网络安全创新大会
Cyber Security Innovation Summit

永安在线 · 业务安全情报专家
EverSafe Online

基于业务安全情报的攻防实践

邓欣 永安在线CTO

永安在线是谁？

➢ 公司简介

永安在线17年以来专注于业务反欺诈行业，创始团队来自于前腾讯攻防反欺诈团队，当前致力于解决反欺诈领域的行业核心问题，为客户提升攻防效率。

➢ 公司规模

公司目前人数近100人，总部设立在深圳，并在上海，北京，重庆设立分部。

➢ 投资机构

公司先后获得真格基金、泰岳梧桐、易合资本、华为多轮投资。

➢ 合作客户

目前合作客户涵盖阿里，腾讯，百度，头条，华为，OPPO，vivo等各大行业TOP客户。

➢ 合作客户

Tencent 腾讯

阿里巴巴 Alibaba.com

今日头条 你关心的 才是头条

JD.京东.COM

拼多多

苏宁易购

目录

业务安全情报的价值

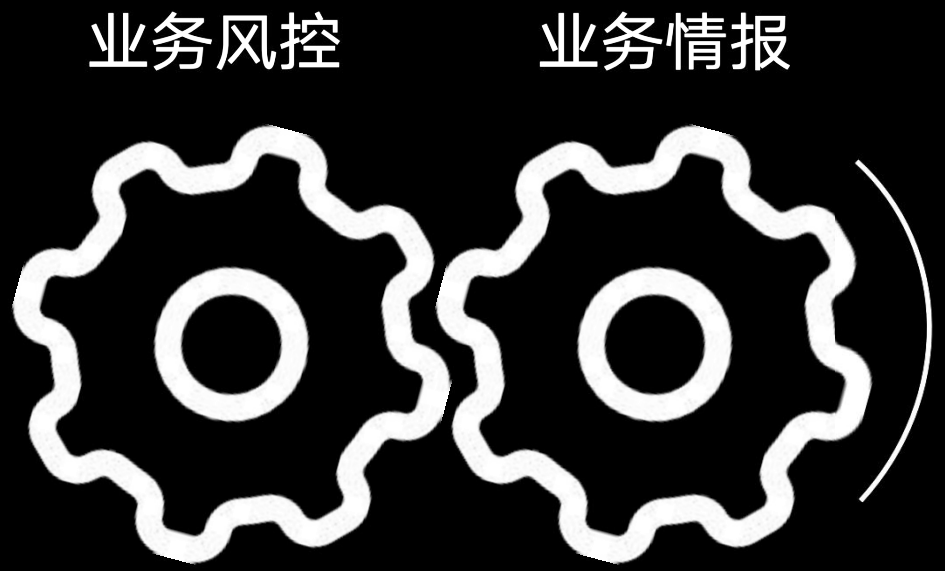
什么是业务安全情报？

业务安全情报是基于某些证据

发现的业务上的风险情况

业务安全情报的价值

业务安全体系



- 提升攻防效率
- 评估攻防成本和效果
- 攻防的可解释性

提升业务安全攻防效率

及时发现业务风险场景

金融 | 电商 | 社交 | 内容 | 出行 | 游戏 | …… ……

业务增长	• 渠道推广作弊 • 营销活动作弊 • 用户拉新、裂变作弊
账号安全	• 扫号、撞库盗号 • 虚假小号、养号 • 资金盗刷
平台生态	• 刷量、刷单 • 黄牛、抢单、外挂 • 内容盗取
监管合规	• 色情、赌博、虚假广告引流 • 水军控评 • 数据泄露、网络诈骗

