基于移动威胁情报的安全价值观

安天移动安全研发中心

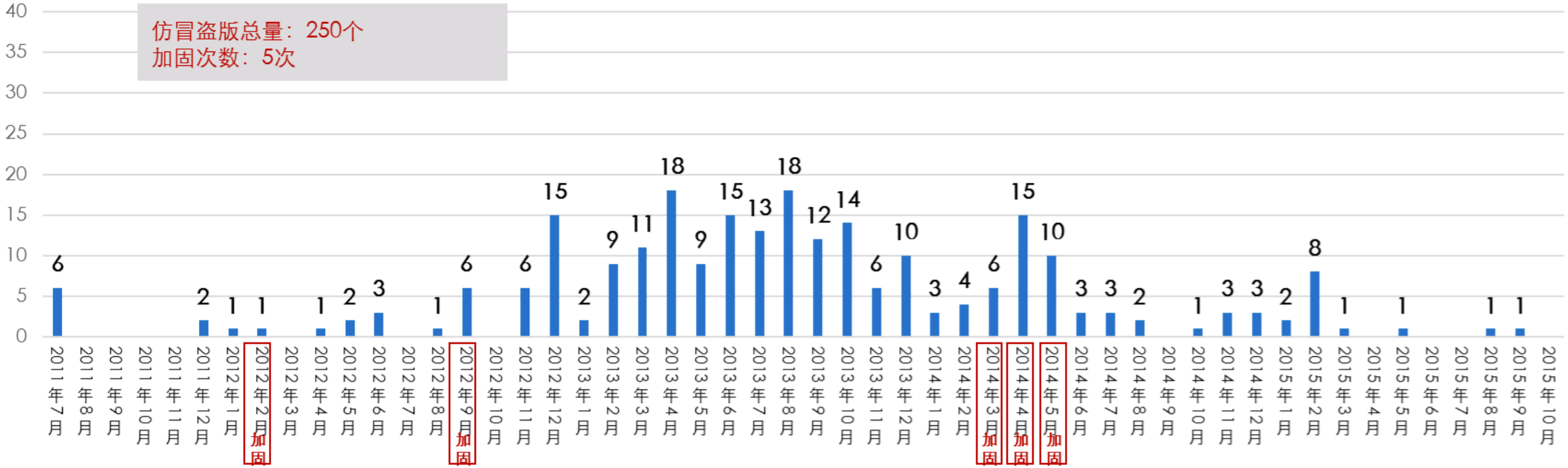
提纲

- 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

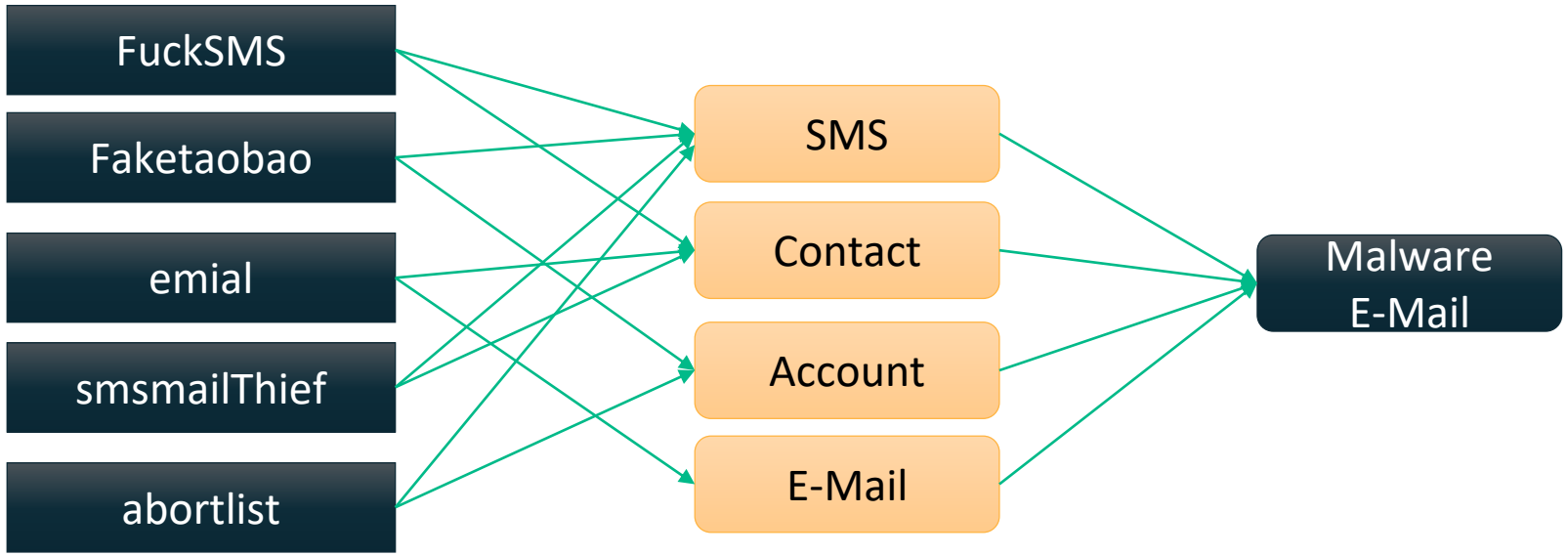
威胁场景下各种信息不对称导致“盲”人摸“象”

