网络空间威胁对抗与态势感知研讨会
暨 第六届安天网络安全冬训营

“三高”网络环境中与敌手的“隔空对决”

安天应急响应中心

战术型态势感知指控积极防御
协同响应猎杀威胁运行实战化

铁流鏖戰

提纲

01 与敌手在“三高”网络中“隔空对决”

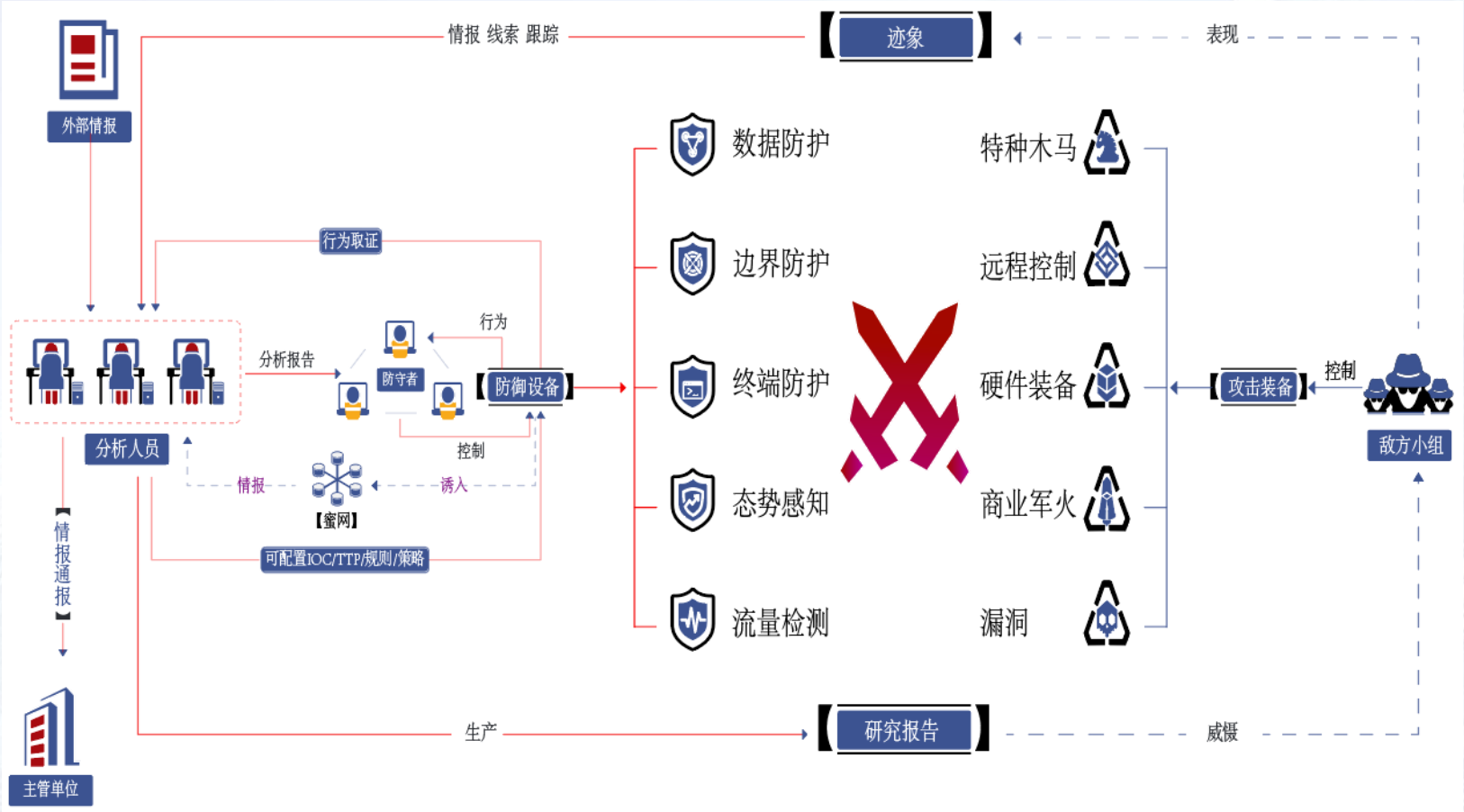
“隔空对决”需要跟踪威胁、掌握敌情 02

03 “隔空对决”需要建立什么？

如何与敌手在网络中“隔空对决” 04

01 与敌手在“三高”网络中“隔空对决”

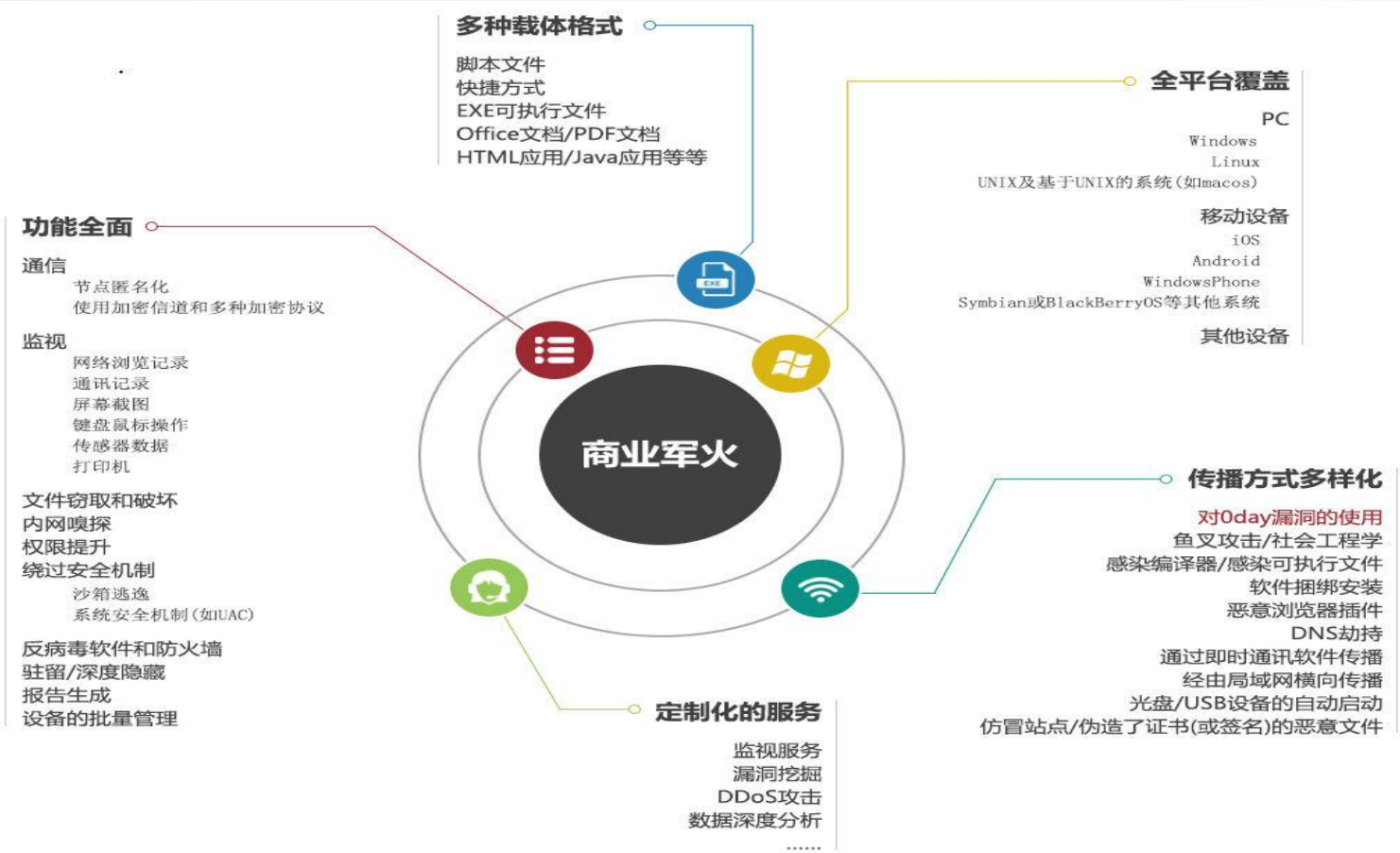
与敌手在“三高”网络中“隔空对决”



