 16:32:18.532 clientHost:
logName: sec.log appName: sinkTime: April 18th 2017, 16:32:18.799 logOffset: 71347649 logID: 11432
projectName: message: auditlog||system=mis||hostIp= ||userName=||userIp= |
url=http:// ||getParams=||postParams
={" ||ti

collectTime: April 18th 2017, 16:32:17.795 cleanTime: April 18th 2017, 16:32:18.532 clientHost:
logName: sec.log appName: sinkTime: April 18th 2017, 16:32:18.818 logOffset: 71354791 logID: 11432
projectName: message: auditlog||system=mis||hostIp= ||userName=||userIp= |
url=http://1 ||getParams=||postParams={"params":"{\"no

collectTime: April 18th 2017, 16:32:16.557 cleanTime: April 18th 2017, 16:32:18.531 clientHost:
logName: arkSafe.log appName: sinkTime: April 18th 2017, 16:32:19.004 logOffset: 113934202
logID: 11434 projectName: SEC message: auditlog||system=ark||hostIp= ||userName= |url=
||getParams= :||postParams=[]||userip= |timestamp=2017
-04-18 16:32:16.357||response= logTime: April 18th 2017, 16:32:16.000 id: type: arksafe.log

username	MailDeviceId	Calling_Station_ID	DeviceType	cs_User_Agent
w ex	S5 T4G7KHUJ87LD10	AC 65	iPhone	Apple-iPhone7C1/1405.304
yr	J5 H6KT49F7VSBSS8	cc- 3e-0f	iPad	Apple-iPad6C3/1405.304
yr	26 IF24CUTT08488S	cc- 3e-0f	iPhone	Apple-iPhone9C2/1405.304
ar	63 F00D	A4 93	Outlook	Outlook-iOS-Android/1.0
zh i	E7 \670	701 E9	Outlook	Outlook-iOS-Android/1.0
gu n	CD E10F	60- 6E-10	Outlook	Outlook-iOS-Android/1.0
zh uang	O7 7ELIDBVAQIUEOC	102 E9	iPhone	Apple-iPhone9C2/1405.304
he	JS IBC5C8EPNBB4KC4	AC 057	iPhone	Apple-iPhone9C2/1402.100
zh	OM 41ALTQFEE63JQMS	2C2 9C	iPhone	Apple-iPhone9C2/1401.551
lic	A4 EA0	584 38	Outlook	Outlook-iOS-Android/1.0
re	0II D8PT1E7TLNQ44	A0 D1	iPhone	Apple-iPhone9C2/1403.92
zh ao	AH .1FTS30F2FPHP8	98- -8E-E2	iPhone	Apple-iPhone8C1/1405.277
ya	3N 9ETHONSQ8I9GFS	341 0F	iPhone	Apple-iPhone7C2/1401.456
zh an	UF FV9G1AG81S65IGG	0C- -42-63	iPhone	Apple-iPhone7C1/1405.304
er	2F _4M0V4HOISCE64	685 88	iPhone	Apple-iPhone8C1/1404.27
ju	OM H4002G9PEUFT90	CC A8	iPhone	Apple-iPhone9C2/1405.304
w j	2E 247	B8 BF	Outlook	Outlook-iOS-Android/1.0

_time	src_ip	user	url	ua	reffer
2017/01/22 15:04:02	1	36 41229	/gu oard	Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/50.0.2661.102 Safari/537.36	http:// n/index.php
2017/01/22 15:04:02	1	36 41229	/gu oard	Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/50.0.2661.102 Safari/537.36	http:// n/index.php
2017/01/22 15:06:03	1	36 41229	/gu iew	Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/50.0.2661.102 Safari/537.36	http:// n/resources/ ?line=1
2017/01/22 15:06:04	1	36 41229	/gu /List	Mozilla/5.0 (Windows NT	http:// lfstream/mis ListView

饿了么安全 Eleme Secur

享安全

抽象指标

聚合事件

提取操作

```
_time user {
action_1/event_1 count,
action_2/event_2 count,
action_3/event_3 count,
……
}
```