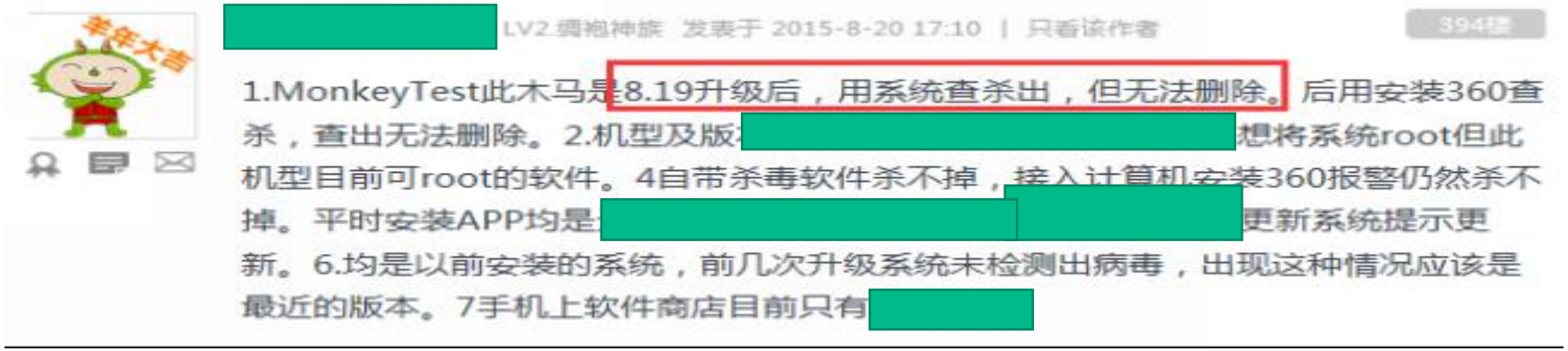
盲人摸象——企业使用安全技术与实际安全威胁的不对称

某游戏应用仿冒盗版样本数量变化趋势

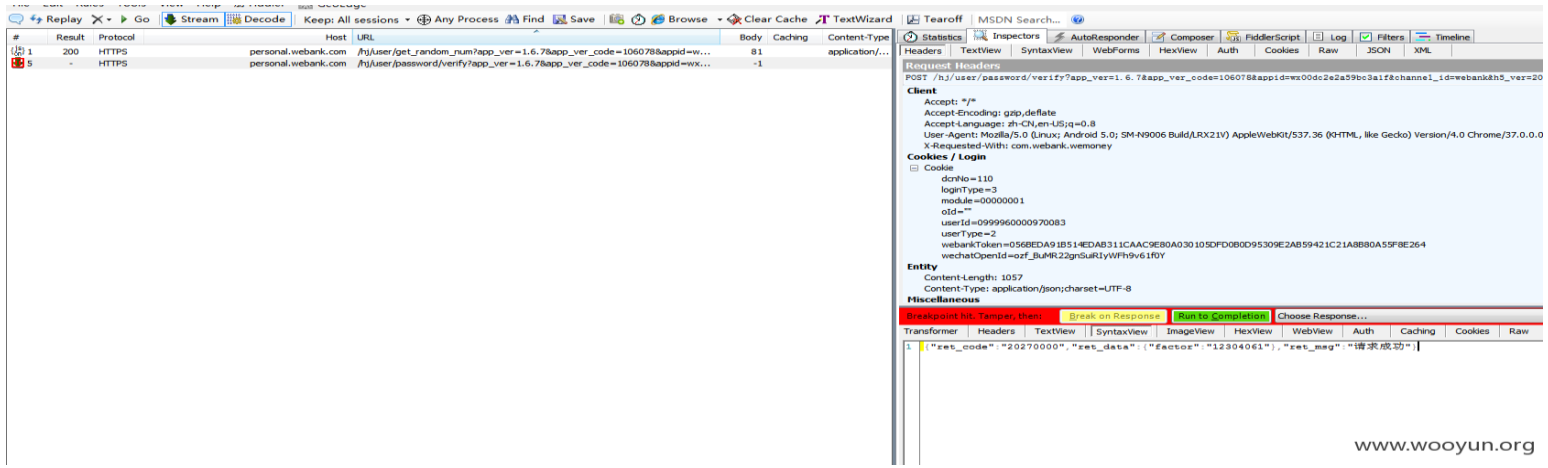


不对称——企业的安全认知与用户威胁场景下的不平衡





不对称——企业的业务发展与企业的安全意识的不平衡



不对称——安全诉求和威胁与实际的安全能力的不平衡

移动应用被攻击方式

伪装/钓鱼	信息窃取	其他攻击
界面劫持	短信监听/拦截	进程注入
钓鱼应用	截屏	条款欺诈
隐藏图标	ID窃取	输入法劫持
重打包	环境录音	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

