移动威胁情报架构解析和实践分享

移动安全研发中心 潘博文

个人简介

潘博文

威胁情报　移动高级威胁　逆向分析

- 移动高级研究员
- 主要研究移动恶意代码对抗技术和高级威胁事件分析，目前主要负责内部威胁情报分析运营体系设计

引子

FSI 2015

基础数据体系和移动威胁情报核心思路

FSI 2016

面向应用的数据画像体系

FSI 819

面向威胁分析的工程化实践

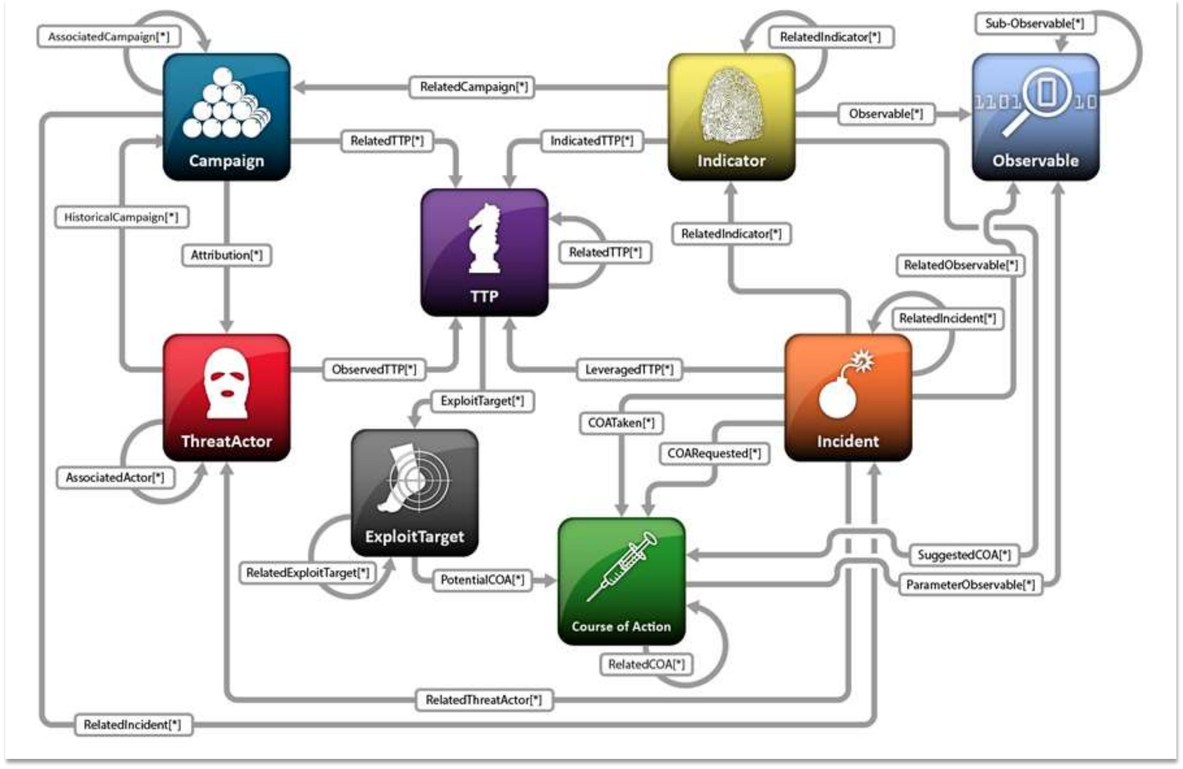
FSI 520

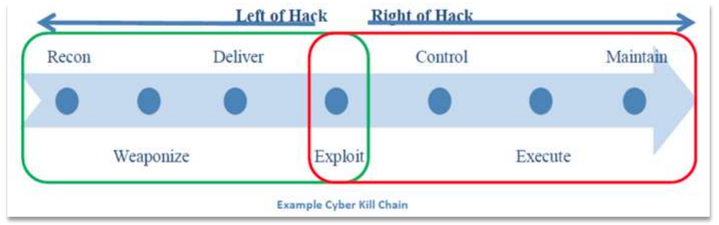
威胁情报产品架构视角

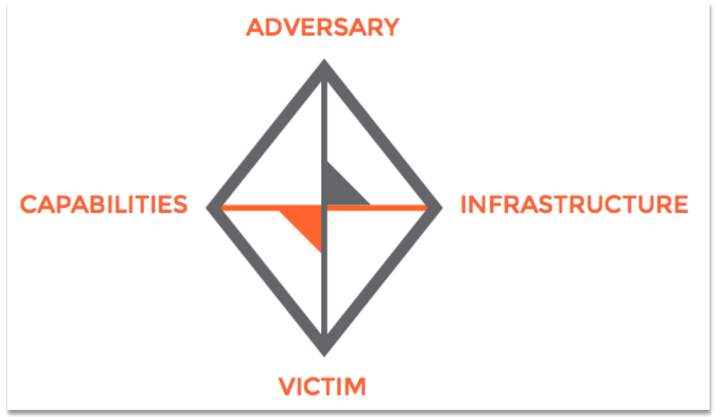
FSI 219

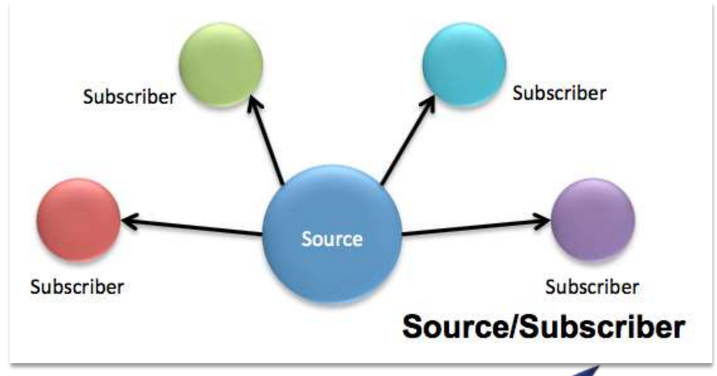
移动威胁情报体系要素

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


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


Left of Hack
Right of Hack
Recon
Deliver
Control
Maintain
Weaponize
Exploit
Execute
Example Cyber Kill Chain


ADVERSARY
CAPABILITIES
INFRASTRUCTURE
VICTIM


Subscriber
Subscriber
Source
Subscriber
Subscriber
Source/Subscriber

CAPEC

MAEC

CybOX

CVE
CWE

“威胁情报”是面向威胁的知识管理和表达

消除知识的不对称性

数据如何驱动为情报？

“威胁情报”是面向交换和分享的，并且是高价值的

用户如何才能使用或者结合“威胁情报”

