执行体全量识别与精细管控

全量执行体识别场景的威胁情报赋能方案

安天 | 威胁情报产品中心

目 录

01 执行体识别与威胁情报

02 基于文件深度分析技术的执行体识别与行为情报生产

03 执行体情报管理与应用

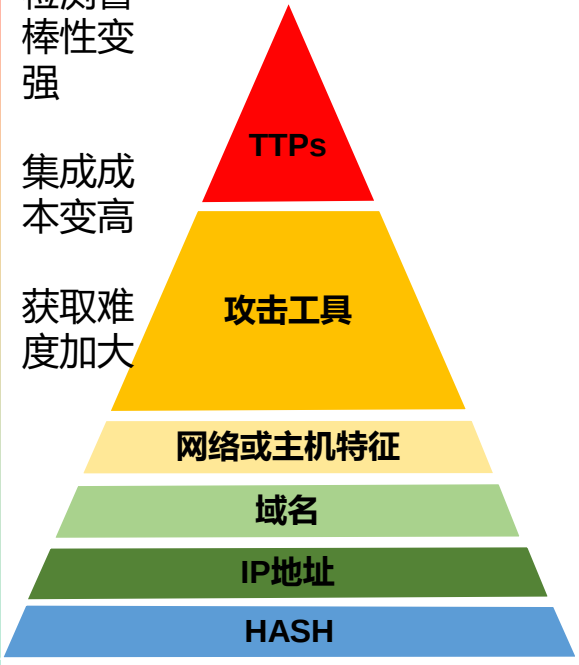
01 执行体识别与威胁情报

应用上的挑战：传统威胁情报的抗变换性与绕过性差

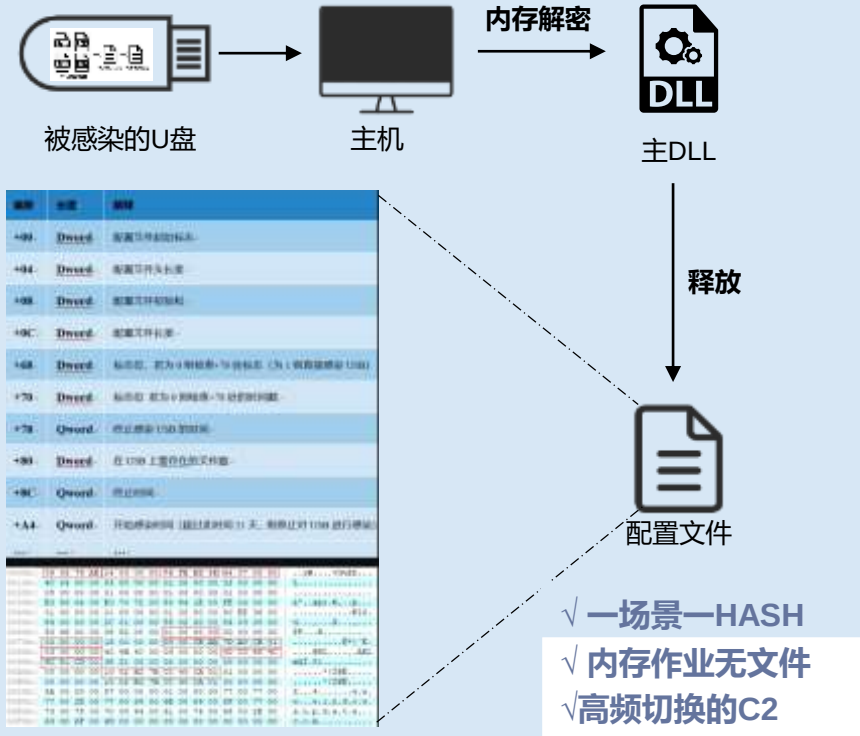
检测鲁棒性变强

集成成本变高

获取难度加大



威胁情报痛苦金字塔



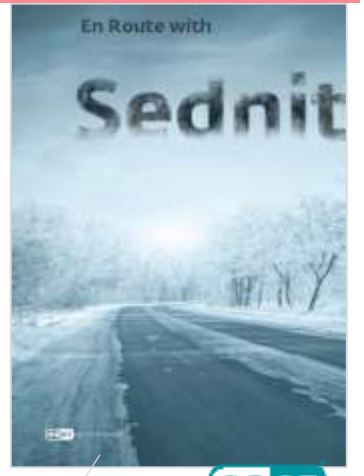
情报金字塔底层已经坍塌

应用上的挑战：更有效的威胁情报，看得见、摸不着、用不了

高价值的威胁情报

KASPERSKY

安天

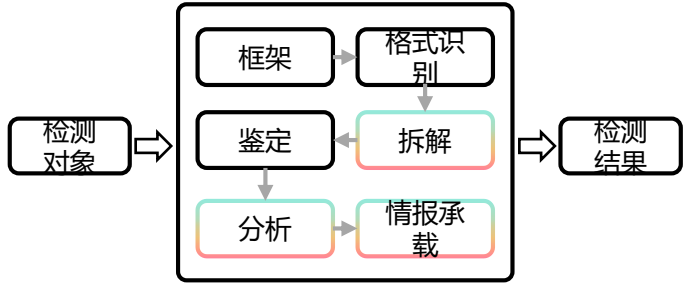


ESET

图例

注册表　互斥量　字符串