02 “隔空对决”需要跟踪威胁、掌握敌情

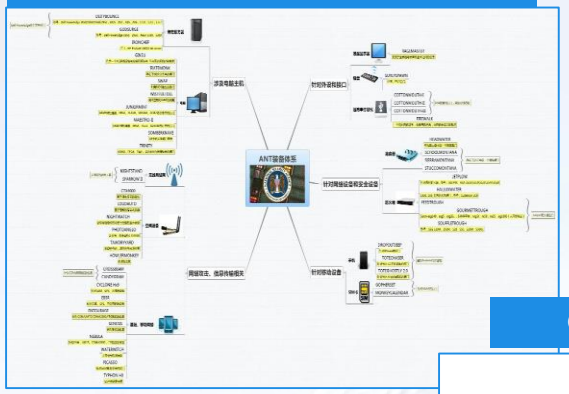
需要对威胁事件的跟踪
需要对国家行为体能力研究

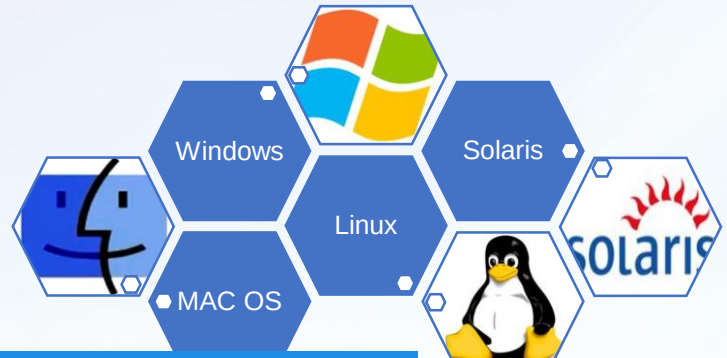
网络威胁中的商业军火覆盖面



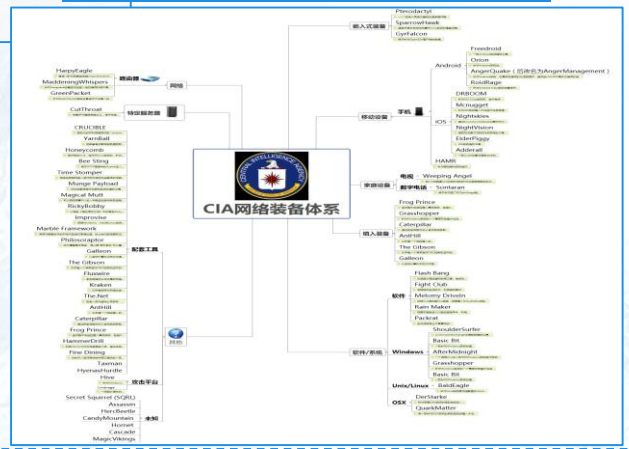
装备体系覆盖全场景、全平台

NSA的ANT攻击装备谱系（截止到2012）





CIA的攻击装备谱系（2016）

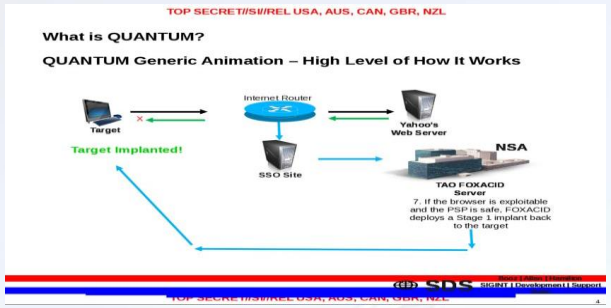


信息	Windows	Linux	Solaris	Oracle-owned Unix	FreeBSD	Mac OS
安天：修改硬盘固件的木马 探索方程式（EQUATION）组织的攻击组件[3]	分析样本载荷和硬盘持久化能力					
安天：方程式（EQUATION）部分组件中的加密技巧分析[4]	分析加密算法					
安天：EQUATION 攻击组织的全平台载荷能力解析（本报告）		曝光存在，分析相关载荷	分析相关载荷			
The Hacker News：《Shadow Brokers reveals list of Servers Hacked by the NSA》			曝光存在	曝光存在	曝光存在	
卡巴斯基：Equation: The Death Star of Malware Galaxy[5]	揭秘方程式攻击组织					
卡巴斯基：A Fanny Equation: "I am your father, Stuxnet"[6]	Fanny 组件分析					
卡巴斯基：Equation Group: from Houston with love[[7]	Doublefantasy 分析					
卡巴斯基：《EQUATION GROUP: QUESTIONS AND ANSWERS》[8]	方程式组织问与答					根据网络特征提出猜测

注：安天在 Solaris 样本中分析出的 User Agent 具有 Solaris 标识，而卡巴斯基在“EQUATION GROUP: QUESTIONS AND ANSWERS”[8]中披露出曾捕获到 Mac OS X 的 User Agent 的信息，由此来看，尽管安天和卡巴斯基厂商目前都尚未捕获 Mac OS X 的样本，但方程式组织针对 MAC OS X 的攻击载荷是真实存在的。

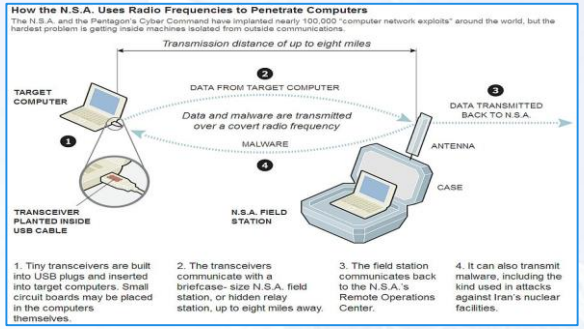
图文来源：安天技术报告《从方程式到“方程组”EQUATION攻击组织高级恶意代码的全平台能力解析》

高单点突破和横向移动能力



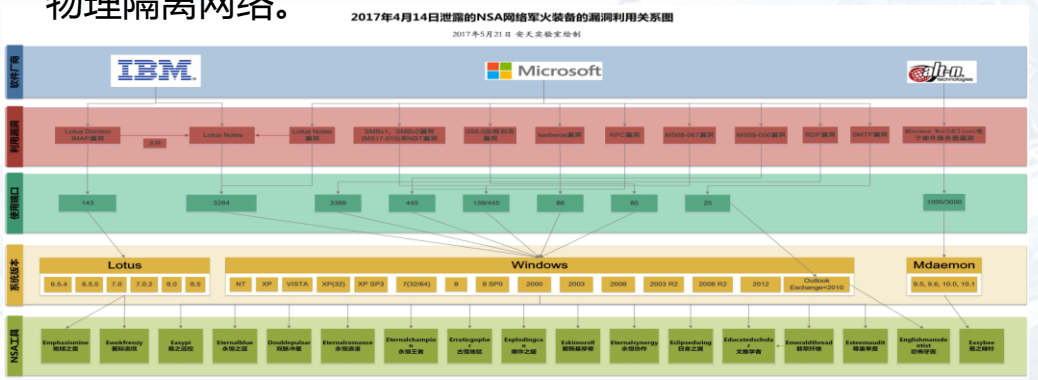
通过浏览器侧大量0day漏洞储备，支撑对互联网目标精准打入能力。亦支撑内网用户打击。

(TS//SI//NF) Left: Intercepted packages are opened carefully; Right: A "load station" implants a beacon



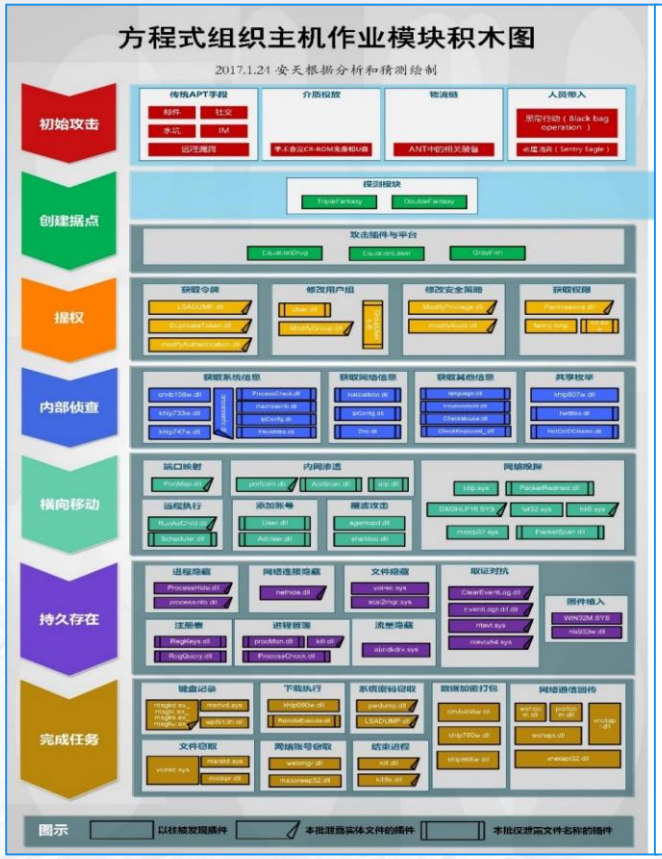
系列装备结合物流链劫持，供应链植入，人员带入等方式，突破物理隔离网络。

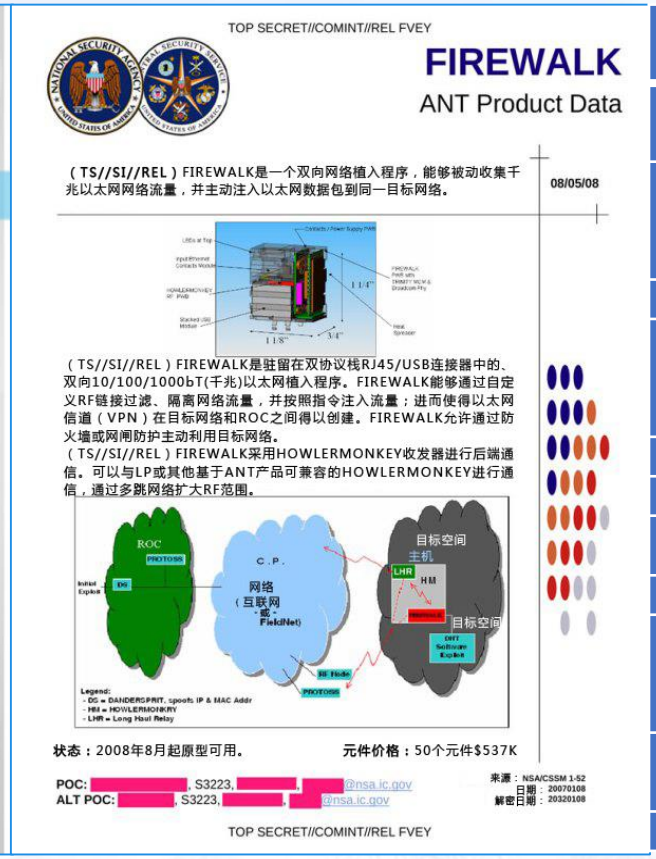
结合人员社会活动入侵重点人员



大量针对开放端口服务的0day漏洞储备，支撑横向移动能力。

功能原子化的积木式木马、精细的作业控制





发包数据第一字节	功能	回包数据第一字节	含义
0x42（B）	清理感染痕迹，删除自身	0x61(a)	收集系统详细信息，大概20类，在上文中对不同系统有过说明
0x4A（J） 0x92（不可显字符）	创建文件	0x42(B)	删除文件成功
0x44（D）	写入文件	0x43(C)	写文件成功
0x56（V） 0x95（不可显字符）	执行文件	0x44(D)	读取文件
0x53（S）	读取文件回传	0x47(G)	创建文件成功
0x4B（K）	设置读取文件指针	0x55(U)	读取完成
0x60（’）	收集大量信息回传	0x71(q)	指令执行失败（多个指令失败，都返回此代码）
0x70（p）	更新样本配置信息	0x73(s)	设置文件偏移成功
0x75（u）	更新样本sleep时间，并重新收集信息回传	0x74(t)	执行文件失败
0x76（v） 0xA2（）	更新远程C&C	0xa1()	更新远程C&C
0x80（）	删除指定文件		