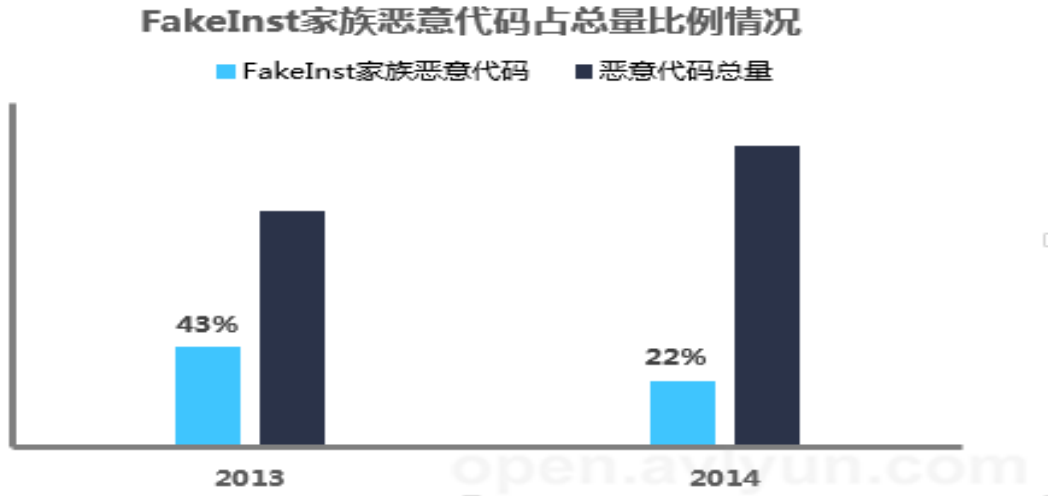
业务发展

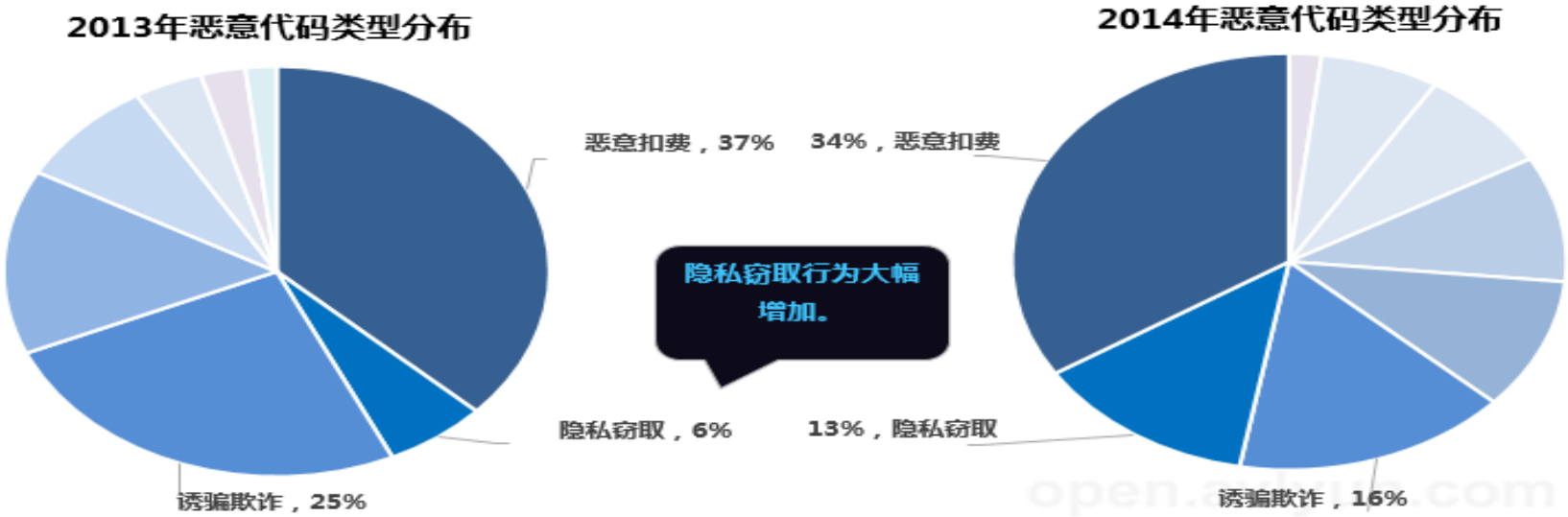
感知能力

业务能力

