阿里安全
ALIBABA SECURITY

ALIBABA SECURITY

攻击过程的威胁情报应对体系

--安全威胁情报中心

自我介绍

- 阿里安全-安全威胁情报中心
  - 技术情报负责人
  - 主要负责：
    - 疑难案件调查溯源
    - 威胁情报外部信源建设与监控体系
    - 黑产情报分析

- 网名 instruder　微信号instruder_cn

ALIBABA SECURITY

0、概述
1、攻击前-提前感知
2、攻击中-线上阻击
3、攻击后-自动溯源
4、总结

阿里安全
ALIBABA SECURITY

威胁情报特性

威胁情报无法兜底性

- 情报也无法替代风控、已有的防御检测
- 更多的是强化、内外弥补

1+1>2

威胁情报外向性

各自为战

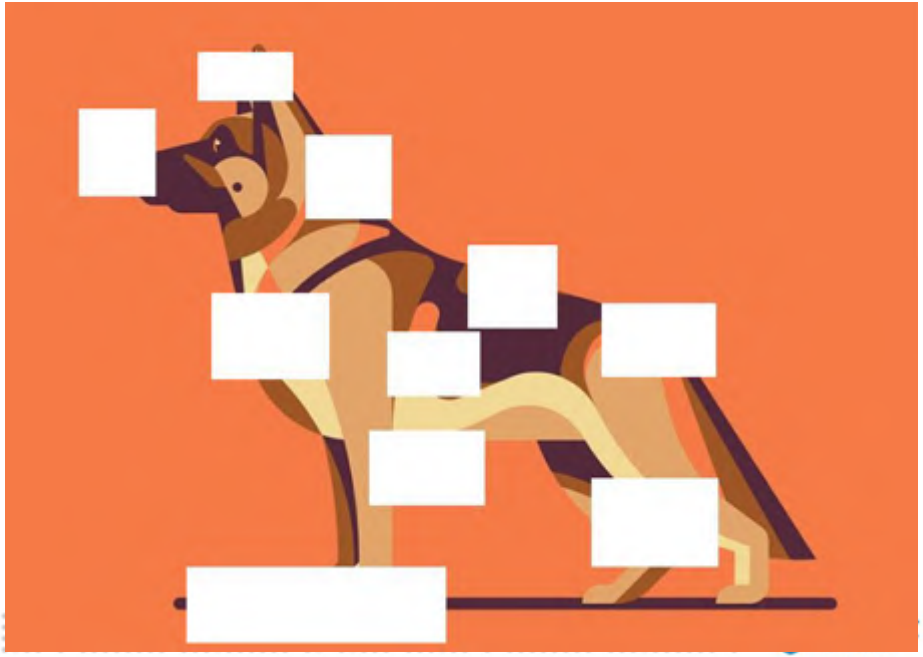
久守必失

威胁为核心？
威胁=能力*意图

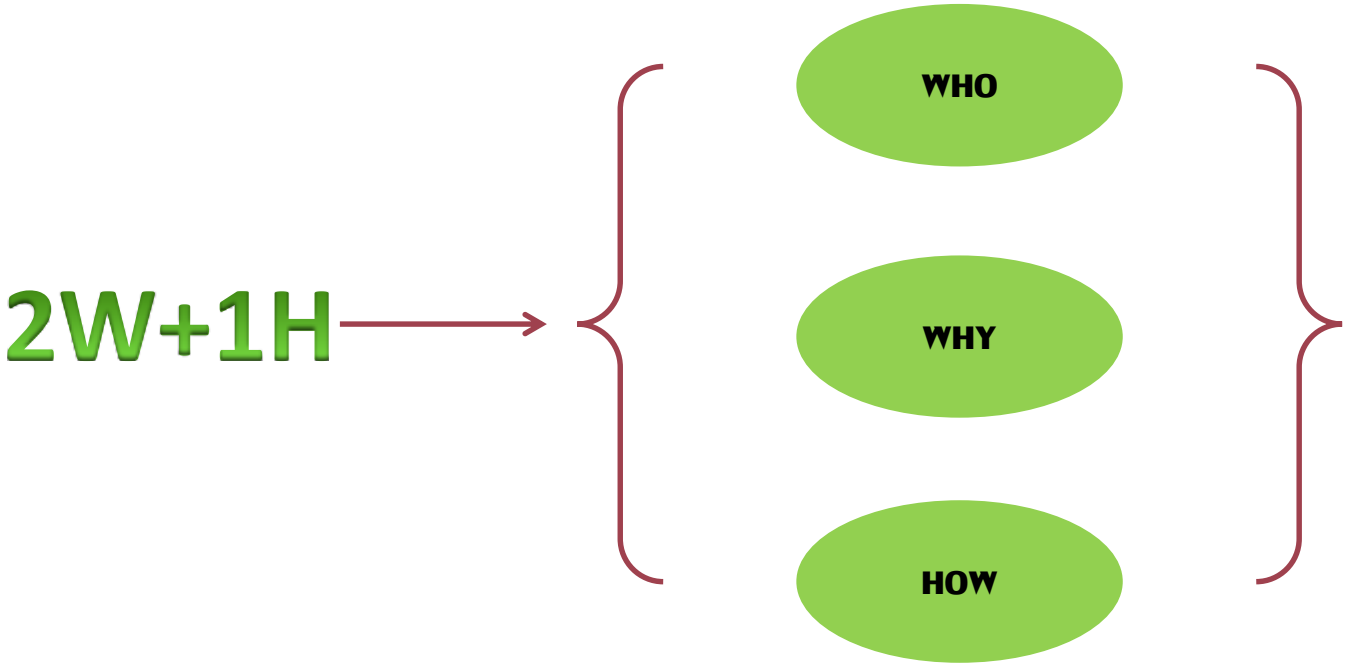
主动出击
攻击敌人-提前

知己知彼
情报更强调知彼！

威胁情报拼图和推理性



威胁情报-溯源特性



攻击生命周期中的威胁情报

攻击生命周期

接单　团伙组织　工具下载、购买　论坛交流、学习

肉鸡　匿名VPN

攻击开始　攻击经过关键资源路径　攻击到达受害者

黑市售卖　收钱结算

攻击酝酿阶段　攻击酝酿阶段　攻击发起阶段　攻击持续阶段　攻击收尾阶段　战果整理、交流、汇报、出售阶段

社交群交流　资源获取　环境准备

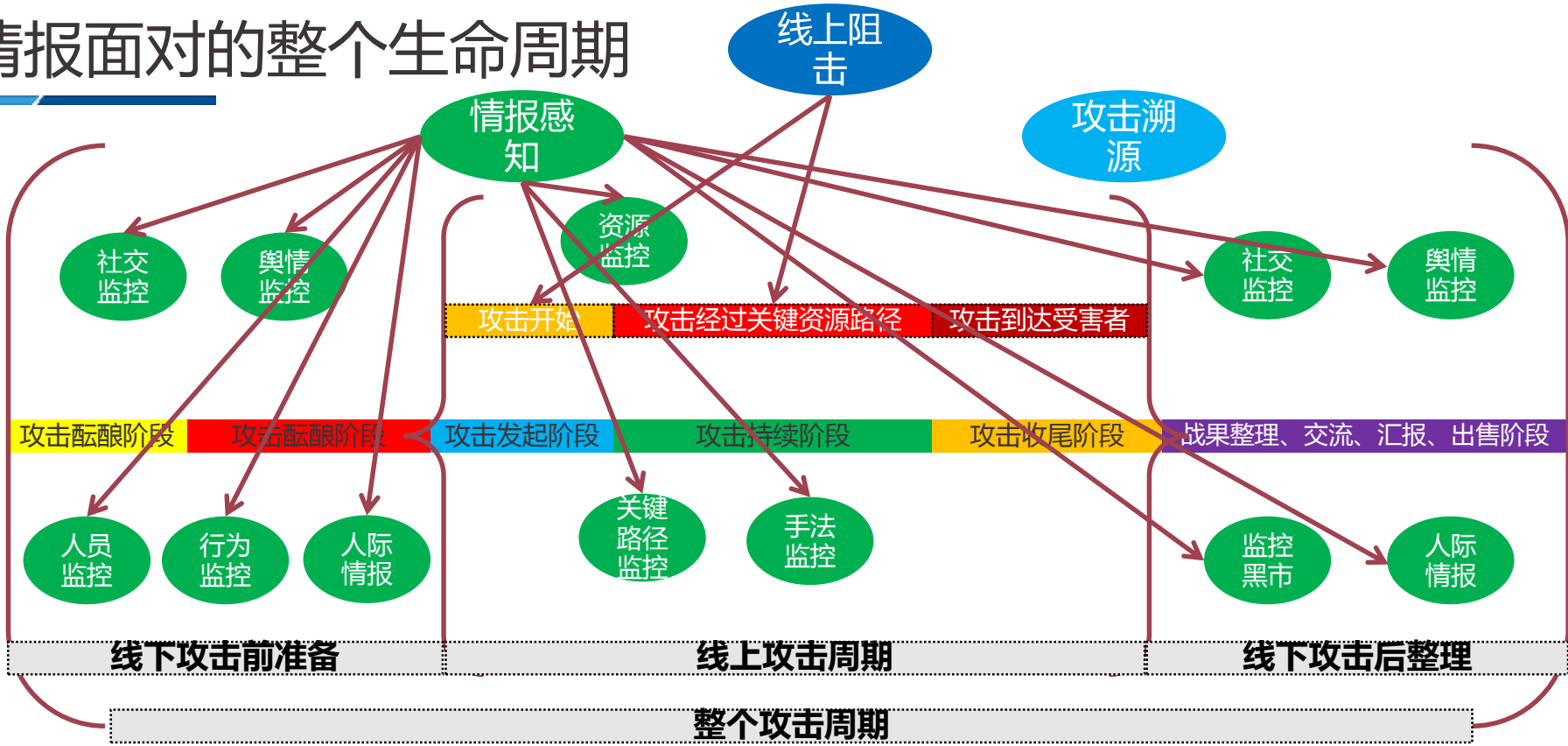
