基于移动安全大数据的

移动威胁场景下的画像线索应用

孙岩　潘博文

AVL移动安全·安天

简短的自我介绍

孙岩

大数据 画像

- 在互联网大数据有丰富经验，目前主要负责内部大数据体系的架构和设计

Data

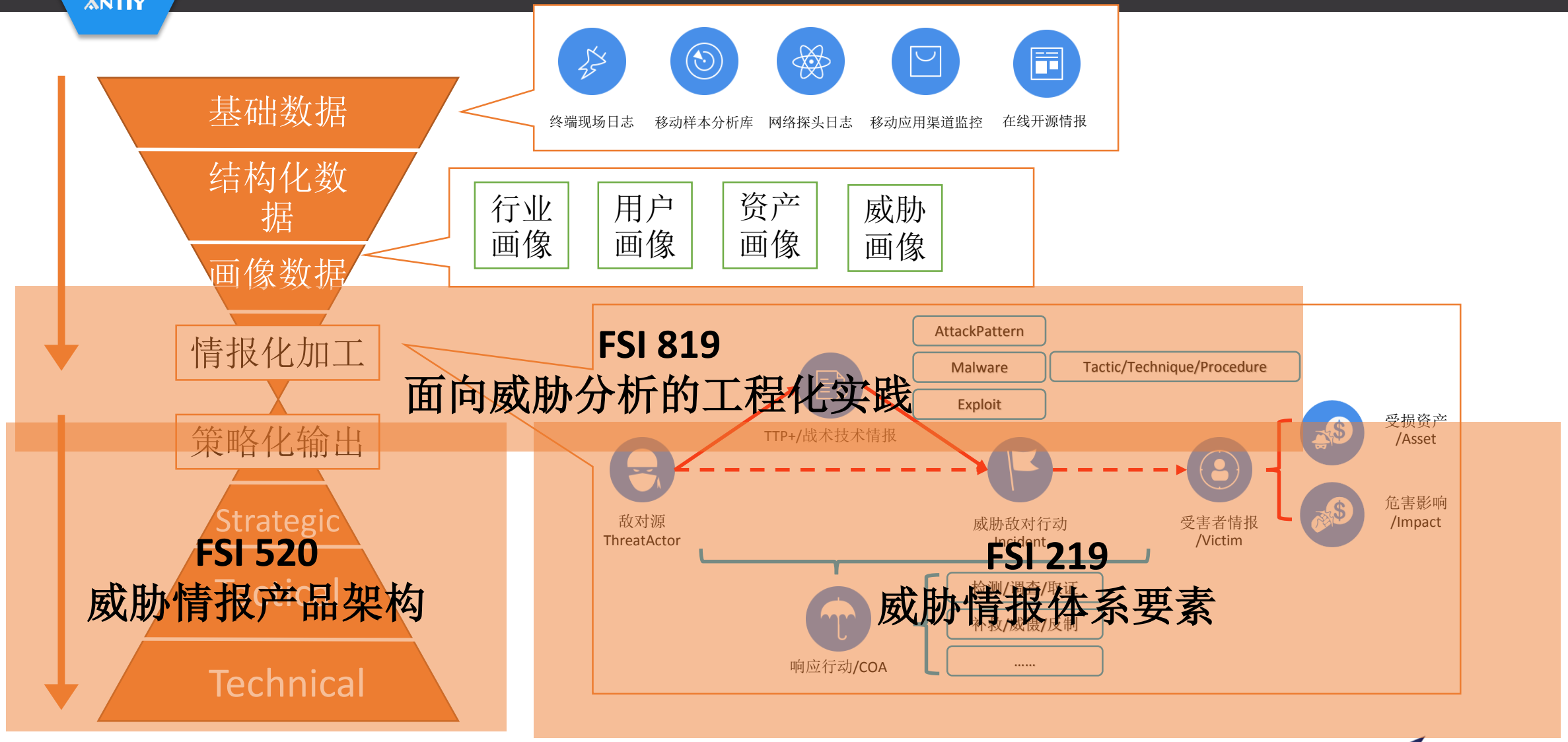
潘博文

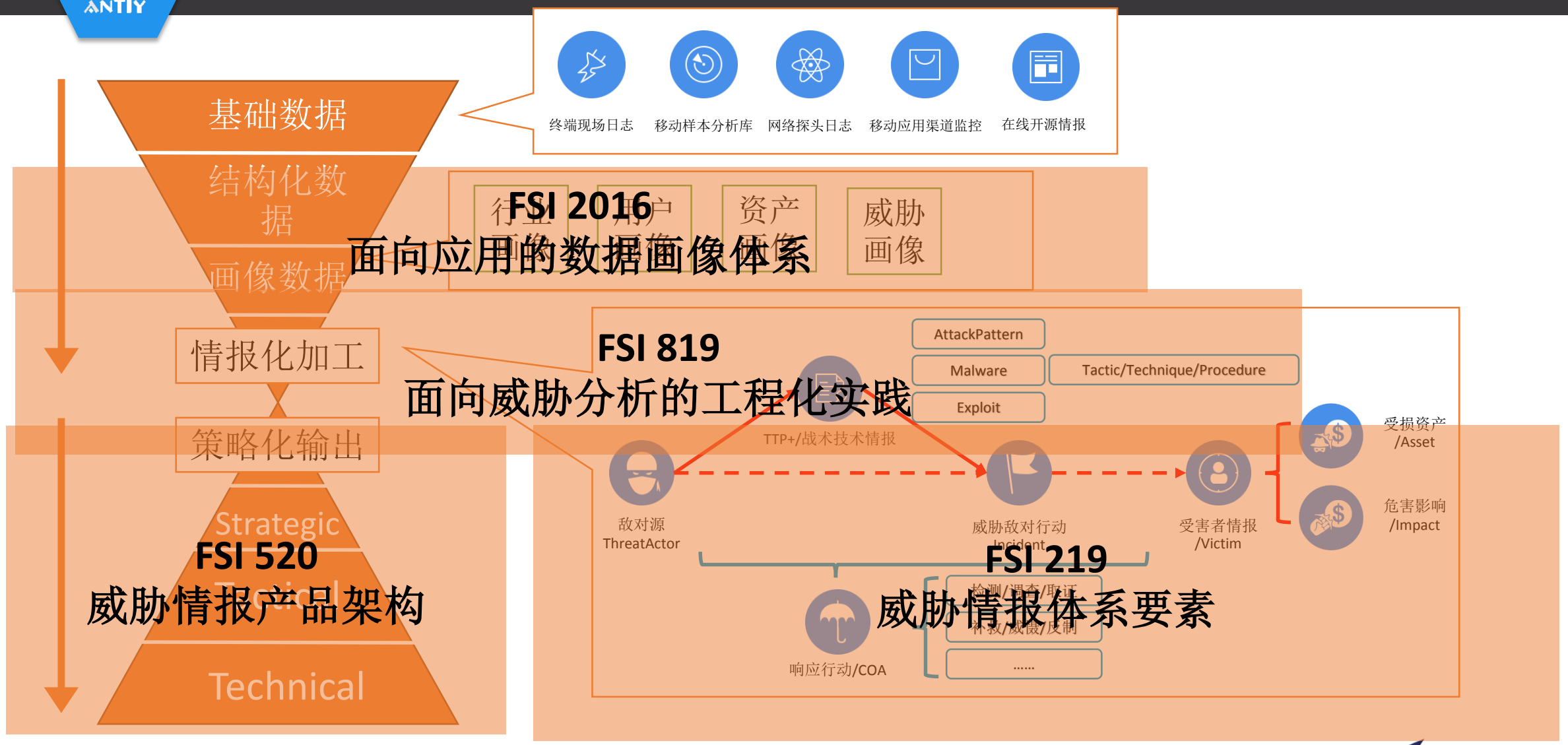
TI 分析

- 主要研究移动恶意代码对抗技术和威胁事件分析，目前主要负责内部威胁情报分析运营体系设计

Analysis

FSI沙龙回顾


基础数据
结构化数据
画像数据
情报化加工
策略化输出
Strategic
Technical
Technical
终端现场日志
移动样本分析库
网络探头日志
移动应用渠道监控
在线开源情报
行业画像
用户画像
资产画像
威胁画像
FSI 819
面向威胁分析的工程化实践
AttackPattern
Malware
Tactic/Technique/Procedure
Exploit
TTP+/战术技术情报
敌对源
ThreatActor
威胁敌对行动
Incident
受害者情报
/Victim
受损资产
/Asset
危害影响
/Impact
响应行动/COA
检测/调查/取证
补救/威慑/反制
.....
FSI 520
威胁情报产品架构
FSI 219
威胁情报体系要素

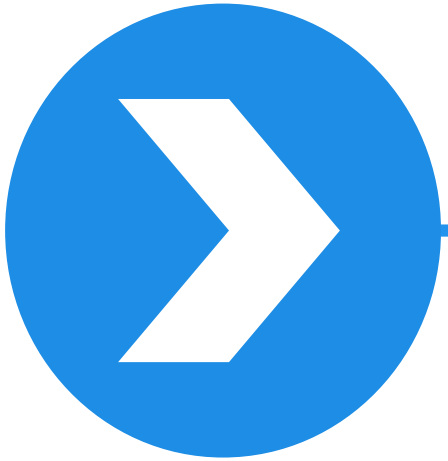


FSI 2016
面向应用的数据画像体系

FSI 819
面向威胁分析的工程化实践

FSI 520
威胁情报产品架构

FSI 219
威胁情报体系要素



画像从互联网到安全

互联网———与生俱来的画像

身长八尺，面如冠玉，头戴纶巾，

身披鹤氅，飘飘然有

互联网————生活痕迹画像

姓名：刘乐乐
性别：女
年龄：20
职业：学生
学历：大二在读
收入：没有收入，都是家里给的，每月不超过1000
爱好：喜欢听歌、看小说比如郭敬明、看韩剧、美剧 、玩小游戏 、偶尔弄些小创意
性格：青春、开朗，喜欢与他人交流

关于微博的经典话语

“微博最看重信息度和人脉吧，信息更新比较快呀，还有在里面认识的人比较多，能拓展本来不认识后来认识的。”
“我觉得里面的笑话非常好，因为我可以分享给别人，我会念出来告诉别人!”
“用微博比较能消遣时间吧，省的无聊.”