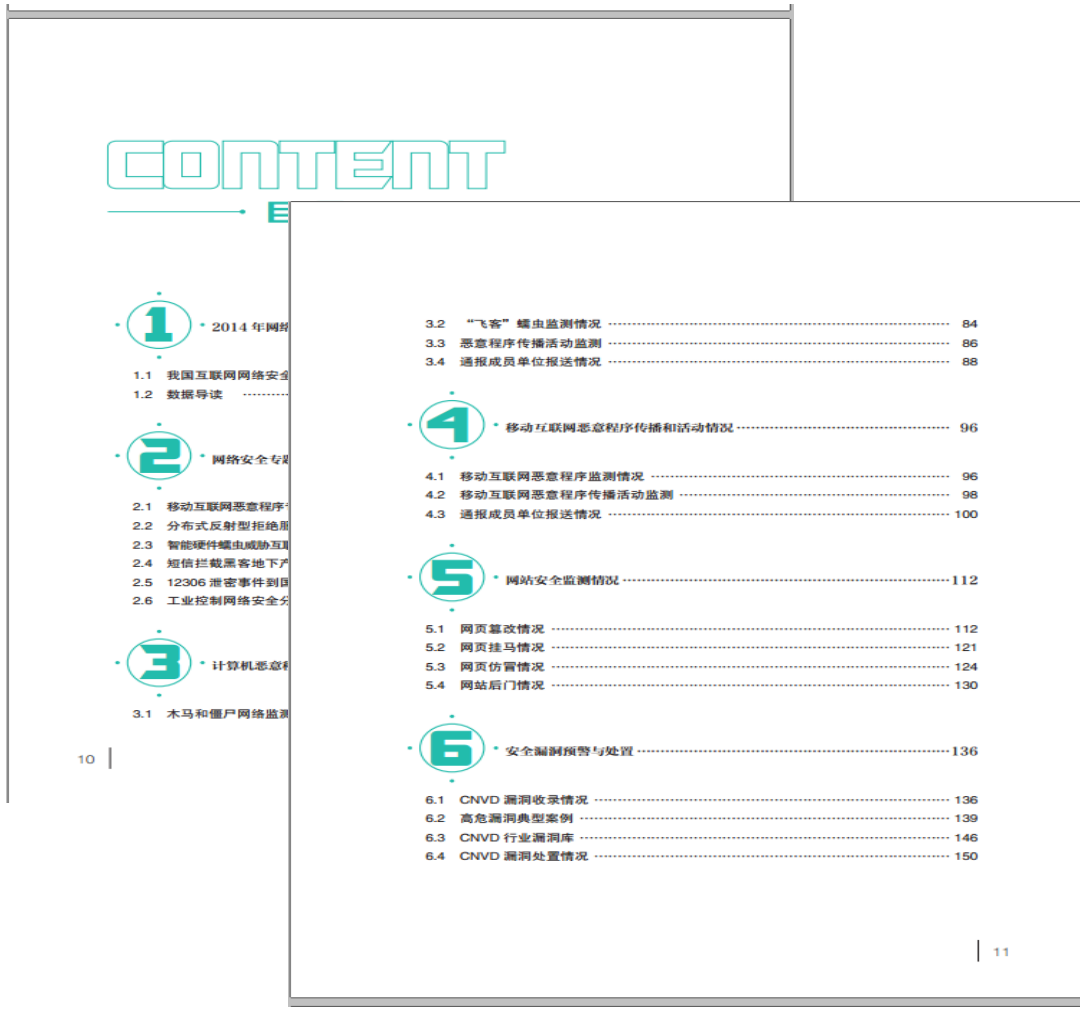
如何基于威胁情报对数据进行组织和驱动方式

数据不等于情报，有价值的数据也不等于情报





数据组织的方式——“安全报告”