配图：引自安天针对方程式攻击组织的系列分析报告之《方程式组织EQUATION DRUG平台解析》

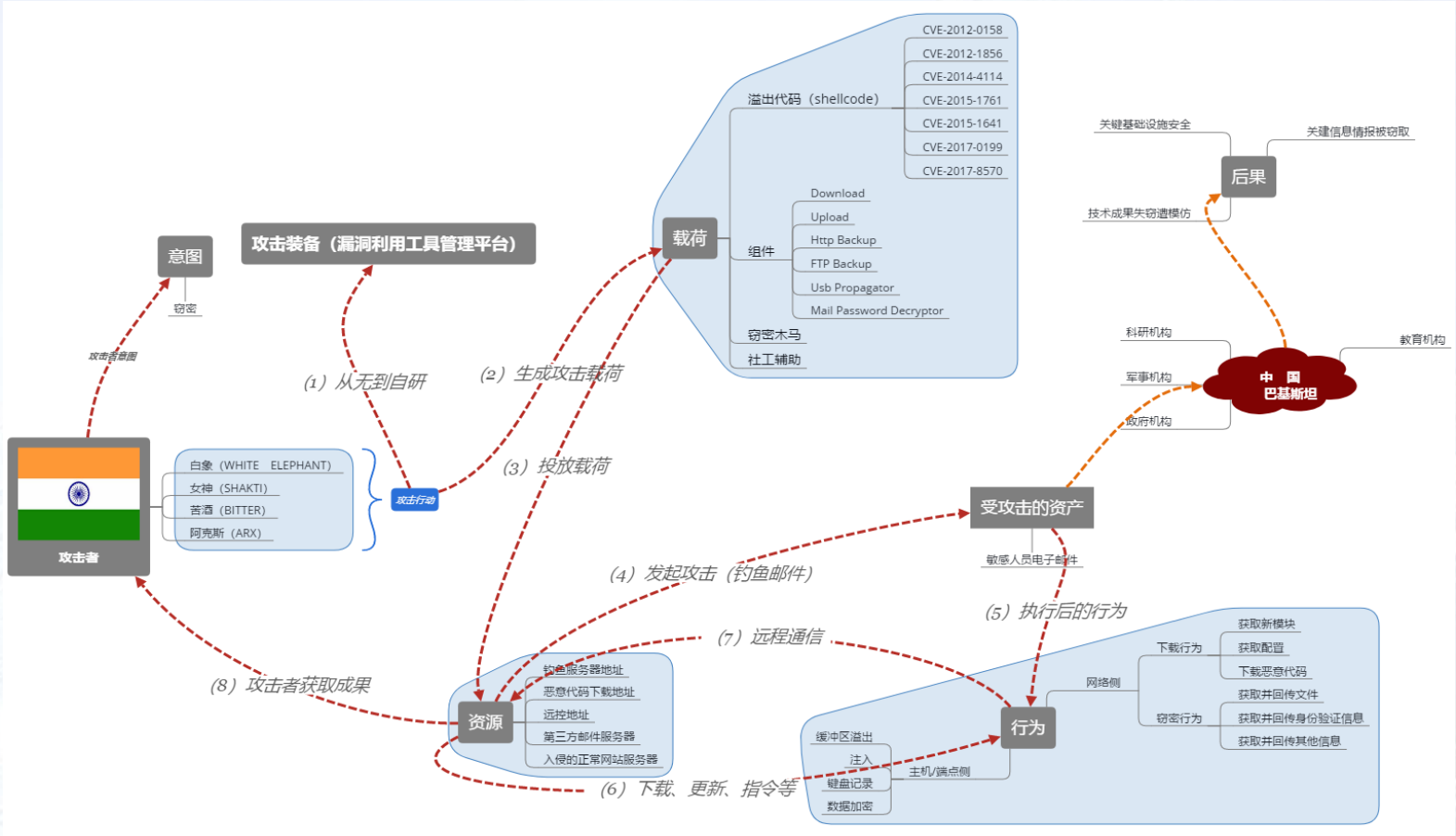
全球APT攻击组织、行动来源分布

APT攻击组织或行动的数量180+
样本数量10000+
涉及的网络地址（C2、诱饵地址、下载地址等）12000+
涉及国家数量为14个，地区数量为3个，其中有1/3的组织或行为无法确定

对威胁事件的跟踪——一般能力国家行为体作业能力

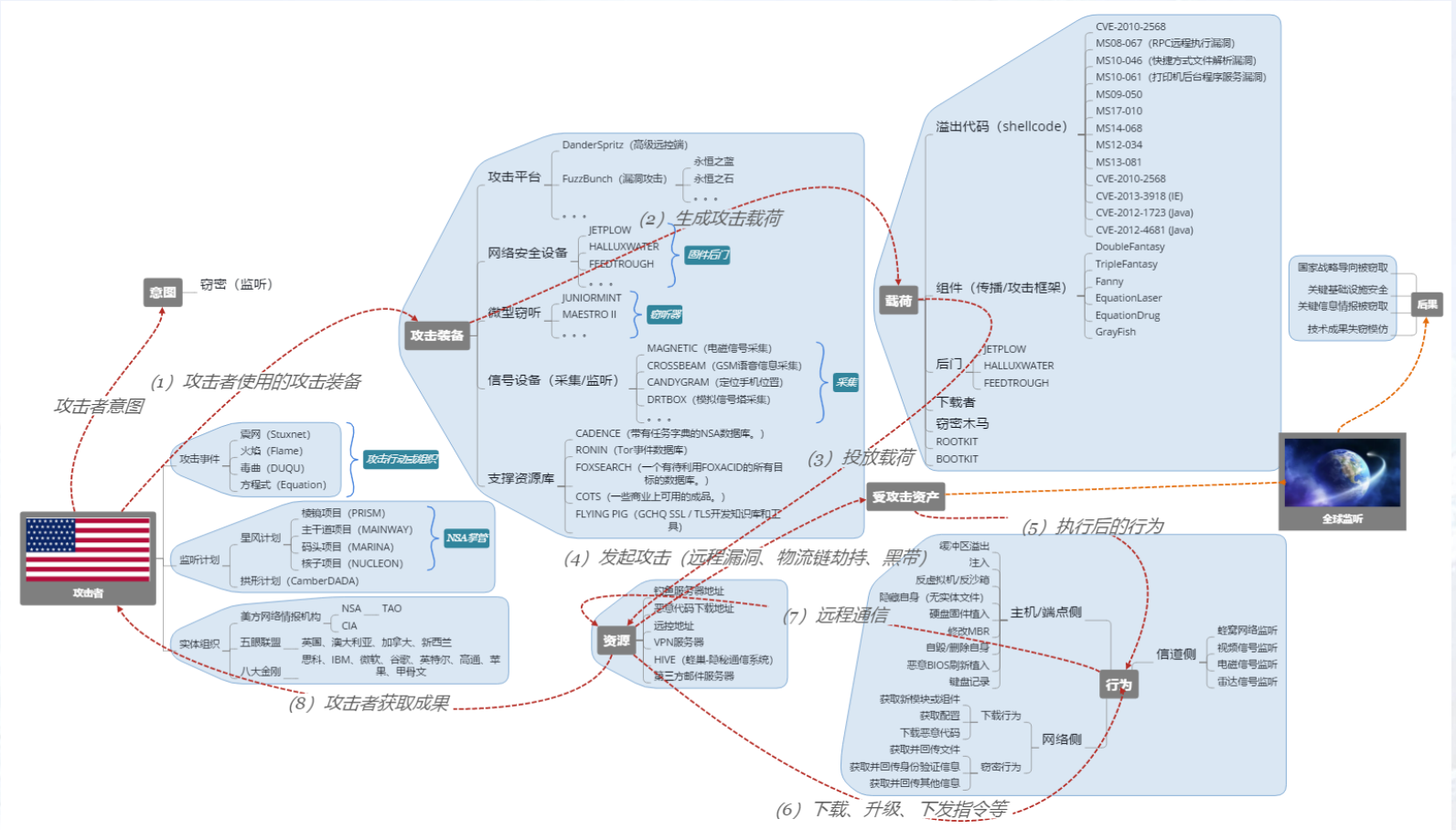
历史上象群作业能力达不到渗透高等防护网络内，但目前很多高信息价值网络并没有达到高防护等级和高信息对抗防御

样本hash数量：
1300+
C2域名/IP：191+，
其中域名120+个，
IP数量71+个



对威胁事件的跟踪——超高能力国家行为体作业能力

方程式：
样本HASH数量：600+
C2域名/IP：144+



从网络的高对抗视角看不同攻击方能力层次

层次	组织	整体能力	我们能做到什么
超高能力 国家/地区行为体	方程式（美）、毒曲（以）等	超级攻击组织，拥有最强的系统化和体系装备。 作业是谨慎和受控的，具有高度隐蔽性，难以分析追溯。	对获得的有限的其投放样本进行分析，根据泄露出的一些信息进行作业复现。
高级能力 国家/地区行为体	破烂熊、沙虫等	拥有高级能力的单兵精英团队， 拥有较高水平的恶意代码和漏洞利用程序。 作业是相对谨慎和受控的。作业相对隐蔽。 与民间能力有深度互动机制。	对其样本进行相对完整的分析，对其作业过程进行沙盘推演分析。
一般能力 国家/地区行为体	白象2（印）、绿斑等	有一定能力的攻击组织。 使用水平不高的自研恶意代码和商业漏洞。 作业相对容易暴露。	可以根据事件线索快速提炼其整个攻击资源，对其攻击作业链进行相对完整的分析。
一般能力 国家/地区行为体	白象1（印）、海莲花等	一般化能力攻击组织 作业是普遍的和失控的。	可以不依赖外部线索捕获其攻击，可以深度分析其比较完整的作业链条，作业回路。基于开放式情报的追踪溯源画像攻击组织，部分可以关联到自然人。

网络安全威胁我们必须考虑到的因素

任何单点环节均可能失陷或失效，包括网络安全环节本身。

高级威胁行为体有突破目标的坚定意志、充足资源、成本准备。并进行体系化的作业。

信息系统规划、实施、运维的全过程，都是攻击者的攻击时点。

防御者所使用的所有产品和环节同样是攻击方可以获得并测试的。

攻击者所使用的攻击装备有极大可能是“未知”的，这种未知是指其因在局部和全局条件下，对于防御方、和防御方的维护支撑力量（如网络安全厂商）来说，是一个尚未获取或至少不能辨识的威胁。

03 隔空对决需要建立些什么?

