

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

AVK 移动安全·安天





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

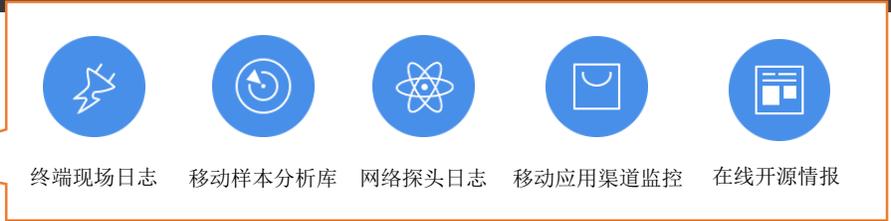
TI

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





基础数据
结构化数据
画像数据



情报化加工
策略化输出

FSI 819 面向威胁分析的工程化实践



TTP+/战术技术情报



FSI 219

威胁情报体系要素



Strategic FSI 520
威胁情报产品架构
Technical



基础数据

结构化数据

画像数据

FSI 2016 面向应用的数据画像体系



情报化加工

FSI 819 面向威胁分析的工程化实践

FSI 819

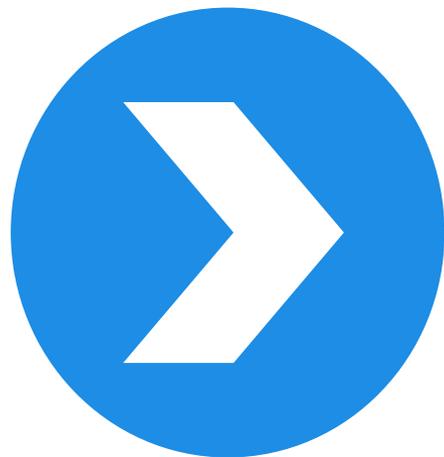


策略化输出

Strategic FSI 520 威胁情报产品架构

Technical





画像从互联网到安全



Antiy Labs

The Next Generation Anti-Virus Engine Innovator

身高八尺，面如冠玉，头戴纶巾，
身披鹤氅，飘飘然有神仙之概。



姓名 奥巴马
性别 男 民族 肯尼亚
出生 1961 年 8 月 4 日
住址 华盛顿特区宜宾法尼亚
大道1600号白宫
公民身份号码 123456196108047890



13 詹姆斯·罗德里格斯
10  180 cm/79 kg
哥伦比亚 1991.07.12
FW 74
CM 74

76	盘带速度	59
51	人盯人	26
67	侵略性	67
67	战术意识	54
58	抢断	35
75	铲断	30
74	GK扑救	17
73	GK手控球	17
	GK大脚开球	17
	GK反应	16
	GK防守站位	9
	GK一对一	

站位	73	视野	78
速度	71	控球	77
加速	73	盘带	78
灵活	73		



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，开始模仿声音。

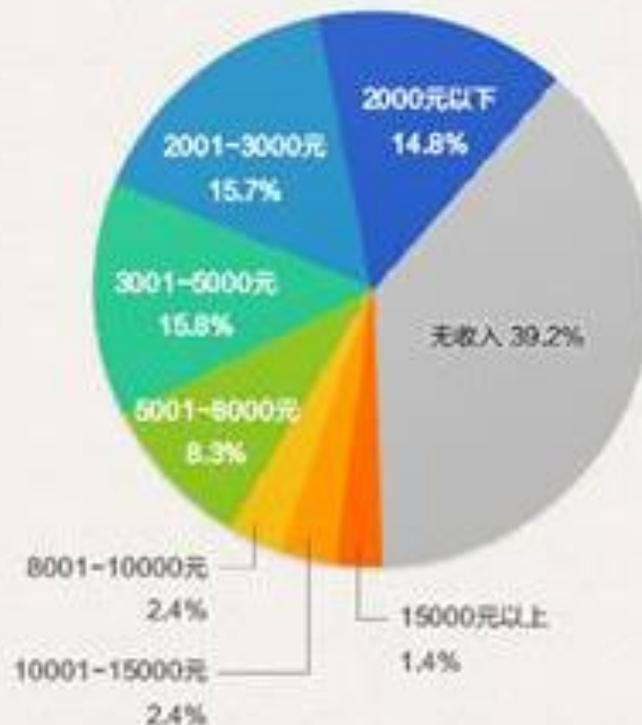


用户属性数据

职业分布



个人月收入





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



原始数据



实事标签

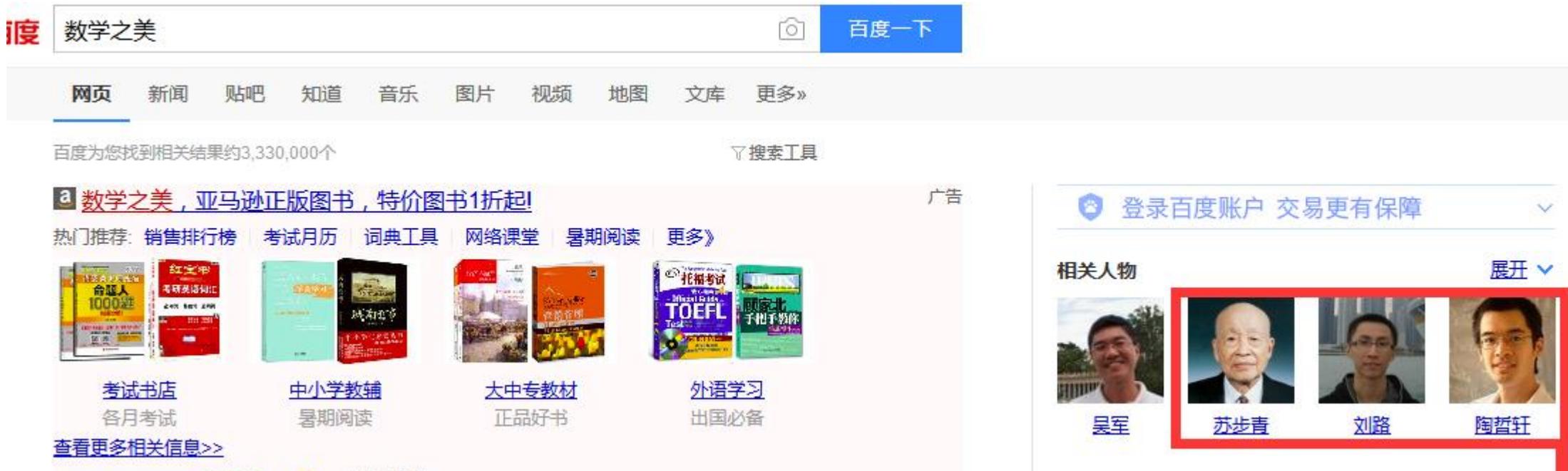
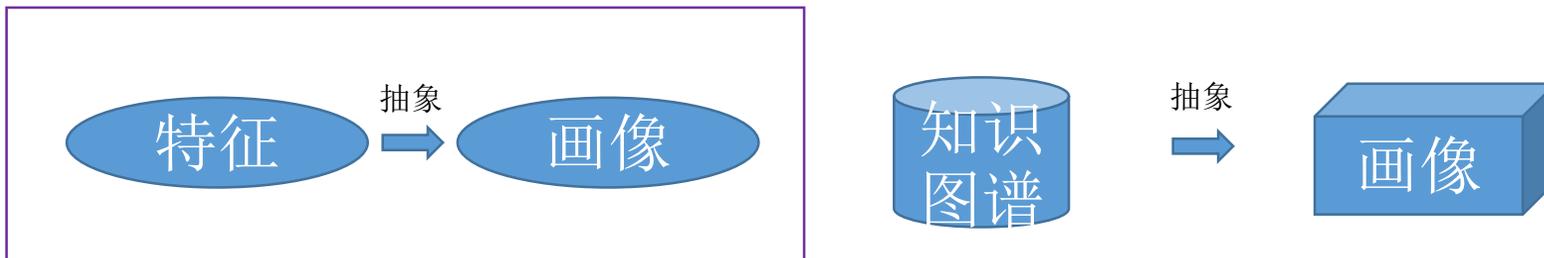