手机使用情况

NOKIA 5230，购买时1500
动感地带，30M流量，话费50元/月

使用目的

跟同学、朋友交流，与跟自己有相同兴趣的人交流；
能了解明星的动态；
看搞笑类的放松；
了解社会时事；
获取学习、励志类的信息

第1个月

宝宝大多数时间在睡觉，对声响刺激和压力、冷热有反应。

第2个月

被逗引时会微笑，并能抓住物体片刻。

第3个月

双眼视物协调，看到奶头能自动张嘴，能发出响亮的笑声。

第4个月

会发出单音，并认出母亲，能抓住玩具。

第5个月

背部能挺直，母亲从腋下撑抱起时双腿能直立，高兴时会呱呱叫。

第6个月

同时可用两手抓两样东西，能辨认陌生人，开始模防声音。

互联网————画像聚合状态

用户属性数据

职业分布

个人月收入

互联网———画像价值

精准广告投放

个性化推荐

风控产品策略

群体特征定位

重点用户发现

提升营销体验

改善用户体验

降低成本

增加收入

实现用户针对性管理

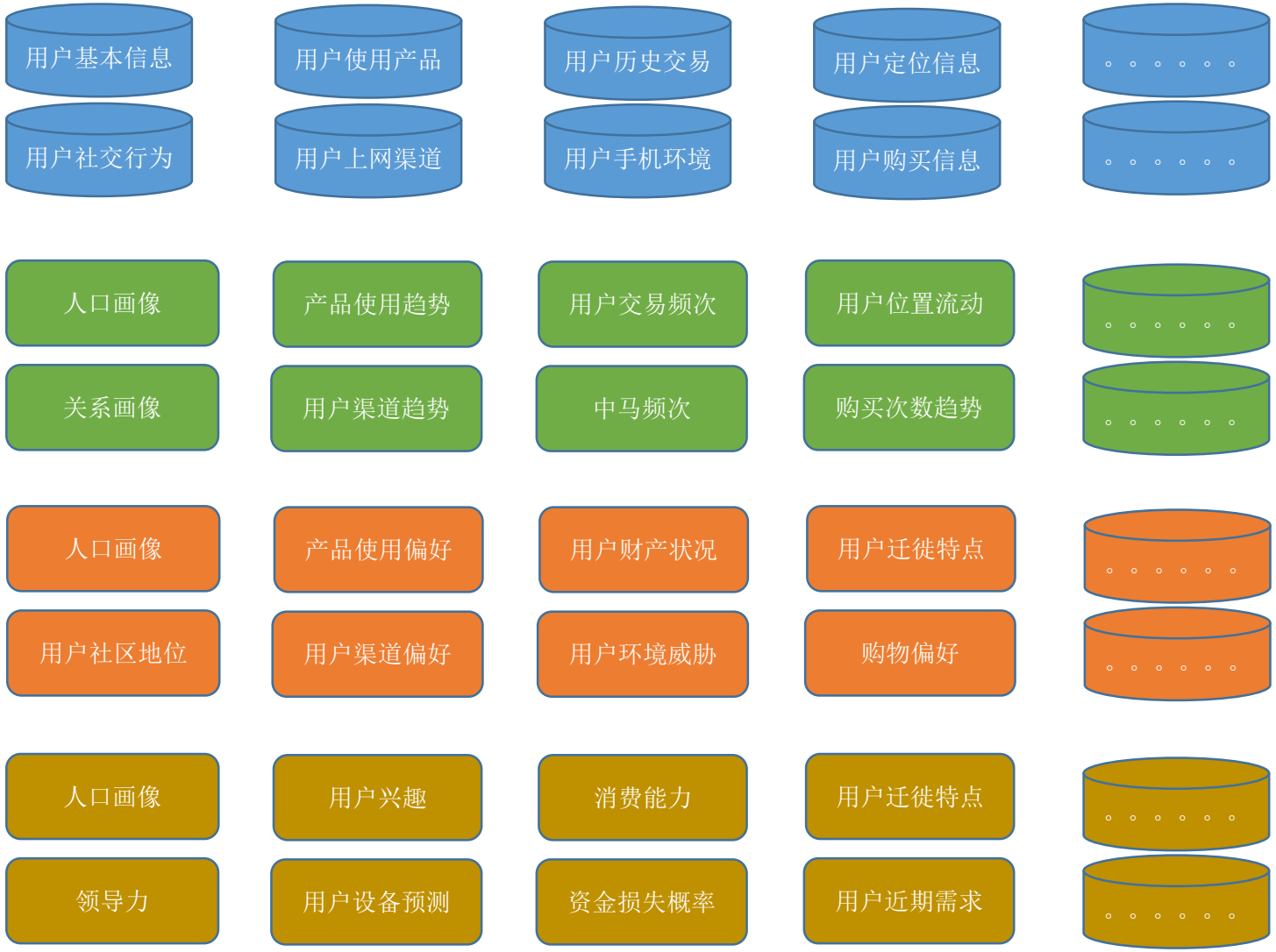
互联网———画像建模

原始数据

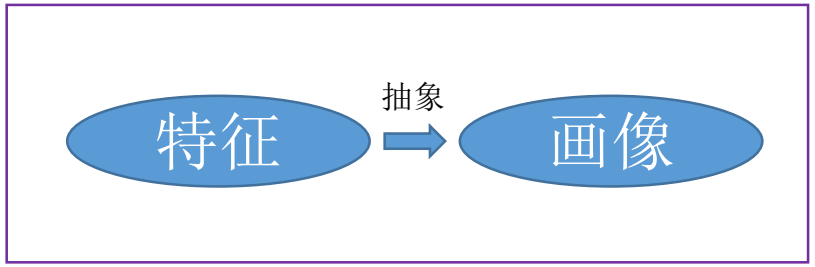
实事标签

模型标签

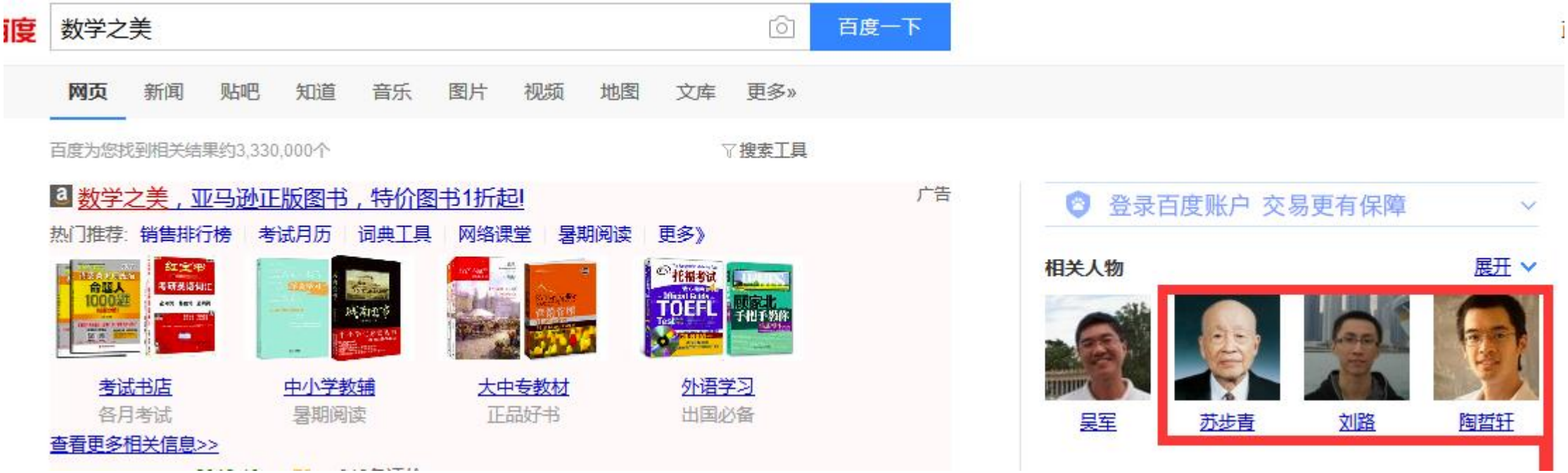
预测标签



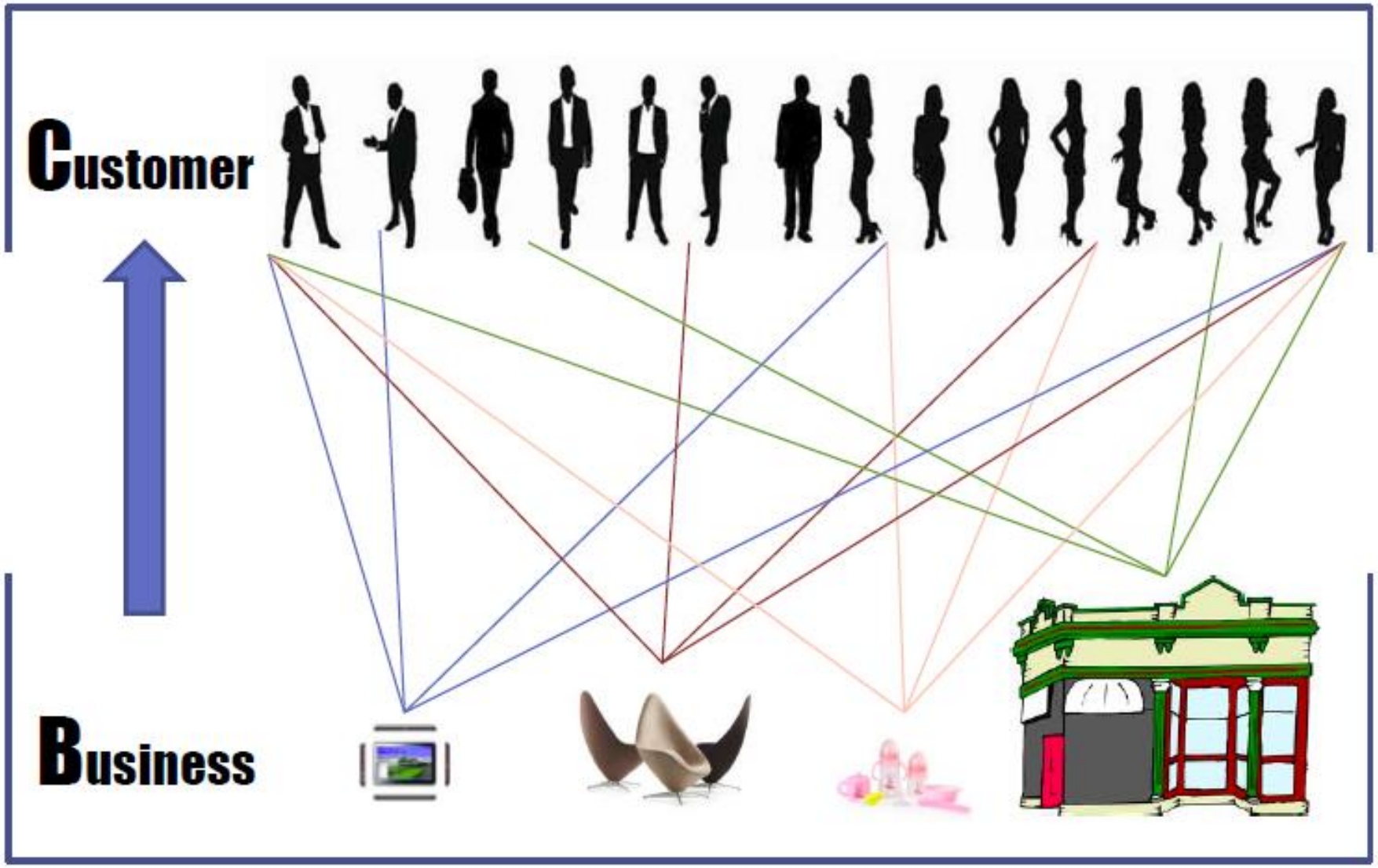
互联网————画像建模


特征
抽象
画像


知识图谱
抽象
画像


数学之美
百度一下
网页 新闻 贴吧 知道 音乐 图片 视频 地图 文库 更多»