需要建立威胁分析团队与技术体系

需要建立多维度信誉资源库支撑对威胁的跟踪分析

需要建立威胁分析团队与技术体系

高级威胁分析师、恶意代码分析师、取证分析师、工具开发师、大数据分析师和响应处置分析师等

网络协议分析、加密解密技术、内存取证、数据库取证、固件取证、数据恢复、情报分析、逆向分析等等

需要建立多维度信誉资源库支撑对威胁的跟踪分析

04 如何与敌手在网络中“隔空对决”

如何发现敌手的活动
威胁分析过程与取证
对威胁事件进行处置
展开全网威胁猎杀

“三高”网络环境特点

高信息价值、高威胁对抗、高防护等级
特点：复杂、高能力对手高度关注

APT事件	目的和行为	技术特点	网络通信特点
震网	破坏伊朗核设施	针对工业控制系统，多个漏洞利用，战场预制	0Day漏洞，U盘感染，内网传播，构建第二信道
Duqu	机密信息窃取	Word 漏洞溢出文档，远程控制，生命周期自定义	80、443端口通信，服务器ssl通信，P2P命令控制
Flame	选择性信息窃取	合法软件伪装，利用Windows漏洞，证书伪造	利用端口22,80,443 利用ssl通信，服务器证书自签名
象群	机密信息窃取	Word 漏洞溢出文档，远程控制，生命周期自定义	80、443端口通信，服务器ssl通信
海莲花	机密信息窃取	商业军火，Word 漏洞溢出文档，证书伪造	利用端口22,80,443 利用ssl通信
方程式	机密信息窃取	高持久化、硬盘固件植入、多个漏洞利用	隐蔽通信