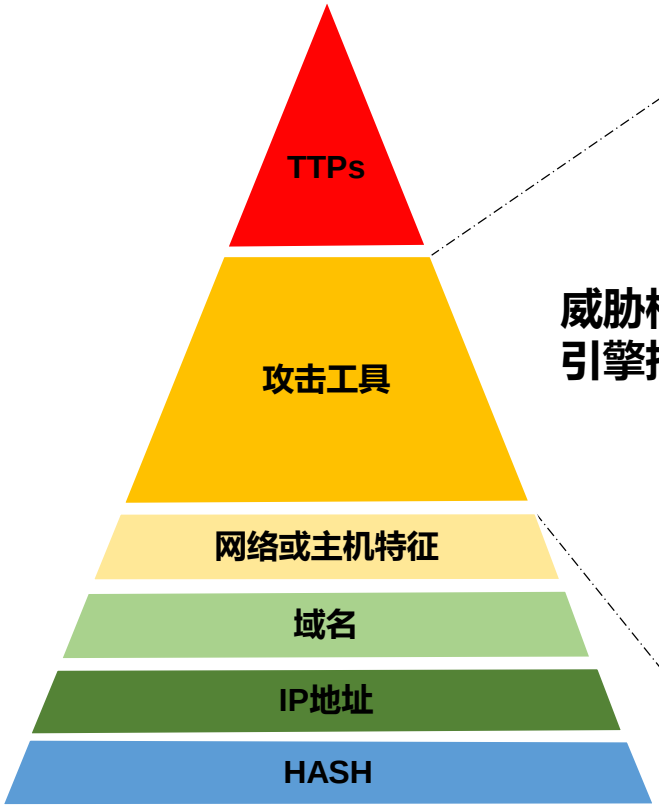
为什么用不了



威胁检测工作过程

能力未开放与输出

向量级威胁情报，承载高价值信息



威胁情报痛苦金字塔

威胁检测引擎抽取

特异性向量

典型字符串
编译环境
签名信息
注册表
互斥量
通讯配置信息
解密密钥
关键代码片段等

什么是向量级威胁情报

向量级威胁情报概念由安天提出，是基于威胁检测引擎的识别和深度拆解能力承载，从执行体中抽取的的能够表征威胁行为体基因特性、具备形式化特征的深度情报。

包括但不限于:环境信息、编译信息、签名信息、通讯配置信息、解密秘钥、关键代码片段等。

多维基础向量

- 基础信息（字符串、编码过的二进制）
- 属性信息（格式、编译器、壳、包、版本信息）
- 结构信息（PE结构、复合文档结构、结构异常）
- 身份信息（开发者、登录ID、密码、邮箱、数字签名）
- 环境信息（注册表、路径、GUID）
- 攻击技术（执行、持久化、提权、防御规避、凭证访问、发现、横向移动、收集）