百度为您找到相关结果约3,330,000个
搜索工具
数学之美，亚马逊正版图书，特价图书1折起!
广告
热门推荐: 销售排行榜 考试月历 词典工具 网络课堂 暑期阅读 更多»
考试书店
各月考试
中小学教辅
暑期阅读
大中专教材
正品好书
外语学习
出国必备
查看更多相关信息>>
登录百度账户 交易更有保障
相关人物
展开
吴军
苏步青
刘路
陶哲轩

互联网————画像B2C模式



B2C模式不适合安全领域

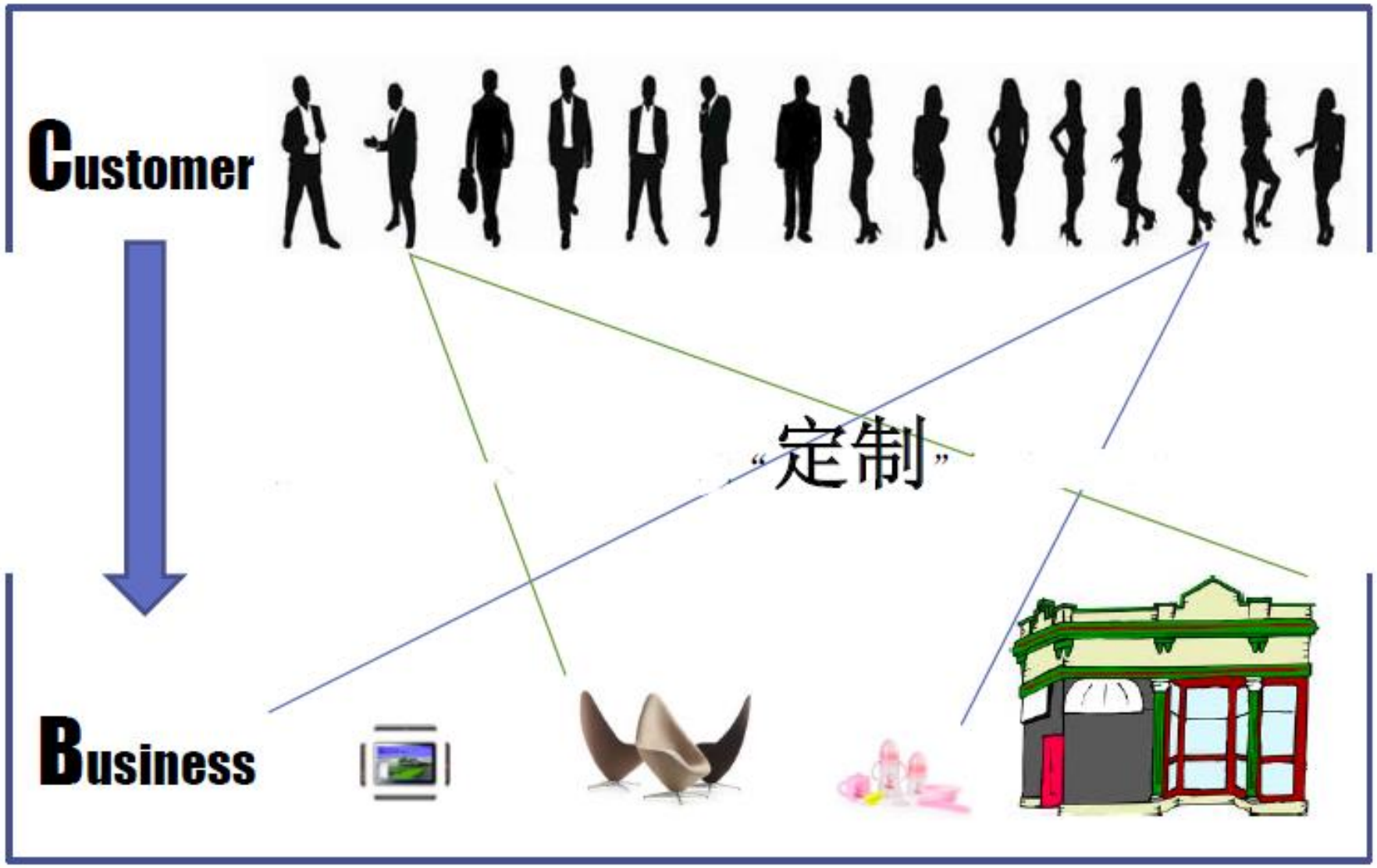
1、互联网画像是商务驱动画像生成，标准，
画像可以是自上而下，也可以是自下而上。

自上而下：“男人”
自下而上：
“坏人” “有钱” “偷钥匙”
“晚上” “惯犯” “瘦”

2、安全画像是发现查询驱动，结构化
他是作为一个线索来发现，需要做二次关联。

“坏人”->目的：偷东西->环境：“晚上”
->手段：“用钥匙开门”->频率：之前很长时间持续

安全数据应用————B2C模式NO



安全数据应用———画像元素

user	ip	url	App(泛)	phone	email	pic	...
• 人口画像 • 风险画像 • 状态画像 • 设备画像 • 应用画像	• 基本画像 • 状态画像 • 关联画像 • 安全画像 • 时间画像	• 基本画像 • 状态画像 • 关联画像 • 安全画像 • 时间画像	• 行业画像 • 类别画像 • 风险画像 • 人群画像	• 属性画像 • 安全画像 • 注册画像	• 来源画像 • 安全画像 • 注册画像	• 来源属性 • 判别属性 • 相似属性	• ...