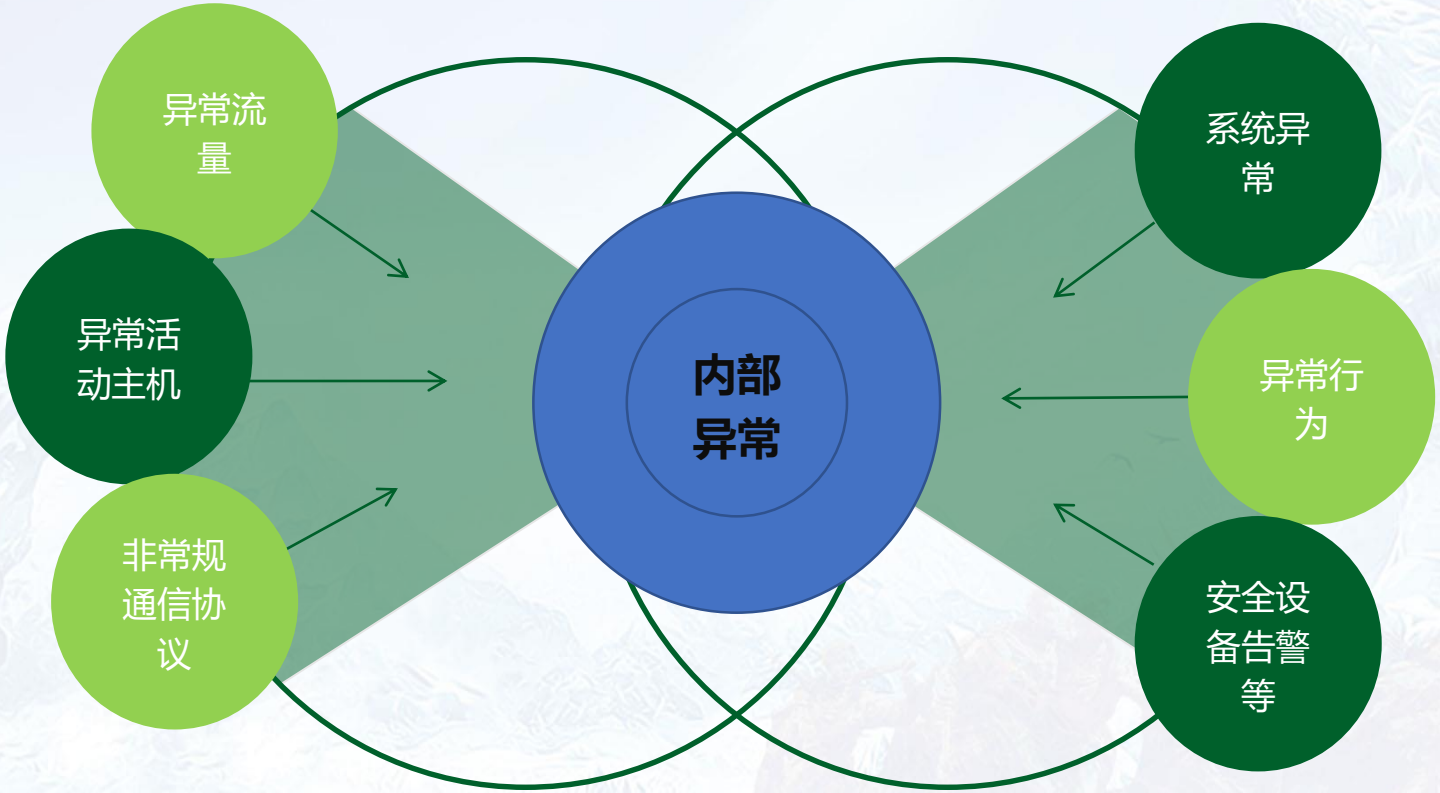
纯内网环境

可上公网的办公环境

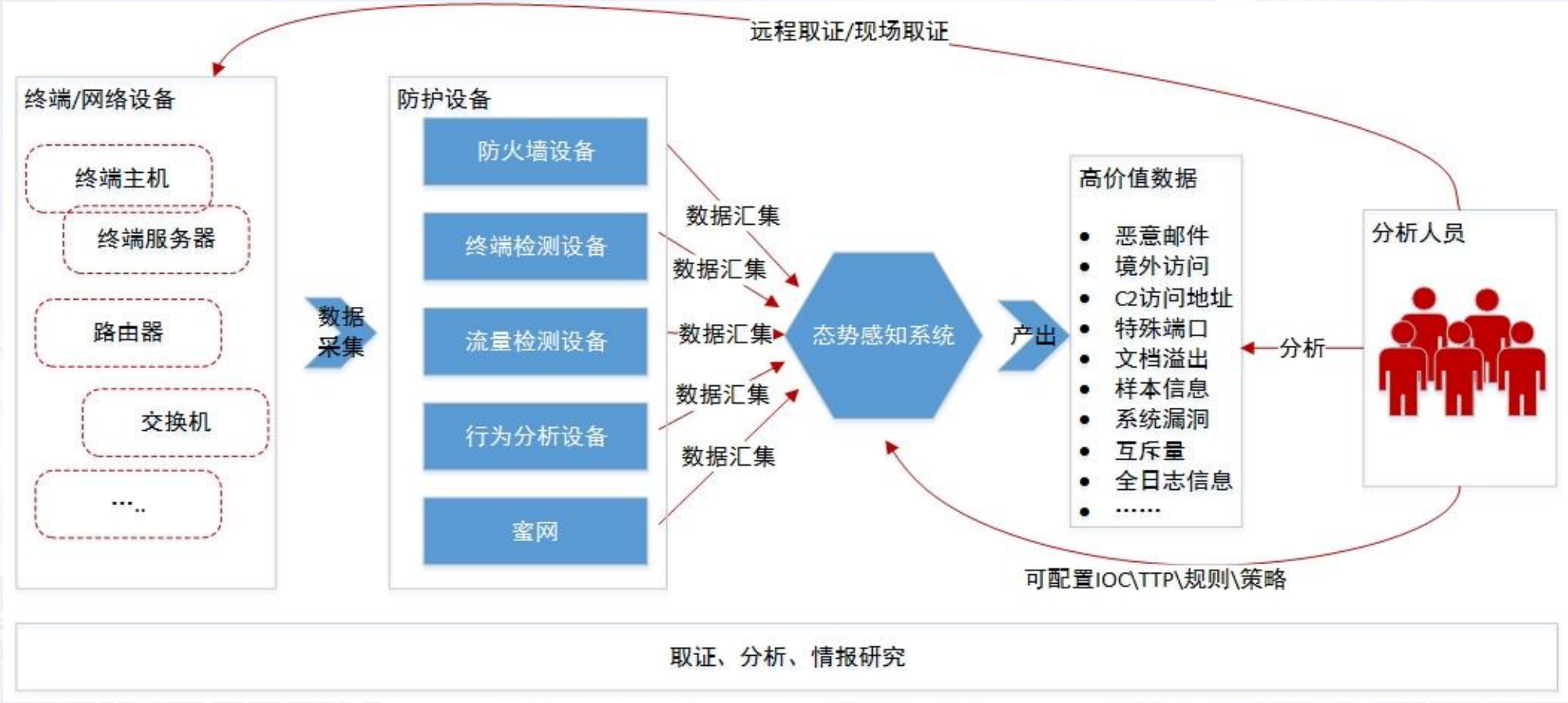
BYOD场景

“三高”网络环境下威胁猎杀过程

发现敌手的活动——内部异常



发现敌手的活动——内部事件发现、取证、分析与情报研究

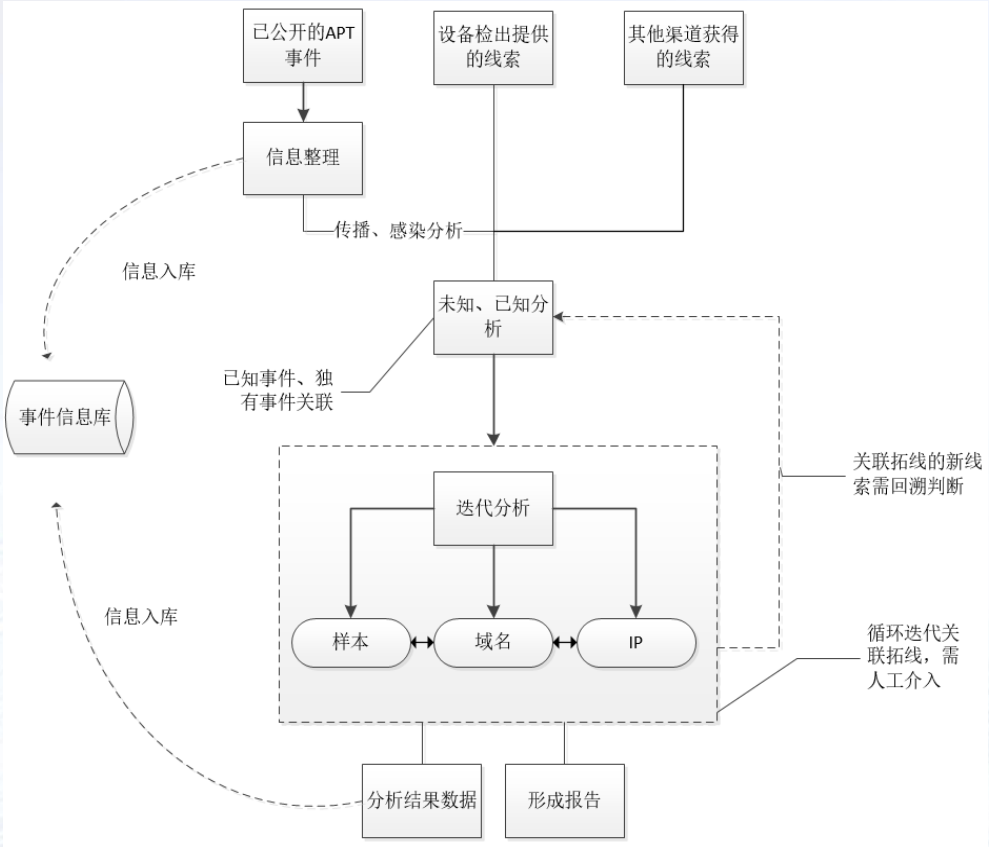


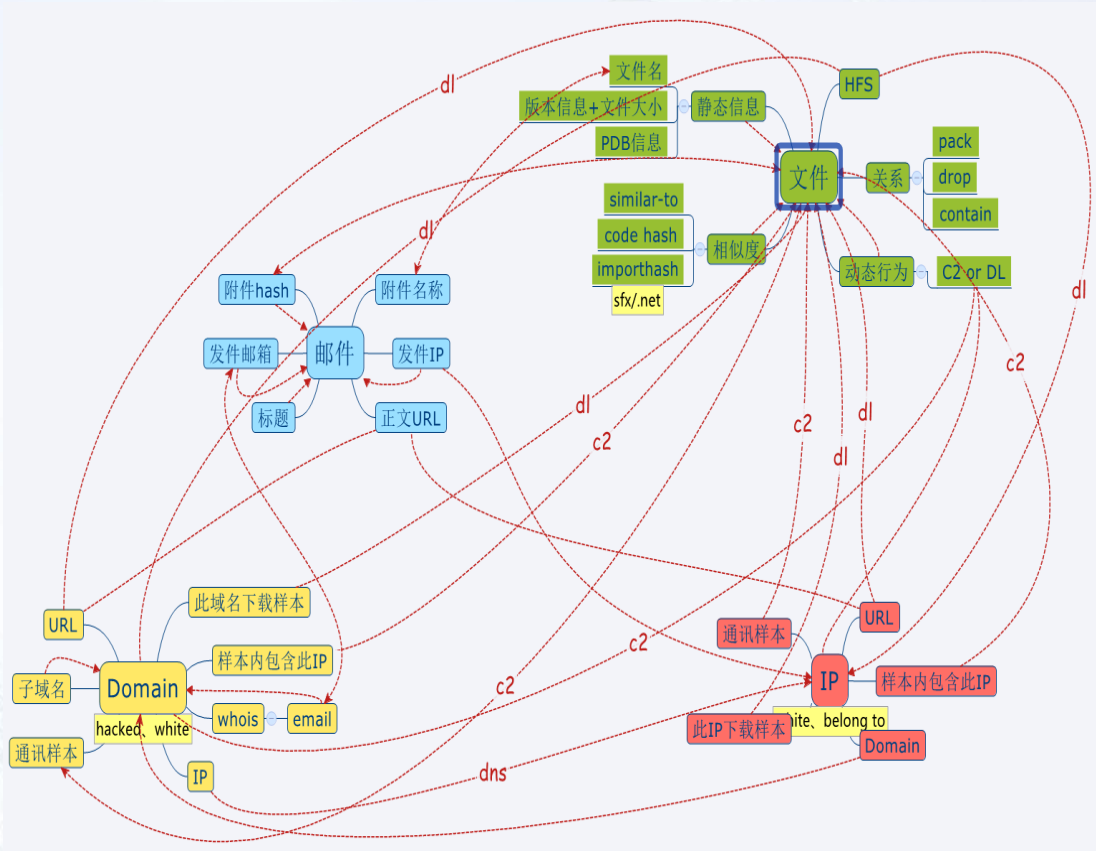
发现敌手的活动——外部情报收集

全向量提取：

- ✓ 特定字符串
- ✓ 版本信息
- ✓ 编译路径
- ✓ 加密算法
- ✓ 特定API
- ✓ 代码片段
- ✓ 特征片段
- ✓ .....