CONTENT

目

数量

- 恶意代码，家族，变种，TOP
- 平台类型，Hash规模

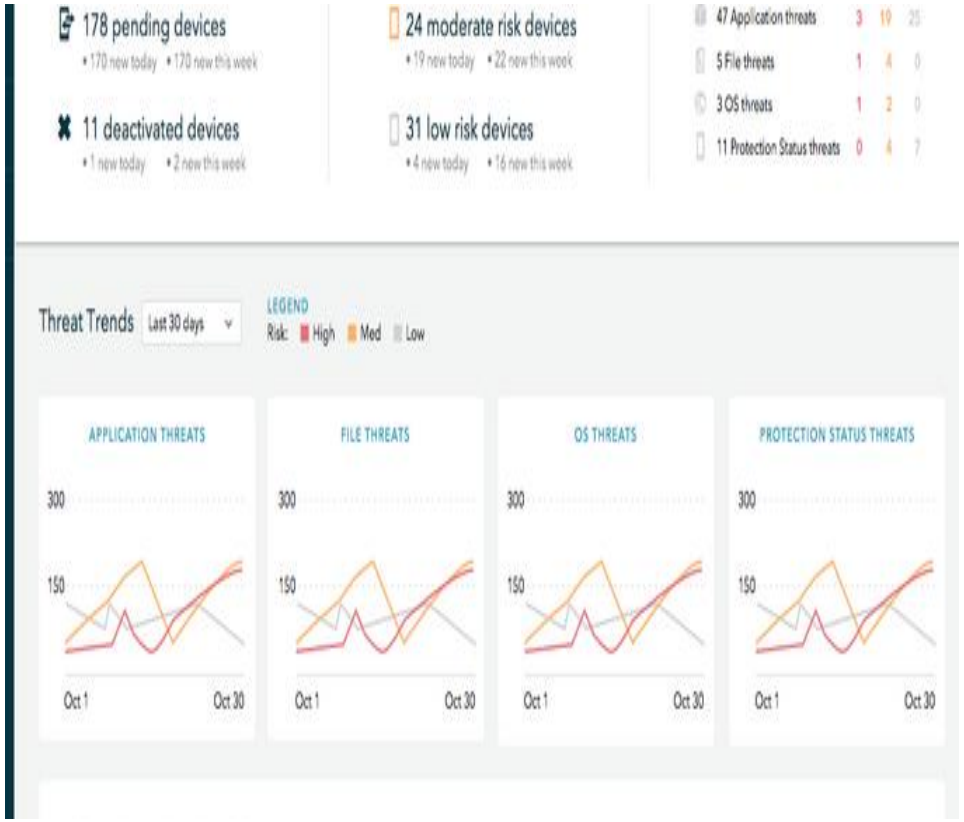
行为

- 类型
- 攻击行为
- 行为模式和特征

渠道

- 应用
- 传播方式

数据组织的方式——“设备&资产视角”



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

数据组织的方式——“风险视角”