什么样的“威胁情报”才是对用户来说高价值的

课程提纲Contents

“移动威胁情报”是

形容词

描述移动场景下的威胁攻击

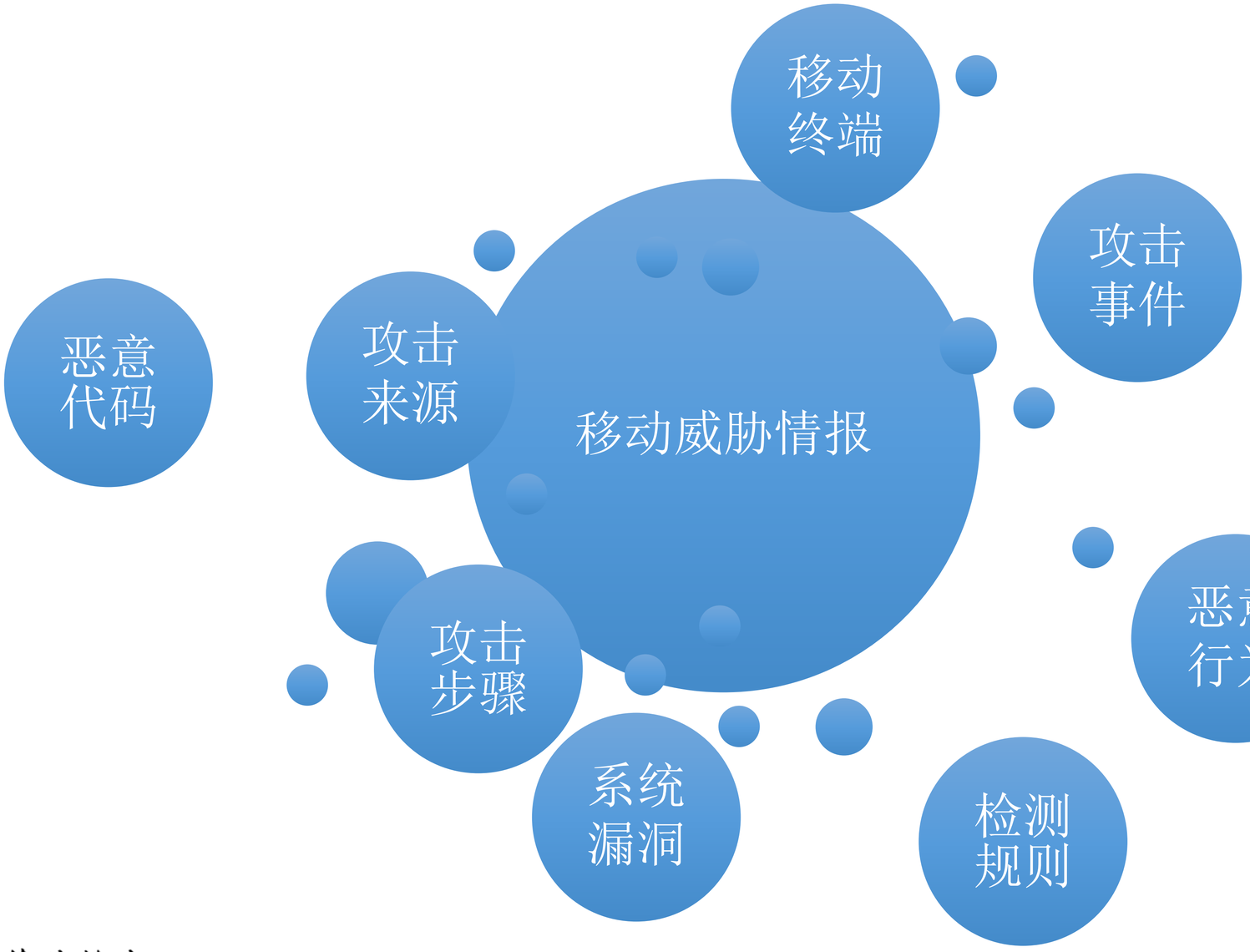
动词

面向运营和分析的驱动和流转

名词

输出服务和响应落地

描述移动场景下的威胁攻击



无差别的海量告警

有效缓解策略的选择

意图、目的和战术

有效防御策略

场景上下文和关联性

事件追溯和影响评估

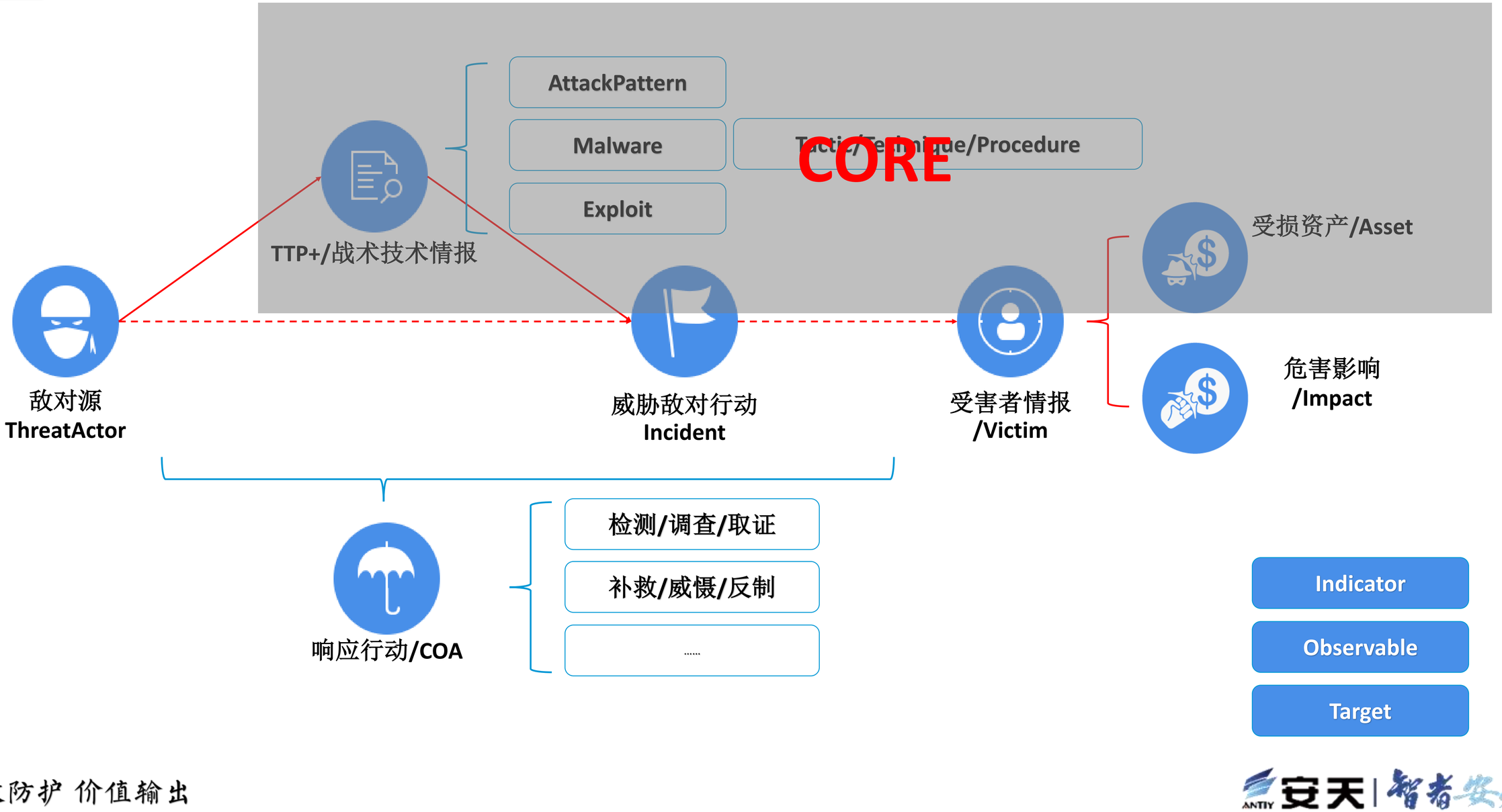
描述移动场景下的威胁攻击

1. 攻击者信息统计.....3
2. 攻击链流程分析.....4
3. 样本所用战术分析.....5
4. 完整攻击链还原分析.....8
   4.1. 隐藏窃取并拦截转发短信行为.....8
      4.1.1. 样本 1.....8
      4.1.2. 样本 2.....17
      4.1.3. 样本 3.....24
      4.1.4. 样本 4.....35
   4.2. 后台网络窃取短信行为.....43
      4.2.1. 样本 1.....43