提升业务安全攻防效率

- 及时发现业务风控盲区

【案例】情报平台捕获到新出现的账号交易店铺

限制黑产养号、卖号

账号 关联 设备

账号-密码-机型-串码

增强黑产设备识别能力
模拟器/改机

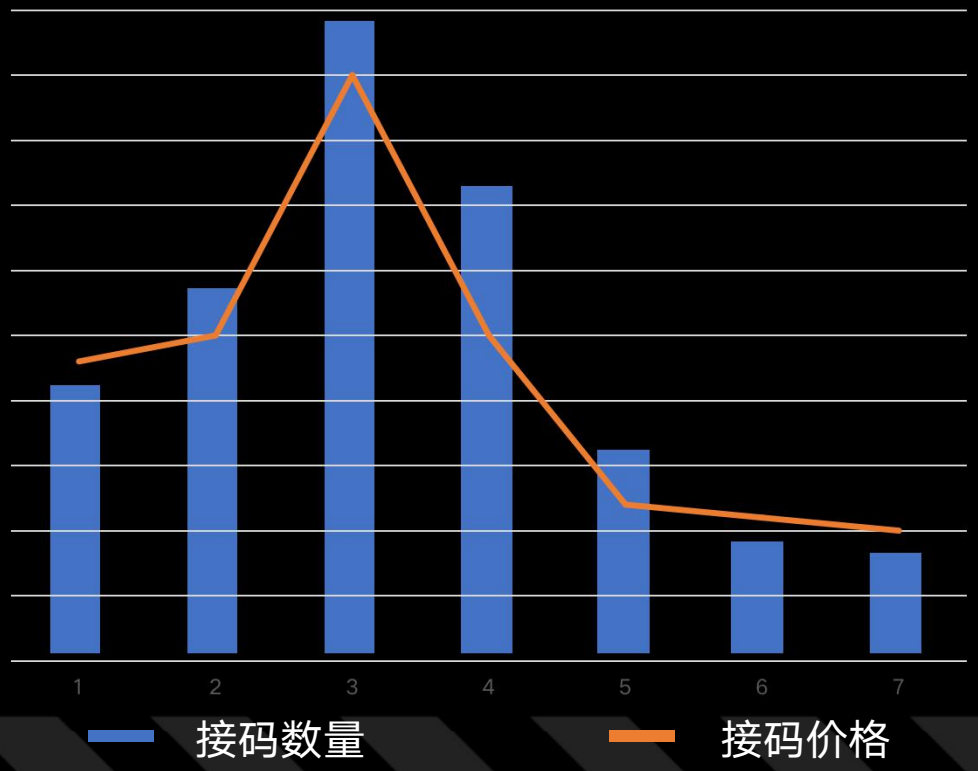
评估攻防成本和效果

攻防成本

- ROI（投入产出比）= 成本 / 收益

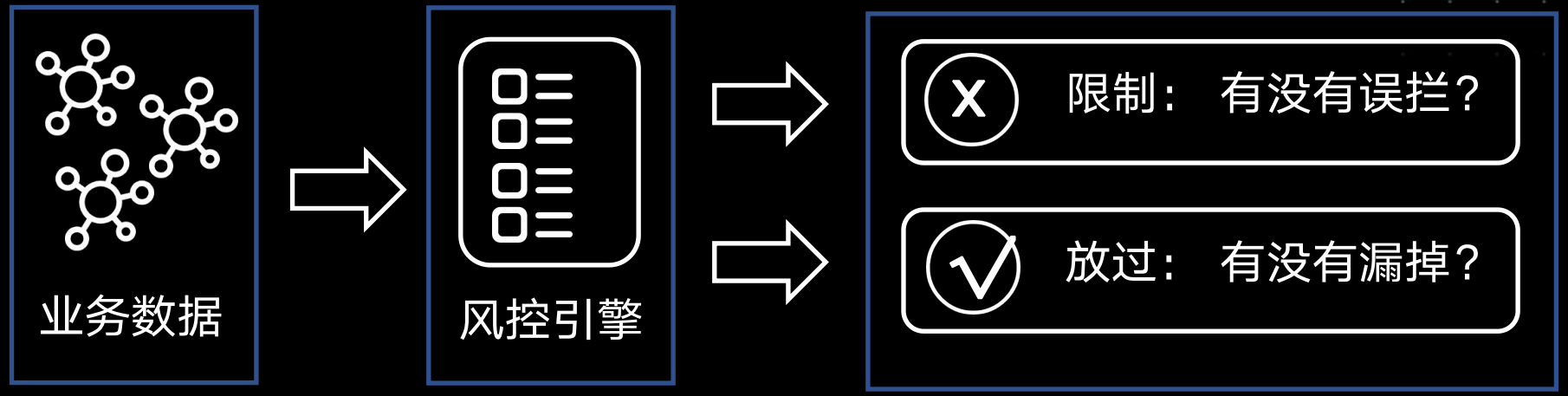
提升成本	降低收益
安卓手机：600元/部 改机工具：1.0元/部天 接码平台：0.5元/次 代理IP：2.0元/部天	话费充值： 每个账号赚差价3.0元 账号倒卖： 每个账号售价2.5元