安全数据应用———安全分析要素

优秀的互联网画像

- 实时的日志数据
- 丰富的行为数据
- 海量的文本数据
- 足够的渠道数据

优秀的安全画像

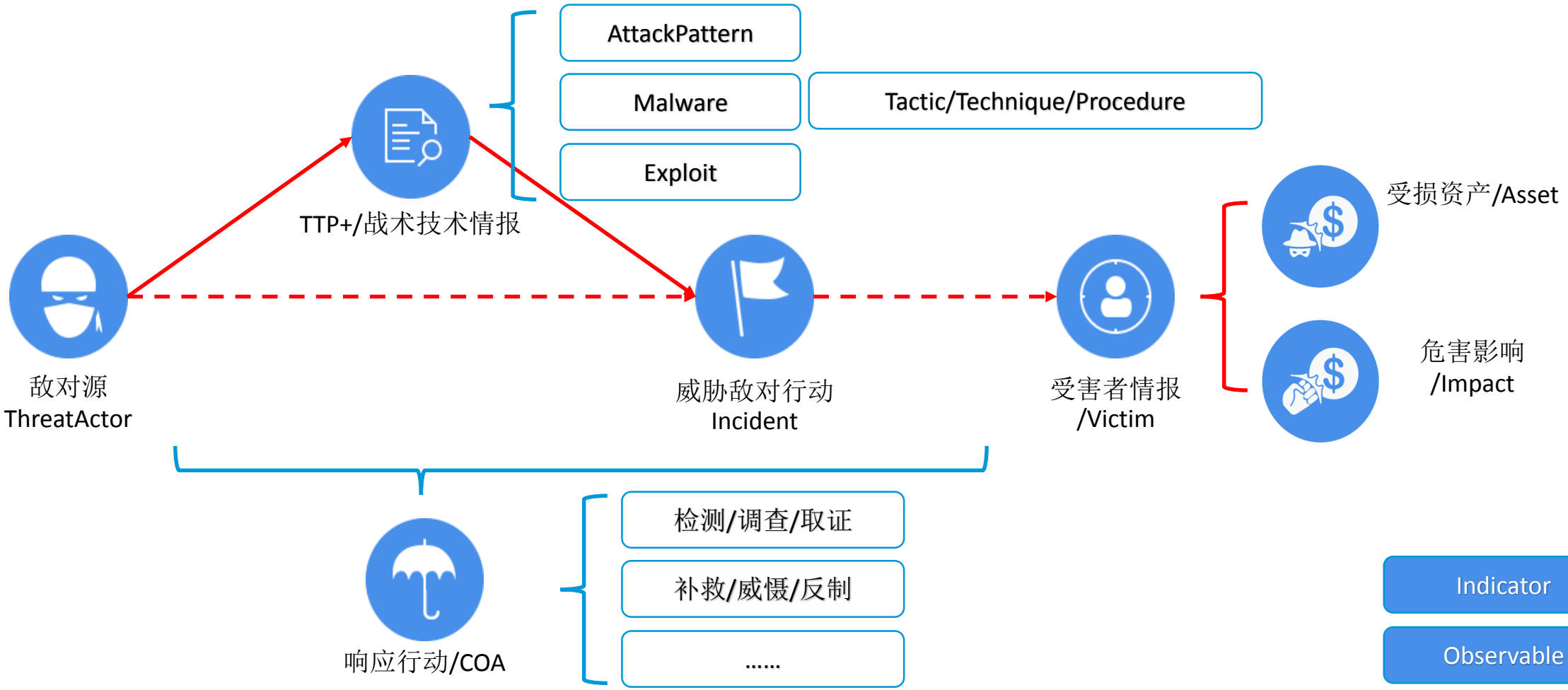
- 实时的端上数据
- 全面的OSINT数据
- 有效的流量数据
- 精准的安全判定

