

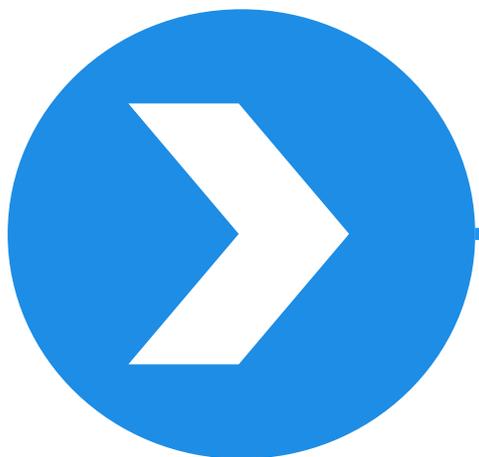


# 基于移动威胁情报的安全价值观

安天移动安全研发中心

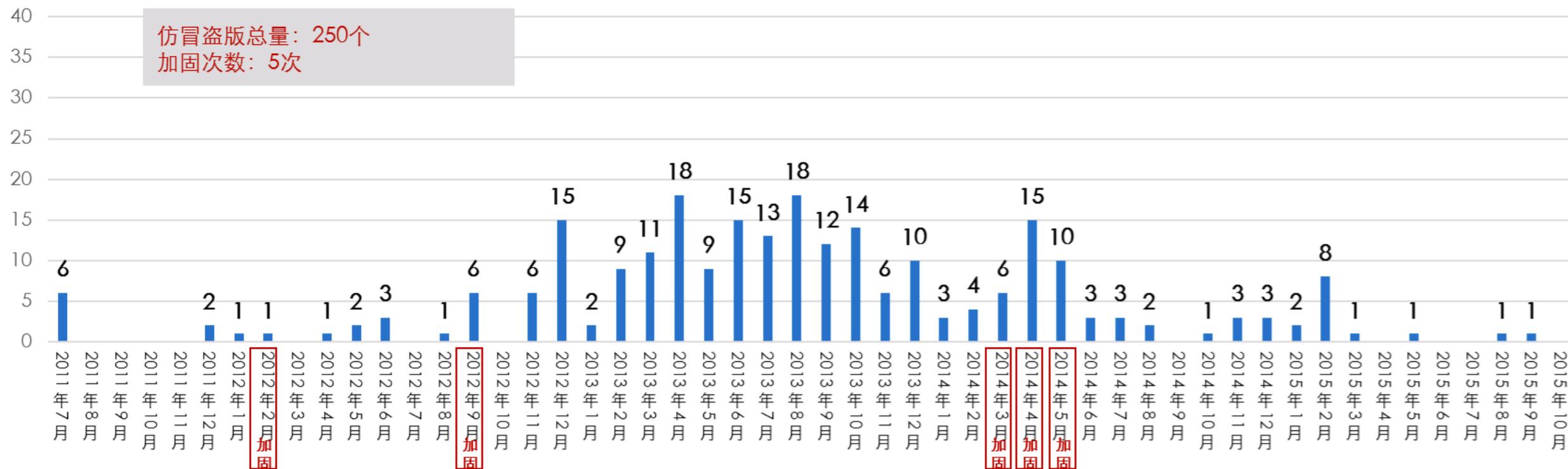


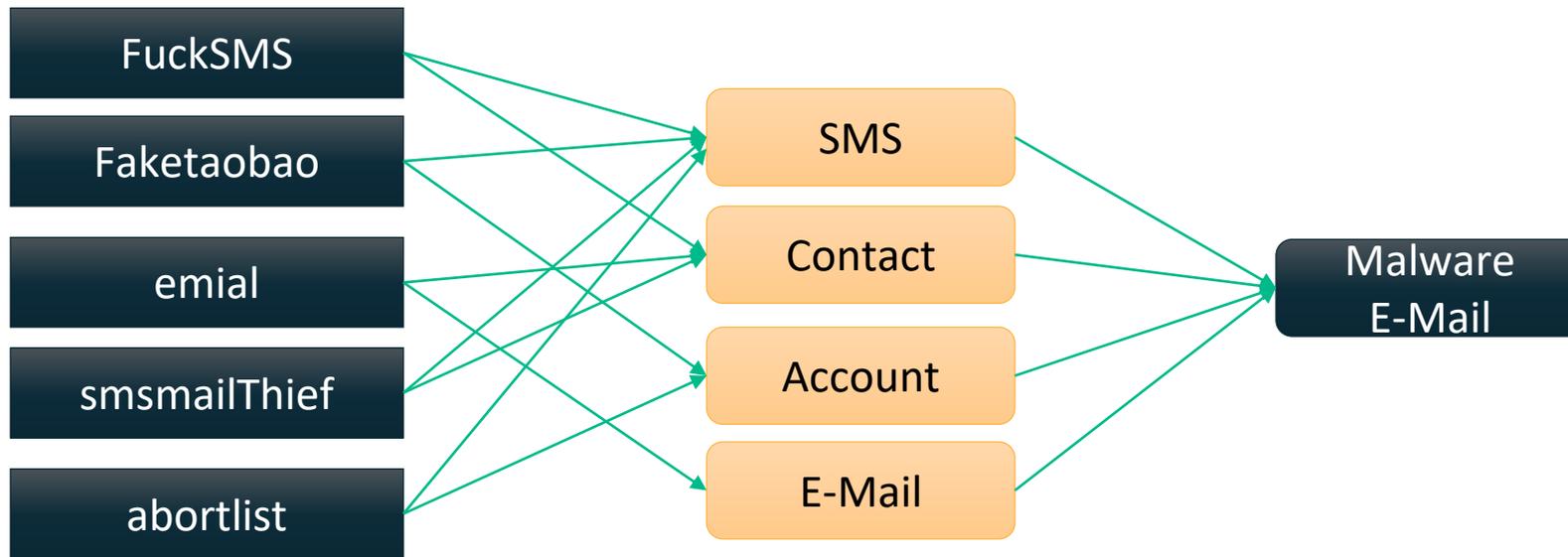
- 威胁场景下各种信息不对称导致“盲”人摸“象”
- 如何基于威胁情报对数据进行组织和驱动方式
- AVL Insight移动威胁情报的源体系
- AVL Insight移动威胁情报的工程实践
- 结束语



威胁场景下各种信息不对称导致  
“盲”人摸“象”

## 某游戏应用仿冒盗版样本数量变化趋势





LV2 调炮神族 发表于 2015-8-20 17:10 | 只看该作者 394楼

1.MonkeyTest此木马是8.19升级后，用系统查杀出，但无法删除。后用安装360查杀，查出无法删除。2.机型及版...想将系统root但此机型目前可root的软件。4自带杀毒软件杀不掉，接入计算机安装360报警仍然杀不掉。平时安装APP均是...更新系统提示更新。6.均是以前安装的系统，前几次升级系统未检测出病毒，出现这种情况应该是最远的版本。7手机上软件商店目前只有...



# 不对称——企业的业务发展与企业的安全意识的不平衡

```
Request Headers
POST /hj/user/password/verify?app_ver=1.6.7&app_ver_code=106078&appid=wx...
Client
Accept: */*
Accept-Encoding: gzip,deflate
Accept-Language: zh-CN,en-US;q=0.8
User-Agent: Mozilla/5.0 (Linux; Android 5.0; SM-N9006 Build(LRX21V) AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0 Chrome/37.0.0.0 X-Requested-With: com.webank.wemoney
Cookies / Login
Cookie
dcnNo=110
loginType=3
module=0000001
otd=""
userId=099996000970083
userType=2
webankToken=056BEDA91B514EDAB31CAAC9E80A030105DFD0B0095309E2AB59421C21A8B80A55F8E264
wechatOpenId=ozf_BuMR22grdSuRlyWFh9v61f0Y
Entity
Content-Length: 1057
Content-Type: application/json;charset=UTF-8
Miscellaneous
{"ret_code": "20270000", "ret_data": {"factor": "12304061"}, "ret_msg": "请求成功"}
```