      4.2.2. 样本 2.....44
   4.3. 伪造界面诱骗信息并转发行为.....47
      4.3.1. 样本详情.....47
      4.3.2. 恶意行为.....47
      4.3.3. 溯源分析.....47
      4.3.4. 制作时间.....48
   4.4. 私自载入及窃取拦截行为.....48
      4.4.1. 样本 1.....48
      4.4.2. 样本 2.....50
   4.5. 实时转发用户输入信息行为.....52

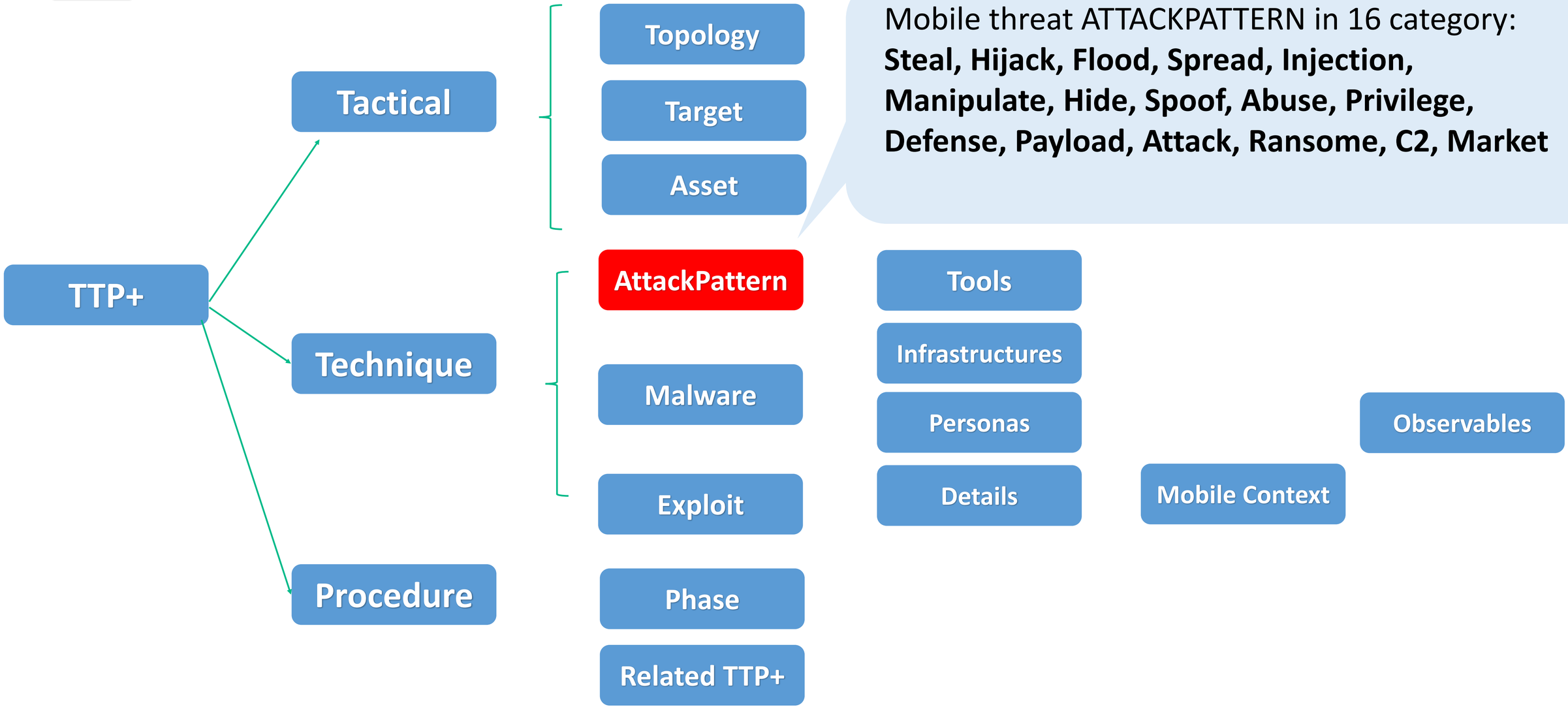
TTP	
ID	example:ttp-7d9fe1f7-429d-077e-db51-92c70b8da45a
Title	Poison Ivy Variant v4392-acc
Behavior	
Malware	
Malware Instance	MAEC4.1InstanceType
Name	Poison Ivy Variant v4392-acc
Type	Remote Access Trojan MalwareTypeVocab-1.0
MAEC	MAEC™