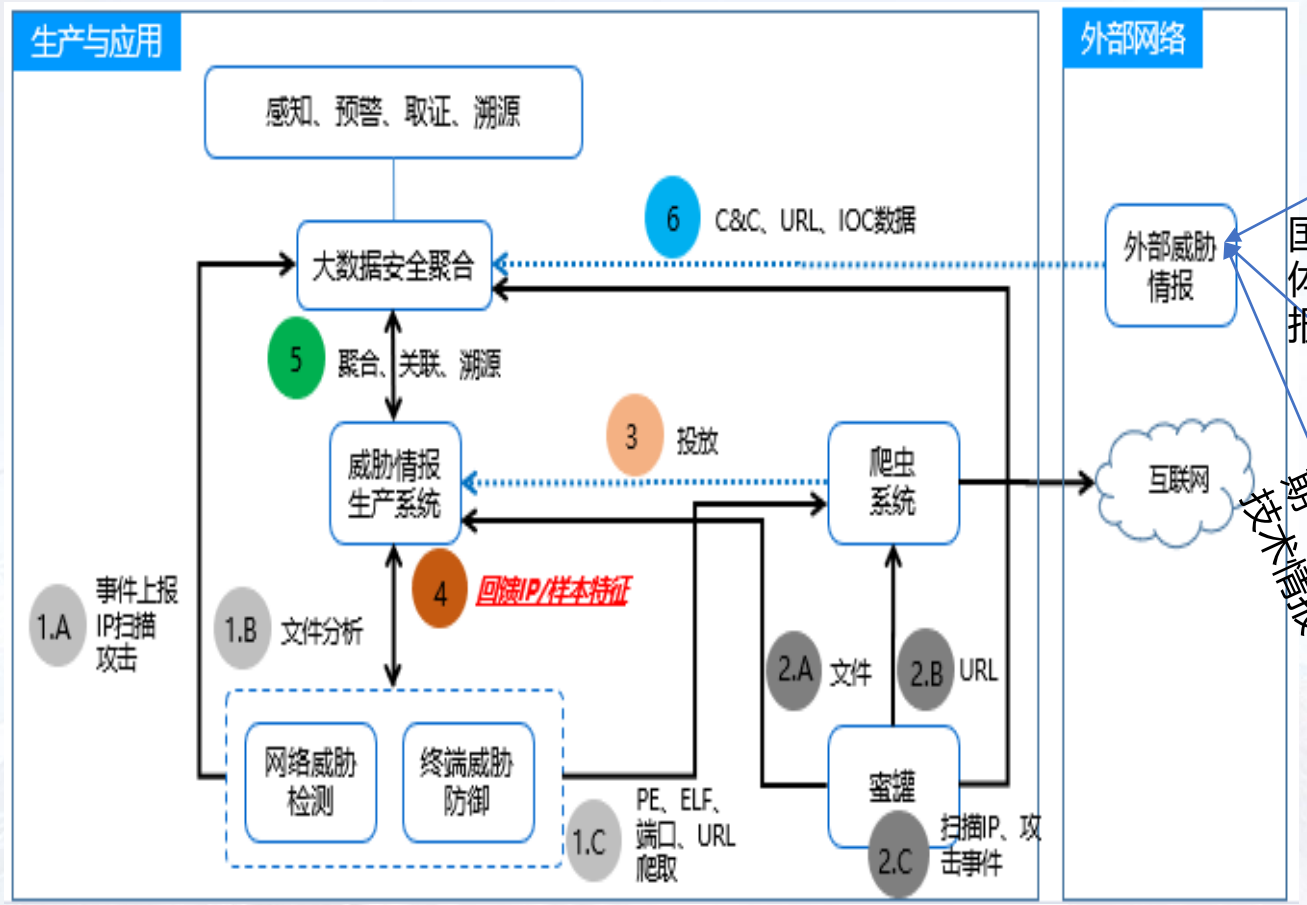
发现敌手的活动——情报分析





关联拓线分析流程

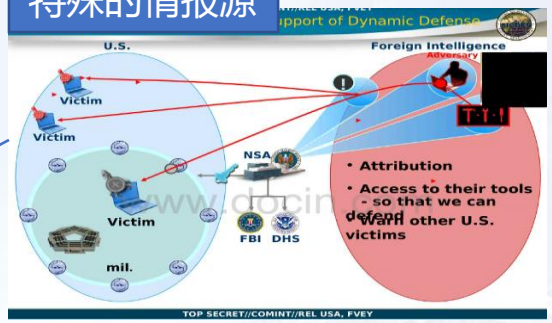
发现敌手的活动——威胁情报生产与应用

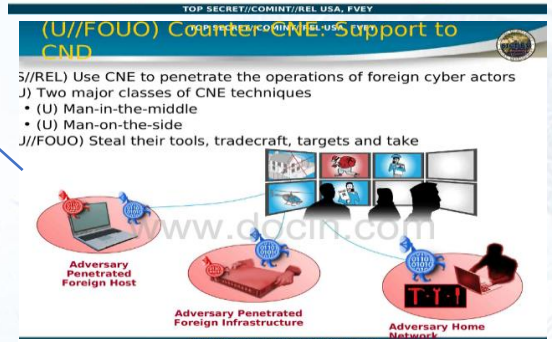


国家行为体威胁情报

开源基础软件生命周期技术情报

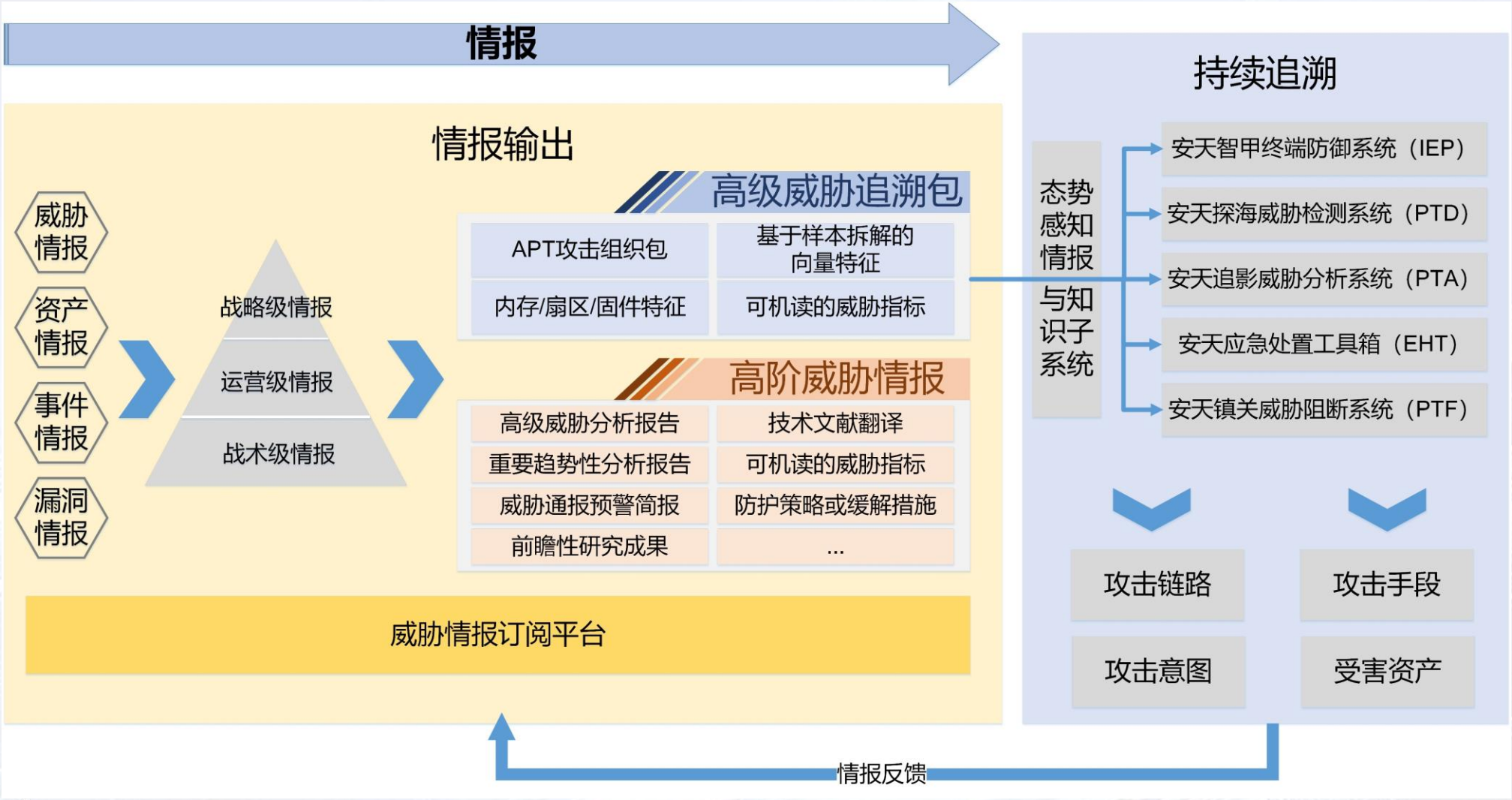
特殊的情报源



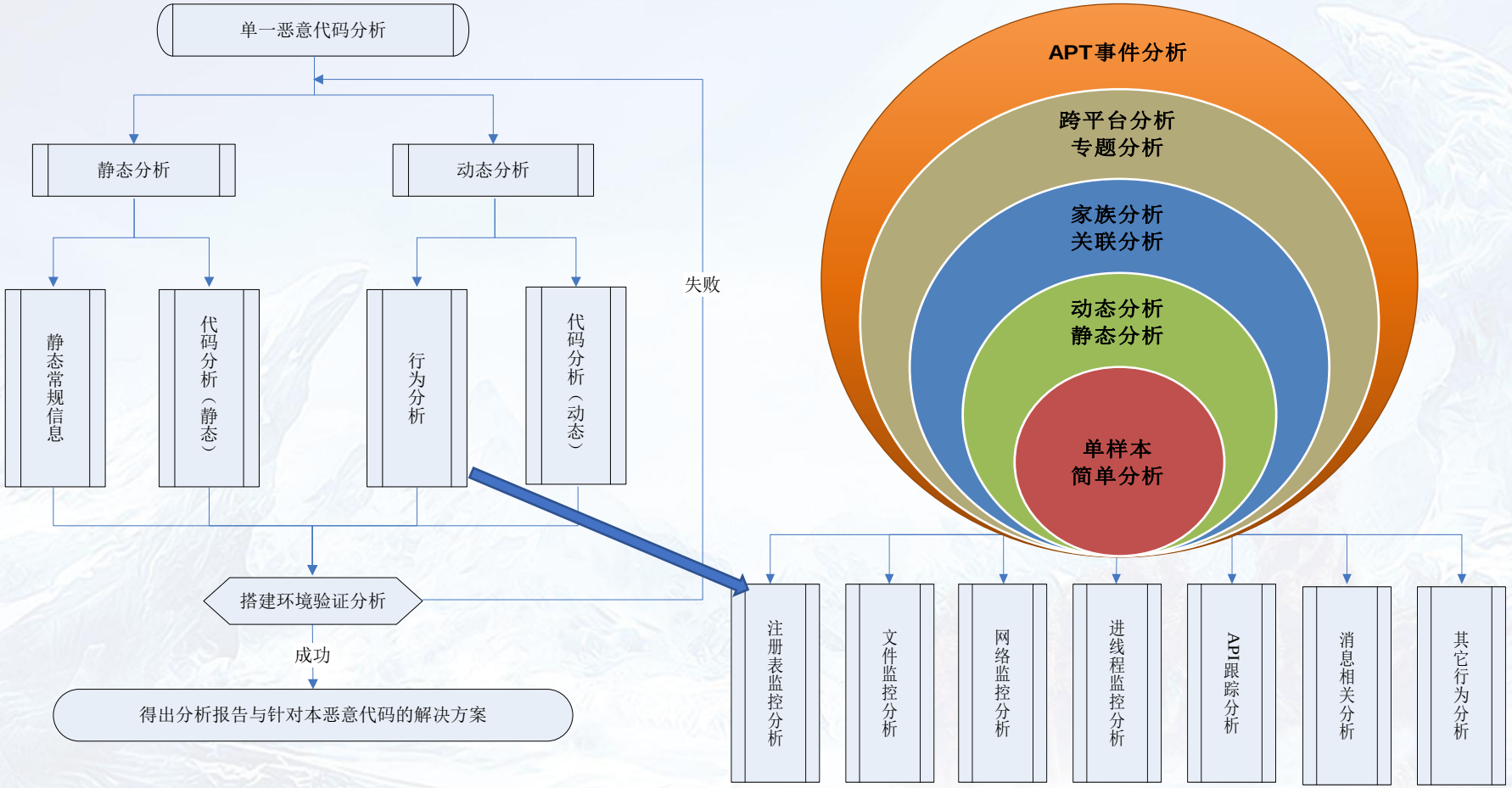


发现敌手的活动——细化情报的应用

威胁情报输出

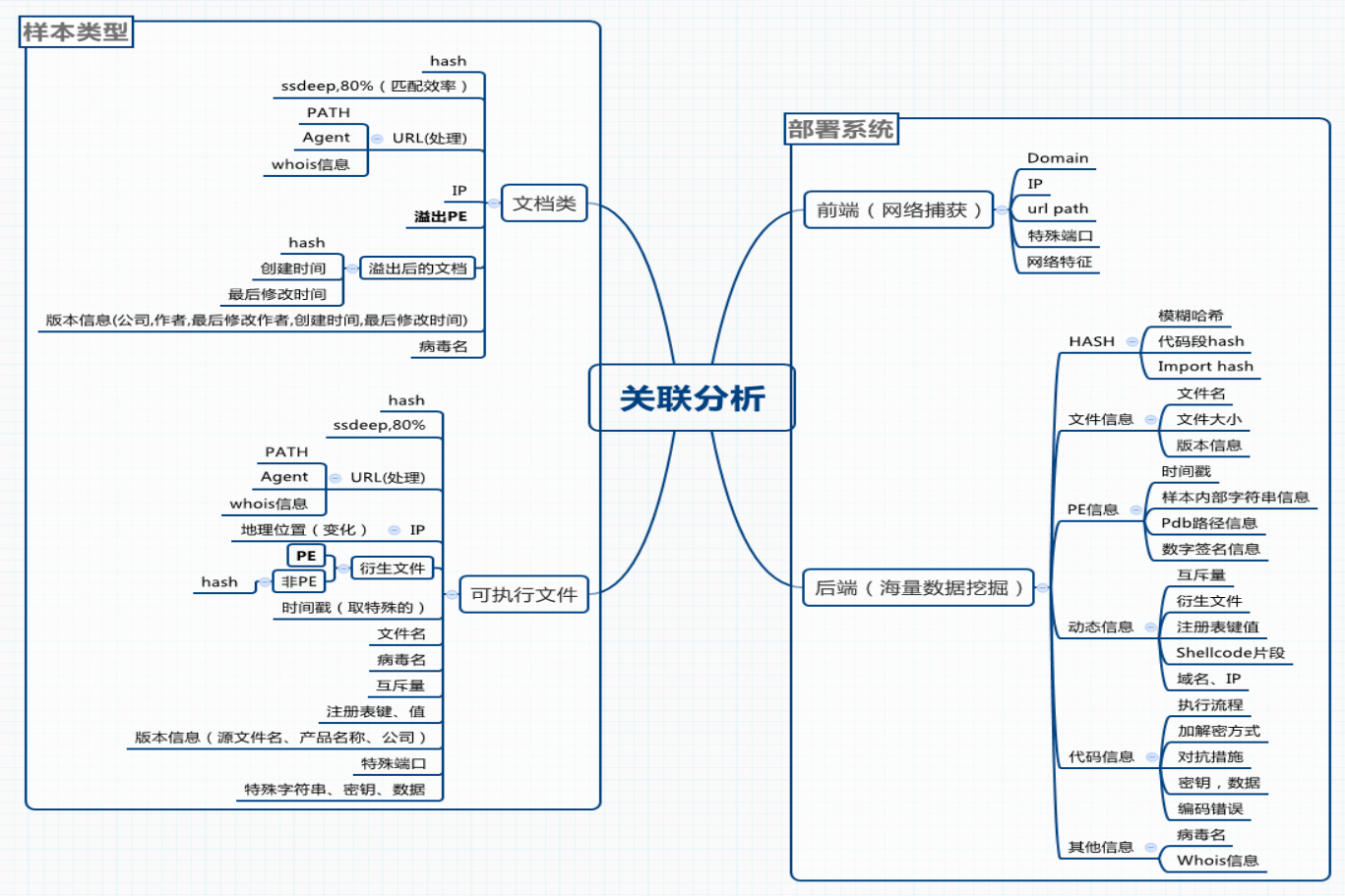

情报
情报输出
威胁情报
资产情报
事件情报
漏洞情报
战略级情报
运营级情报
战术级情报
高级威胁追溯包
APT攻击组织包
基于样本拆解的向量特征
内存/扇区/固件特征
可机读的威胁指标
高阶威胁情报
高级威胁分析报告
技术文献翻译
重要趋势性分析报告
可机读的威胁指标
威胁通报预警简报
防护策略或缓解措施
前瞻性研究成果
...
威胁情报订阅平台
持续追溯
态势感知情报与知识子系统
安天智甲终端防御系统（IEP）
安天探海威胁检测系统（PTD）
安天追影威胁分析系统（PTA）
安天应急处置工具箱（EHT）
安天镇关威胁阻断系统（PTF）
攻击链路
攻击手段
攻击意图
受害资产
情报反馈

威胁分析过程与取证——样本分析传统流程及演进



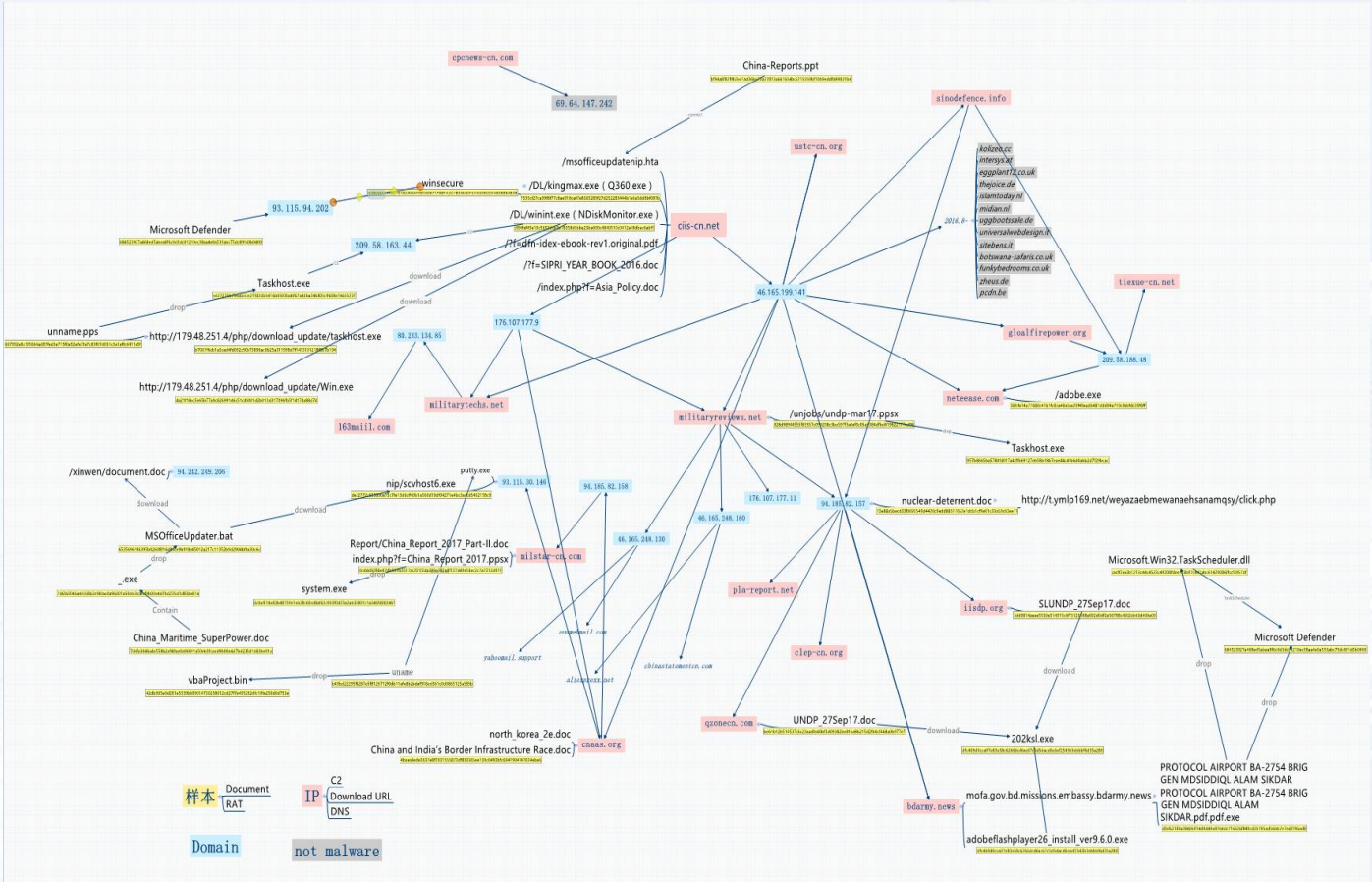