各种资源平台调用　各种渠道

移交下一链条　洗钱变现

线下攻击前准备　**线上攻击周期**　**线下攻击后整理**

整个攻击周期

情报面对的整个生命周期



威胁情报应用-线上 vs 线下

- 情报线下应用
  - 越提前
  - 越能提前防御，减少损失
  - 事实越难还原
  - 不容易与攻击直接关联
  - 效率，单个CASE性

- 情报在线应用
  - 系统化解决
  - 比如线下应用晚，但是比风控、防御早
  - 效率高

攻击前-情报提前感知

情报提前感知-核心思想

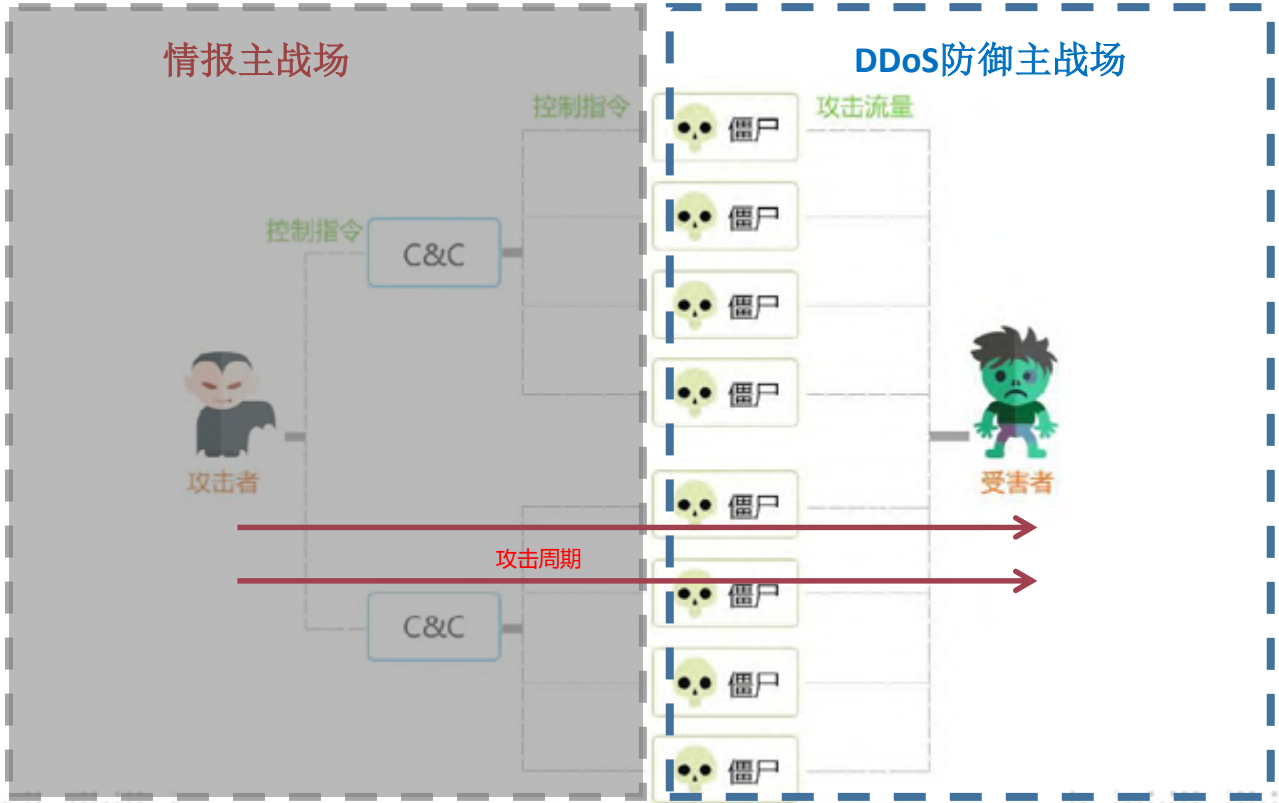
- 为什么要这么做：
  - 情报一定要是提前的！

- 以攻击人员（组织、特征）或人员使用的关键资源作为抓手，在攻击中能够先于到达被攻击端防控（防御边界）感知，称之为攻击的威胁情报提前感知体系；

四要素

- A、时间要素：
  - 比到达被攻击端防控（防御边界）时间要早；
- B、周期要素：
  - 在攻击发起前期、攻击酝酿阶段就能感知到；
- C、位置要素：
  - 一定不是被攻击端防控（防御边界）感知；
  - 感知的地方和被攻击的地方相对于情报一方必须处于不同的位置；
- D、攻击者要素：
  - 基于攻击者、攻击者控制的资源、平台维度；

情报提前感知-DDOS提前感知



情报提前感知-DDOS提前感知

情报提前感知-DDOS提前感知

- 提前感知
  - 在攻击发起瞬间，就能感知到
  - 不仅知道打了我们，还知道他有没有打其他人,打了多长时间？
  - 攻击方式、攻击程序用的什么？
  - 背后的中控，此次攻击用了几个中控？