- 大量的人工预处理作业
- 完善易用的规则优化后台

- 大量的人工安全分析判定
- 高效的分析业务流转结构化

重新审视数据画像------传统分析报告

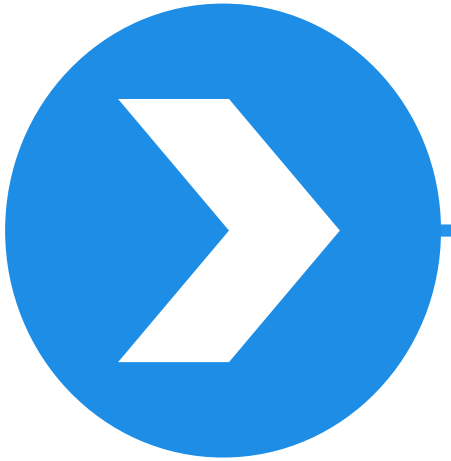
重新审视数据画像------基于数据画像的分析场景



Indicator

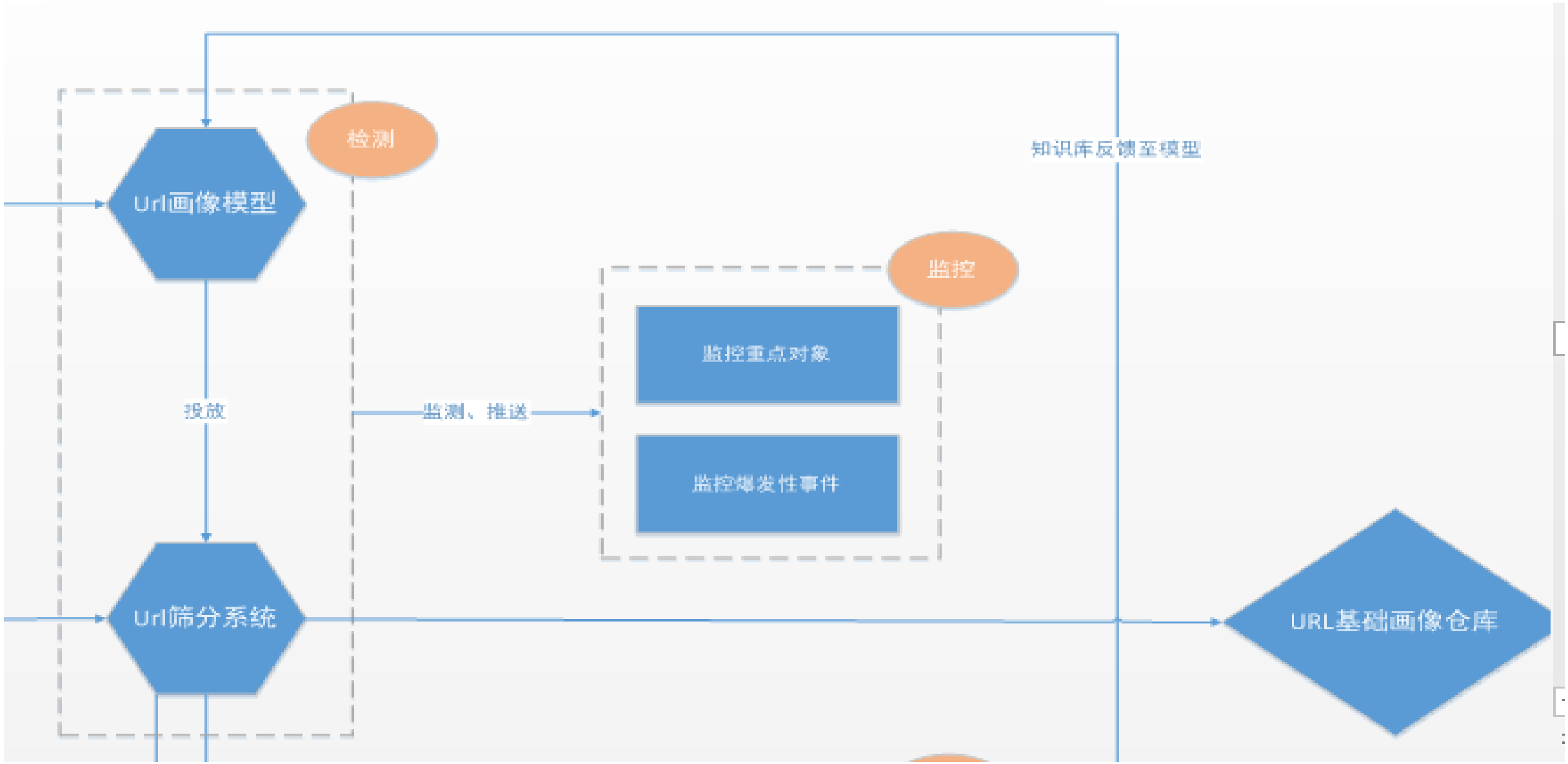
Observable

Target

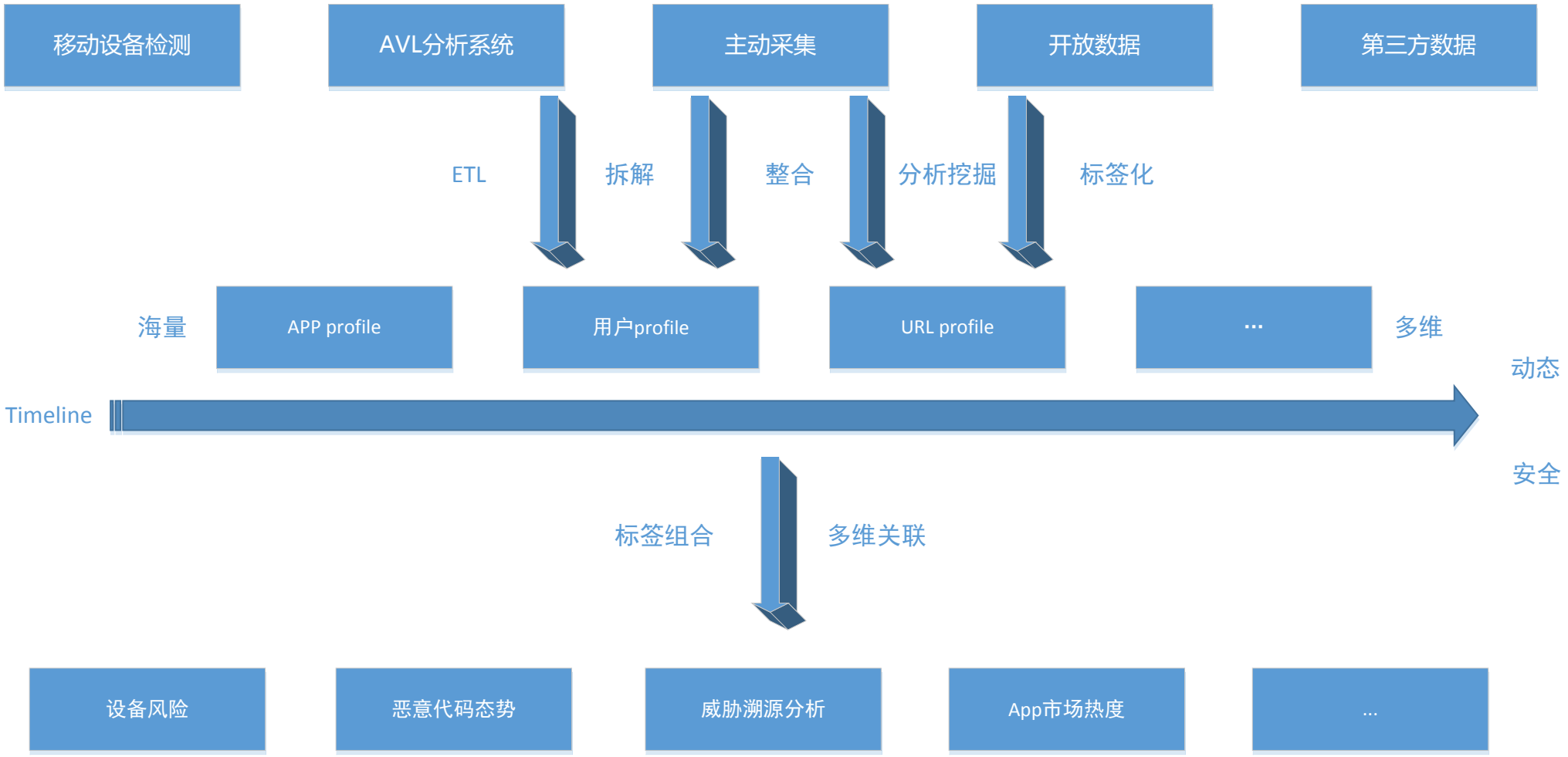


安全画像构建

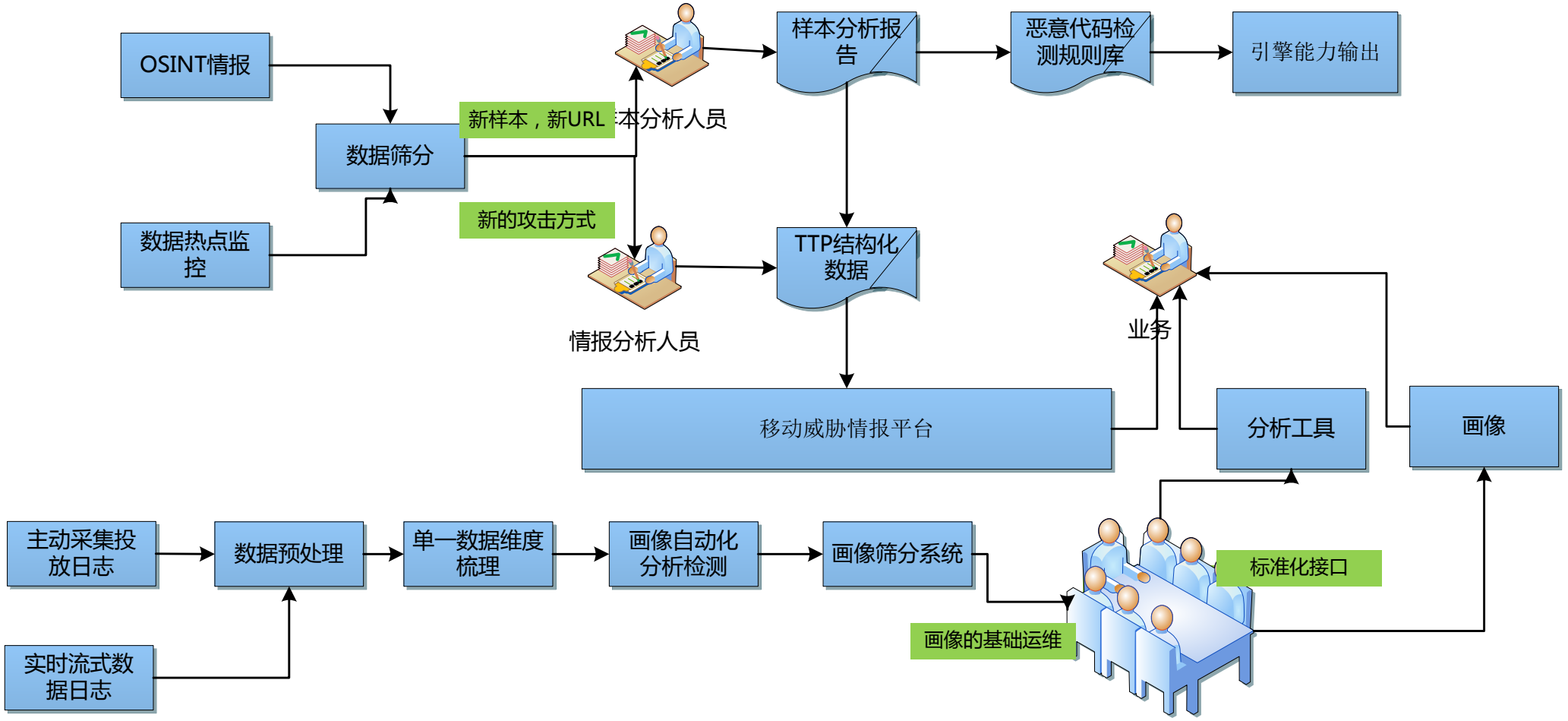
画像数据架构———数据仓库搭建



画像数据架构———画像生成体系



画像数据架构———人机协作


OSINT情报
数据筛分
数据热点监控
新样本，新URL
新的攻击方式
样本分析人员
情报分析人员
样本分析报告
恶意代码检测规则库
引擎能力输出
TTP结构化数据
移动威胁情报平台
业务
分析工具
画像
主动采集投放日志
实时流式数据日志
数据预处理
单一数据维度梳理
画像自动化分析检测
画像筛分系统
画像的基础运维
标准化接口

情报画像示例————画像标签构造

- 1、自身维度

- 统计标签化

标签	规则	ip数量（9月）	月同比增长
检出恶意量异常ip	检出恶意样本>=10		
检出恶意用户量异常ip	检出恶意样本用户>=10		
聚合性ip	设备量>=20,安装某app占比>=20%		

- 时间线标签化

hash	检出名	9月检出事件数	8月检出事件数
B2601******	Tool/Android.Kingroot.a[sys,cls]		
2B0EC******	PornWare/Android.sexplayer.a[rog,crt]		
E9D1E******	PornWare/Android.sexplayer.a[rog,gen]		

- 自身维度关系（样本相似度）

- 2、旁路维度

- 标签化传播

学习中国	侨联通	Juiker	whatsapp	telegram	军事情报
政府人员	华侨	台湾企业人员	用户量大，无特别指向性	情报人员	情报人员、军事爱好者