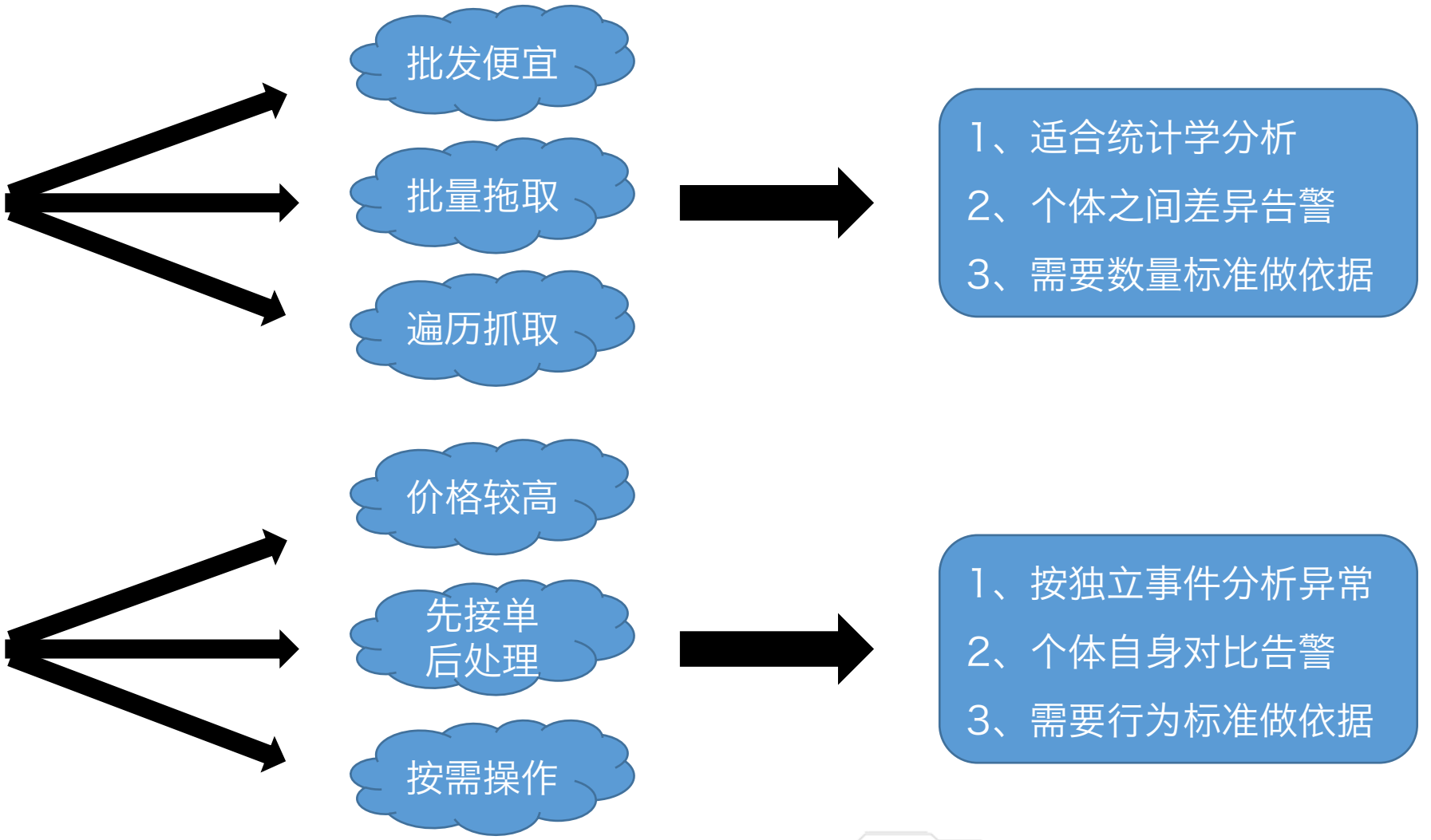
```
date=2017-04-19
00:00:00,user=zhu       ,k       i=0,get       =0,get       =2,close      =0,show       =1
1,show       =0,(       =0,(       _=0,addC
(       =0,       =0,       =0,(       =0
```