细节关联与拓线揭示出威胁隐匿行为的痕迹

- 密钥
- 协议
- 算法
- 代码
- BUG



通过多维度的溯源分析威胁的行动轨迹

- 传统域名IP溯源
- Whois信息溯源
- 注册邮箱溯源
- 通IP关联信息溯源
- 时区分析判定溯源
- 语言分析判定溯源
- 编译用户ID分析判定溯源
- ……



网络威胁数据分析

对网络中非常规协议、后门上线协议、控制协议、攻击协议、周期性访问境外C2、与协议不匹配等

对特殊数据、加密数据、隐写数据、流量伪装、隐蔽通道等数据进行分析

分析访问日志、事件日志、告警日志、异常日志和其它可疑记录等

访问境外、上传数据、隐秘通讯、即时通信行为、间断性访问白域名行为等进行分析

边界设备威胁分析

具有针对不同架构下系统内存取证分析能力，目前高级威胁形为体的技术能力，已经不只是windows系统，对多平台的攻击也越来越多。

高级威胁形为体的技术能力早前几年前就将攻击方向转成固件，像方程式作业中使用的持久化能力植入硬盘固件，还有一些IOT设备中出厂就带有后门，对固件的分析是必须的。

对于一些边界设备系统日志往往是被忽略的，如攻击者最开始的目标就是边界设备，哪么系统日志就必须纳入分析对像。 NSA方程式组织攻击中东地区最大的SWIFT提供商EastNet，就是最先攻击的边界设备。

对威胁事件进行处置


自动化处置工具
定制化处置工具
安全加固方案
恢复方案
可配置的IOC/TTP/策略
恶意代码定点清除
网络流量阻断
安全加固
系统配置恢复
业务恢复
数据恢复
威胁反制

展开全网威胁猎杀

最少见数据流量；

有规律的数据流量；

非常规通信协议；

非常规文件格式；

境外数据；

.....

