唯品会 | 唯品会安全应急响应中心

因唯安全 所以信赖

2017唯品会第二届电商安全峰会

——深度揭秘唯品会信息安全建设实践

苏州
中国·苏州

那些年我们追过的威胁情报

——吴灵敏

关于我

- 建设威胁情报体系
- 黑灰产情报分析
- 各类事件调查

议题内容

- 威胁情报路
- 案例分析
- 谈谈未来

威胁情报-？

?之后

线上我们关注的情报

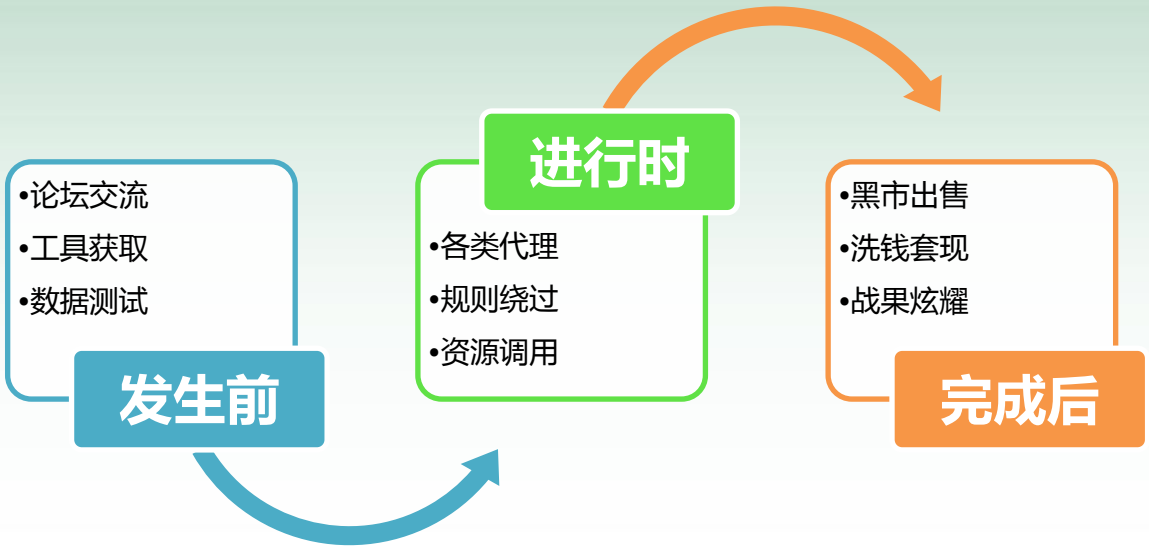
业务情报

- 策略绕过
- 支付套现
- 信息泄露
- 薅羊毛
- 钓鱼欺诈
- 流量劫持
- 数据贩卖
- etc

网络情报

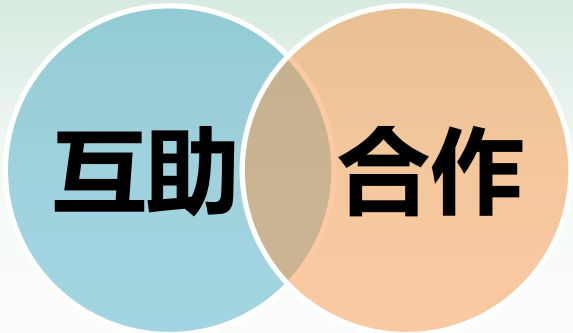
- ip
- DNS
- domian
- etc

一个事件过程



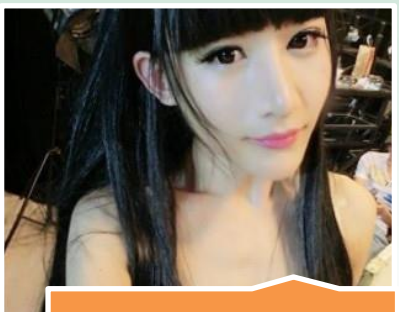
线上整个周期情报

线上威胁情报-自身之外



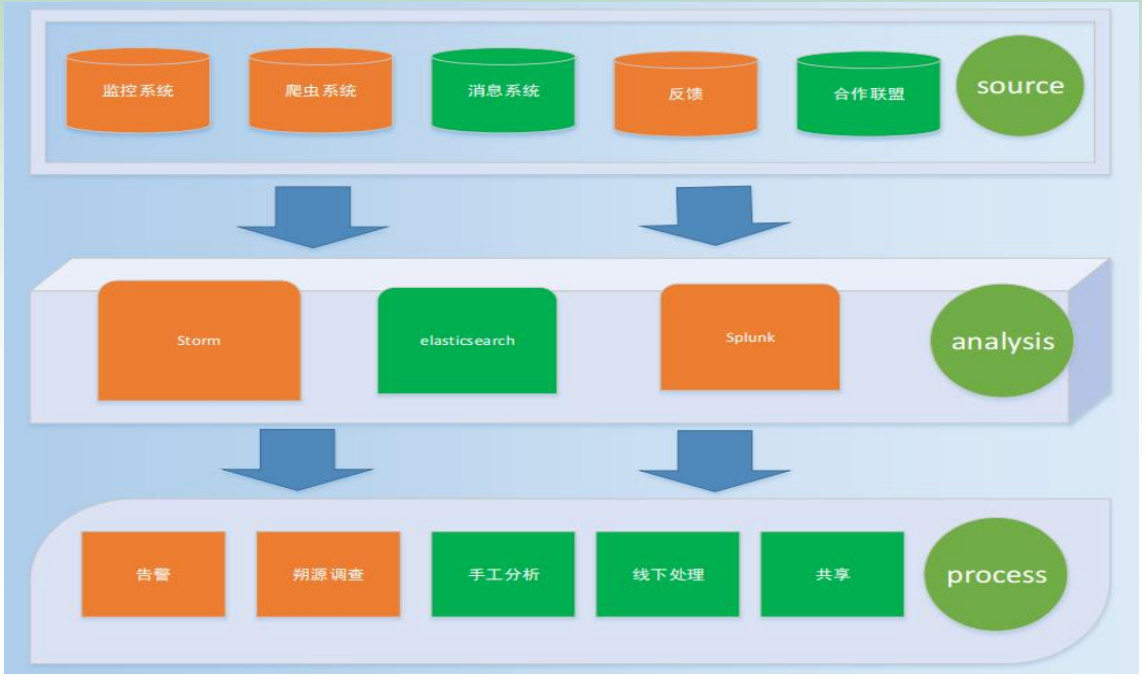
威胁情报-线下

上得了厅堂



扮得了伪娘