1、量小，计算快

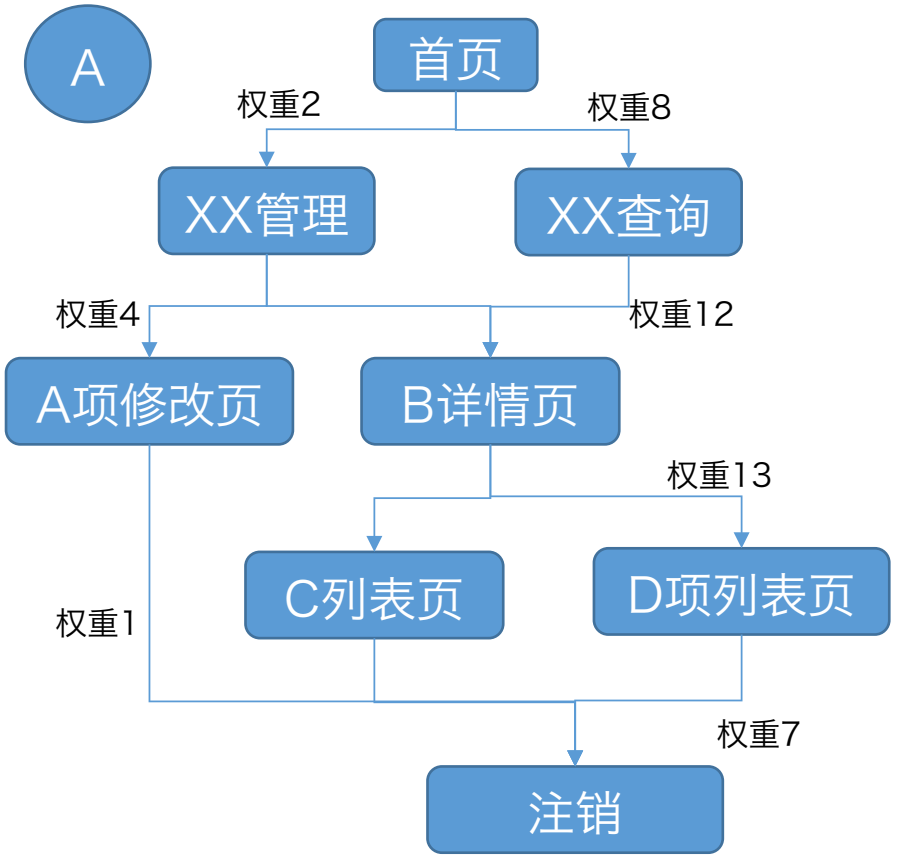
2、便于做规则

规则运营

- 打包销售：
  - 个人身份信息
  - 网购订单信息
  - 快递信息
  - 航班信息
  - ……
- 定向出售：
  - 开房记录
  - 通信记录
  - 个人征信数据
  - ……



规则运营



每一个个体都有自己的树

每一个角色都有自己的树

Reffer、时间、会话标识——绘路径

频度——绘权重

1、离散点/集中点

2、个体自身变化

3、同类角色之间差异

Demo

id	session_mark	user	start_time	end_time	host	request_flow	type	probability
9123871	3a3748269e3f86d7	Mark.Hu	2017-03-11 08:19:42	2017-03-11 08:32:11	www.di***inc.com	/res***1;/sat***g;/get***tt	query	0.18129%
9123872	0e179aa42316ee02	Steven.Tan	2017-03-11 08:19:42	2017-03-11 08:37:21	www.di***inc.com	/aas****x;/tes****e;/set****a;/add****s	query	0.63521%
9123873	5064f1741297a7b1	Johnny.Ma	2017-03-11 08:19:44	2017-03-11 08:22:39	www.ta****ect.com	/del***d;/kes****x;/job***9	modify	2.46521%
9123874	74a4a1002cfc3474	Rickey.Hu	2017-03-11 08:20:02	2017-03-11 08:21:21	www.de****euy.com	/cas***r;/ttl***8	query	5.21231%
9123875	50df10088d840f02	Johnny.Ma	2017-03-11 08:20:24	2017-03-11 08:31:59	www.ta****ect.com	/del***d;/set****a;/add****s;/set****a	modify	0.02231%
9123876	f2255f6e546ff5f1	Luke.Wang	2017-03-11 08:20:26	2017-03-11 08:28:19	www.di***inc.com	/ass***r;/tal***e;/sda***7;/see***1	query	1.23901%
9123877	04154b2e2b6f29ee	Mars.Yang	2017-03-11 08:20:33	2017-03-11 08:32:12	www.di***inc.com	/add***r;/tse***p;/saa***s	query	1.03113%