	TTP	TTP+
结构	结构化	结构化，适当冗余
处理	机可读	机可读，机可用
规范	统一结构，面向情报交换	面向机可用流程

移动威胁（情报）要素

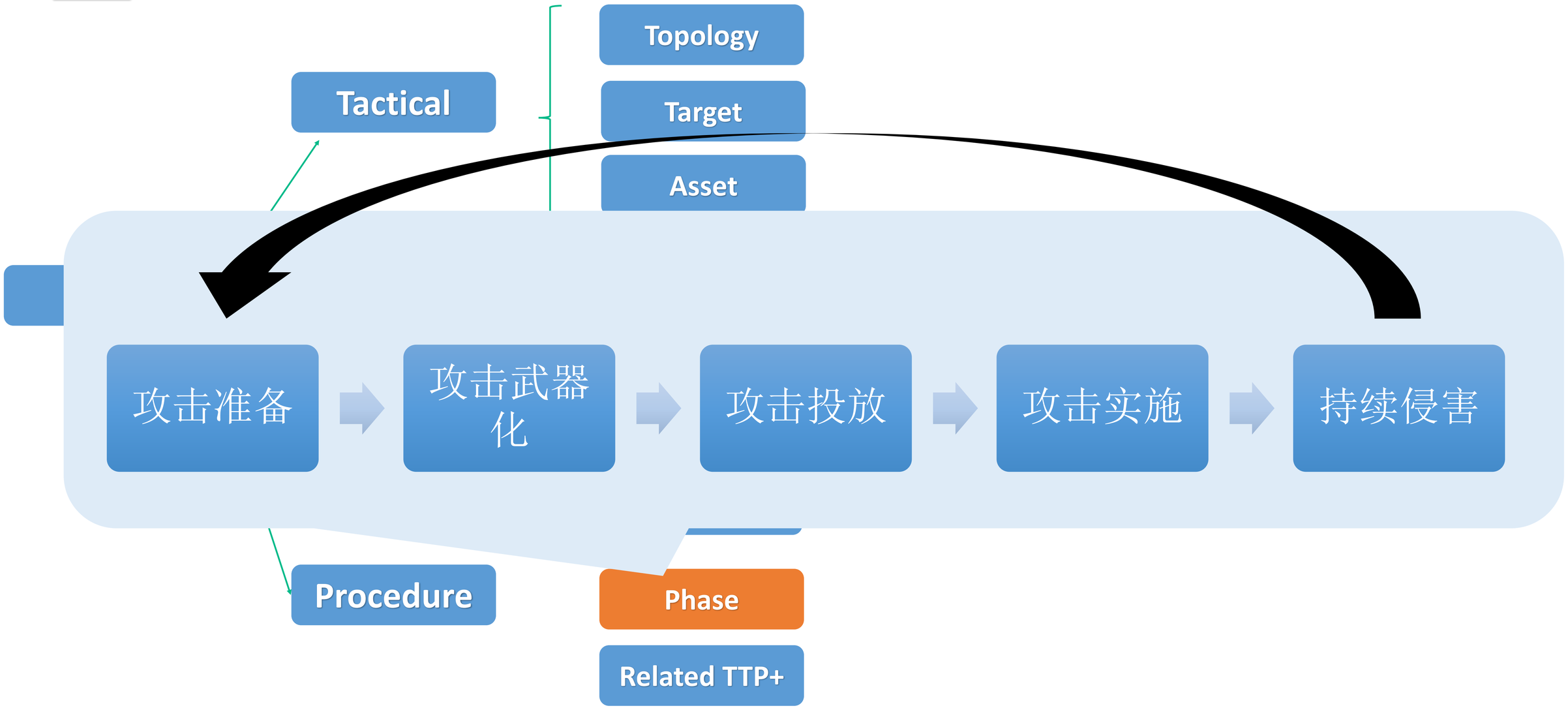

AttackPattern
Malware
Tactic/Technique/Procedure
Exploit
CORE
TTP+/战术技术情报
受损资产/Asset
危害影响
/Impact
敌对源
ThreatActor
威胁敌对行动
Incident
受害者情报
/Victim
响应行动/COA
检测/调查/取证
补救/威慑/反制
.....
Indicator
Observable
Target

TTP+描述

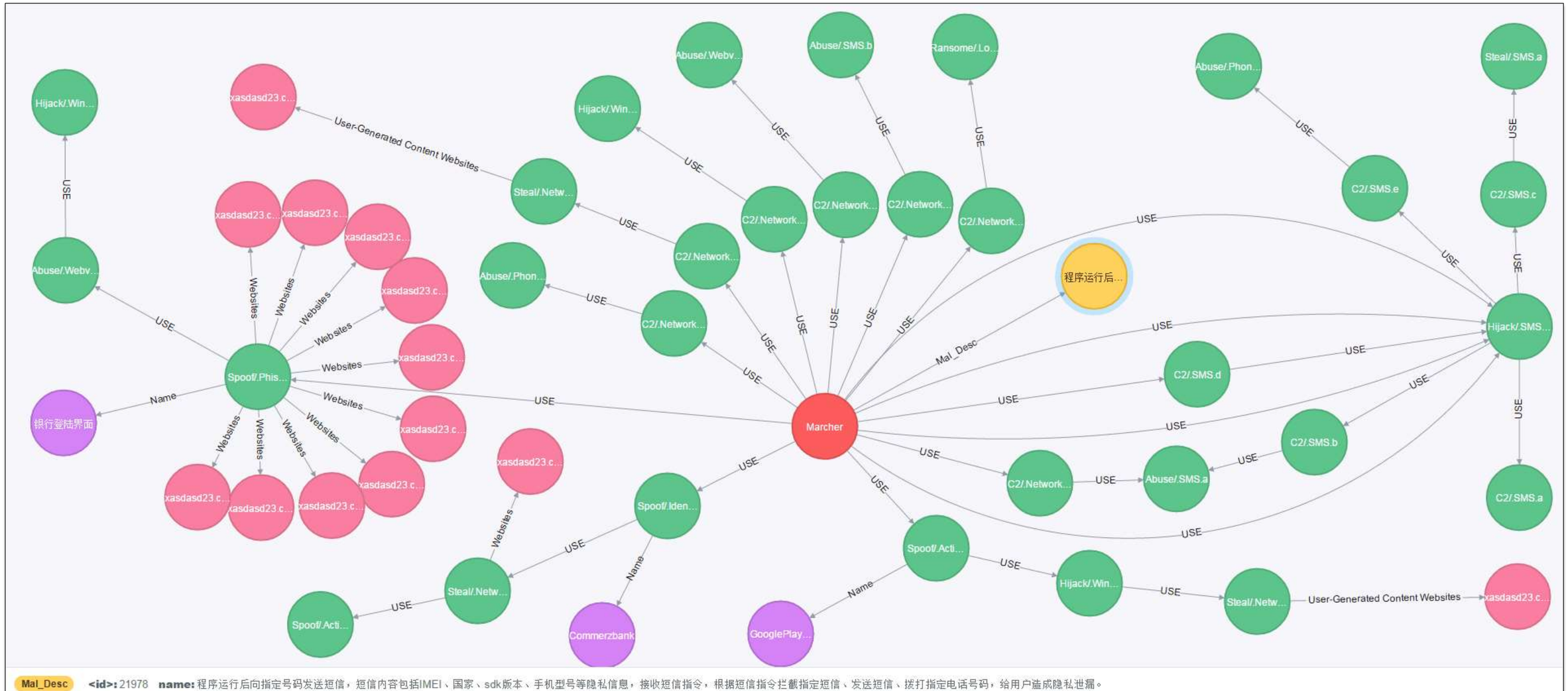


Mobile threat ATTACKPATTERN in 16 category:
Steal, Hijack, Flood, Spread, Injection, Manipulate, Hide, Spoof, Abuse, Privilege, Defense, Payload, Attack, Ransome, C2, Market