攻防效果

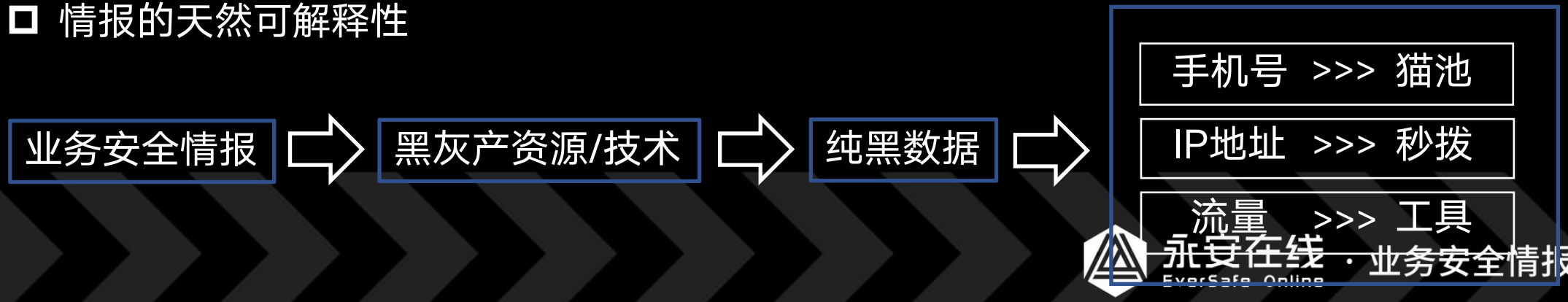


为风控攻防提供的可解释性说明

- 风控的不可（不好）解释性

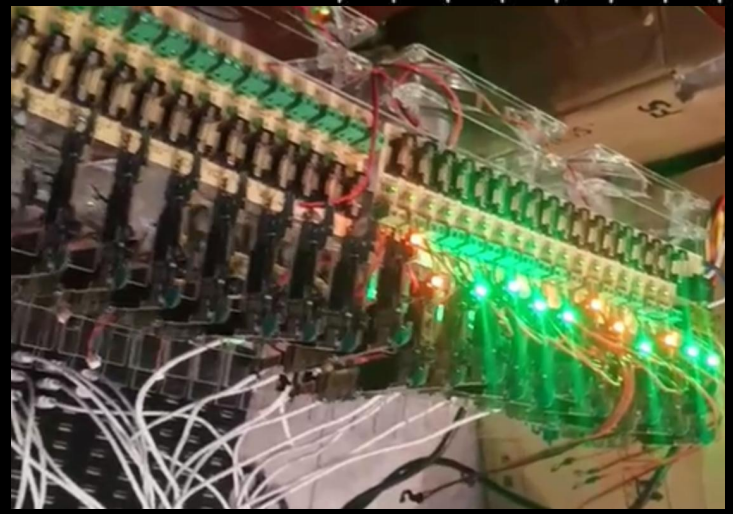


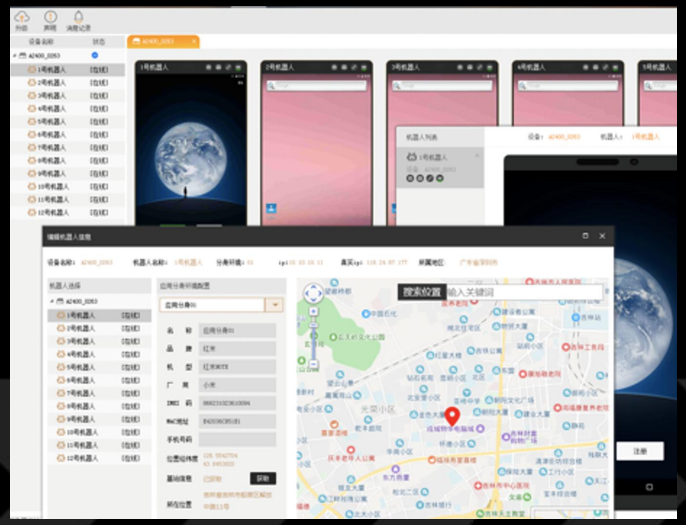
- 情报的天然可解释性

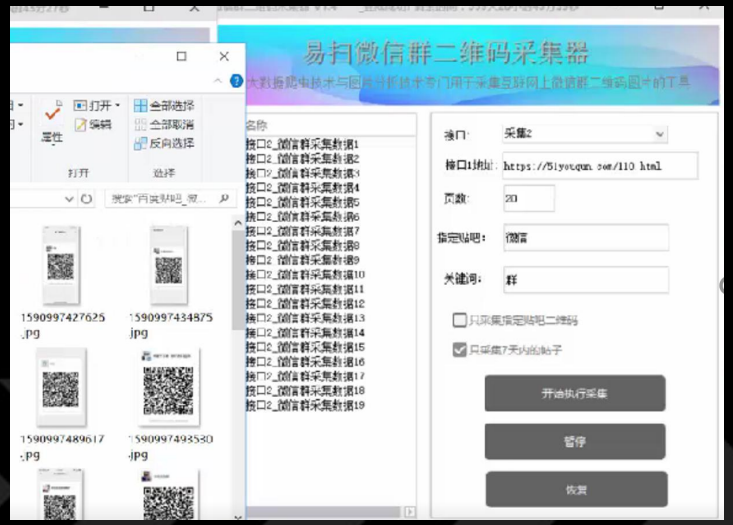


业务安全情报的生产

业务安全情报的生产 – 数据来源

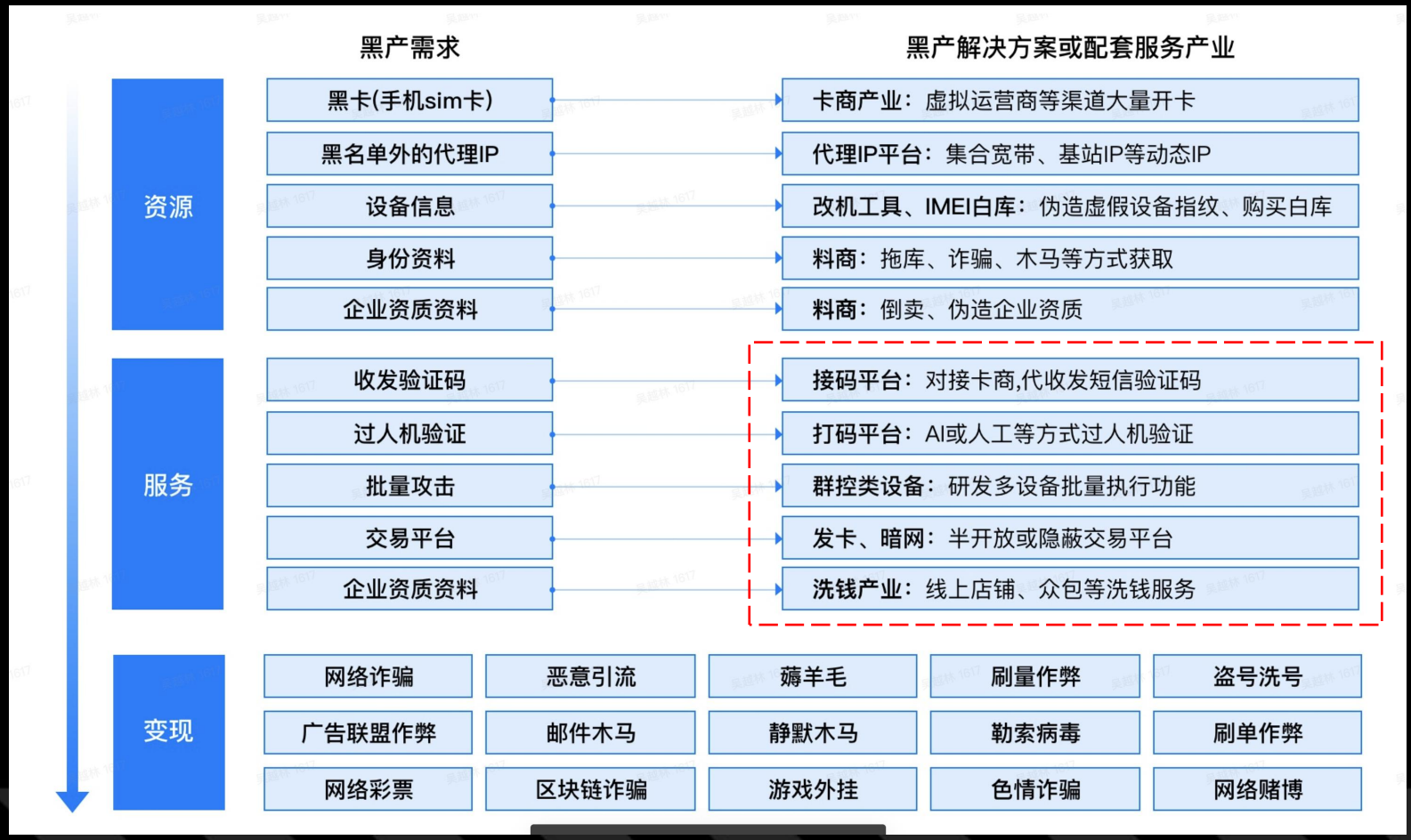






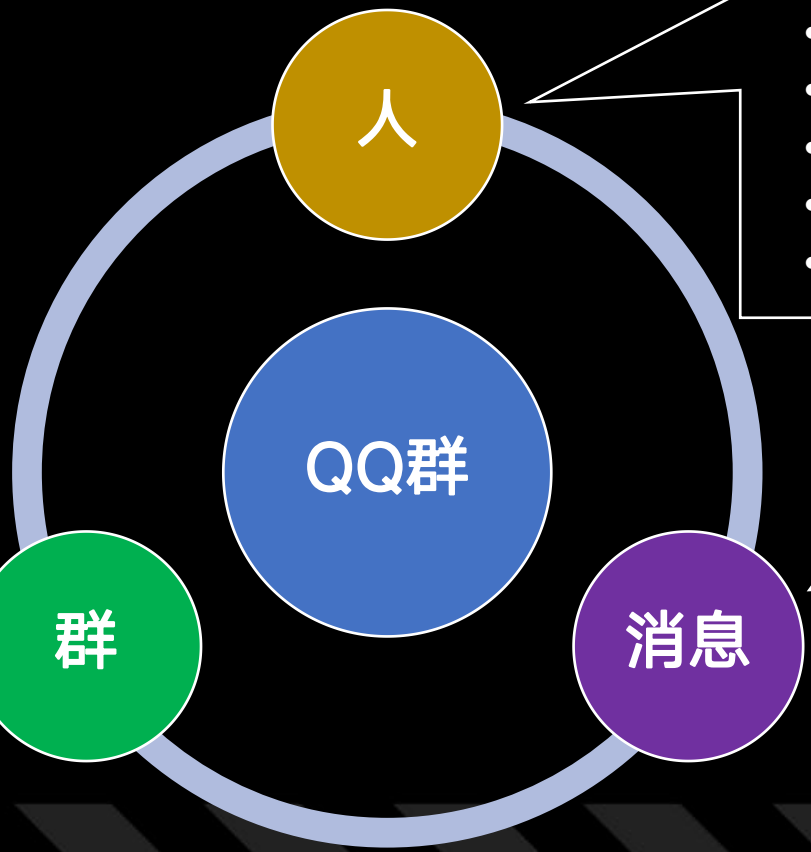
业务安全情报的生产 – 数据来源

分析黑灰产业链条，找到并监控上下游聚集，交流、交换信息、交易物品的中间平台



业务安全情报的生产 – 数据加工

原始数据提炼



- 群号
- 昵称
- 身份（群主/管理员）
- 所在群
- 入群时间
- 发送消息数量

- 群ID
- 群成员
- 群公告
- 群消息数量