www.wooyun.org

微众卡  
623

南国利剑

消息

个人信息

密码管理

风险偏好 未评估

联系客服

常见问题

关于我们

www.wooyun.org



## 移动应用被攻击方式

伪装/钓鱼

界面劫持

钓鱼应用

隐藏图标

重打包

信息窃取

短信监听/拦截

截屏

ID窃取

环境录音

其他攻击

进程注入

条款欺诈

输入法劫持

逻辑漏洞



# 不对称——安全诉求和威胁与实际的安全能力的不平衡

## 信息不对称

安全技术

安全认知

安全能力

安全意识

应用安全

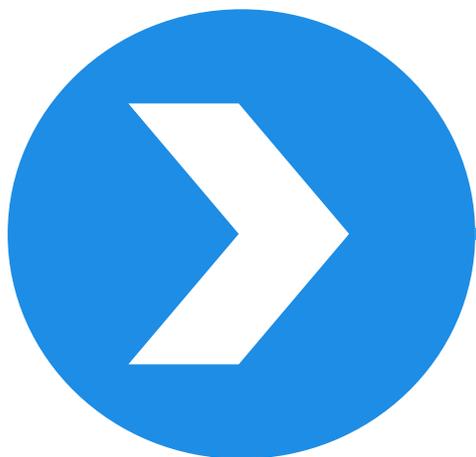
环境安全

用户需求

业务发展

感知能力

业务能力

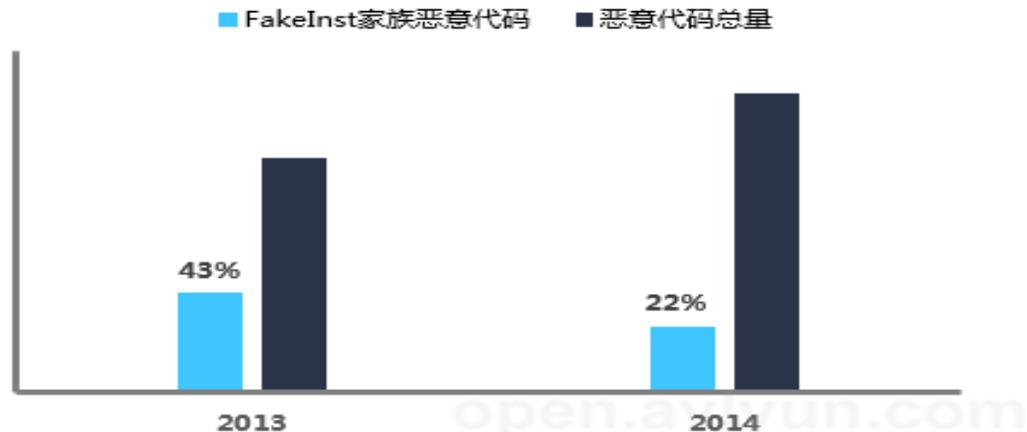


# 如何基于威胁情报对数据进行组织和驱动方式

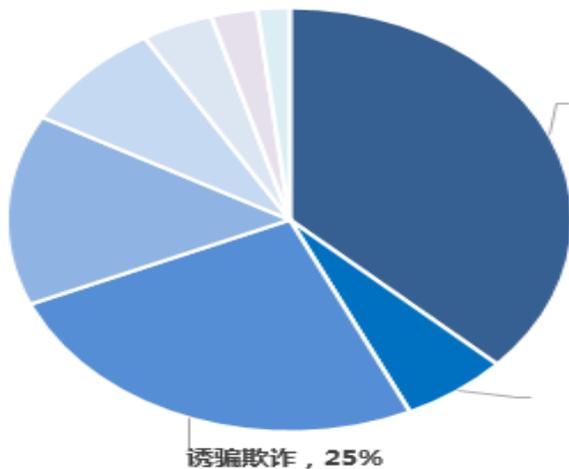
Android恶意代码数量变化情况



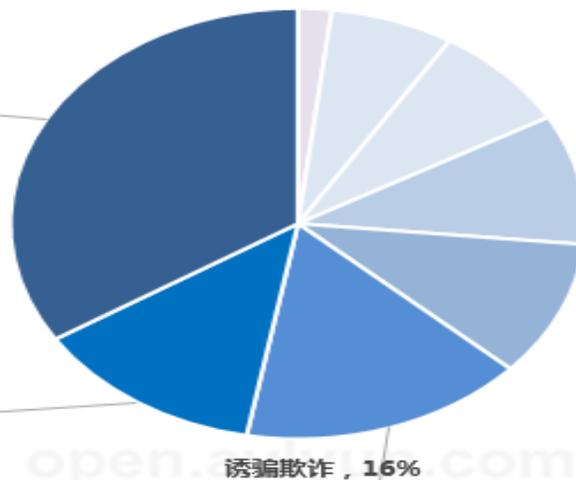
FakeInst家族恶意代码占总量比例情况



2013年恶意代码类型分布



2014年恶意代码类型分布



隐私窃取行为大幅增加。

隐私窃取, 6%

13%, 隐私窃取

CONTENT

<p><b>1</b> · 2014年网络安全</p> <p>1.1 我国互联网网络安全 1.2 数据导读</p> <p><b>2</b> · 网络安全专题</p> <p>2.1 移动互联网恶意程序 2.2 分布式反射型拒绝服务 2.3 智能硬件蠕虫威胁互阻 2.4 短信拦截黑客地下产 2.5 12306 泄密事件到日 2.6 工业控制网络安全分</p> <p><b>3</b> · 计算机恶意程序</p> <p>3.1 木马和僵尸网络监测</p>	<p>3.2 “飞客”蠕虫监测情况 ..... 84</p> <p>3.3 恶意程序传播活动监测 ..... 86</p> <p>3.4 通报成员单位报送情况 ..... 88</p> <p><b>4</b> · 移动互联网恶意程序传播和活动情况 ..... 96</p> <p>4.1 移动互联网恶意程序监测情况 ..... 96</p> <p>4.2 移动互联网恶意程序传播活动监测 ..... 98</p> <p>4.3 通报成员单位报送情况 ..... 100</p> <p><b>5</b> · 网站安全监测情况 ..... 112</p> <p>5.1 网页篡改情况 ..... 112</p> <p>5.2 网页挂马情况 ..... 121</p> <p>5.3 网页仿冒情况 ..... 124</p> <p>5.4 网站后门情况 ..... 130</p> <p><b>6</b> · 安全漏洞预警与处置 ..... 136</p> <p>6.1 CNVD 漏洞收录情况 ..... 136</p> <p>6.2 高危漏洞典型案例 ..... 139</p> <p>6.3 CNVD 行业漏洞库 ..... 146</p> <p>6.4 CNVD 漏洞处置情况 ..... 150</p>
---	---