- 标签关联传播

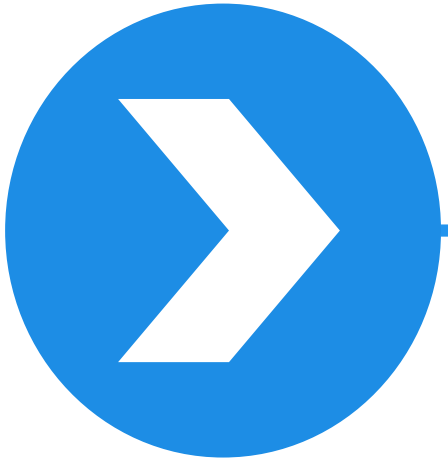
恶意样本--------C&C--------恶意样本

- 第三方私有数据标签化

- 3、基于数据挖掘判别的数据标签化

训练用于 NSFW 识别的深度网络

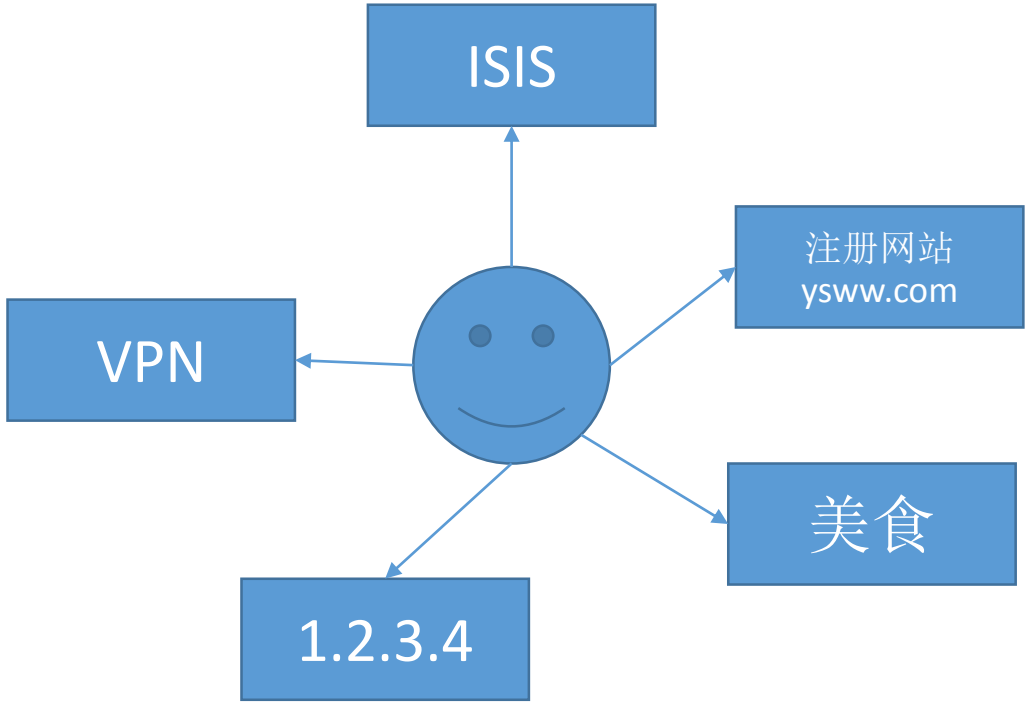
判别恶意样本的bayes判别

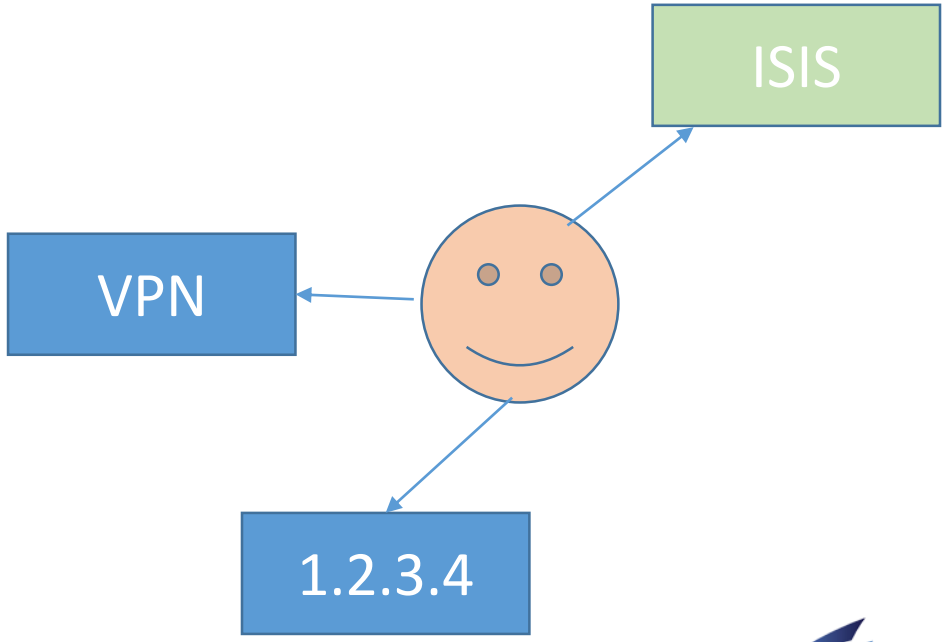


画像的AVL insight实践

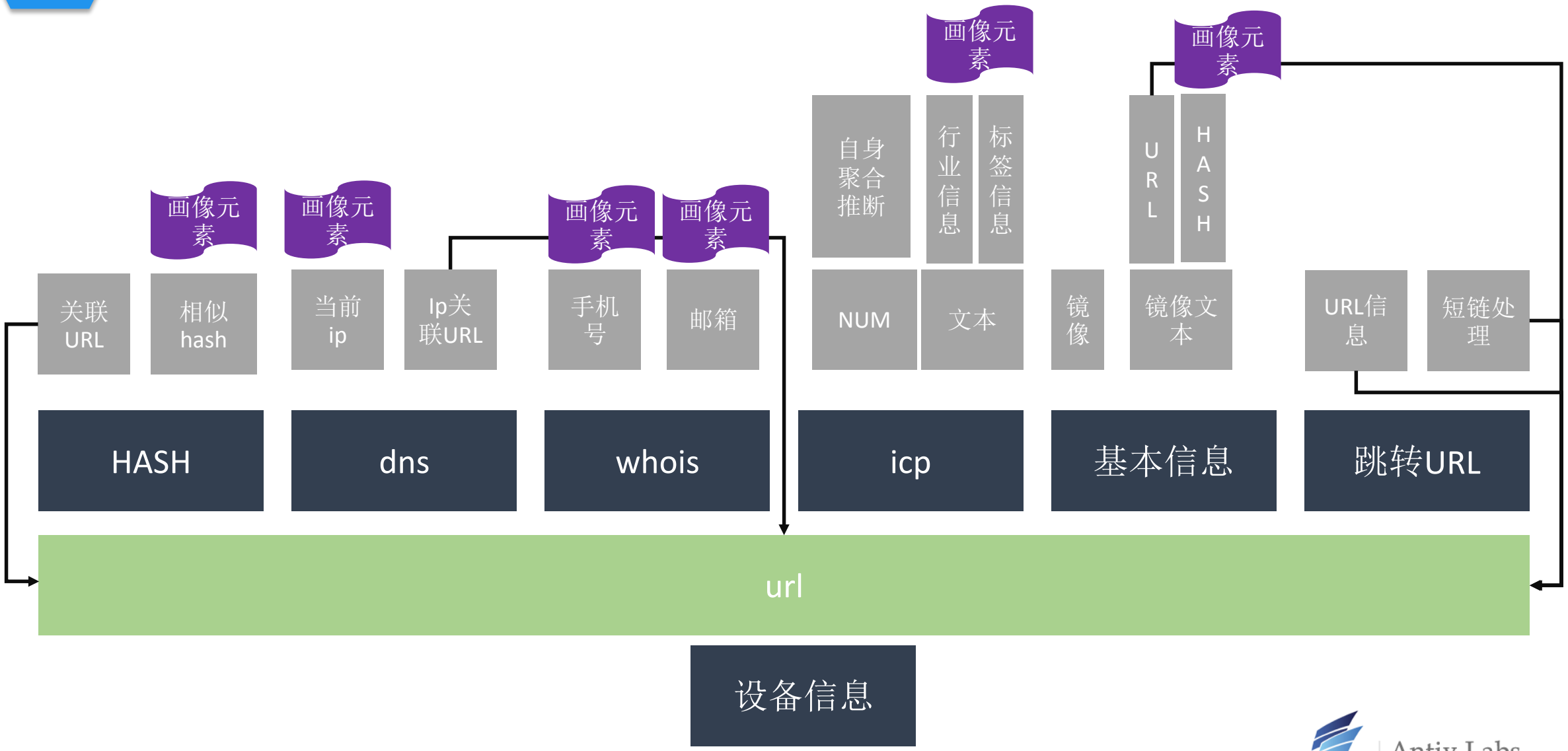
情报画像示例————画像标签传播

- 由于数据碎片化，很多单一维度的数据无法很好的描绘主题。
- 基于已知画像，通过重要维度推断未知画像



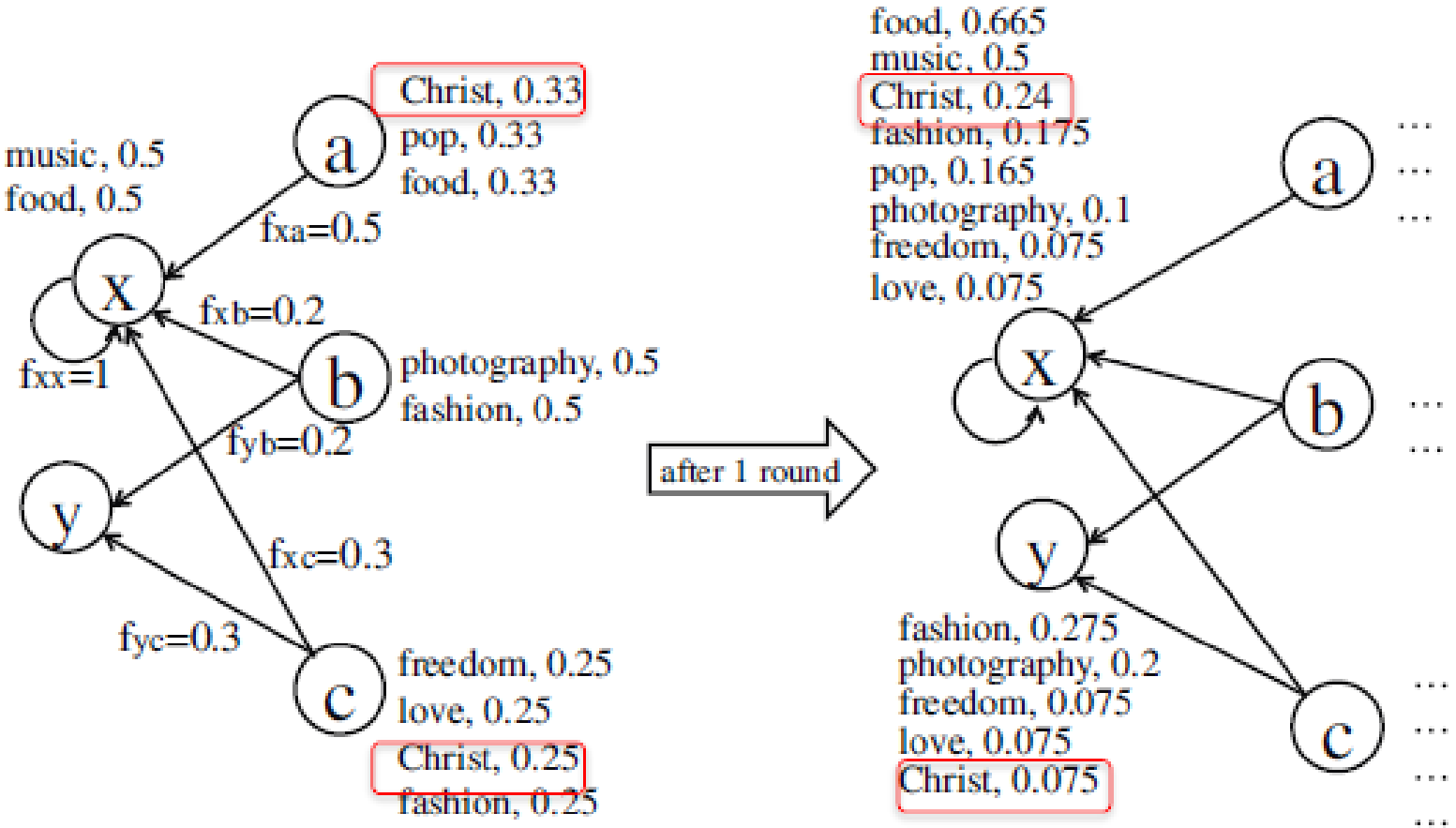


情报画像示例———画像标签传播