模型标签

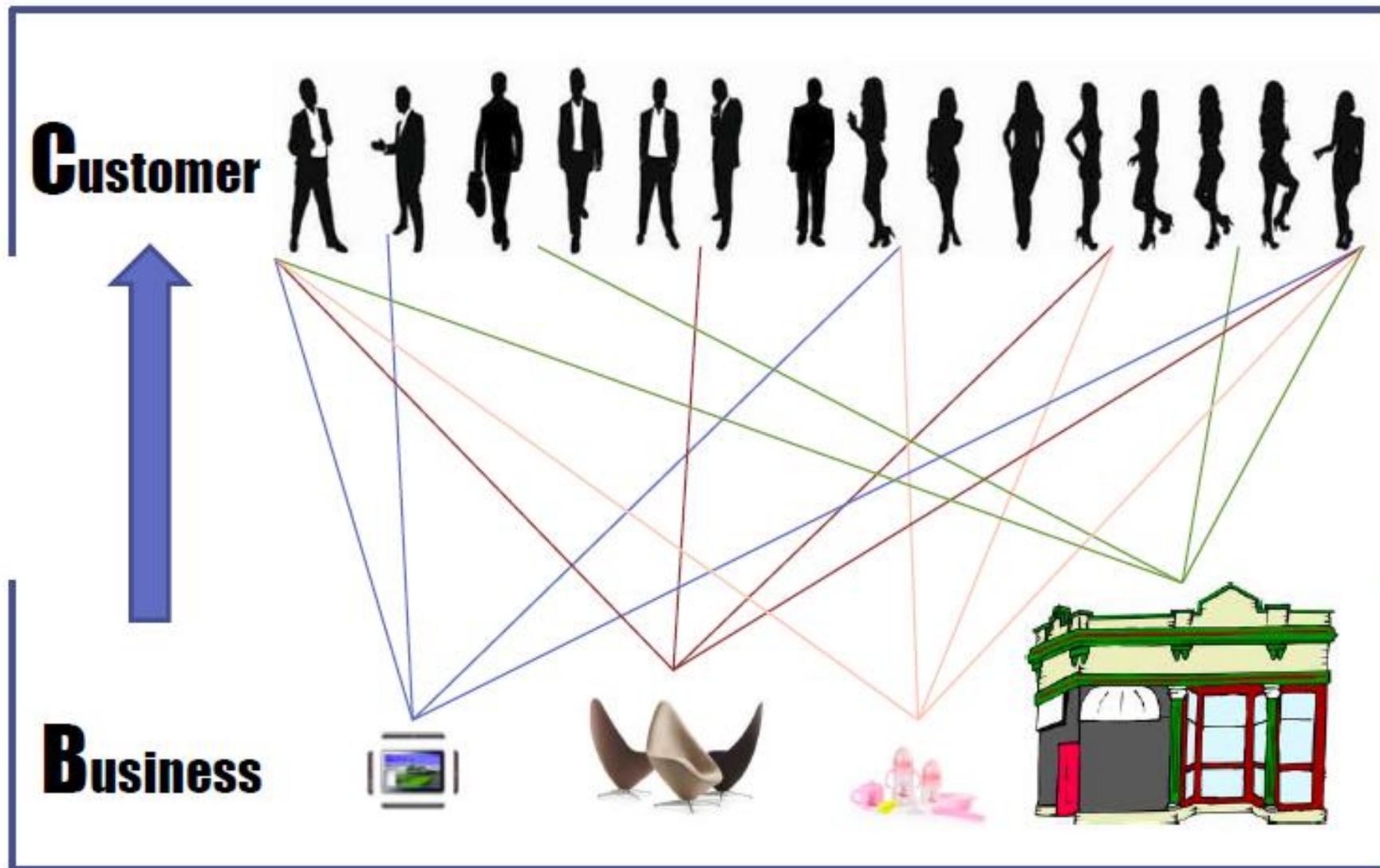


预测标签





The screenshot shows a Baidu search result for '数学之美' (Beauty of Mathematics). The search bar contains the text '数学之美' and a '百度一下' (Baidu Search) button. Below the search bar is a navigation menu with options: '网页' (Webpages), '新闻' (News), '贴吧' (Tieba), '知道' (Zhidao), '音乐' (Music), '图片' (Images), '视频' (Videos), '地图' (Maps), '文库' (Library), and '更多' (More). The search results indicate approximately 3,330,000 related results. An advertisement for '数学之美, 亚马逊正版图书, 特价图书1折起!' (Beauty of Mathematics, Amazon authentic books, special price books 10% off!) is displayed, featuring various book covers and categories like '考试书店' (Exam Bookstore), '中小学教辅' (Primary and Secondary School Textbooks), '大中专教材' (University and College Textbooks), and '外语学习' (Foreign Language Learning). On the right side, there is a section for '相关人物' (Related People) with a '展开' (Expand) button. It shows four portraits: 吴军 (Wu Jun), 苏步青 (Su Bqing), 刘路 (Liu Lu), and 陶哲轩 (Tao Zhexuan). The portraits of 苏步青, 刘路, and 陶哲轩 are highlighted with a red border.



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：

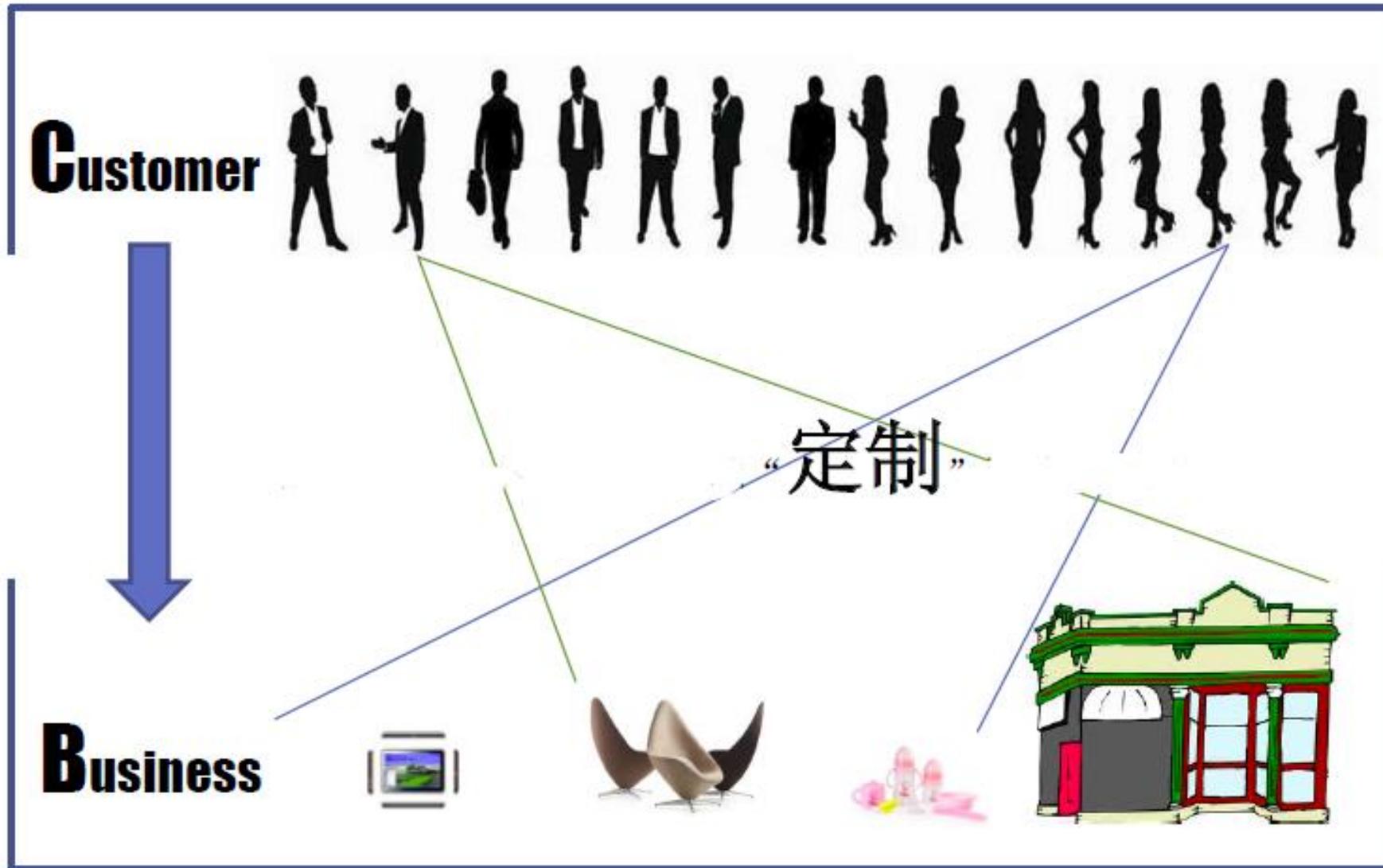
“坏人” “有钱” “偷钥匙”