## 数量

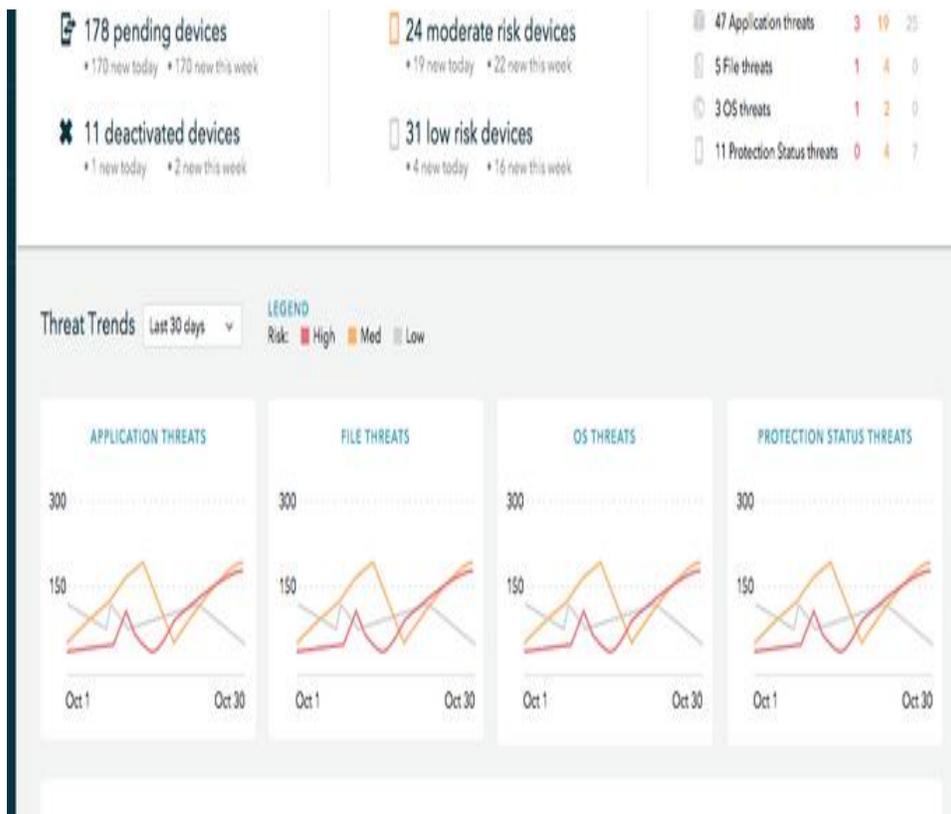
- 恶意代码，家族，变种，TOP
- 平台类型，Hash规模

## 行为

- 类型
- 攻击行为
- 行为模式和特征

## 渠道

- 应用
- 传播方式



## 设备

- 激活，越狱
- 设备管理，访问控制

## 威胁

- 威胁类型
- 威胁程度
- 响应和解决

## 策略

- 分组&控制
- 管理&策略下发



## 漏洞

- 业务接口暴露
- 关键数据泄露

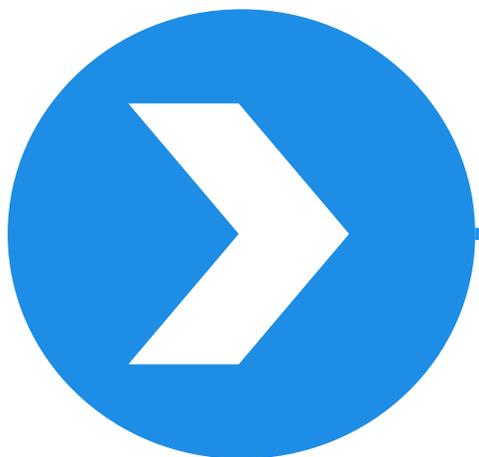
## 风险/脆弱点

- 自身编码
- 开发环境
- 第三方SDK引入
- 权限过多开放

## 仿冒&分发安全

- 仿冒/山寨应用
- 分发渠道



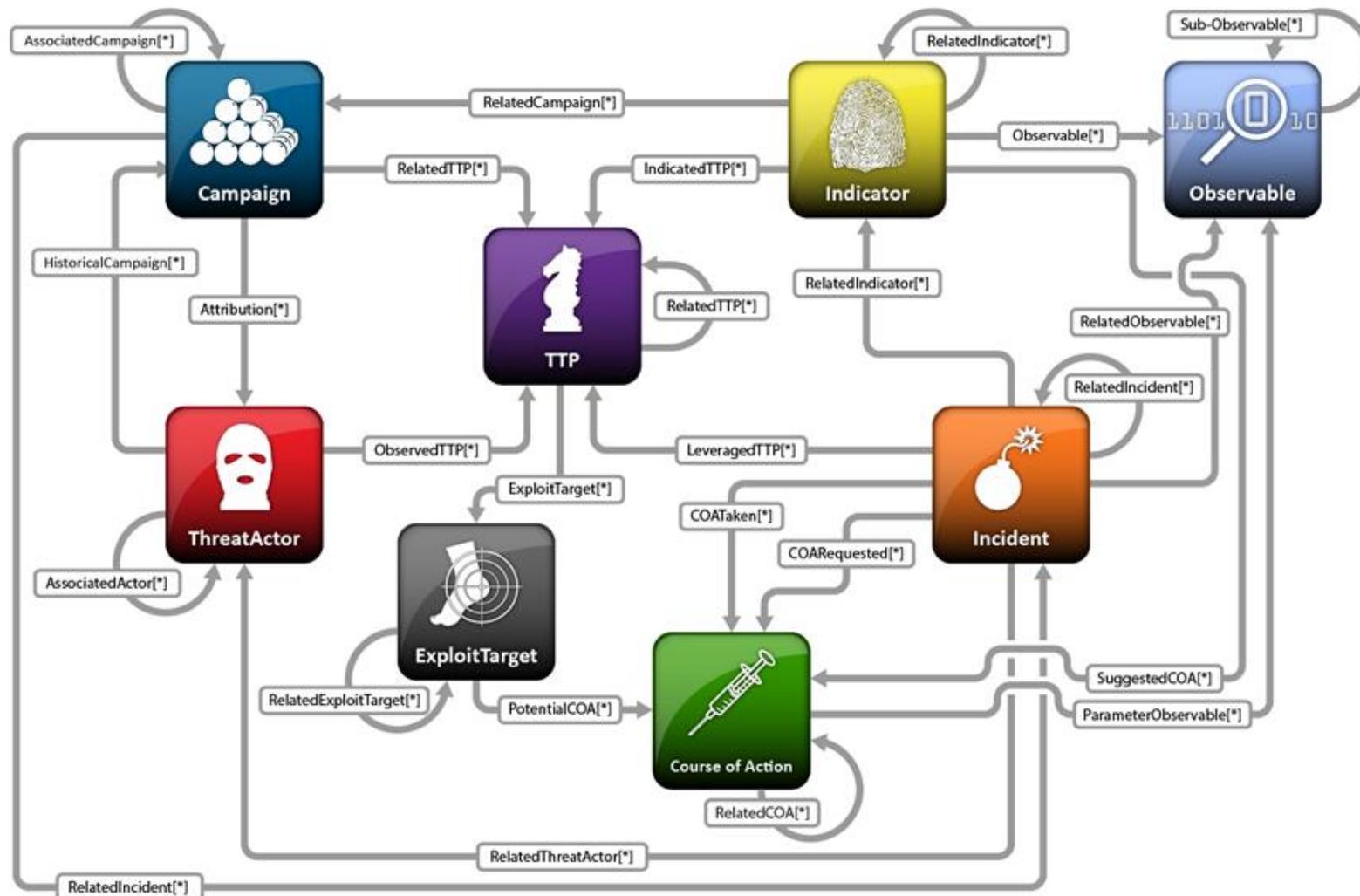


# AVL Insight移动威胁情报的源 体系



相关的概念体系	出现的背景
Threat/Risk/Exposure/Asset.....	西方的IT管理和标准化的背景
DREAD,STRIDE,PASTA, Attack Tree.....	微软和相关安全厂商所推出的风险管理模型
CAPEC,CWE,CVE,CVRF, MAEC, NVD.....	对攻击模式, 脆弱点, 漏洞等各种基础的安全元素的标定和描述结构
Threat Modeling	各种威胁建模的方法论, 工具, risk-centric, data-driven等等
Kill Chain,钻石分析,TTP.....	面向Cyber和更高强度的攻击和对抗的场景的分析工具和分析方法
CybOX,TAXII, OpenIOC.....	面向Cyber和信息交换的描述和标准体系
STIX	面向更完整的综合性的情报分析/作业/交换的体系