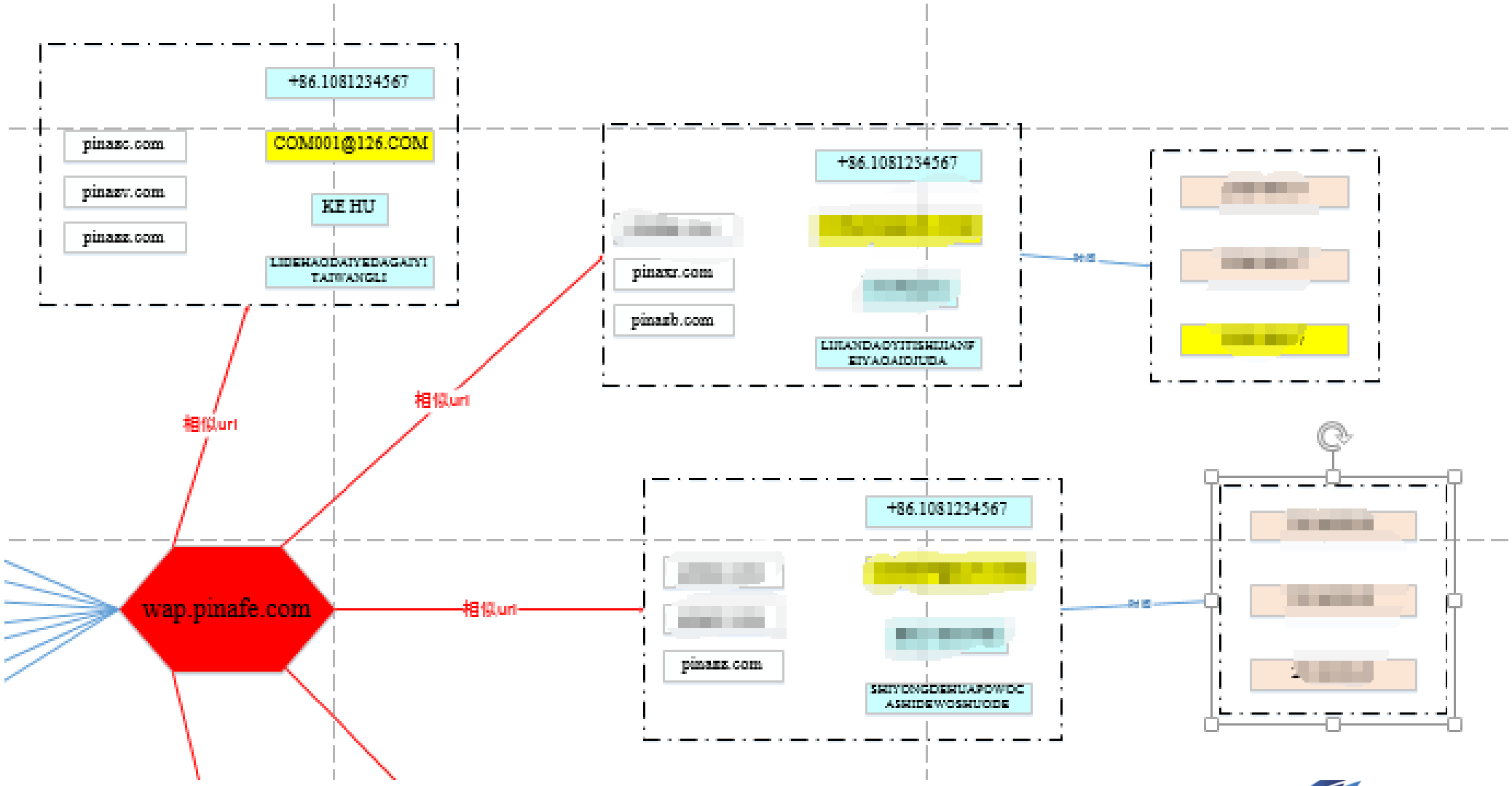


情报画像示例————画像标签传播

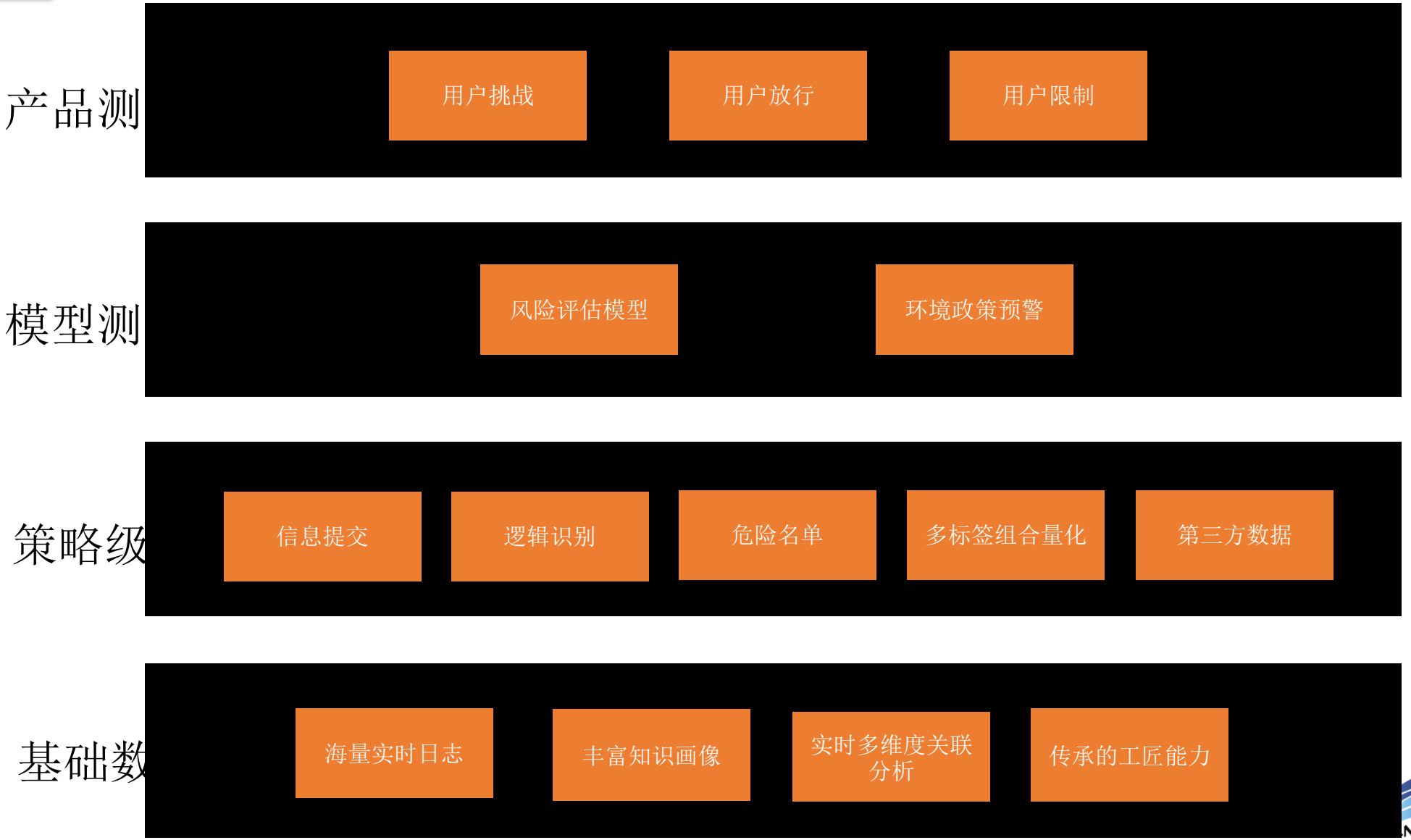
- 画像标签传播就是需要确定好传播关键路径和概率判别模型



情报画像示例————URL



画像数据应用————监控预警模型



画像数据应用———公开情报分析

支付宝木马安卓短信窃取者分析

发布时间：2016-04-27 16:06:00 来源：论坛 作者：红黑联盟

关键字：

前言

最近关于"点了一条短信 银行卡被盗刷好几千"之类的银行卡盗刷、各类理财账号被莫名转账等新闻越来越多。在这些案例中，非常多受害者都提到手机、验证码等关键词。是的，当前智能手机接收验证码用于更改密码、转账等操作，已经被用在各种产品中。如果这类重要短信被黑客偷偷上传并利用，后果不甚设想，很可能就会成为上面新闻报道的案例。