- 情报价值
  - 攻击溯源
  - 源头感知及时防御
  - 攻击分析

情报提前感知

- 业界案例
  - ◆基于DGA的监控，第一时间掌握新变种及规模；
  - ◆基于网页钓鱼的监控，第一时间掌握最新生成的钓鱼域名；
  - ◆……

攻击中-线上阻击

线上阻击-核心思想

- 为什么要这么做：
  - 最好的防御就是主动出击！

- 在攻击的持续过程中，能够对攻击者使用的关键资源能够直接给予阻击拦截，而不是对本身受到的攻击做清洗、拦截、ip、账号封堵；

2要素

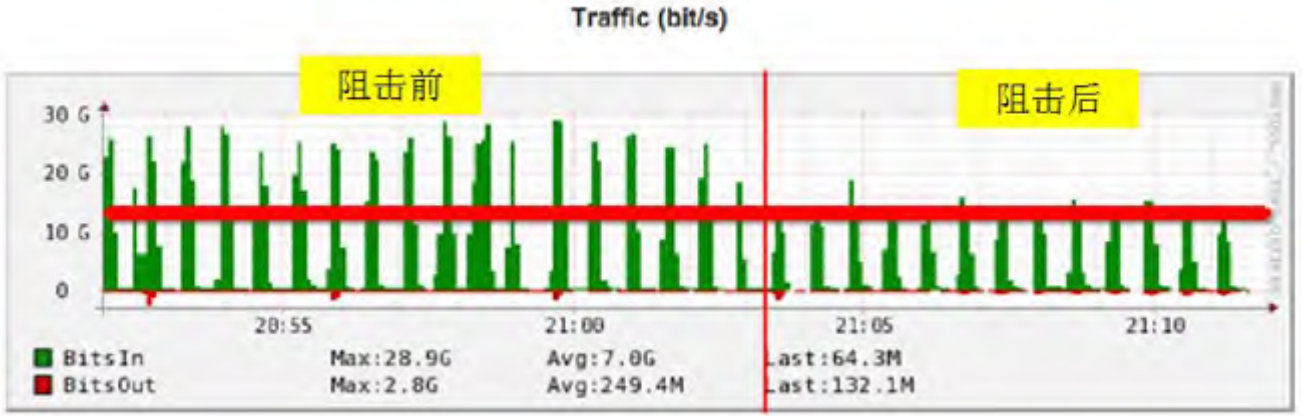
- A、阻击点位置要素：能够对发起点、中间过程发起点、关键资源点造成影响，造成攻击无法持续，而不是到达点；

- B、影响要素：不能仅仅是改变只对自己（保护的边界）的影响；

线上阻击-DDOS阻击

- DDOS防御
  - 黑洞
  - 近目的清洗
  - 近源清洗(属于线上阻击
  - ……
- DDOS防御主动出击，不再被
- 情报应用一定是主动的！

线上阻击-DDOS阻击


Traffic (bit/s)
阻击前
阻击后
30 G
20 G
10 G
0
20:55
21:00
21:05
21:10
BitsIn
BitsOut
Max:28.9G
Max:2.8G
Avg:7.0G
Avg:249.4M
Last:64.3M
Last:132.1M


400 G
300 G
200 G
100 G
0
阻击前
263G
阻击后
80G
21:00
21:20
21:40
22:00
BitsIn
BitsOut
Max:263.6G
Max:17.7G
Avg:7.0G
Avg:14.0G
Last:1.6G
Last:11.6G