- 群共享文件

- 消息内容
- 发送时间
- 发送者
- 发送的群
- 发送的数量

业务安全情报的生产 – 数据加工

黑产话术字典

国内实卡发送 可接30-50W 机房稳
定到达率98
可接CP BC PZ 6H QP WZ
需要的请拍下详谈。

CP	=	彩票
BC	=	博彩（菠菜）
PZ	=	配资
6H	=	六合彩
QP	=	棋牌
WZ	=	网赚

业务安全情报的生产 – 数据加工

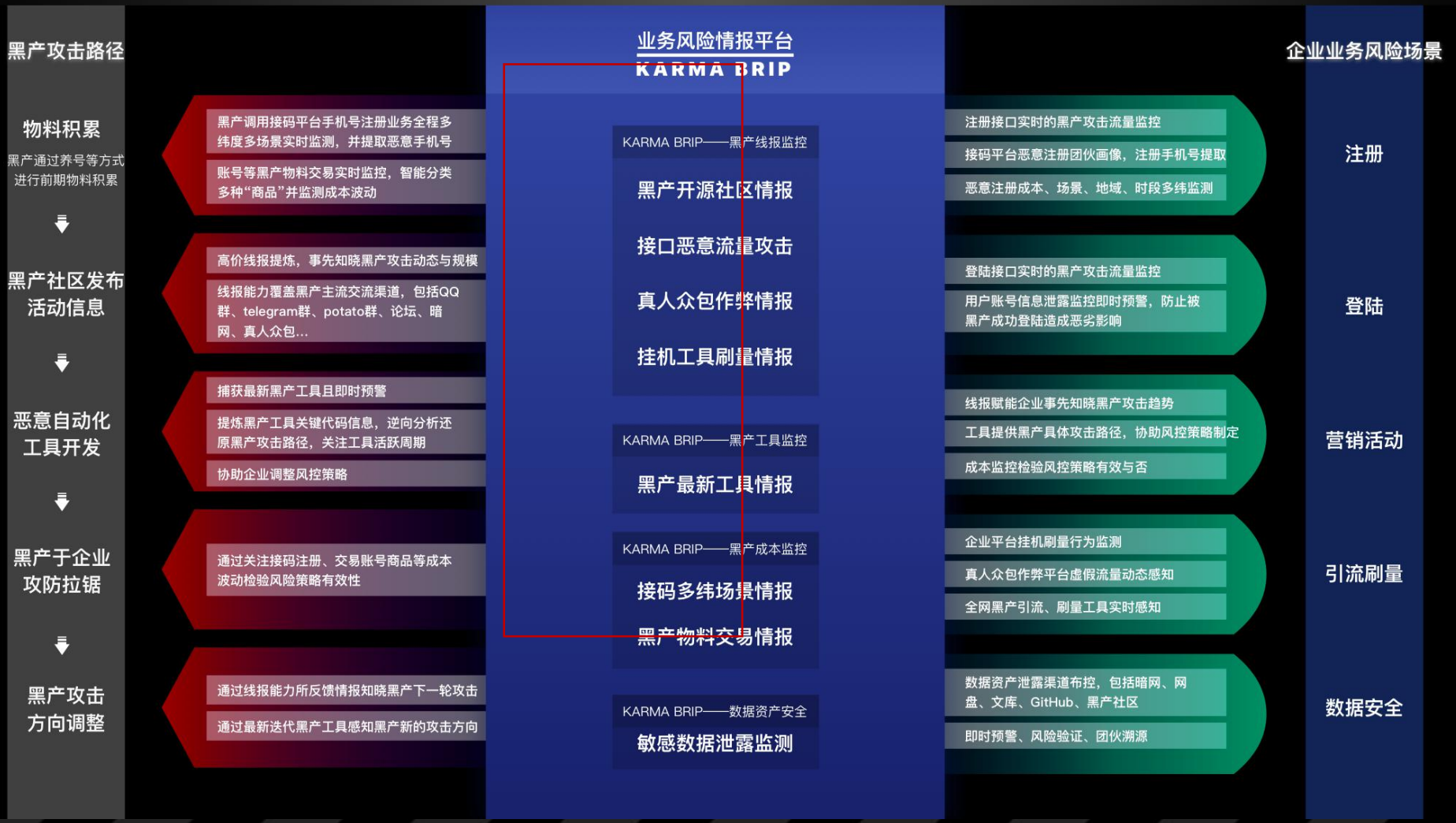
消息
高置信度

群
高质量群

人
团伙核心角色

业务安全情报的生产

业务风险场景与黑产攻击链路全景覆盖



- 业务安全情报的运用

业务安全情报的运用

态势

话题讨论热度	接码价格走势	接码数量走势
工具数量走势	商品数量走势	商品数量走势

提炼风险事件

风险事件处置

预警 → 验证/排查 → 反制

业务安全情报的运用 – 真人众包作弊情报

Step1 解析任务内容

Step2 提取作弊对象标识（邀请码）

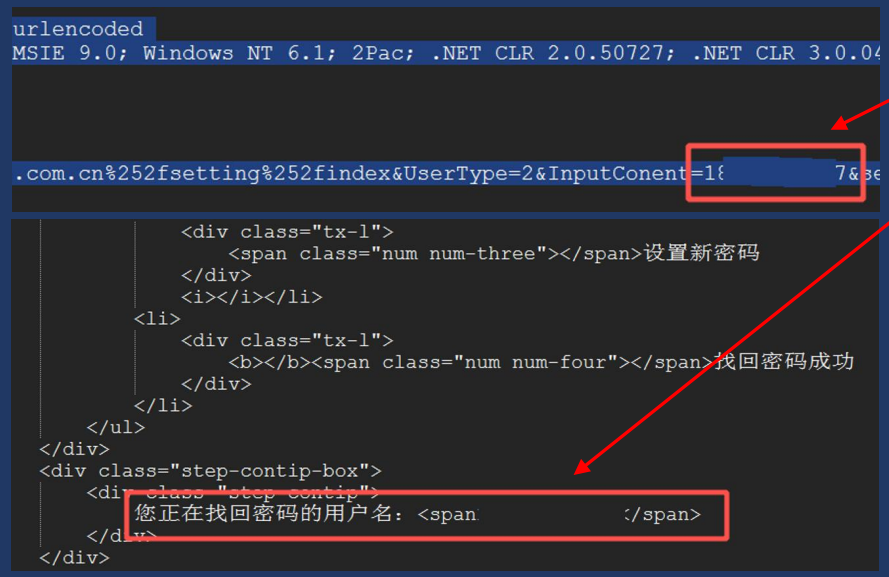