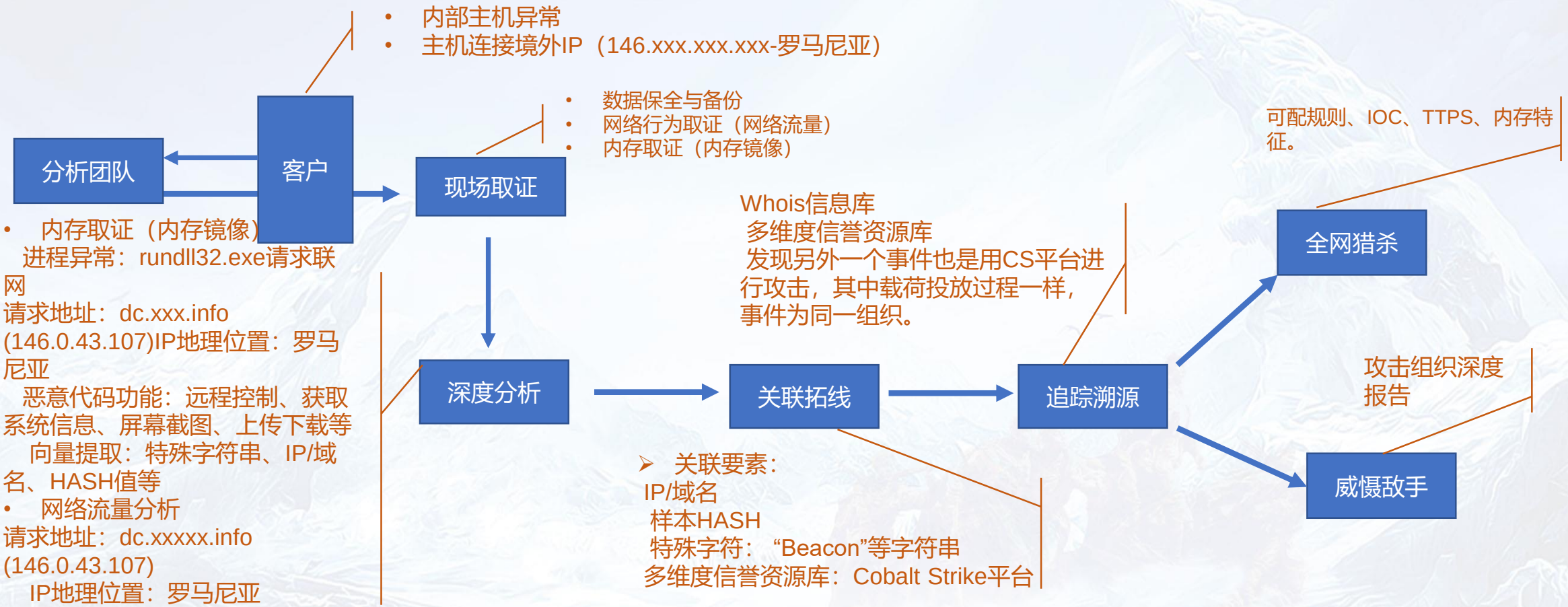
假想

分析
确定

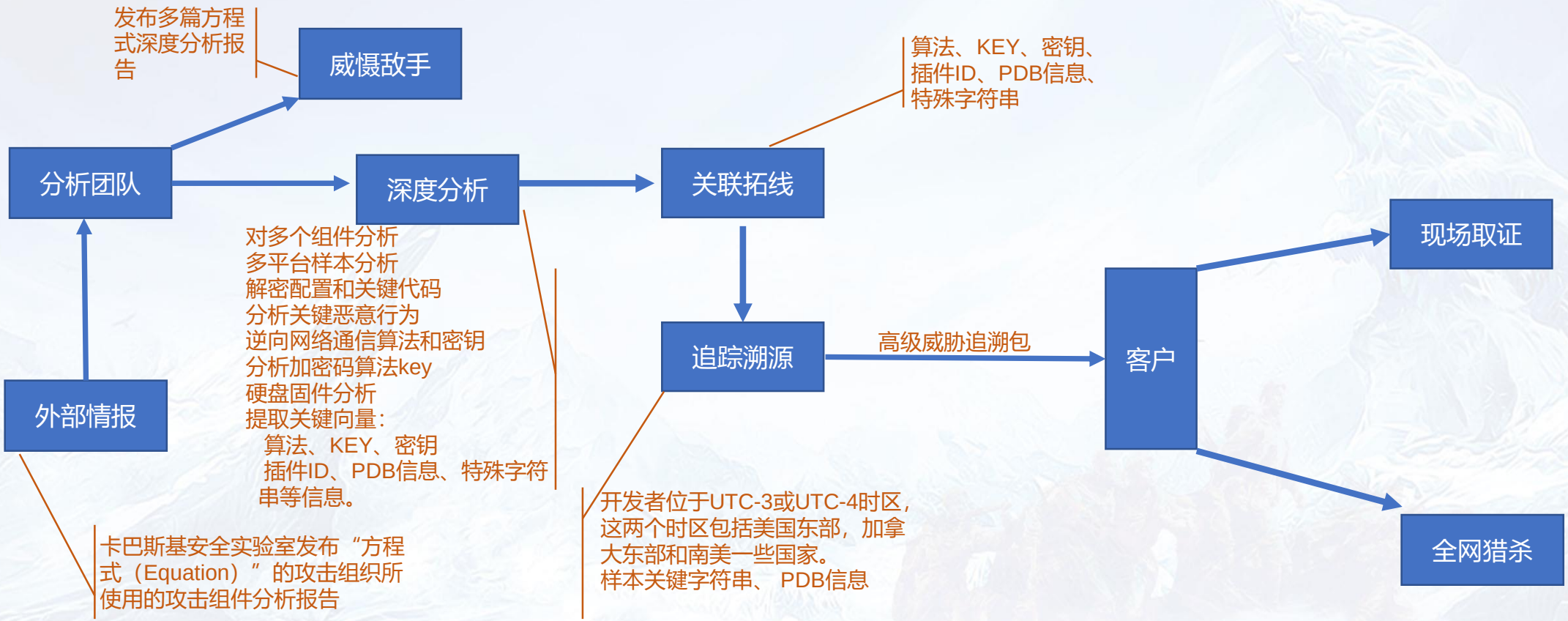
猎杀

实战化猎杀威胁服务能力

案例1——TOCS（海莲花）


内部主机异常
主机连接境外IP（146.xxx.xxx.xxx-罗马尼亚）
分析团队
客户
现场取证
数据保全与备份
网络行为取证（网络流量）
内存取证（内存镜像）
可配规则、IOC、TTPS、内存特征。
Whois信息库
多维度信誉资源库
发现另外一个事件也是用CS平台进行攻击，其中载荷投放过程一样，事件为同一组织。
全网猎杀
攻击组织深度报告
内存取证（内存镜像）
进程异常：rundll32.exe请求联网
请求地址：dc.xxx.info
(146.0.43.107)IP地理位置：罗马尼亚
恶意代码功能：远程控制、获取系统信息、屏幕截图、上传下载等
向量提取：特殊字符串、IP/域名、HASH值等
网络流量分析
请求地址：dc.xxxxx.info
(146.0.43.107)
IP地理位置：罗马尼亚
深度分析
关联拓线
追踪溯源
威慑敌手
关联要素：
IP/域名
样本HASH
特殊字符：“Beacon”等字符串
多维度信誉资源库：Cobalt Strike平台

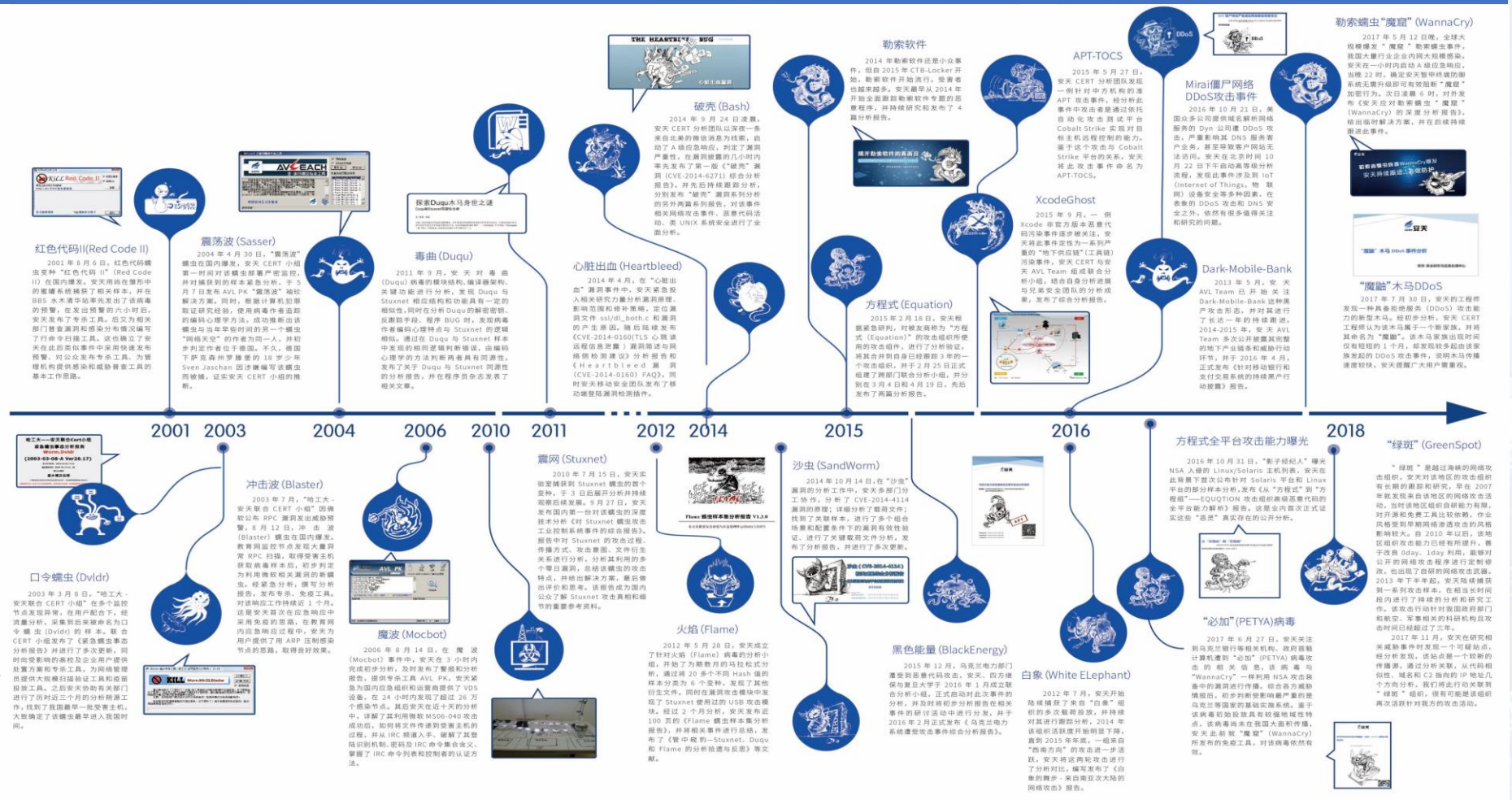
案例2——方程式


发布多篇方程式深度分析报告
威慑敌手
分析团队
深度分析
关联拓线
算法、KEY、密钥、插件ID、PDB信息、特殊字符串
对多个组件分析
多平台样本分析
解密配置和关键代码
分析关键恶意行为
逆向网络通信算法和密钥
分析加密码算法key
硬盘固件分析
提取关键向量：
算法、KEY、密钥
插件ID、PDB信息、特殊字符串等信息。
现场取证
追踪溯源
高级威胁追溯包
客户
外部情报
卡巴斯基安全实验室发布“方程式（Equation）”的攻击组织所使用的攻击组件分析报告
开发者位于UTC-3或UTC-4时区，这两个时区包括美国东部，加拿大东部和南美一些国家。
样本关键字符串、 PDB信息
全网猎杀

高价值威胁情报产出

安天是中国网络安全应急响应和深度分析中最重要的企业节点之一

从2001年到2018年，安天曾率先发现预警红色代码II、口令蠕虫等恶意代码，并对冲击波、震荡波、魔波等恶意代码做出深度分析；2010年之后，安天全面致力于深入分析境外发动的APT攻击，包括震网、毒曲、火焰、方程式、白象等重大APT事件，为国家主管部门和客户提供了有力的技术支持。



多年来持续与敌手隔空对决

网络空间威胁对抗与态势感知研讨会
暨 第六届安天网络安全冬训营

THANKS

扫码关注冬训营动态

战术型态势感知指控积极防御
协同响应猎杀威胁运行实战化

铁流鏖戰