强烈的外在和内在的面向威胁的知识管理体系/方法

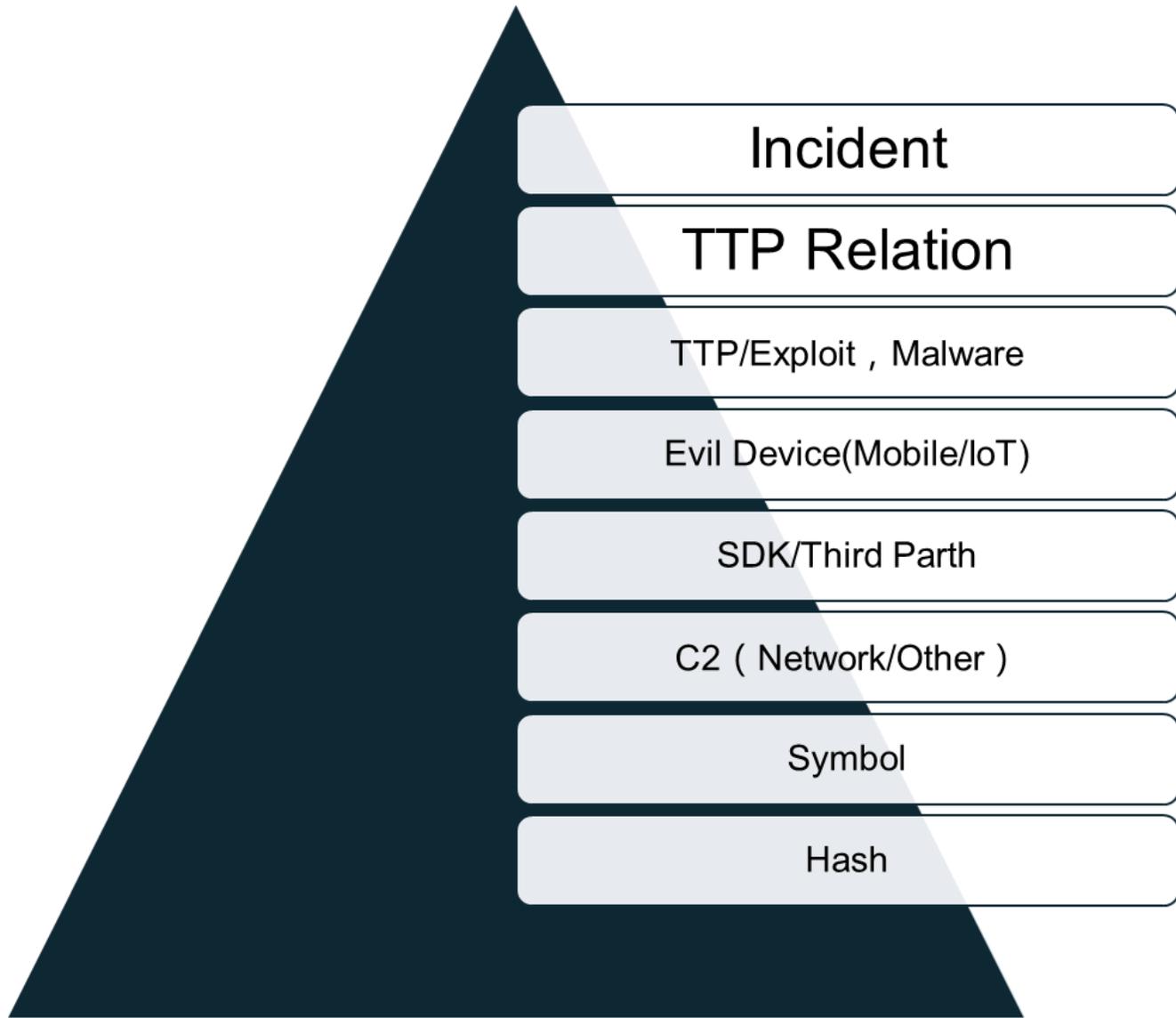


## • 情报的认识

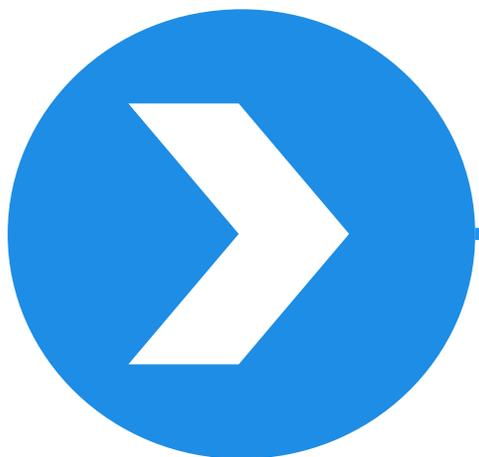
- \* 数据（线索），有价值数据不等于情报
- \* 情报是有驱动力的有价值数据

## • 移动威胁情报和Cyber威胁情报的差异性

- \* 具备更强的实效性
- \* 关联的关系复杂度在规模上更大
- \* 情报的数据和信息构成多样化



- 隐晦
- 复杂