TTP+描述


Topology
Tactical
Target
Asset
攻击准备
攻击武器化
攻击投放
攻击实施
持续侵害
Procedure
Phase
Related TTP+

案例 – Marcher(金融移动威胁)



数据驱动为情报

攻击准备 → 攻击武器化 → 攻击投放 → 攻击实施 → 持续侵害

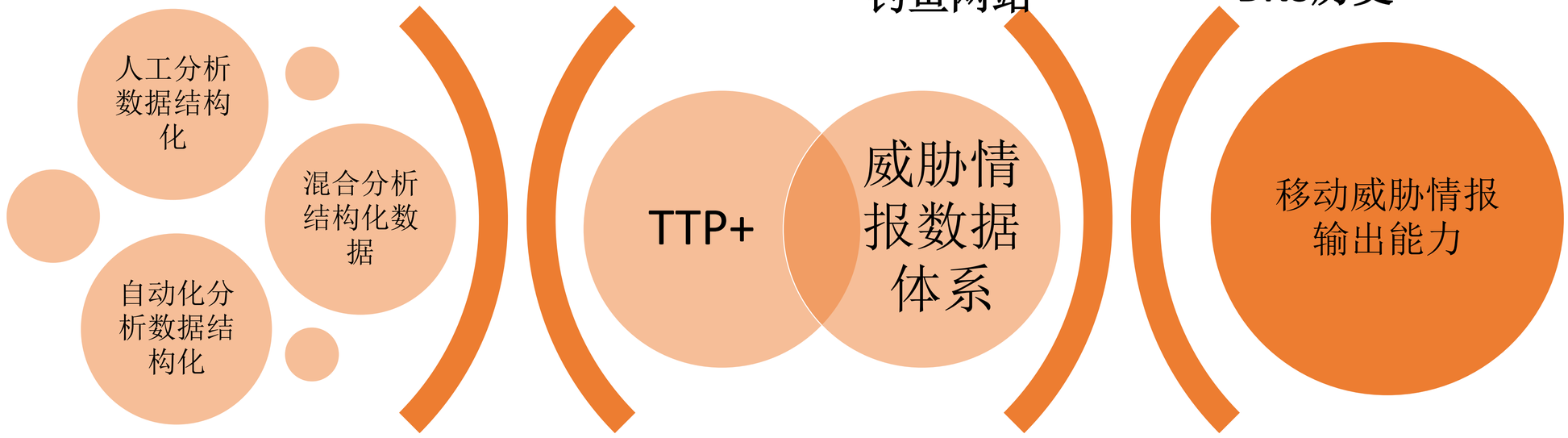
OSINT情报
域名注册信息

样本信息
样本行为

应用商店
网络流量
钓鱼网站

移动终端
恶意代码

泄露资产
控制基础设施
DNS历史



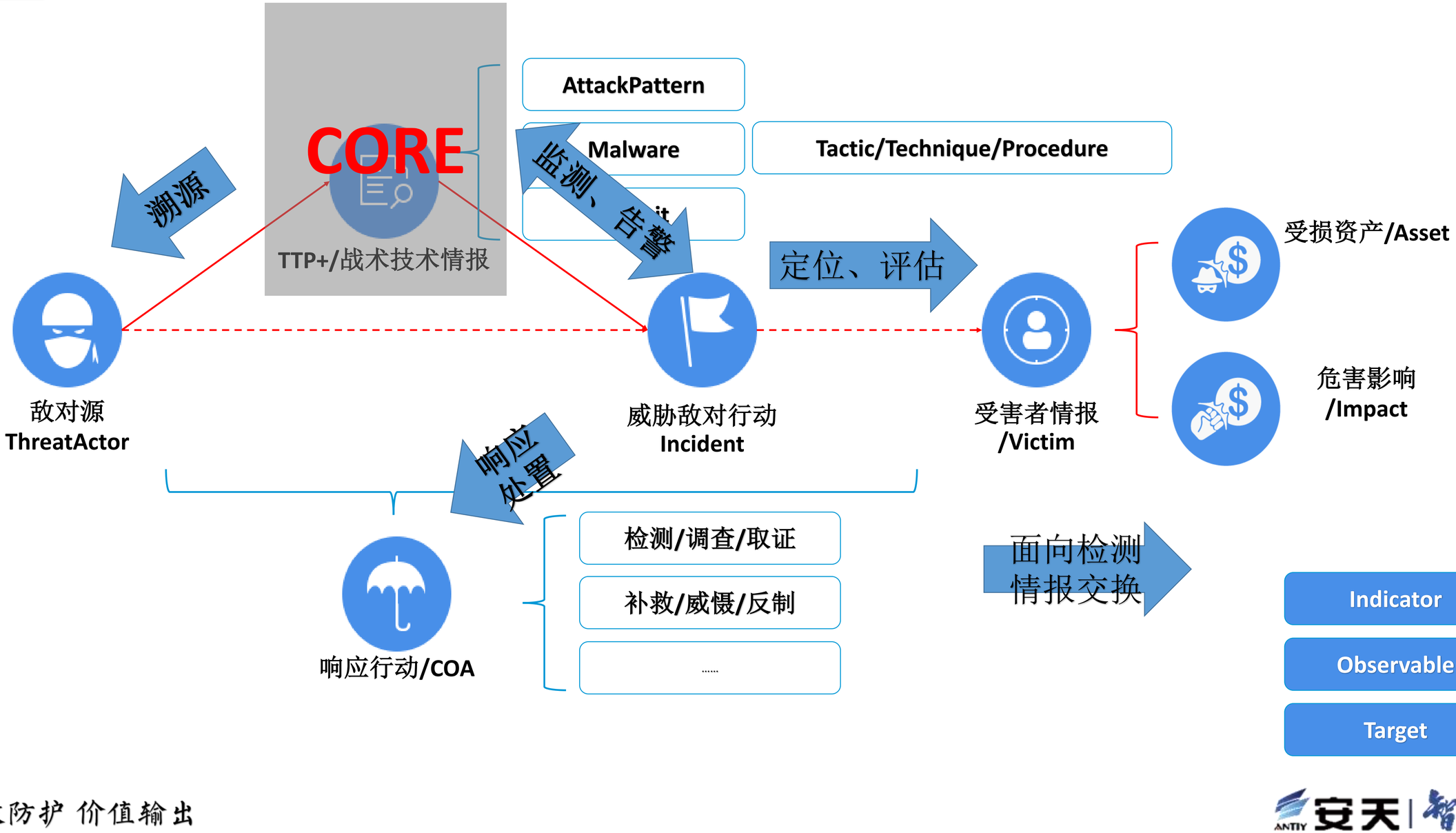