向量级威胁情报，具备高鲁棒性、强语义表征与深层次揭示能力

共享方式	SDK	规则	本地化平台	部署环境	互联网	隔离网	半开放环境

高鲁棒性检测能力

基础向量

```
*(_DWORD *)a1 = a1 ^ 0xAE1979DD;
*(_DWORD *)(a1 + 4) = 0;
*(_DWORD *)(a1 + 12) = sub_10002334;
return 0;
```

解密密钥

释放文件的相对偏移及长度

更强的带有语义表征的支撑

传统病毒特征：无语义（一段二进制串）

向量：有语义（开机启动）

深层次揭示载荷能力

VS

总结：高质量威胁情报生产和消费设施的要求

情报生产设施要具备**专属化、向量级的威胁情报生产能力**

- **专属化情报**，补充开源情报覆盖面不足的问题，**让情报成为一种攻击者难以预测的安全能力**
- **向量级威胁情报生产**，提升对高级威胁的**抗绕过能力**

消费设施要具备**向量级威胁情报的消费能力**

- 可基于注册表、文件路径、GUID等情报，检测免杀威胁
- 可基于互斥量情报，进行威胁检测和关联
- 可基于数字签名情报，进行APT组织溯源识别
- 可基于文件结构异常情报，进行异常文件识别，辅助威胁狩猎