漏洞

- 业务接口暴露
- 关键数据泄露

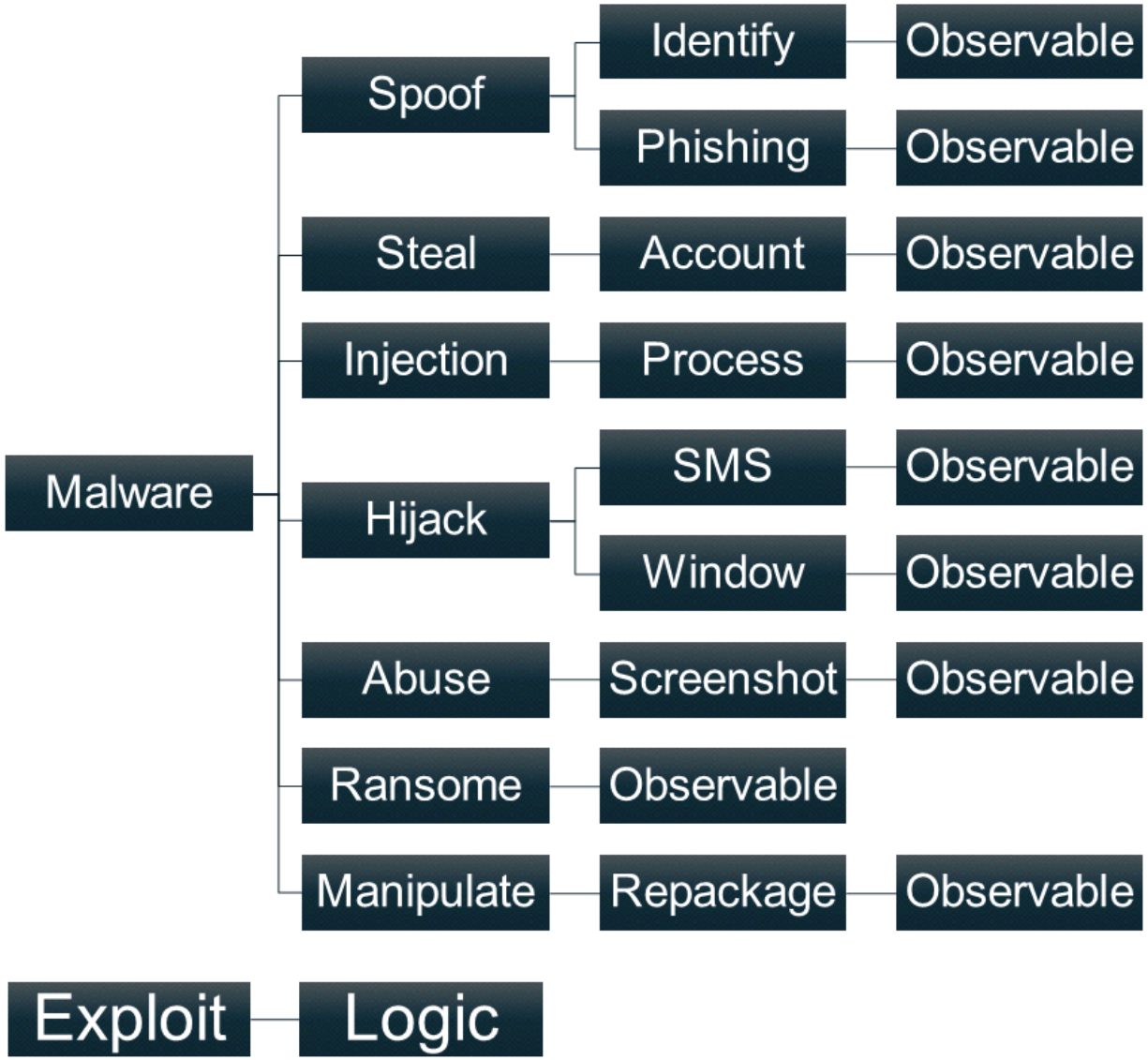
风险/脆弱点

- 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

数据组织的方式——尝试用情报的描述结构的拆解



钓鱼应用

条款欺诈

ID窃取

进程注入

界面劫持

输入法劫持

截屏

短信监听/拦截

环境录音

重打包

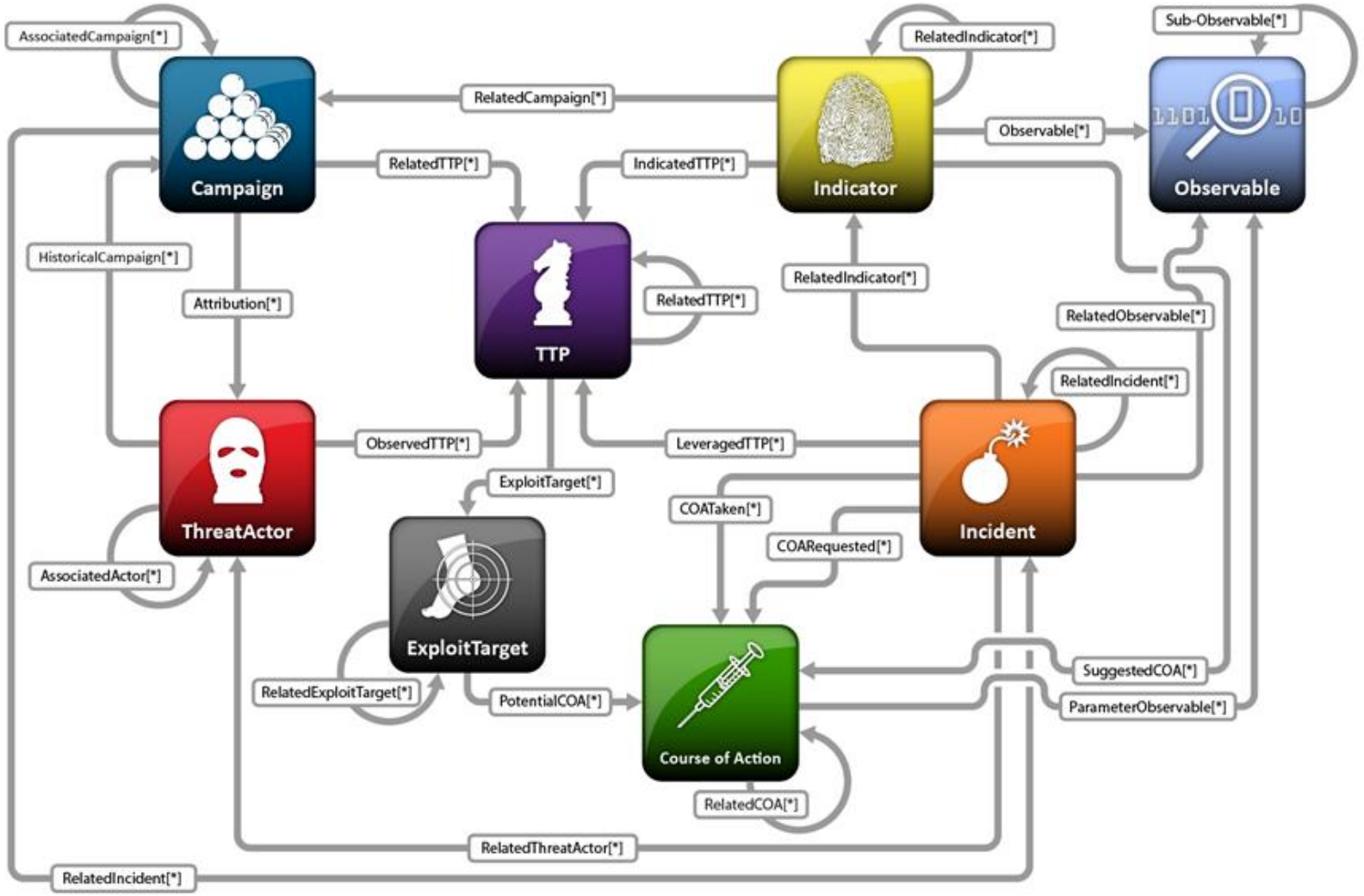
逻辑漏洞

AVL Insight移动威胁情报的源体系

我们认为的威胁情报的价值观——情报不是从石头里面蹦出来的

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

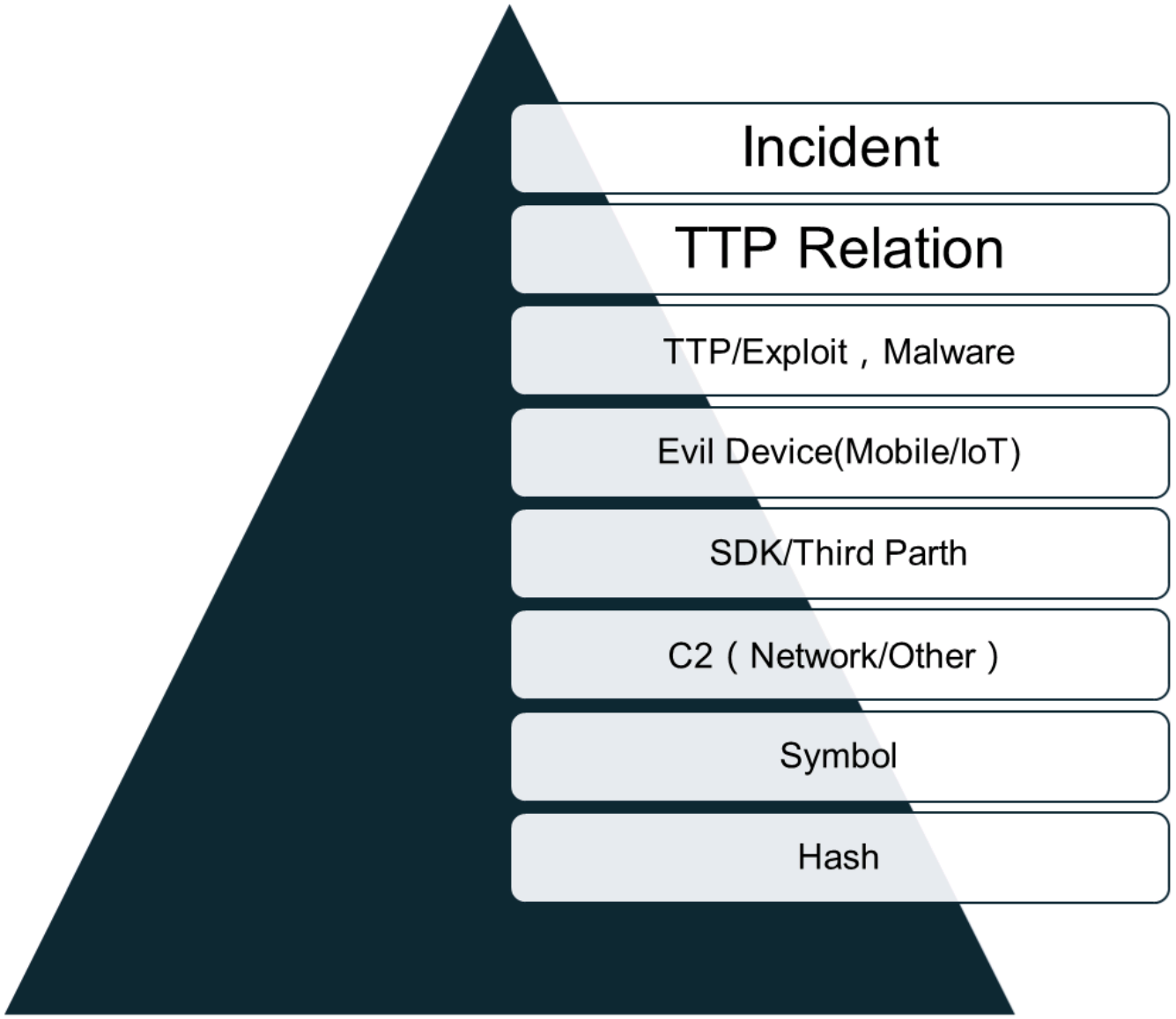
强烈的外在和内在的面向威胁的知识管理体系/方法


AssociatedCampaign[*]
RelatedIndicator[*]
Sub-Observable[*]
RelatedCampaign[*]
Observable[*]