“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







user

- 人口画像
- 风险画像
- 状态画像
- 设备画像
- 应用画像

ip

- 基本画像
- 状态画像
- 关联画像
- 安全画像
- 时间画像

url

- 基本画像
- 状态画像
- 关联画像
- 安全画像
- 时间画像

App(泛)

- 行业画像
- 类别画像
- 风险画像
- 人群画像

phone

- 属性画像
- 安全画像
- 注册画像

email

- 来源画像
- 安全画像
- 注册画像

pic

- 来源属性
- 判别属性
- 相似属性

...

- ...





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

大量的人工预处理作业

完善易用的规则优化后台

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

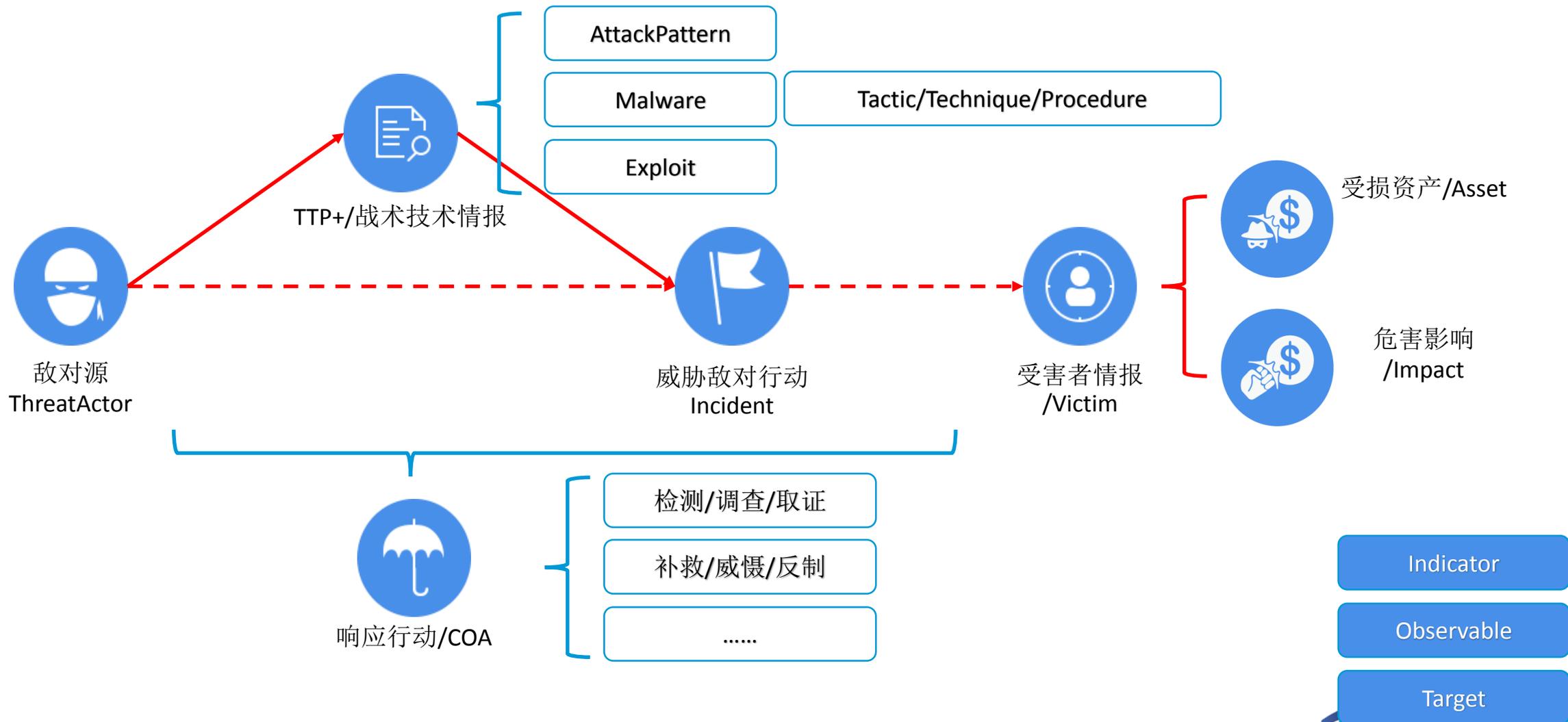
大量的人工安全分析判定

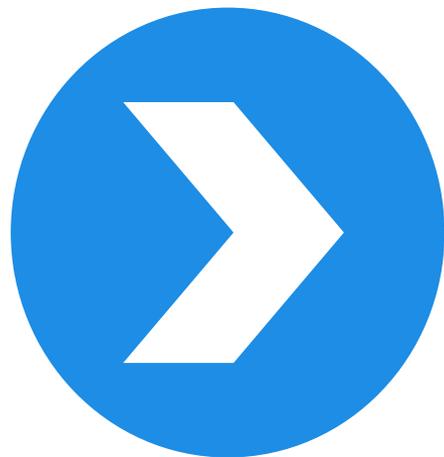
高效的分析业务流转结构化



- 1. 攻击者信息统计.....3
- 2. 攻击链流程分析.....4
- 3. 样本所用战术分析.....5
- 4. 完整攻击链还原分析.....8
 - 4.1. 隐藏窃取并拦截转发短信行为.....8
 - 4.1.1. 样本 1.....8
 - 4.1.2. 样本 2.....17
 - 4.1.3. 样本 3.....24
 - 4.1.4. 样本 4.....35
 - 4.2. 后台网络窃取短信行为.....43
 - 4.2.1. 样本 1.....43
 - 4.2.2. 样本 2.....44
 - 4.3. 伪造界面诱骗信息并转发行为.....47
 - 4.3.1. 样本详情.....47
 - 4.3.2. 恶意行为.....47
 - 4.3.3. 溯源分析.....47
 - 4.3.4. 制作时间.....48
 - 4.4. 私自载入及窃取拦截行为.....48
 - 4.4.1. 样本 1.....48
 - 4.4.2. 样本 2.....50
 - 4.5. 实时转发用户输入信息行为.....52