数据到信息

知识结合场景上下文

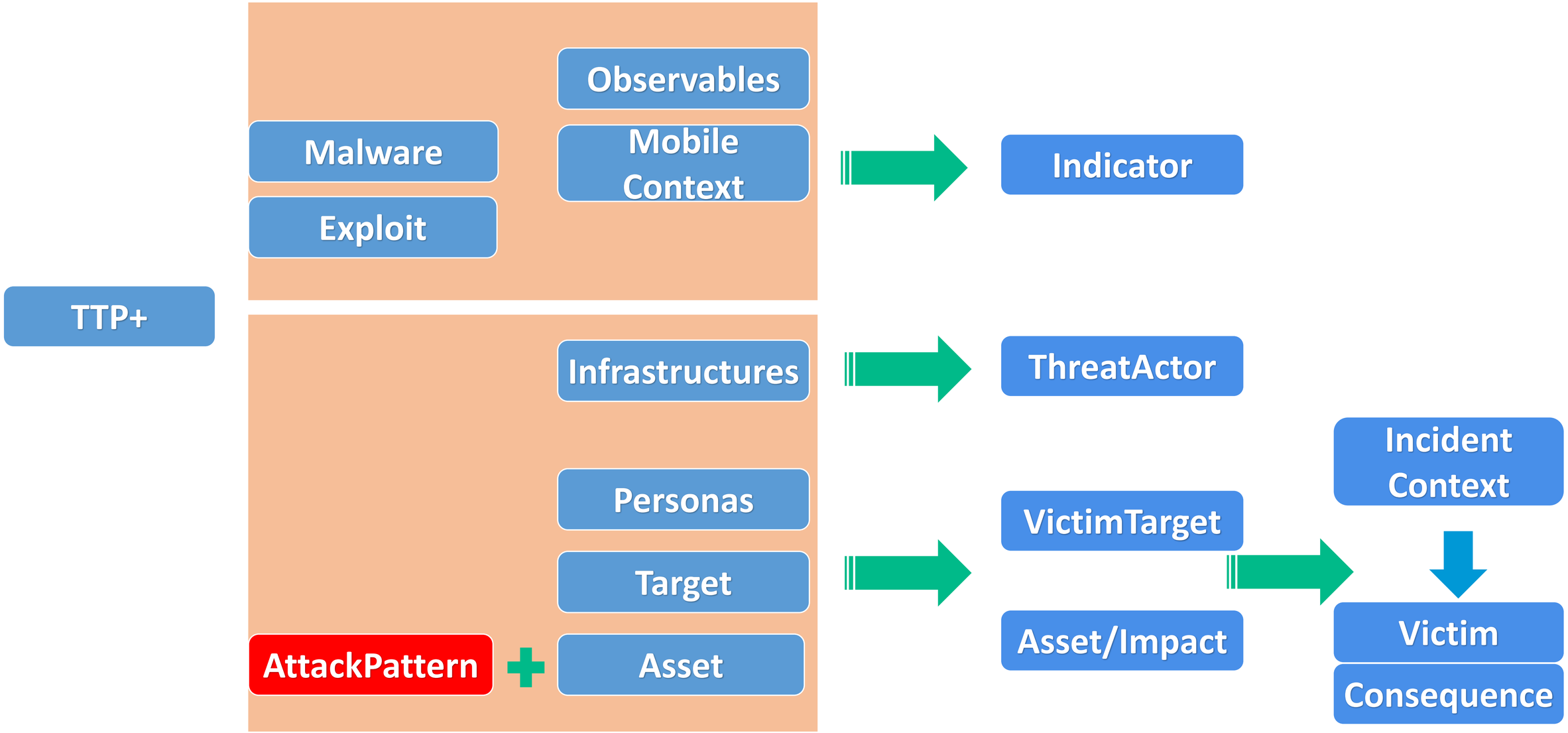
威胁情报

有效防护 价值输出

移动威胁情报数据流转


CORE
TTP+/战术技术情报
AttackPattern
Malware
Tactic/Technique/Procedure
it
溯源
监测、告警
定位、评估
敌对源
ThreatActor
威胁敌对行动
Incident
受害者情报
/Victim
受损资产/Asset
危害影响
/Impact
响应处置
响应行动/COA
检测/调查/取证
补救/威慑/反制
.....
面向检测
情报交换
Indicator
Observable
Target