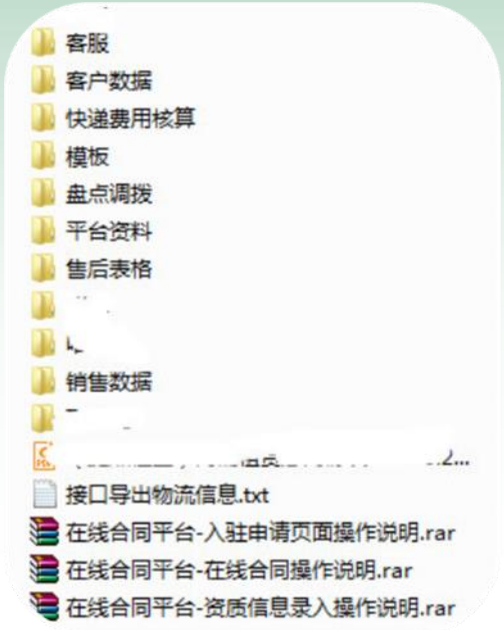
整体流程



案例

案例一、远方的价值

- 一段告警
- 一场事故
- 一次分析



案例二、比黑更黑

- 一次反馈

某月某日某用户下某个订单
盼天盼地盼星星没盼来快递

快递去哪里了？

案例三、致富路


今天给大家带来一个首发 唯品会抓
包撸手机教程。
唯品会
一家专门做特卖的网站
订单提交成功，还差一步就抢到心爱的商品
共1张订单，订单详情，请在 11 分 32 秒内完成支付。
待支付：¥0.8
微信支付
使用：微信支付
支付：¥0.8


发教程
搞不定
开会员
授杀技
冷落你

谈谈未来

- 以前我用一辆单车
- 现在我用共享单车

威胁情报共享

谢谢您的倾听！

唯品会 | 唯品会安全应急响应中心

VIP Security Response Center

唯品会安全应急响应中心

专业

我们致力于保护用户信息安全

我们积极营造更加安全的

线上电商购物平台

微信号：VIP_SRC

官方网站：http://sec.vip.com

微信公众号：唯品会安全应急响应中心

漏洞接收邮箱：sec@vipshop.com