告警处理

1、权限是否满足

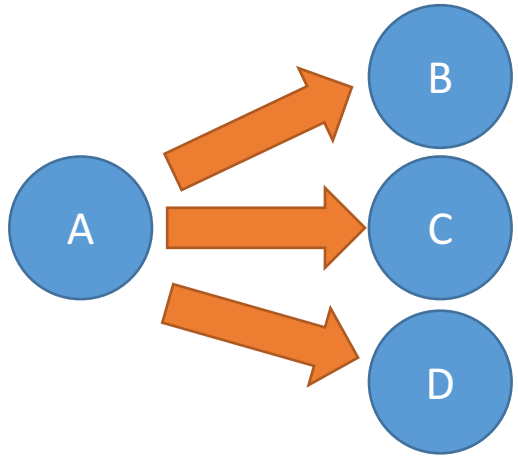
2、这个场景下是否应该用这个权限

3、账号本身是否有异常

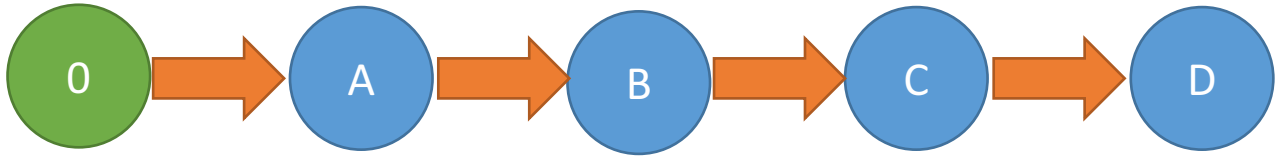
4、是否有安全漏洞

…… ……

业务风险改造



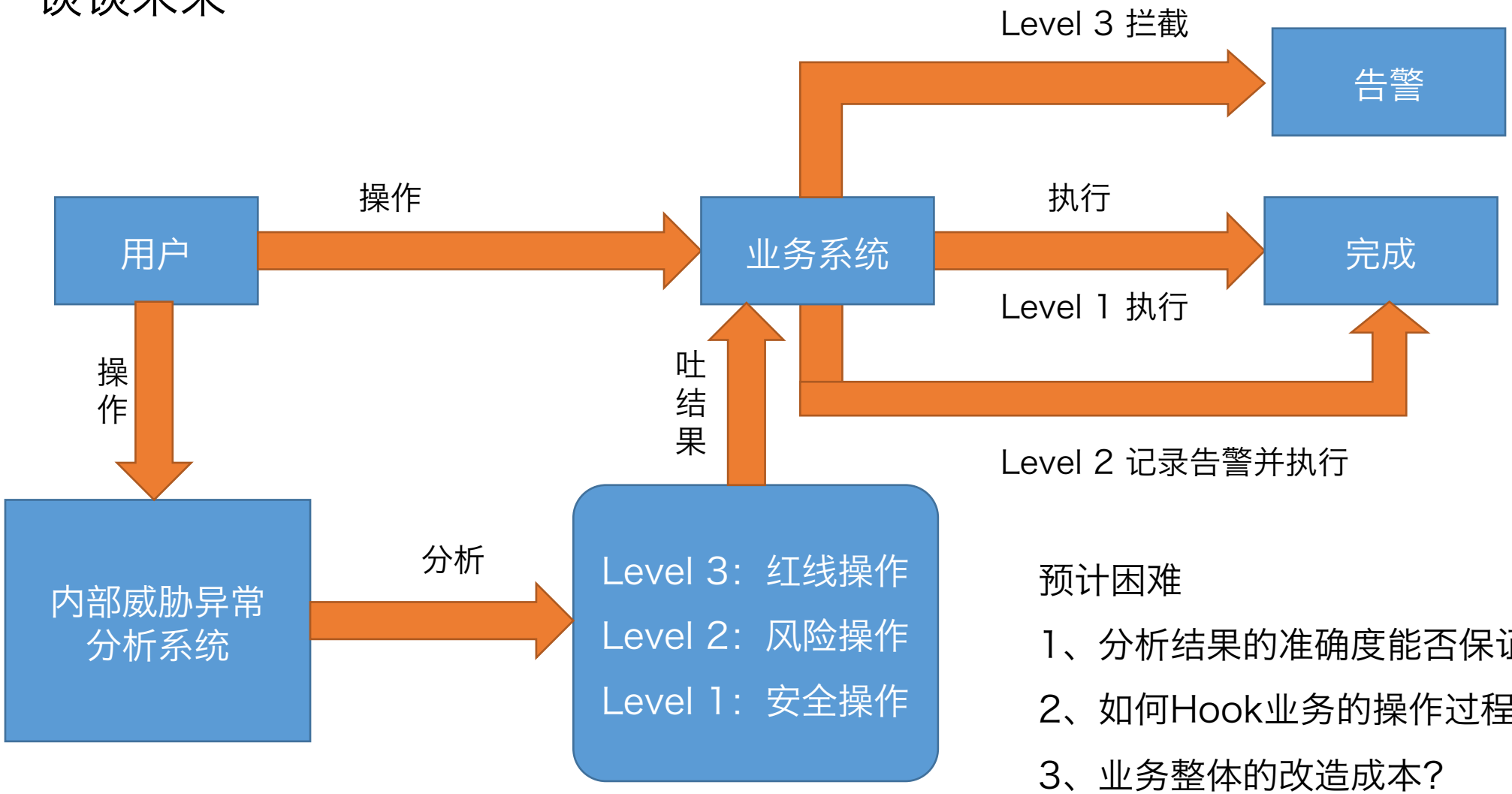
1、业务流程、安全漏洞



2、账号管理

3、权限梳理

谈谈未来



预计困难

1、分析结果的准确度能否保证?

2、如何Hook业务的操作过程?

3、业务整体的改造成本?

4、特殊的业务需求和场景维护

饿了么安全应急响应中心
Eleme Security Response Center

THANKS