消费设施，可低成本接入**外源的高质量人读情报，并驱动威胁检测、溯源与响应**

- 吸收利用公开APT分析报告和内部人工分析报告中的高质量情报
  - 注册表键值、PDB路径、数字证书发布者、关键字符串等

总结：高质量威胁情报管理平台的要求

外源情报扩展接入与多源汇聚能力

- **补充本地情报的视角**
- 出厂预置多家主流第三方情报源
- 灵活的自定义情报源适配能力

管理向量级威胁情报的能力

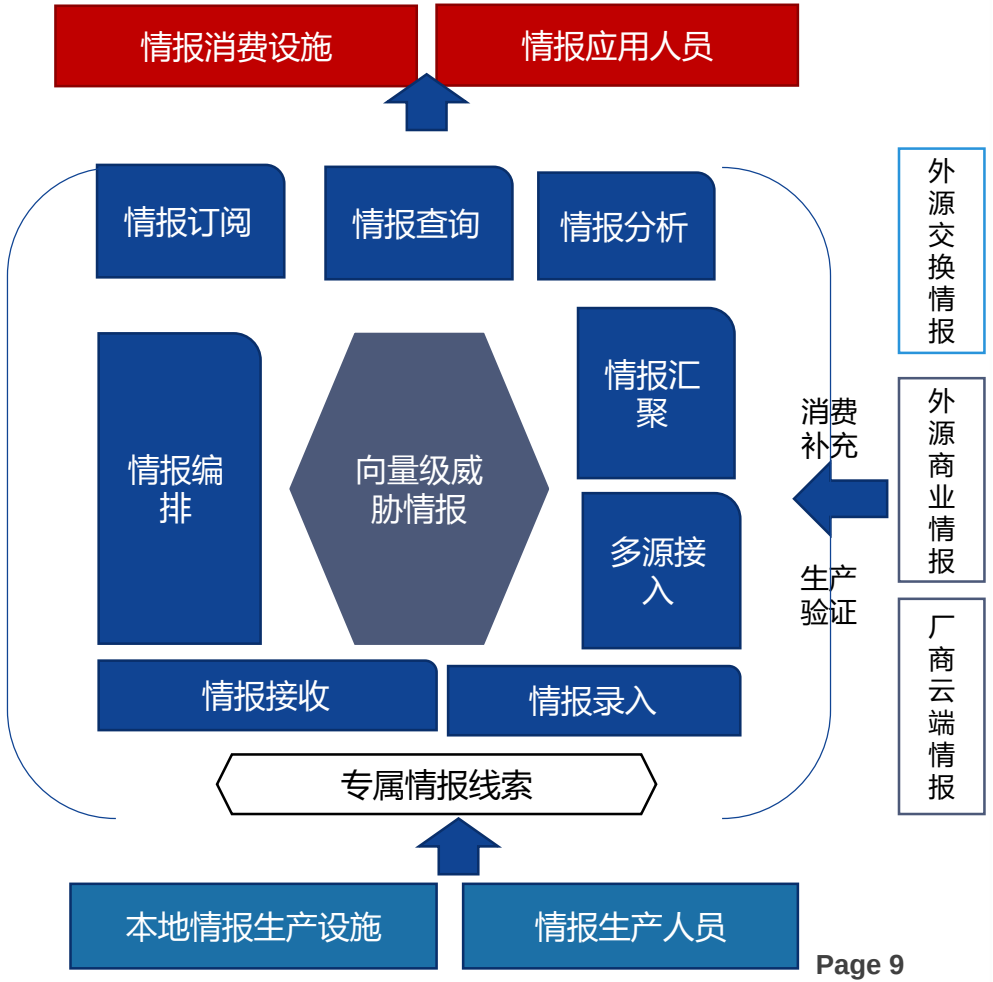
- 可接收、管理、订阅向量级威胁情报
- 确保对高级研究成果的吸收

威胁情报再编排能力

- **为消费设施提炼感兴趣的主题情报**
- 可按场景要求，编排过滤可消费的专题情报

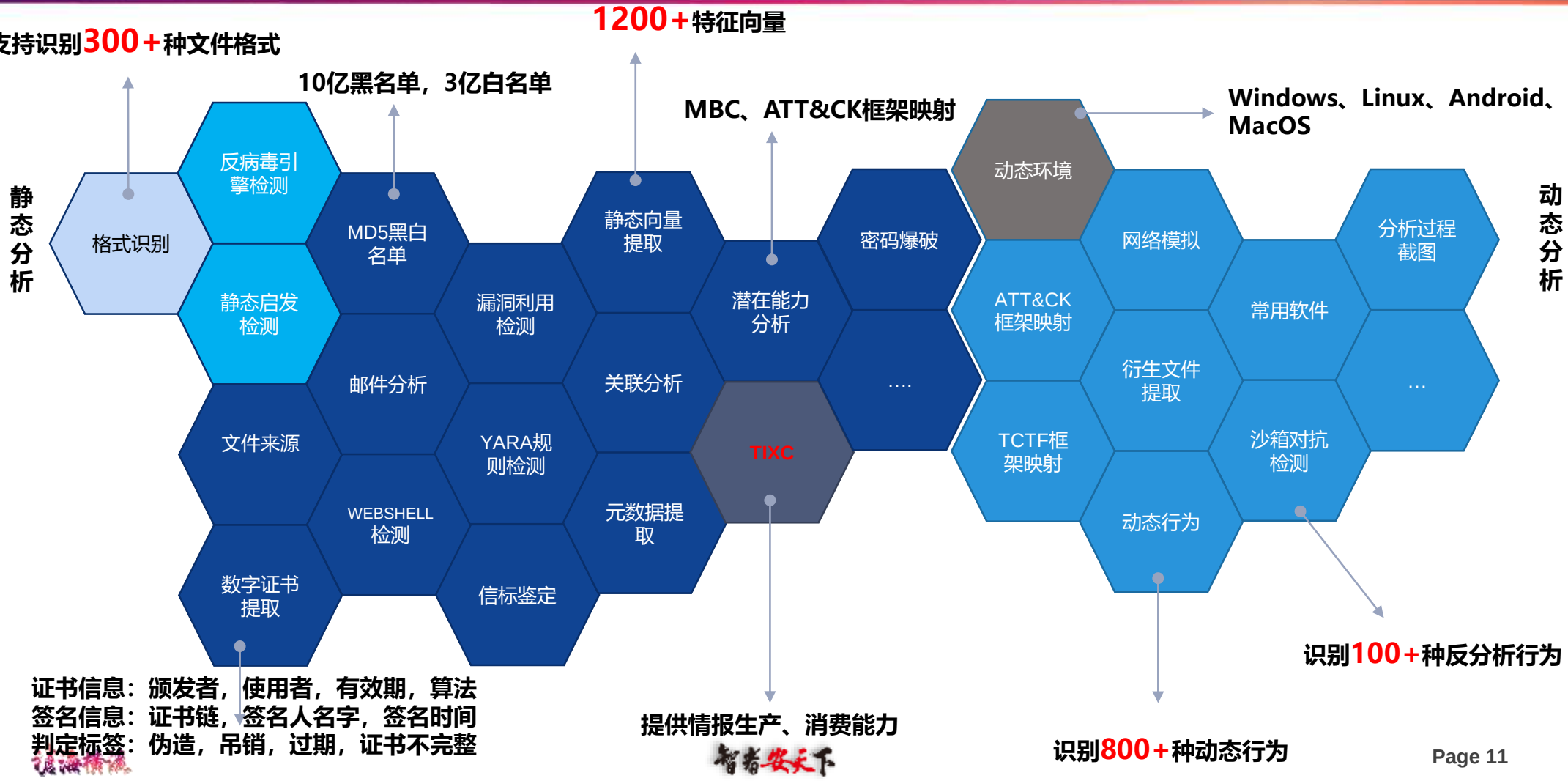
情报关联与事件挖掘分析能力

- 复杂攻击事件，关联拓线，挖掘更丰富的线索
- 基于同源分析技术，识别组织与来源关系



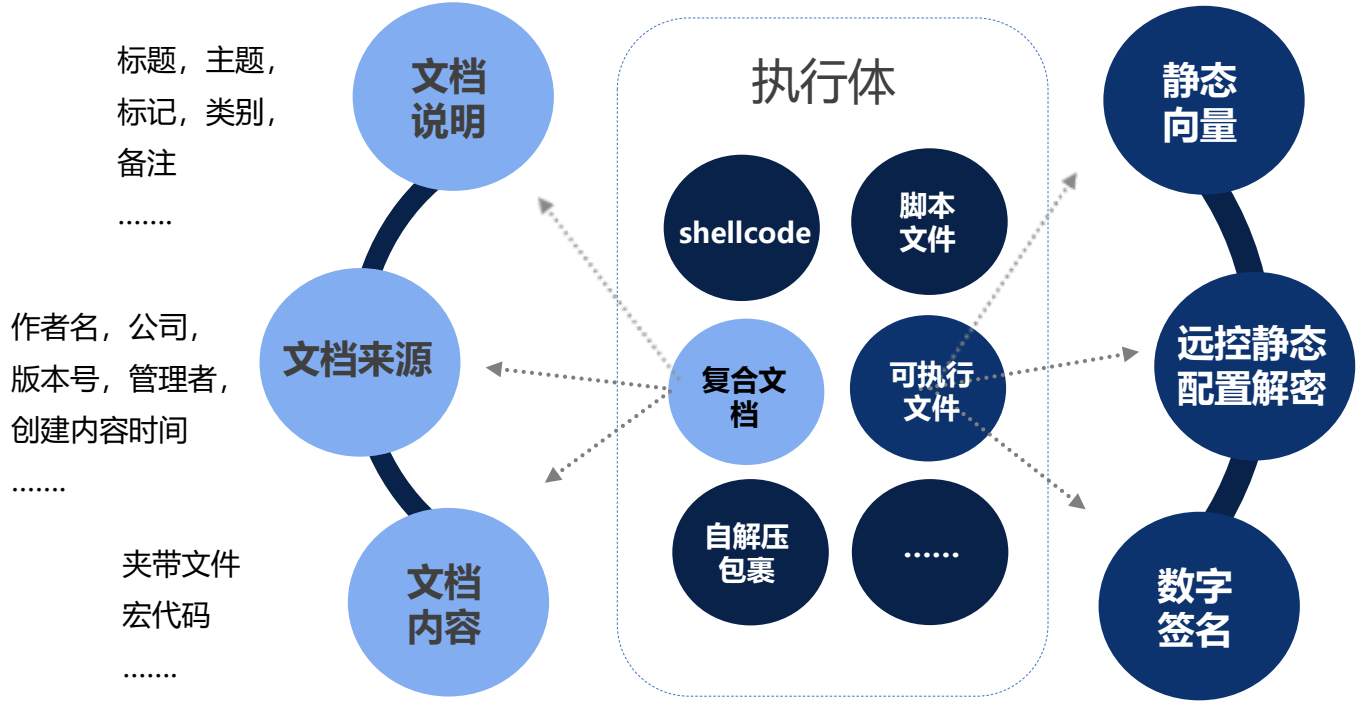
02 基于文件深度分析技术的执行体识别与行为情报生产

多维动静态分析手段，识别标定已知执行体信誉



深度格式解析，静态提取未知执行体线索基因

细粒度拆解，提取多维特征向量，支撑异常检测、关联拓线分析



行为

IP，信息获取
URL，对抗
传播，隐藏