- 高对抗
- 穿透
- 不可控
- 方式多样性
- 符号多样性
- 繁琐, 低效



# AVL Insight移动威胁情报的工程实践



## 感知&发现

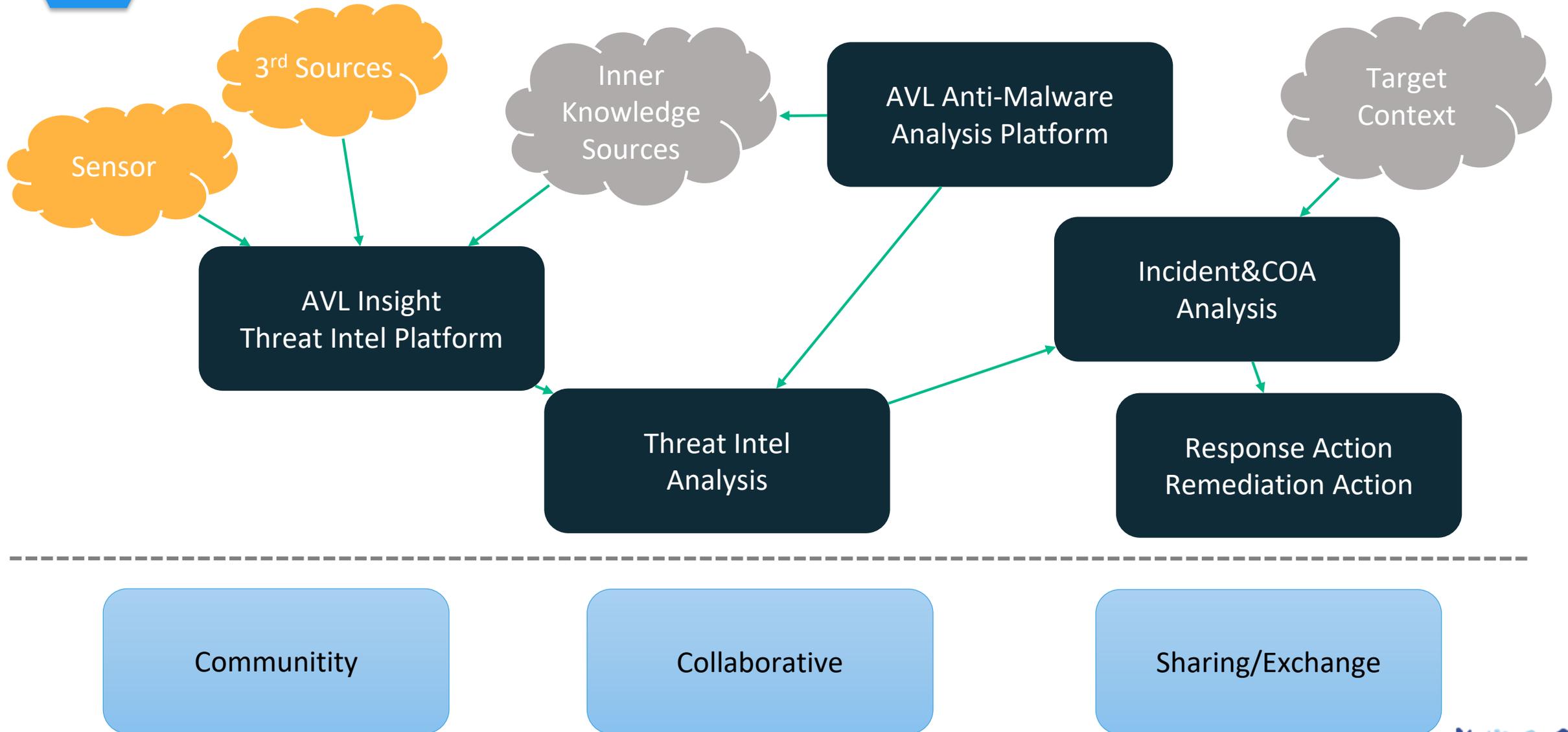
- Incident
- Asset , Impact , Victim

## 分析&呈现

- TTP+
- Malware/Exploit/AttackPatterns
- Technique Details
- ThreatActor/Targets