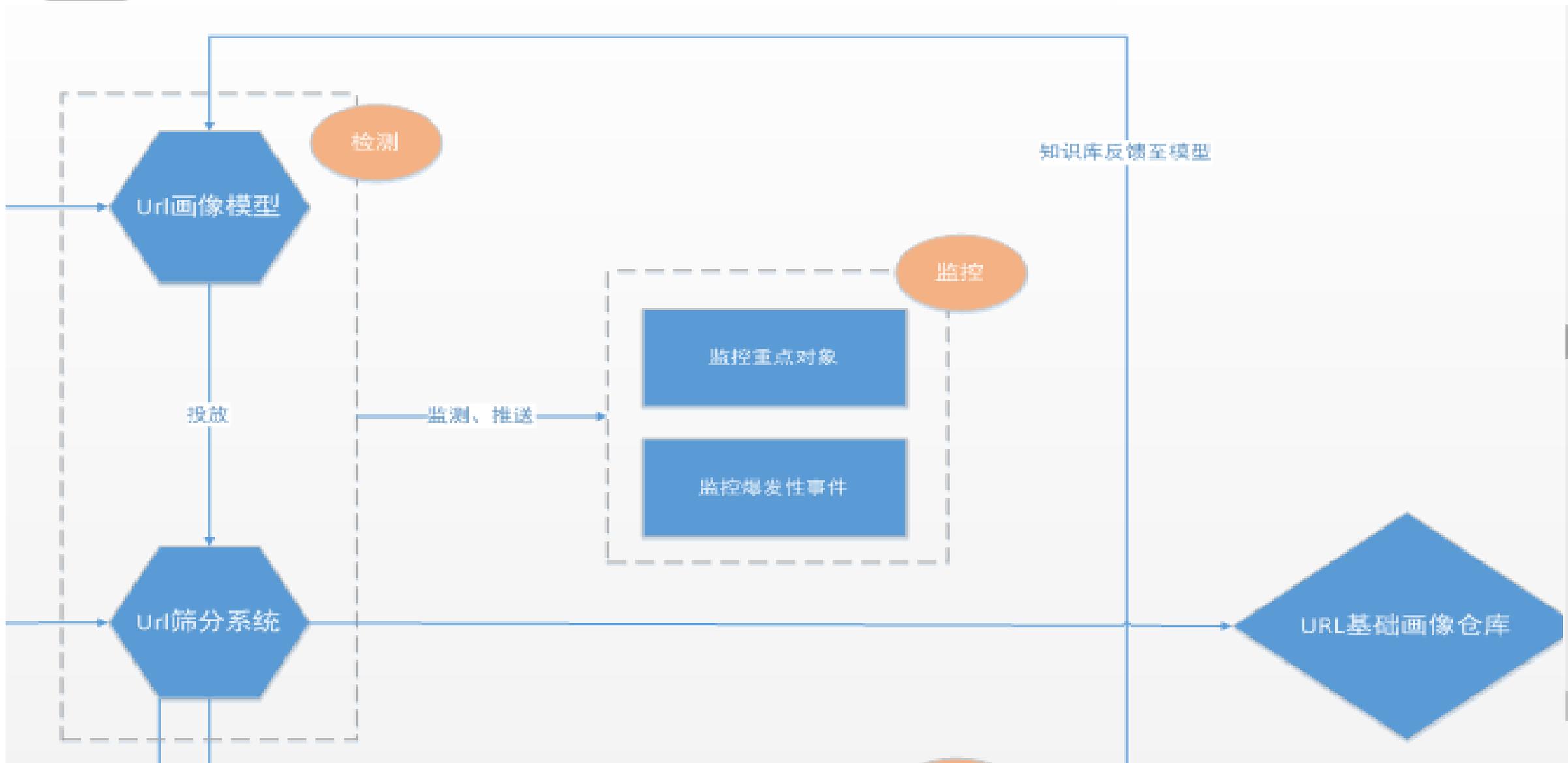


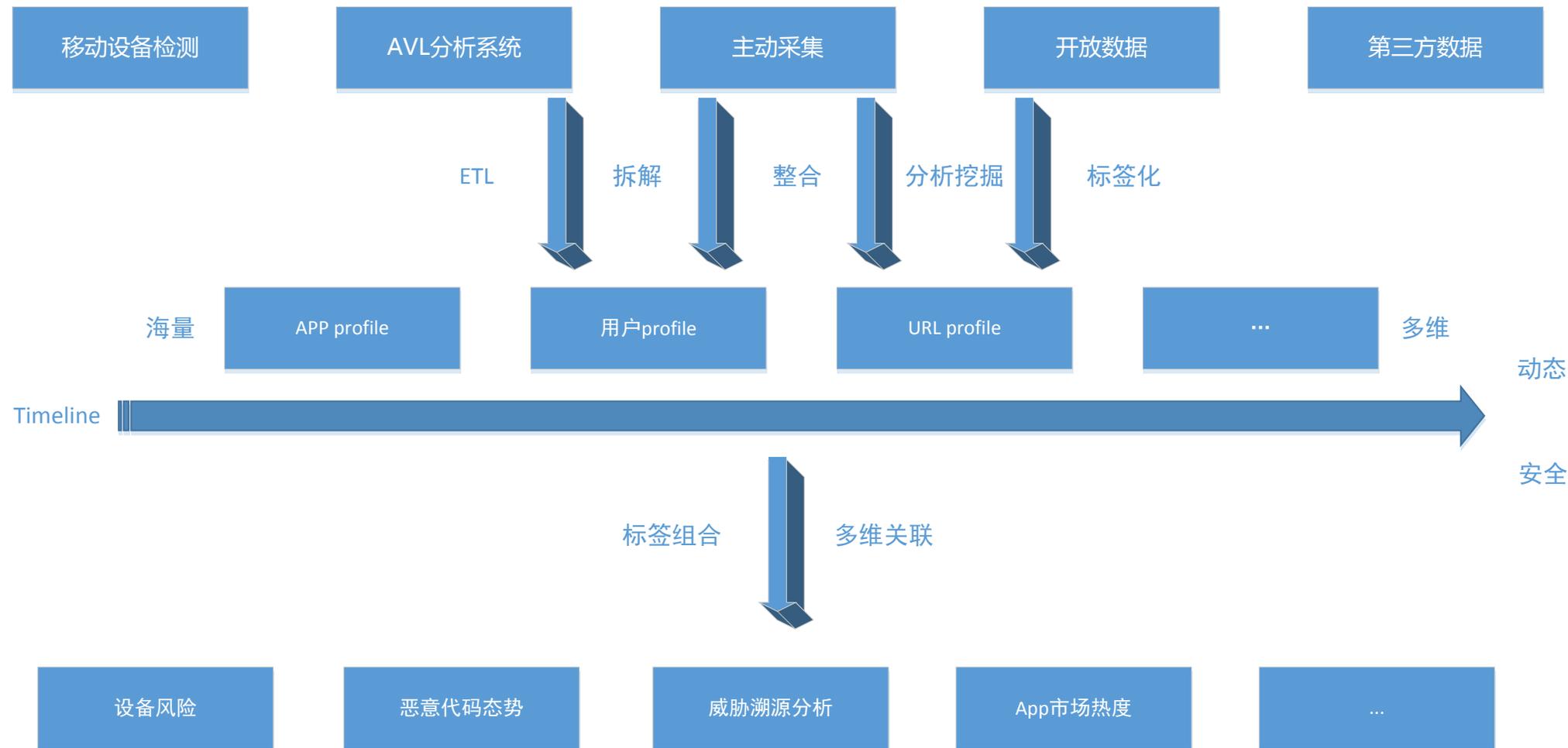
安全画像构建

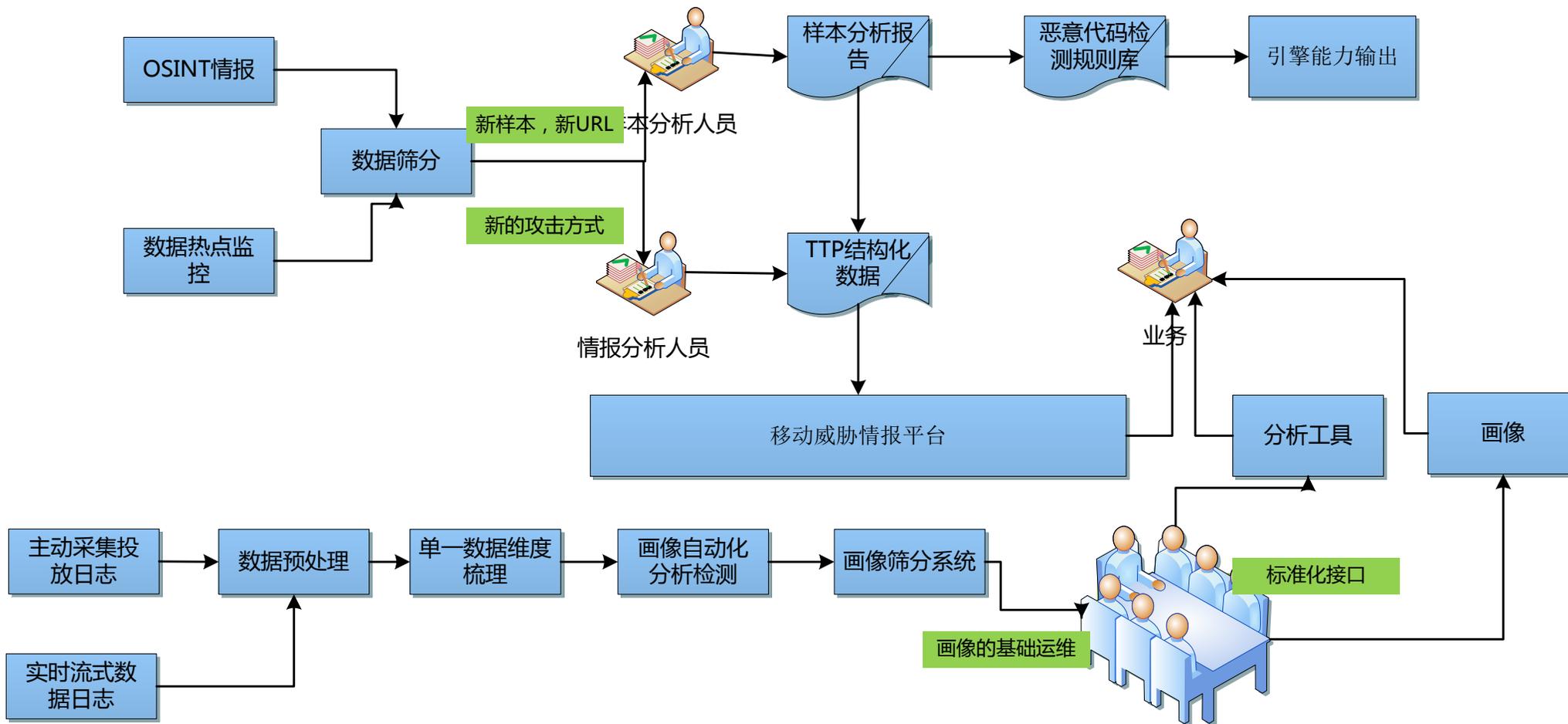


Antiy Labs

The Next Generation Anti-Virus Engine Innovator







- 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	[Redacted]	[Redacted]
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 $\geq 20\%$		