Campaign
Indicator
Observable
RelatedTTP[*]
IndicatedTTP[*]
HistoricalCampaign[*]
TTP
RelatedTTP[*]
RelatedIndicator[*]
Attribution[*]
RelatedObservable[*]
RelatedIncident[*]
ThreatActor
ObservedTTP[*]
LeveragedTTP[*]
Incident
ExploitTarget[*]
COATaken[*]
COARequested[*]
AssociatedActor[*]
ExploitTarget
SuggestedCOA[*]
RelatedExploitTarget[*]
PotentialCOA[*]
ParameterObservable[*]
Course of Action
RelatedCOA[*]
RelatedThreatActor[*]
RelatedIncident[*]

情报的认识和移动威胁情报的差异性

- 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
  - 情报的数据和信息的构成多样化

移动威胁情报的困难度金字塔



- 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

面向移动威胁的情报作业实践

感知&发现

- Incident
- Asset，Impact，Victim

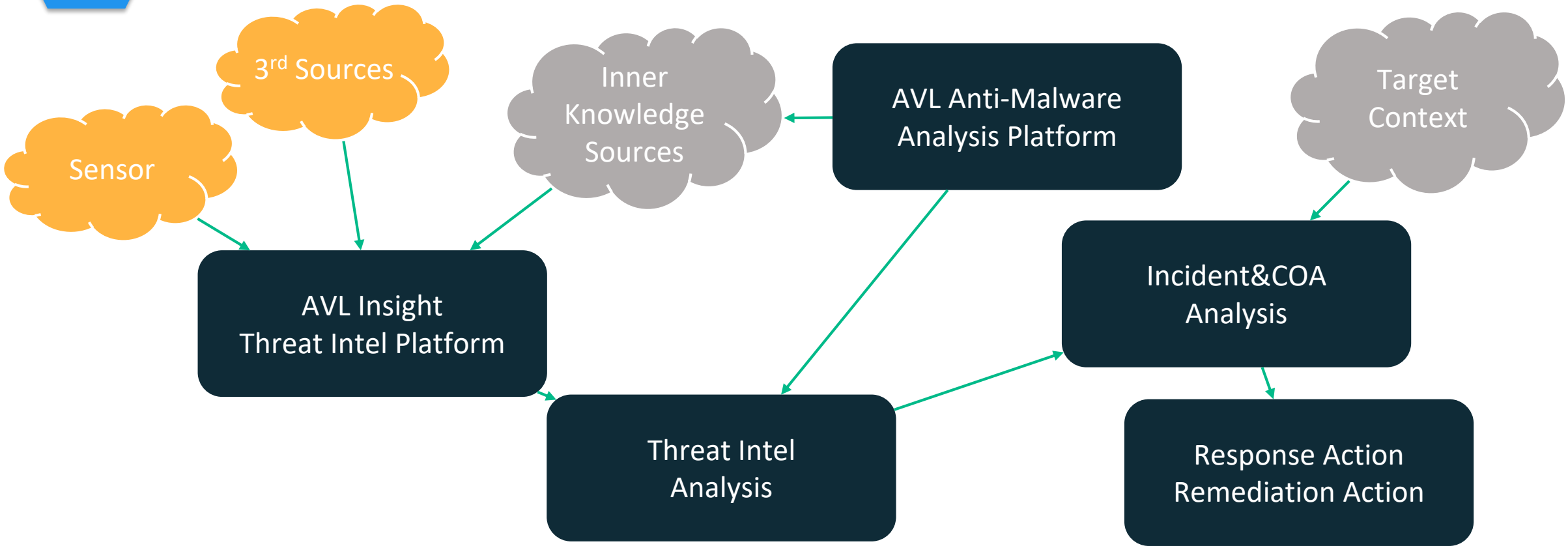
分析&呈现

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

决策&响应

- COA

面向移动威胁的情报作业实践



Communitity

Collaborative

Sharing/Exchange

面向移动威胁的情报作业实践——数据源体系

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

基于情报和威胁分析的去不平衡

引擎终端探头　　样本库

感知

TTP+情报　　样本库

分析

威胁事件*/Incident　　响应形成*/COA

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