## 决策&响应

- COA



面向威胁作业



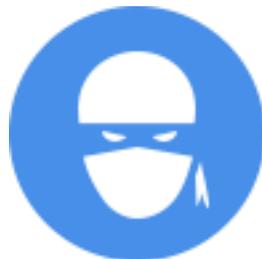
TTP+情报



威胁关联关系



受害源/Victim



攻击源\*/ThreatActor

面向元数据



引擎探头



样本库



网络探头



风险库\*/Exploit+Vuln

面向基础数据



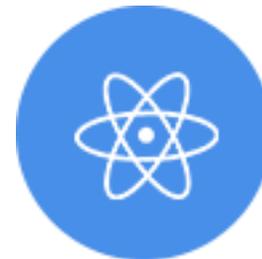
应用商店监控



技术新闻情报



Whois



域名

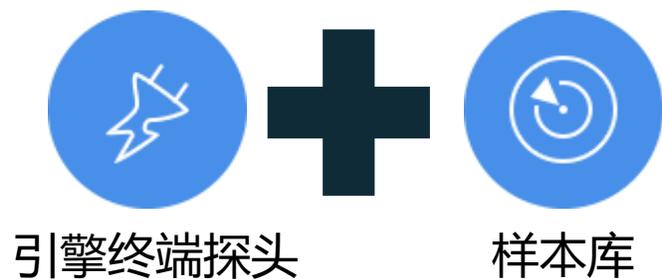
面向威胁量化和响应



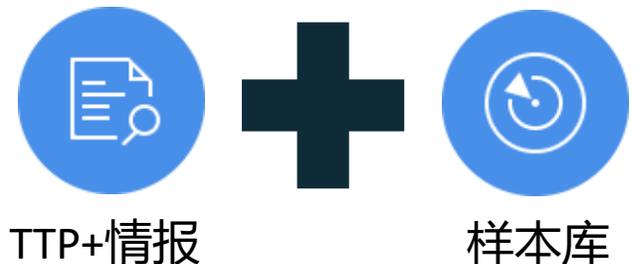
威胁事件\*/Incident



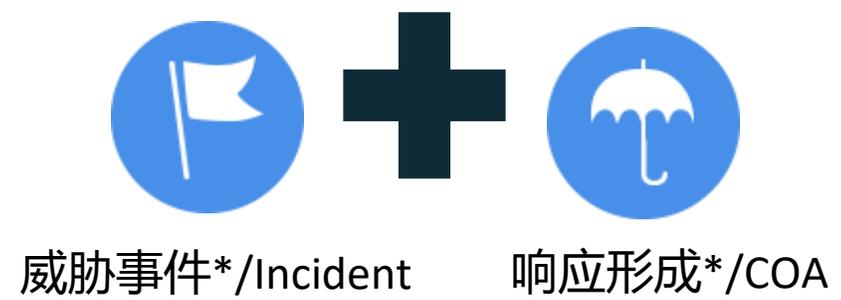
响应形成\*/COA



感知



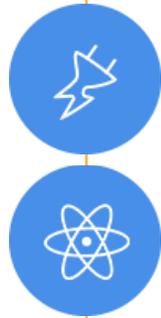
分析



决策

## • 某银行APP一个月监控数据

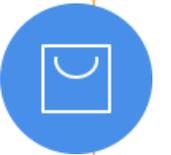
- 非正版下载量：  
2499
- 非正版下载源：  
223



- 恶意代码变种：3
- 恶意代码总量：6
- 广告件总类：4
- 广告件数量：24
- 支付件：0
- 用户环境中存在恶意代码变种：405
- 用户环境存在恶意代码数量：5014
- 用户环境中存在风险应用：253264



- 应用商店：25
- 网盘：4
- 未知：5



- 虽然只有少量应用被篡改
- 但用户环境存在大量安全问题
- 当整个用户环境都不安全的时候，银行APP还能保障业务安全么？



# 谢谢大家

THANK YOU FOR YOUR ATTENTION