- 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]	[Redacted]	[Redacted]
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

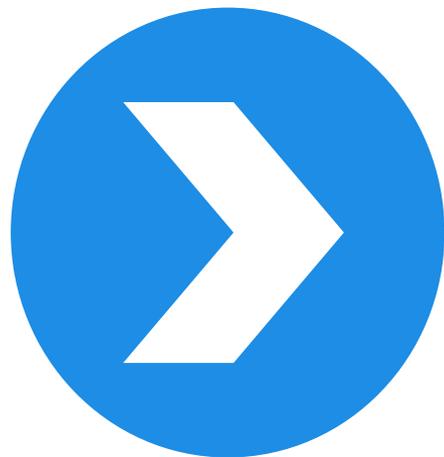
- 第三方私有数据标签化

- 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



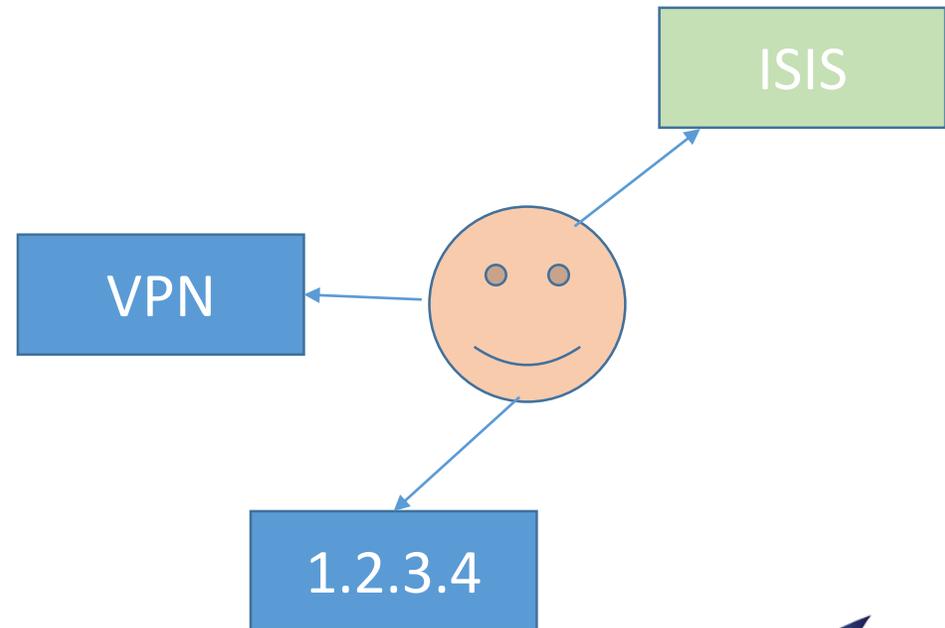
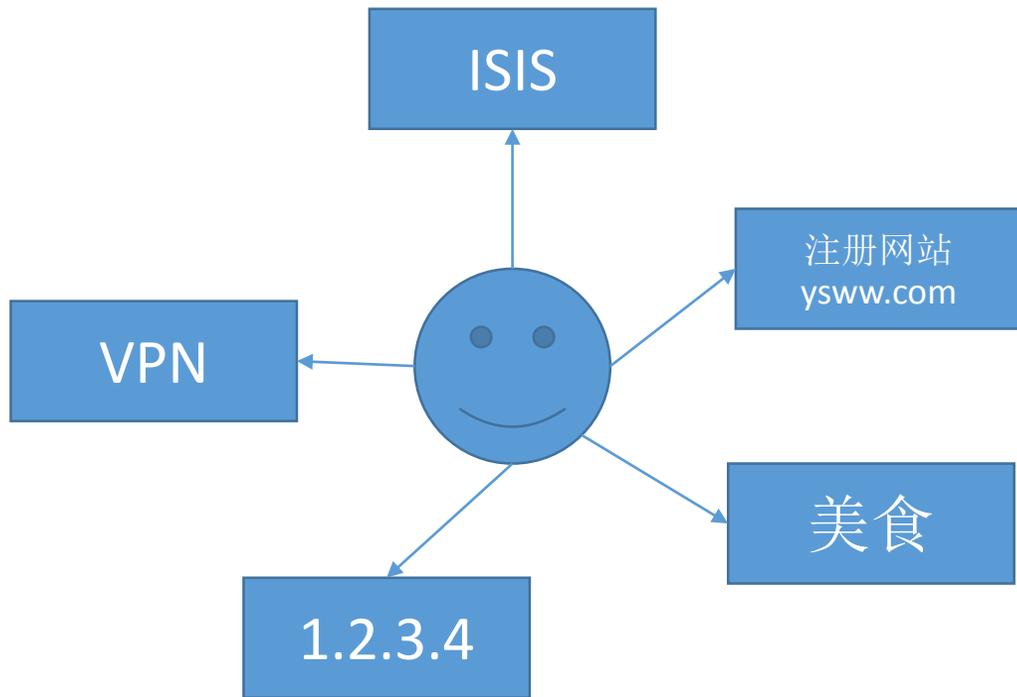
判别恶意样本的bayes判别