TTP为中心的情报驱动流



TTP为中心的情报作业流

样本库 引擎探头 网络探头 应用商店 OSINT 基础设施

移动终端 移动网络 企业内网

设备画像 IP画像 用户画像

基础数据

结构化数据

画像数据

情报化加工

策略化输出

Strategic

Tactical

Technical

相关性

有效性

可量化

Context目标 + 基础画像

TTP清单 相关性数据

Context资产 Asset/Target AttackPattern TTP+

TTP驱动 关键知识数据

Context指标 TI Object

策略监测

事件发现

技术分析

线索关联

追踪溯源

提取特征

有效防护 价值输出

“有价值”的威胁情报

- 用户业务场景相关的或者用户真实关心的
- 用户可以应用于自身场景并解决问题

仿冒

拦截马

钓鱼

有效防护 价

组织:中国建设银行 组织安全指数: 70.94

威胁事件排名

恶意木马	34 k
仿冒篡改应用	113 k
钓鱼URL	56 k
拦截马	6 k

组织:民生银行 组织安全指数: 73.73

威胁事件排名

恶意木马	5 k
仿冒篡改应用	7 k
拦截马	1 k
钓鱼URL	563

组织:浦发银行 组织安全指数: 73.77

威胁事件排名

恶意木马	3 k
拦截马	618
仿冒篡改应用	17
钓鱼URL	12

组织:湖北银行 组织安全指数: 73.55

威胁事件排名

恶意木马	47
拦截马	19
钓鱼URL	10
仿冒篡改应用	0

组织:中国工商银行 组织安全指数: 71.06

威胁事件排名

恶意木马	41 k
钓鱼URL	39 k
仿冒篡改应用	16 k
拦截马	8 k

组织:招商银行 组织安全指数: 73.68

威胁事件排名

恶意木马	20 k
钓鱼URL	58 k
拦截马	4 k
仿冒篡改应用	383

威胁情报服务形态

SAAS模式

- 不仅需要获得威胁情报，并且能够自助发现
- 交互、流程

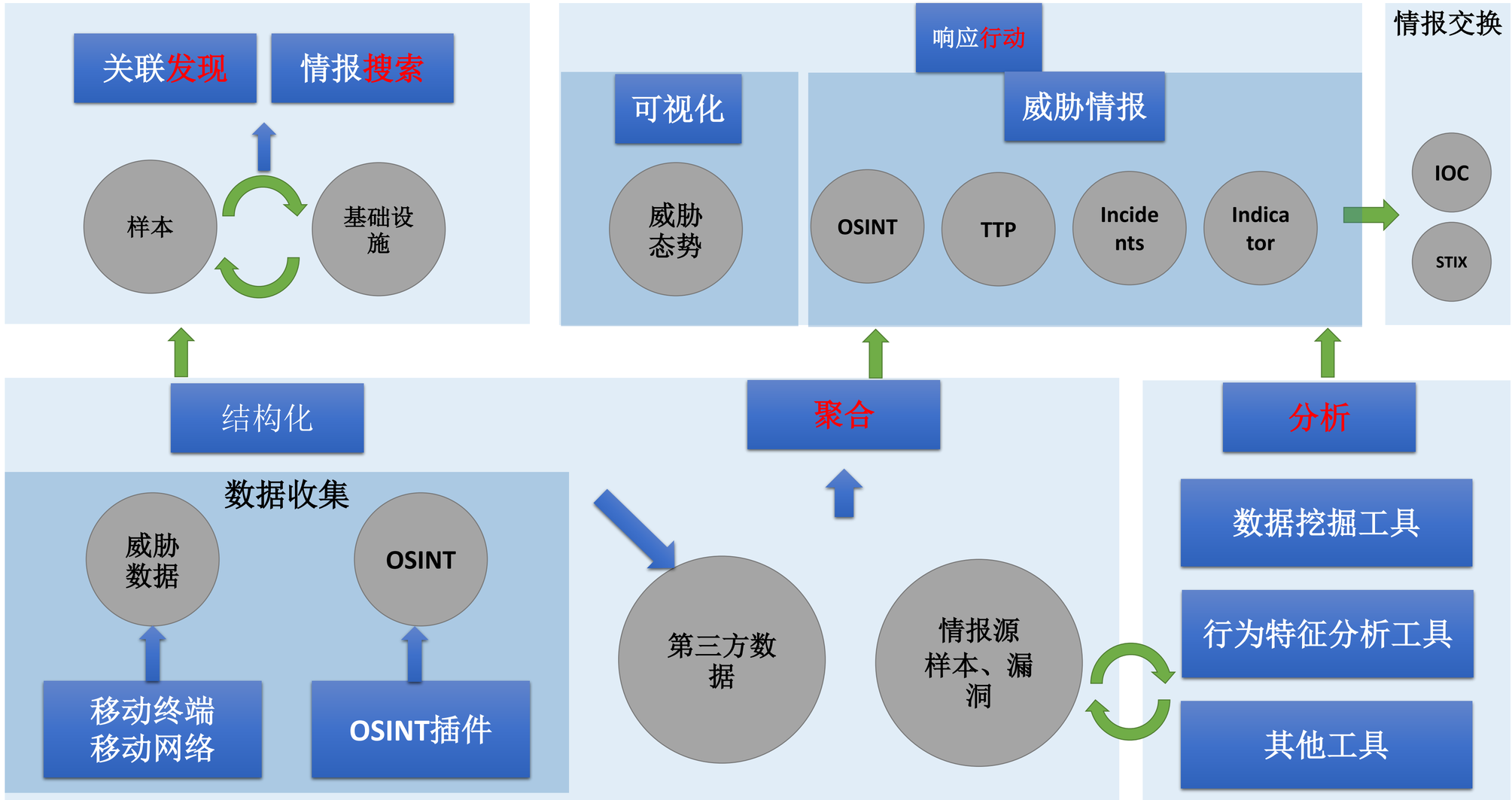
PAAS模式

- 企业私有数据的管理和处理和面向企业内部的威胁情报流转和输出
- 满足私有云部署
- 交互、流程

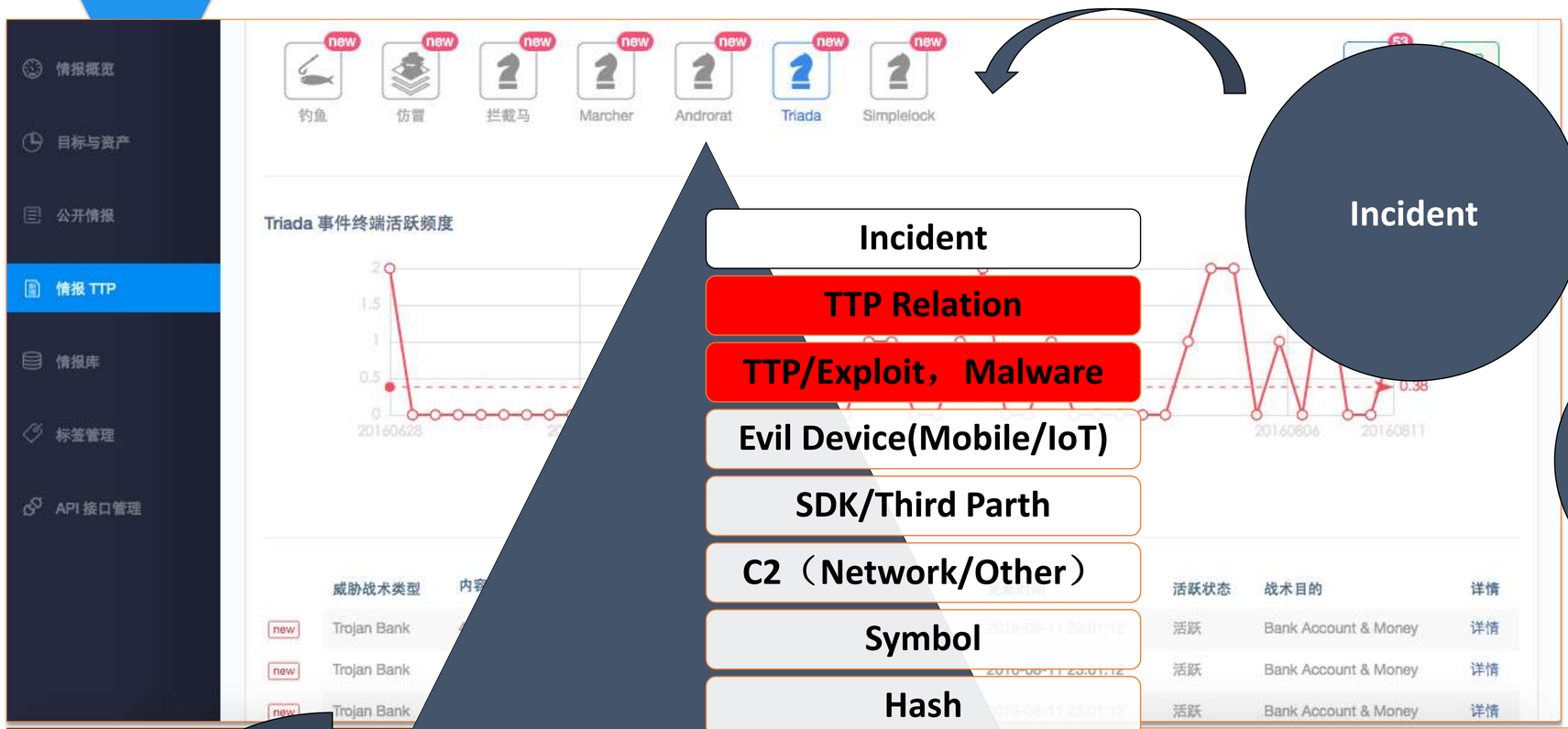
DAAS模式

- 需要威胁情报结果和企业内部数据的碰撞
- 抛弃部署的复杂性

威胁情报平台架构


关联发现
情报搜索
样本
基础设施
响应行动
可视化
威胁情报
威胁态势
OSINT
TTP
Incidents
Indicator
情报交换
IOC
STIX
结构化
聚合
分析
数据收集
威胁数据
OSINT
移动终端
移动网络
OSINT插件
第三方数据
情报源
样本、漏洞
数据挖掘工具
行为特征分析工具
其他工具

威胁情报价值金字塔



Incident

TTP Relation

TTP/Exploit， Malware

Evil Device(Mobile/IoT)

SDK/Third Parth

C2（Network/Other）

Symbol

Hash