Step3 通过标识关联作弊用户

Step4 实施处罚：限制or封禁

业务安全情报的运用 – 黑产工具情报

【排查】业务接口存在的漏洞或缺陷

找回密码接口导致的信息泄露



填入任意手机号

返回该手机号注册的明文用户名信息

爬取该用户在平台留下的信息，从而勾勒出用户画像。

【危害】

- 暴破所有用户的手机号和用户画像
- 数据售卖 or 电话诈骗
- 公关/信任/监管危机

【修复】

- 返回的用户名信息部分打码
- 通过短信验证码进行身份核验

业务安全情报的运用 – 黑产工具情报

【排查】业务风控被绕过

- 内置秒拨拨号或代理IP绕过IP风控
- 内置打码平台绕过人机识别验证码
- 破解和伪造接口签名算法
- 破解和伪造设备指纹

伪造设备信息

伪造设备品牌

```
B0587 dd 1                              ; DATA XREF: gen_brand_50E1AA+2↑o
  dd 0CDh
  dd offset aSamsungB7330 ; "SAMSUNG B7330"
  dd offset aSamsungB7300 ; "SAMSUNG B7300"
  dd offset aSamsungI350  ; "SAMSUNG i350"
  dd offset aSamsungI637  ; "SAMSUNG i637"
  dd offset aSamsungSghI688 ; "SAMSUNG SGH-i688"
  dd offset aSamsungSghI728 ; "SAMSUNG SGH-i728"
  dd offset aSamsungSchM490 ; "SAMSUNG SCH-M490"
  dd offset aSamsung931sc ; "SAMSUNG 931SC"
  dd offset aSamsungC6625 ; "SAMSUNG C6625"
  dd offset aSamsungB7610 ; "SAMSUNG B7610"
  dd offset aSamsungSphP900 ; "SAMSUNG SPH-p9000"
  dd offset aSamsungSphP920 ; "SAMSUNG SPH-P9200"
  dd offset aSamsungB7620 ; "SAMSUNG B7620"
  dd offset aSamsungI8000 ; "SAMSUNG i8000"
  dd offset aSamsungI8180c ; "SAMSUNG i8180C"
  dd offset aSamsungI8305 ; "SAMSUNG i8305"
  dd offset aSamsungI8320 ; "SAMSUNG i8320"
  dd offset aSamsungI920  ; "SAMSUNG i920"
  dd offset aSamsungB7350 ; "SAMSUNG B7350"
  dd offset aSamsungI770  ; "SAMSUNG i770"
  dd offset aSamsungSghI780 ; "SAMSUNG SGH-i780"
  dd offset aSamsungSghI788 ; "SAMSUNG SGH-i788"
  dd offset aSamsungSghI600 ; "SAMSUNG SGH-i600"
```