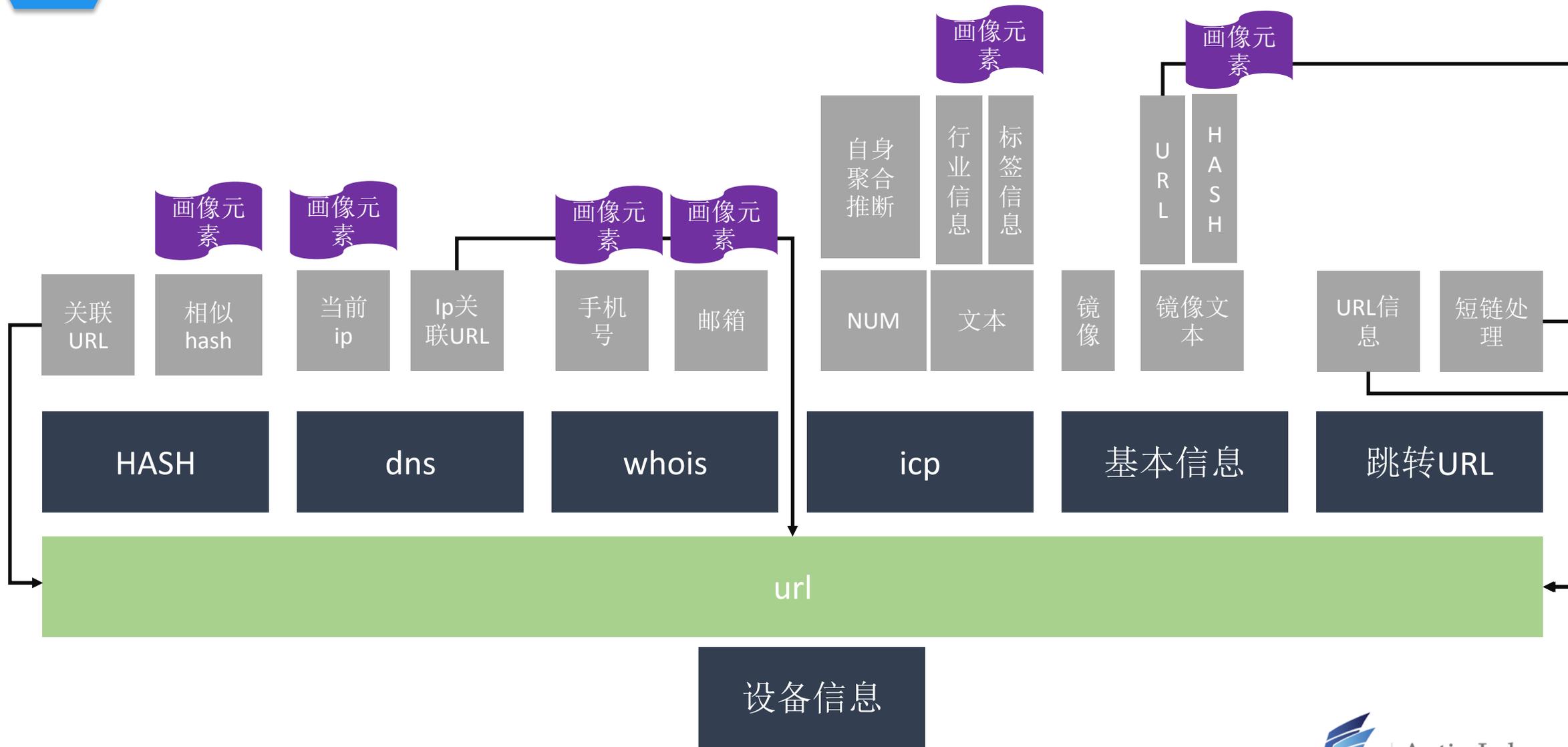


画像的AVL insight实践

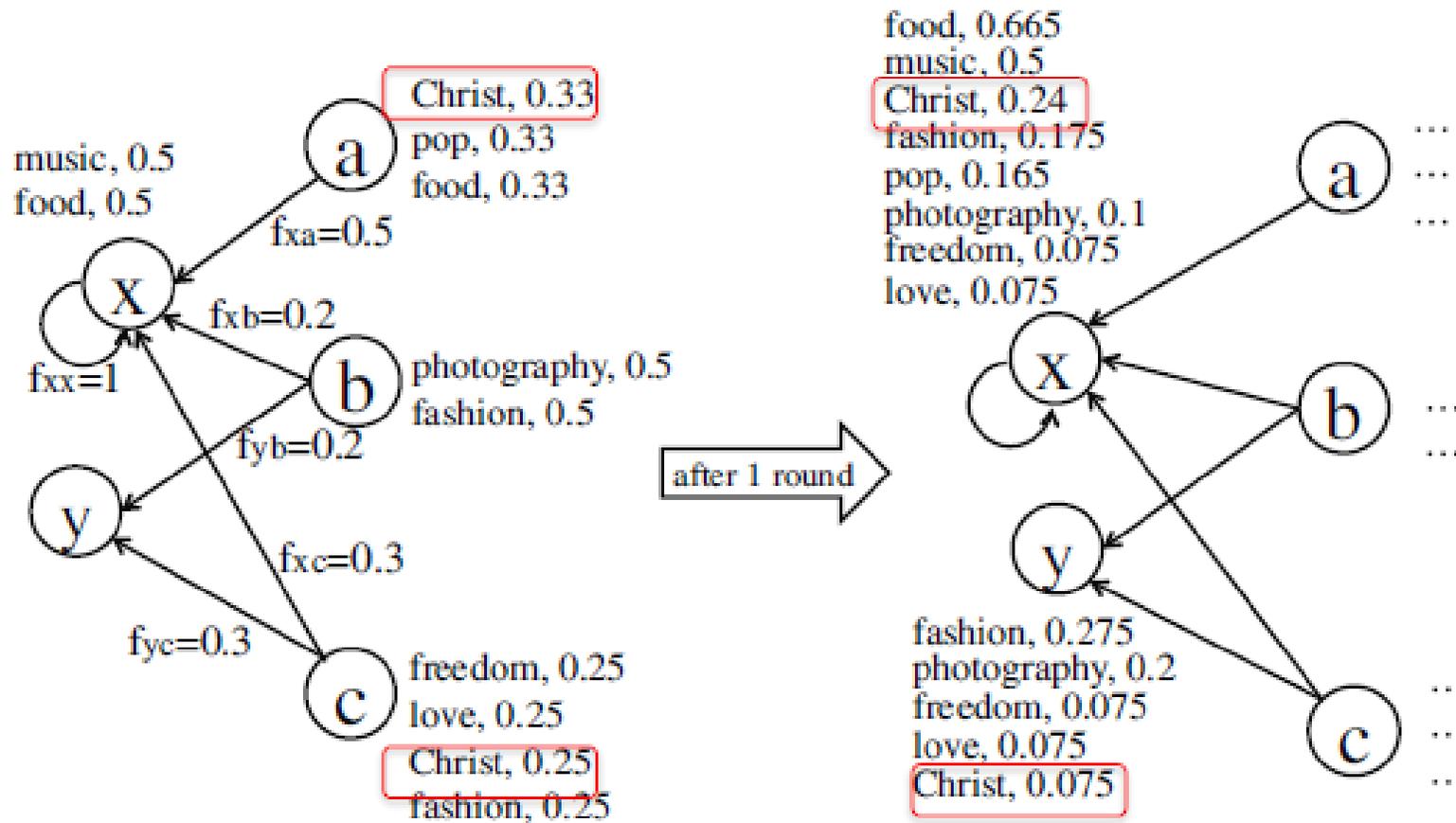


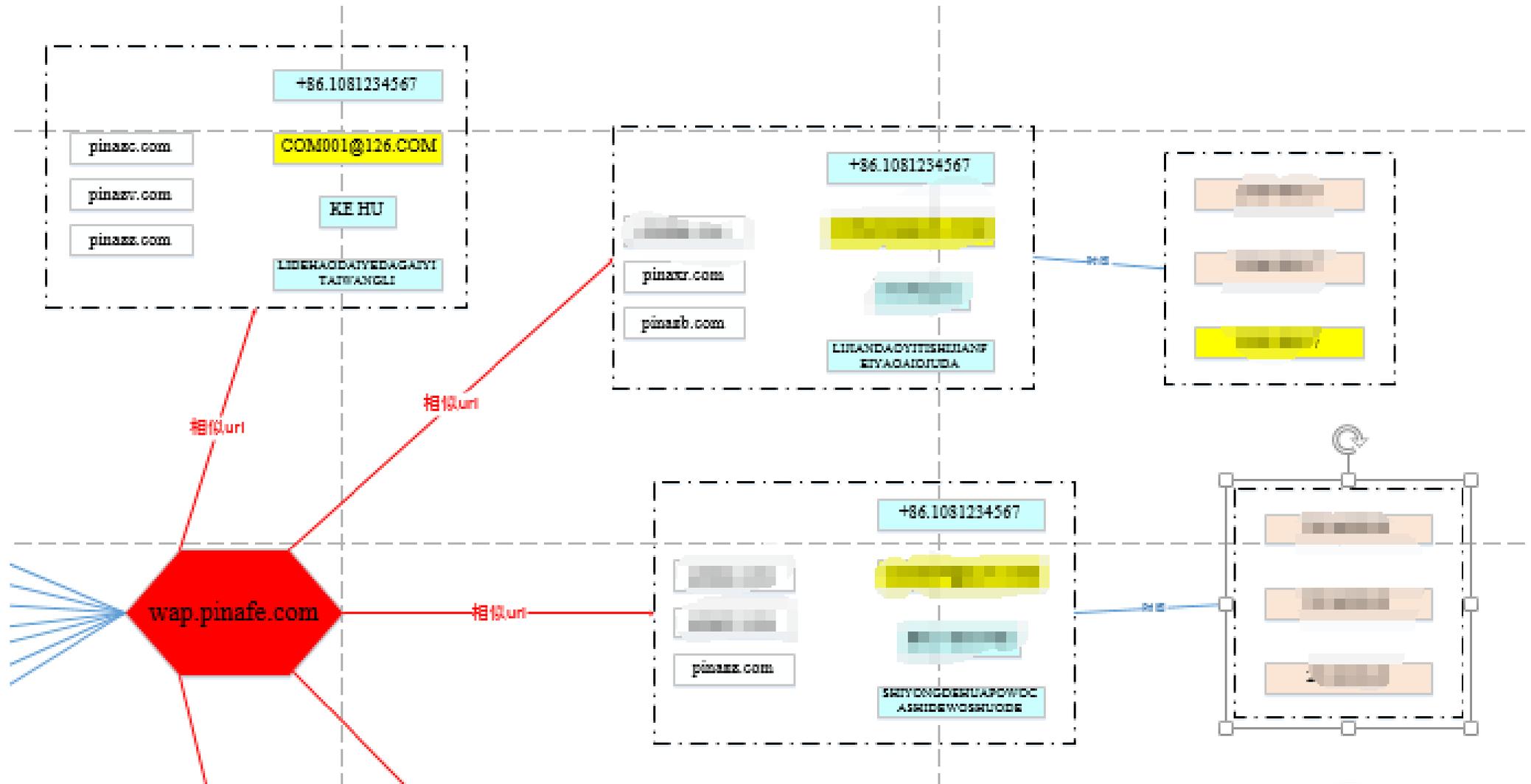
- 由于数据碎片化，很多单一维度的数据无法很好的描绘主题。
- 基于已知画像，通过重要维度推断未知画像





- 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





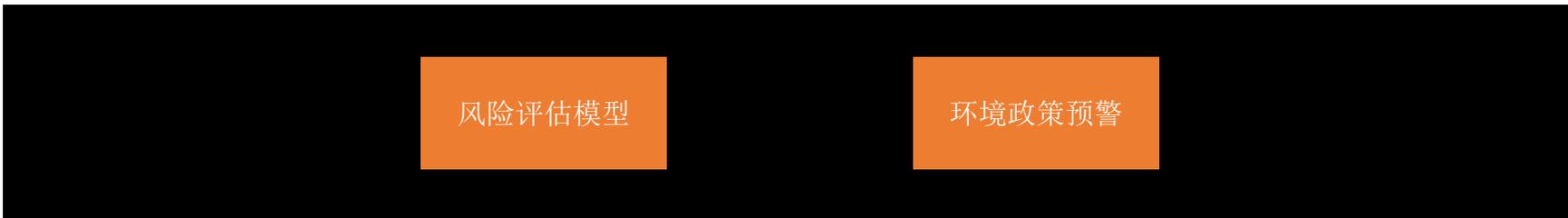


画像数据应用——监控预警模型

产品测



模型测



策略级



基础数



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

A+ A-

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，后果不堪设想，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。