下文就分析这样一个针对支付宝用户的木马App，它伪装成安全软件，运行时会窃取各类重要短信并上传到指定服务器。

以下内容翻译、整理自

伪装成支付宝安全控件的木马App

应用名：安全控件

Md5：fad55b4432ed9eeb5d7426c55681586c

包名：com.bing.receive**

此木马起名"安全控件"并使用支付宝应用图标，使受害者误认为它是一个用于增强支付宝安全的应用。运行之后，木马会隐藏自身图标。同时，木马会注册多个services，正是这些services窃取短信，并发送到命令&控制(C&C)服务器。

技术细节分析

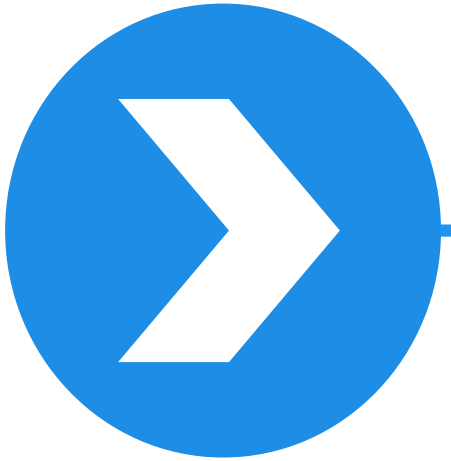
安装之后，此木马看起来就像是阿里系的应用

此木马起名"安全控件"并使用支付宝应用图标，使受害者误认为它是一个用于增强支付宝安全的应用。运行之后，木马会隐藏自身图标。同时，木马会注册多个services，正是这些services窃取短信，并发送到命令&控制(C&C)服务器。

技术细节分析

安装之后，此木马看起来就像是阿里系的应用

一旦受害者点击运行之后，将出现一个引导页面。3秒之后，这个页面与程序图标都会消失。



面向现场分析的画像实践

行为画像
偏好、模式、步骤

攻击武器化 → 攻击投放 → 攻击实施 → 持续侵害

攻击者画像

角色
身份
能力
资源

线索 → 现场 → 还原 → 画像 → 线索

事件画像
时间线、背景、动机、意图

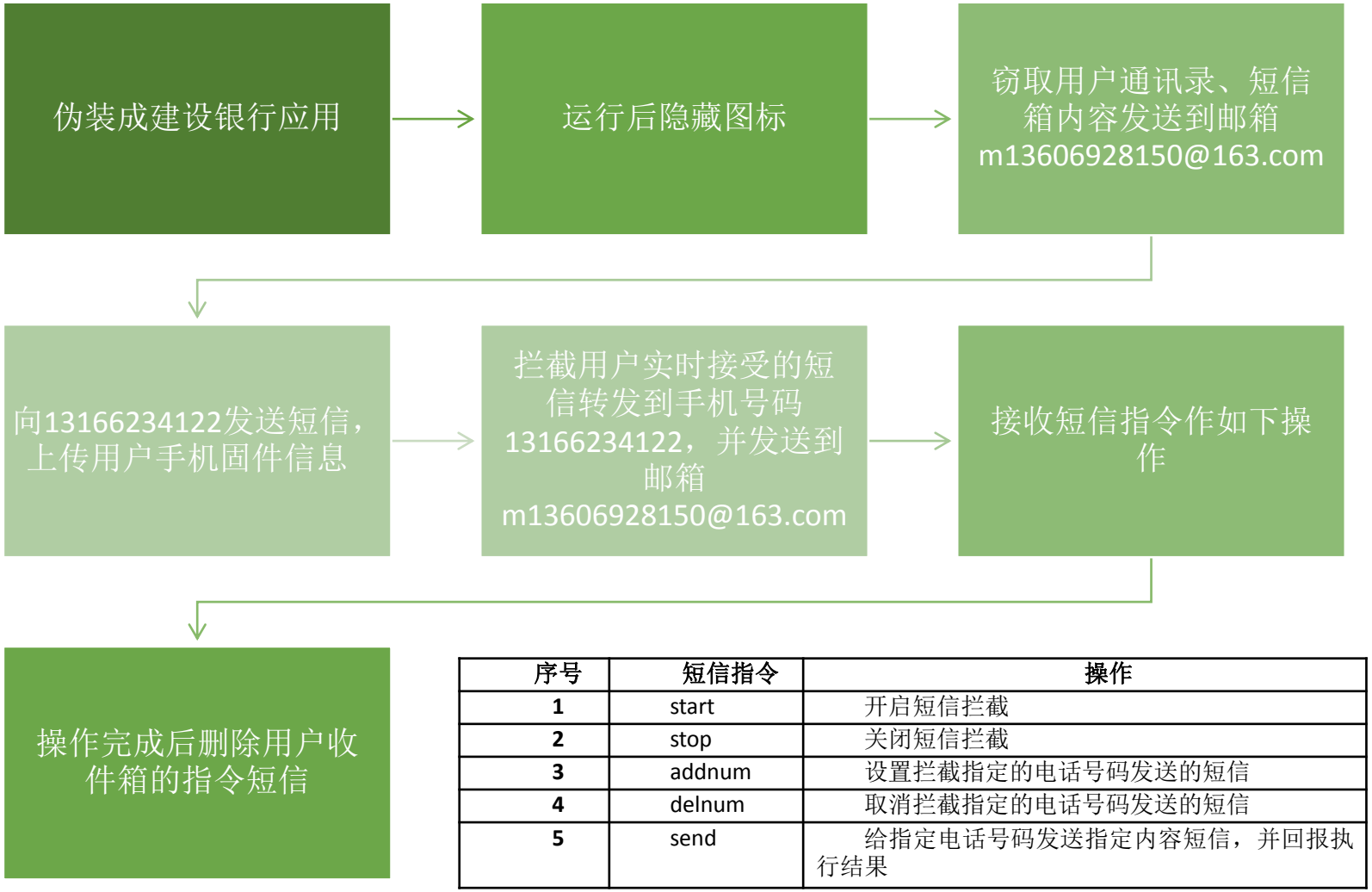
受害者画像

资产
设备
身份
角色

行为画像


95533
建设银行普通纪念币预约服务。[建设银行]
建行喜讯通知：您账户已满20000积分可兑换5%的现金，请于今日及时登录手机网 wap.xxcrep.cc 查询兑换，逾期失效【建设银行】
建行喜讯通知：您账户已满20000积分可兑换5%的现金，请于今日及时登录手机网 wap.ybckcb.cc 查询兑换，逾期失效【建设银行】
键入信息
积分兑换现金
注册卡（账）号
6位数交易密码
真实姓名
身份证号
银行预留手机号码
上一步
提交
中国建设银行
建行手机网
简洁版
完整版
客户服务热线：95533
导航
动态
查询
行情
微博
虚拟付款验证，完成提现
系统将自动发送6位短信验证码验证身份，完成积分 10000分兑换500元现金业务【建设银行】
虚拟金额：5000元(不作于扣费处 理)
请输入验证码
重新发送(111)
温馨提示：您的手机将收到6位短信验证码，验 证1至20000不等的虚拟付款金额（此验证非真实扣款）
http://wap.ybckcb.cc/online.asp
系统正在为您验证提现
请稍等！系统正在核对为您验证提现！请勿关闭网页
上一步
©版权所有 中国建设银行版权所有 京ICP备 13030780号
京公网安备 110102000450

行为画像



序号	短信指令	操作
1	start	开启短信拦截
2	stop	关闭短信拦截
3	addnum	设置拦截指定的电话号码发送的短信
4	delnum	取消拦截指定的电话号码发送的短信
5	send	给指定电话号码发送指定内容短信，并回报执行结果

受害者画像

国外某安全企业技术管理层？

安全性偏执

重度安全产品用户

技术背景

管理背景

国外

APP

安装62个安全类应用

6个金融理财

3个算法和人工智能类

2个管理类

3个VPN代理类

语言

中文

英文

IP

美国

挪威

行为

每隔2-3天扫描一次

没有检出过恶意样本

攻击者画像

黑产职业从业人员

2012~2016

外挂、QQ盗号、拦截马

能力

资源

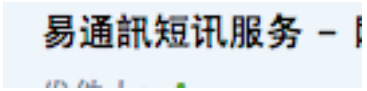
角色

木马制作

社工库

钓鱼网站制作

游戏外挂



注册一些游戏

用户ID

平安贷款、铂涛酒店、支付宝

事件画像

2013.1~2013.末	2014年上半年	2015.5~2016.2
• 最早的移动攻击活动最早的证书生成时间是2013.1.3，并且在早期就进行了木马原型的开发和功能测试，其主要伪装成系统应用图标和名称，早期的木马分发主要结合钓鱼来进行，并且早期攻击平台除了Android，还有BlackBerry	• 攻击组织开始尝试结合新闻类应用，形成新的投放方式和模式	• 攻击组织形成了明确的攻击模式，制作伪装成社交应用的木马程序，并借助Google Play应用商店进行投放和推广，在程序的开发周期和数量上都比前期显著提高，证明攻击组织在这个阶段无论从能力还是资源方面都有显著提升

公开线索 → 分析 → 关联 → 聚合

THANKS

AV移动安全·安天

www.antiy.cn

ANTIY 安天