Incident

Victim

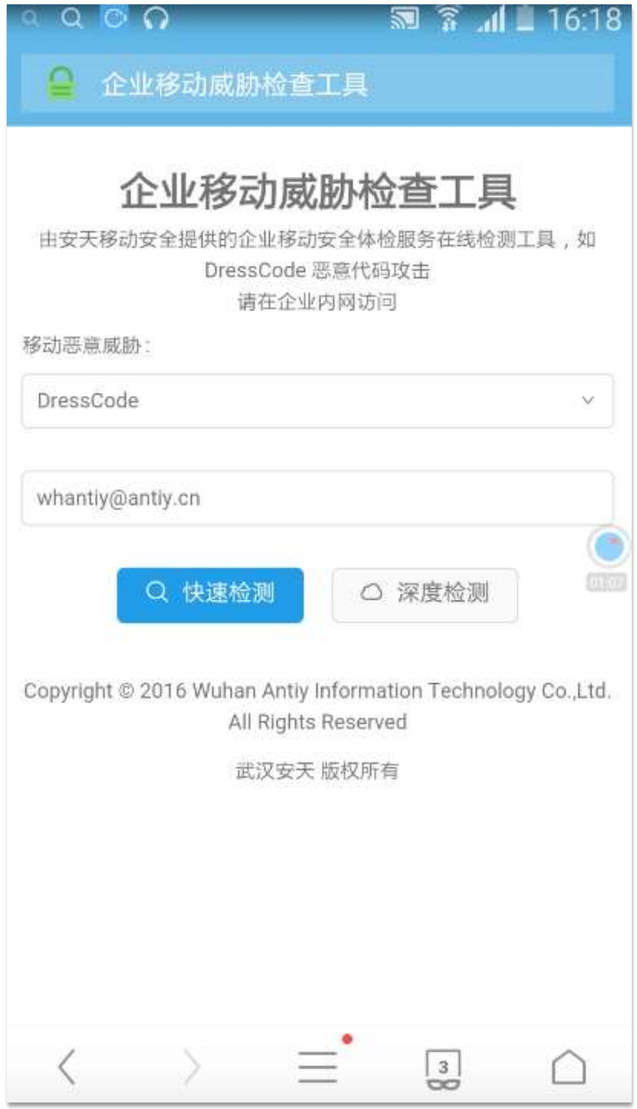
Indicator

Threat Actor

屡屡见诸报端的APT小组
Fancy Bear又名APT 28, Pawn Storm, Sednit, Sofacy。近几年来，这个APT以各种身份出现在各种攻击事件中：
2015年8月，电子前哨基金会声称遭到了Fancy Bear的钓鱼攻击。
今年6月，Pawn Storm被发现攻击4000个Google账户。
今年9月，Palo Alto的研究人员发现Fancy Bear小组使用Mac恶意软件对航空行业发起攻击。
而在今年的美国大选期间，该组织还攻击了民主党基金会，泄露了大批文件，影响了美国大选。
此次攻击中，黑客编写恶意程序用于跟踪乌克兰炮兵部队的地理位置并监听通信。这些情报很可能被乌克兰东部的亲俄派
量用来发动攻击。
调查经过
2016年夏季，CrowdStrike公司的研究人员们开始调查‘Пｏｎｐ-Д30.apk’ (MD5: 6f7523d3019fa190499f32721
可疑安装包。
用手机从锁定的计算机中偷取凭证...
添加为 域名
添加为 端口
添加为 邮箱
添加为 电话号码
添加为 用户名
添加为 密码
添加为 包名
添加为 Bundle ID
添加为 证书
添加为 SHA1
添加为 标题
添加为 MD5
添加为 URL
添加为 IP
添加为 检出名
添加为 .....
添加自定义字段
关联搜索

我的情报库
自定义字段
搜索
标题
日期
2016/12/04
至
2017/01/03
搜索
我的情报库
导出
序号
ID
标题
时间
操作
全选
1
16122995492497
Switcher: Android joins the 'attack-the-route...
2016-12-29 11:18:43
详情
2
16122887310967
俄罗斯APT小组利用Android木马追踪乌克兰...
2016-12-28 21:03:24
详情
首页
尾页
1
/ 1
GO

企业移动威胁检查工具


16:18
企业移动威胁检查工具
企业移动威胁检查工具
由安天移动安全提供的企业移动安全体检服务在线检测工具，如
DressCode 恶意代码攻击
请在企业内网访问
移动恶意威胁：
DressCode
whantiy@antiy.cn
快速检测
深度检测
Copyright © 2016 Wuhan Antiy Information Technology Co.,Ltd.
All Rights Reserved
武汉安天 版权所有

16:18
企业移动威胁检查工具
企业移动威胁检查工具
由安天移动安全提供的企业移动安全体检服务在线检测工具，如
DressCode 恶意代码攻击
请在企业内网访问
内网设备存在风险
感染时间: 2016/12/16 13:56:39
知道了
Copyright © 2016 Wuhan Antiy Information Technology Co.,Ltd.
All Rights Reserved
武汉安天 版权所有
01:12
-00:45

感谢大家参与本次交流