伪造系统版本

```
_31B08F3+4↑o                            ; DATA XREF: gen_os_
  dd 9
  dd offset a8_0_0        ; "8.0.0"
  dd offset a5_1_0        ; "5.1.0"
  dd offset a5_0_1        ; "5.0.1"
  dd offset a5_1_1        ; "5.1.1"
  dd offset a6_0_1        ; "6.0.1"
  dd offset a5_0_0        ; "5.0.0"
  dd offset a4_4_4        ; "4.4.4"
  dd offset a810_0        ; "8.1.0"
  dd offset a4_4_1        ; "4.4.1"
```

伪造API版本

```
v22 = sub_405FCE(v37, "6.0") == 0;
if ( v37 )
  j__krnl_MFree(v37);
if ( v22 )
  return "23";
v8 = *a2;
if ( !*a2 )
  v8 = &unk_64E2AC;
v38 = (_BYTE *)j__krnl_MCallKrnlLibCmd(2, (char)v8);
v23 = sub_405FCE(v38, "5.1") == 0;
if ( v38 )
  j__krnl_MFree(v38);
if ( v23 )
  return "22";
```

【反制】提取自动化攻击特征

- 硬编码的接口参数
- 固定的操作步骤
- 应用包名+签名

前后接口参数不一致

访问接口A:

```
","version_code":290,"timezone":8,"access":"wifi","os":"A
'ndroid","os_version":"5.1.1","os_api":22,"device_model":'
'"{device_model}","device_brand":"{device_brand}","device'
'_manufacturer":"HUAWEI","language":"zh","resolution":"17'
'76x1080","display_density":"mdpi","mc":"{mc}","carrier":'
'"中国联通","mcc_mnc":"46001","clientudid":"{clientudid}","
'stall_id":"{iid}","device_id":"{device_id}","sig_hash":"'
```

手机品牌是华为

访问接口B:

```
'.8.1&device_type=GT-I8160&ssmix=a&iid=65072164728&os_
'=17&device_id=57227320366&resolution=900*1440&device_
'nd=Meizu&aid=1128&manifest_version_code=181&app_name=
'me&_rticket=1551628001037&os_version=4.2.2&device_pla
'rm=android&version_code=181&update_version_code=18108
'wifi&dpi=320&uuid=864895021524242&language=zh&channel
```

手机品牌是魅族

【反制】提取工具内置信息

- 作者联系方式
- 售后/交流群
- 工具后台信息

工具内置了访问后台数据库的连接信息

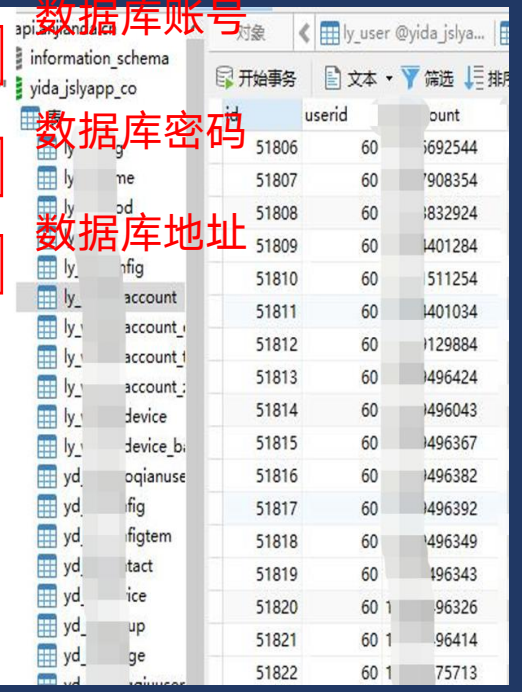
```
push    80000004h
push    0
push    offset password ; "ZF                Jwtm"
push    80000004h
push    0
push    offset username ; "yi                _co"
push    80000004h
push    0
push    offset db_Url   ; "ap                cn"
```

```
select * from          by regtime desc
select * from          e usercode='
select * from          e username='
select * from          where userid='
select * from          unt where userid='
select * from          unt_email where userid='
select * from          unt_tixian where userid='
select * from          unt_zhuanzhang where userid='
select * from          ce where userid='
select * from          ce_backup where userid='
```

数据库账号

数据库密码

数据库地址



永安在线安全团队出品

扫码下载

《2020年黑灰产攻防研究

年度总结报告》

欢迎交流