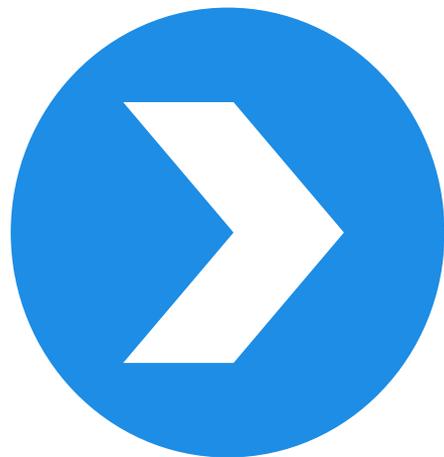
技术细节分析

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。





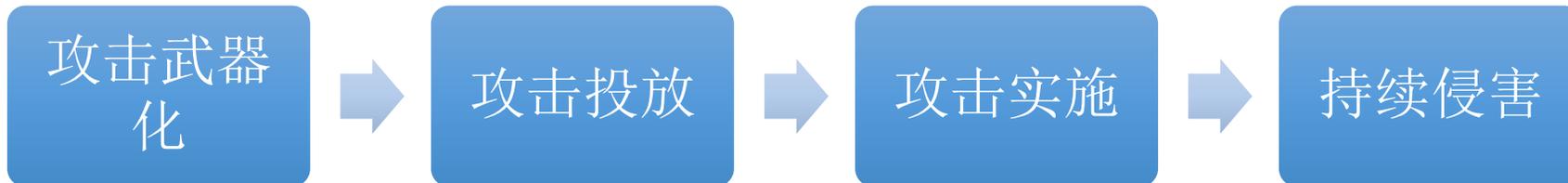
面向现场分析的画像实践



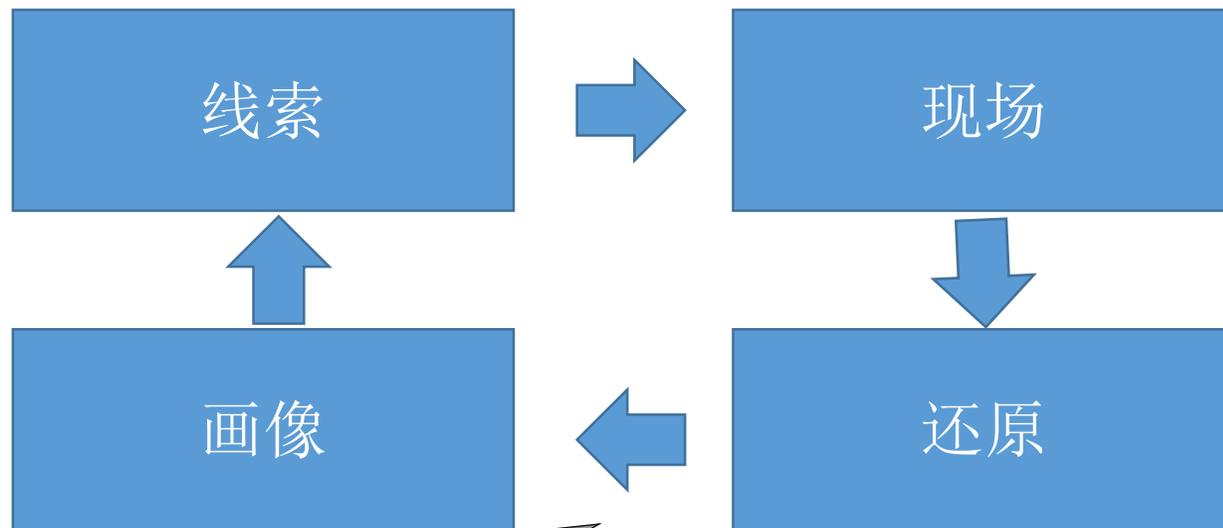
Antiy Labs

The Next Generation Anti-Virus Engine Innovator

行为画像
偏好、模式、步骤



攻击者画像
角色
身份
能力
资源



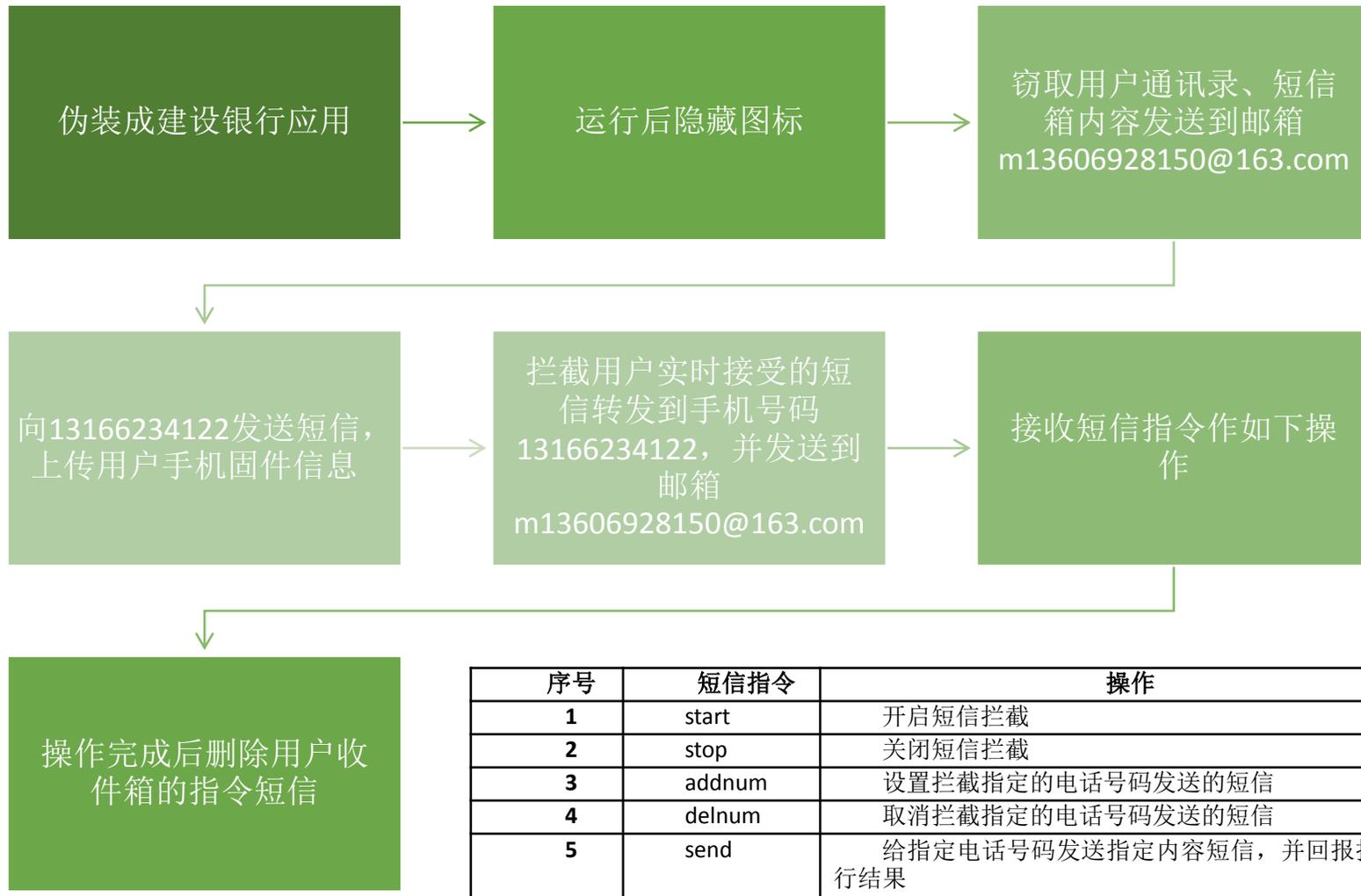
事件画像
时间线、背景、动机、意图

受害者画像
资产
设备
身份
角色



The screenshots illustrate a user's behavior on the CCB mobile app:

- Notification:** The user receives a message about redeeming 20,000 points for 5% cash. The notification includes a link to wap.xxcrep.cc and wap.ybckcb.cc.
- Registration Form:** The user is prompted to register for a virtual payment verification service. The form includes fields for:
 - Registered Card (Account) Number: 6217 [redacted] 2328
 - 6-digit Transaction Password: [redacted]
 - Real Name: 姜 [redacted]
 - Identity Card Number: 370 [redacted] 53
 - Bank Pre-registered Mobile Number: 13 [redacted] 70
- Verification Screen:** The user is informed that the system will automatically send a 6-digit short message verification code. The virtual amount is 5000 RMB (not for fee deduction). The user is asked to enter the verification code, with a "Resend (111)" button.
- Loading Screen:** The system is currently verifying the user's identity. A loading spinner is shown, and the user is advised to wait and not close the browser.



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

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

语言

IP

行为

安装62个安
全类应用

6个金融理财

中文

美国

每隔2-3天扫
描一次

3个算法和人
工智能类

2个管理类

英文

挪威

没有检出过
恶意样本

3个VPN代理
类

黑产职业从业人员

2012~2016

外挂、QQ盗号、拦截马



能力

资源

角色

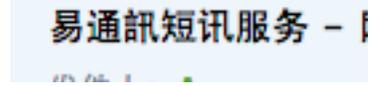
木马制作

社工库

注册一些游戏

钓鱼网站制作

游戏外挂



用户ID

平安贷款、铂涛酒店、支付宝

2013.1~2013.末

- 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

2014年上半年

- 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

2015.5~2016.2

- 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