线上阻击-DDOS阻击

- 线上阻击
  - 直接降低攻击流量

- 情报价值
  - 关键防御手段-救命稻草
  - 成本非常低

线上阻击

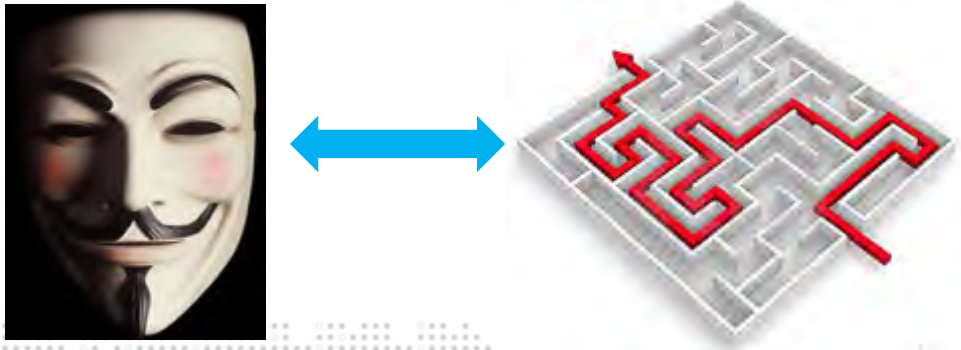
- 另一个典型案例

攻击后-自动溯源

自动溯源-核心思想

- 为什么要这么做：
  - 情报一定要解决谁在攻击我、怎么攻击进来的 这个命题！

- 在攻击过程或者结束时，能够自动反向溯源出此次攻击我的人是谁,同时也在解决攻击者的路径，如何攻进来?完整攻击路径还原

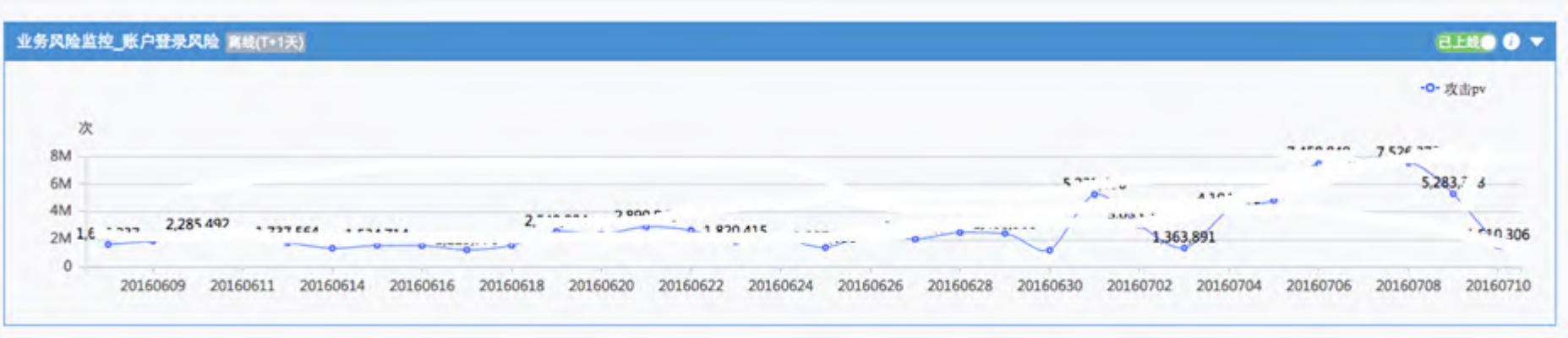


要素

- A、关联要素：自动关联出攻击的人员网络身份或者真人身份，并且可以对整个攻击过程可以进行场景还原；

自动溯源-账号登录攻击自动溯源

- 账号登陆攻击
  - 刷库
  - 撞号
  - 盗号
  - ……



自动溯源-账号登录攻击自动溯源

选择时间范围:

2016-07-03 2016-07-10

溯源详情 溯源统计

每页显示 10 条记录 搜索

开始时间	结束时间	数据来源	登陆来源	攻击次数	使用IP数	关联路径	关联[illegible]账号
2016-07-09 00:00:02	2016-07-10 19:19:05	wwlogin	wangwang#8.60.00C	89956	10	查看详情	[illegible]
2016-07-09 00:00:02	2016-07-10 19:19:05	wwlogin	wangwang#8.60.00C	89956	10	查看详情	[illegible]
2016-07-03 03:20:51	2016-07-03 18:06:35	havanalogin	icbu	10011	190	查看详情	[illegible]
2016-07-03 03:21:05	2016-07-03 13:56:37	havanalogin	icbu	8719	159	查看详情	[illegible]
2016-07-03 08:47:45	2016-07-03 18:03:30	havanalogin	icbu	6108	115	查看详情	[illegible]
2016-07-03 03:20:51	2016-07-03 14:34:24	havanalogin	icbu	3995	75	查看详情	[illegible]
2016-07-03 03:20:51	2016-07-03 14:34:24	havanalogin	icbu	3995	75	查看详情	[illegible]
2016-07-07	2016-07-10	durex	#23078558	3471	36	查看详情	[illegible]

自动溯源-账号登录攻击自动溯源

- 情报价值-另一个维度
  - 人
    - 看到的不是今天发生了多少次攻击，而是今天谁、谁、谁 在攻击我们，占了总体攻击百分比；
    - 这个人历史上已经攻击我们多次！这人一直在盯着我们！

  - 路径
    - 都是从哪些路径来的？完整攻击链路

自动溯源

- 更多案例应用
  - 敏感文件数据泄密自动溯源
  - 黑客攻击自动溯源
  - 网络钓鱼攻击自动溯源
  - ……

总结

- 基于在线业务攻击场景的威胁情报体系需要更多的思考和创新
- 也不是每个业务攻击场景都可以有这样的在线情报体系可以实现，只能通过线下弥补
- 基于这些思想来进行情报应用，会更好的来指导我们思考情报应用

THANKS