窃取，欺骗
.....

API

模块相关操作
网络访问相关
文件基本操作
进程基本操作
.....

文件结构

导入导出表
编译器信息
节信息
数字签名
.....

IP，URL
MAIL，DOMAIN

证书信息：颁发者，使用者，有效期，算法

签名信息：证书链，签名人名字，签名时间

判定标签：伪造，吊销，过期，证书不完整

结构特征、属性特征、通信特征、行为特征、切片特征、签名特征…

虚拟运行未知执行体，揭示行为线索，生产专属化情报

多手段行为监控

应用层监控：行为解读更精准

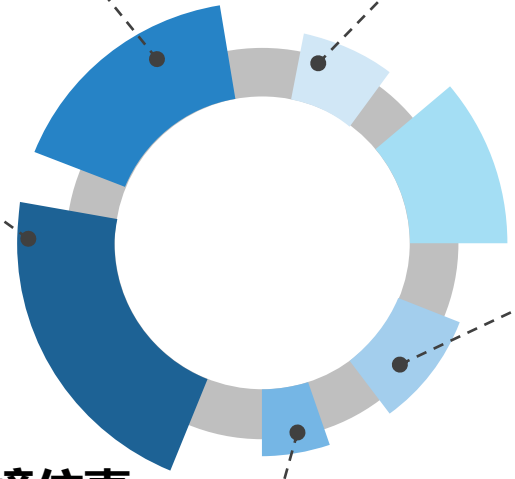
驱动层监控：权限高、数据全、运行时间早

丰富的主机模拟环境

操作系统：Windows、Linux、国产操作系统、Android、MacOS

软件环境：office、pdf阅读器、浏览器、解压软件、

自定义环境：定制化软件环境



网络环境仿真

网络连接模式：隔离局域网、模拟网络、互联网连接

模拟网络：模拟网络协议的响应情况

Pcap获取：捕获样本在运行种产生的数据包进行下载

对抗反分析技术

诱饵文件动态生成及投放

模拟移动介质：光盘、U盘拔插等

模拟外设操作：鼠标点击、鼠标移动、键盘输入等

人工干预分析：通过脚本干预样本运行时的操作

对抗行为揭示：注册表标识伪装、隐藏虚拟机自身特征、随机化分析起始路径等

细粒度行为揭示

主机侧：注册表、文件、进程操作、动态截屏、内存DUMP文件

网络侧：TCP、UDP、DNS、FTP、HTTP、HTTPS、POP3、SMTP等解析揭示

行为模式：800+种动态行为签名

执行体情报输出案例—窃密

包含反分析、进程注入、监听键盘等行为组合

分类	gid组	源IP	源端口	目的IP	目的端口	协议	签名	签名ID	修订版本
疑似木马通信	1	192.0.2.124	80	192.168.122.131	1036	TCP	ET POLICY PE EXE or DLL Windows file download HTTP	2018959	3
webby后门	1	192.0.2.124	80	192.168.122.131	1036	TCP	Win.Backdoor.Webby	900148	1

疑似木马通信告警

HTTP信息

请求方法	URL	端口
GET	http://codiumsecurity.com/peoplesstubs/EABTFES.html	80
GET	http://codiumsecurity.com/MIBtoCPUAK.dll	80

对外访问下载可执行组件

执行体情报输出案例—窃密

窃密木马典型特征：

- **持久化自身**
- **隐藏自身**
- **获取信息**
- **通信特征**

ATT&CK框架映射呈现样本各个阶段行为！

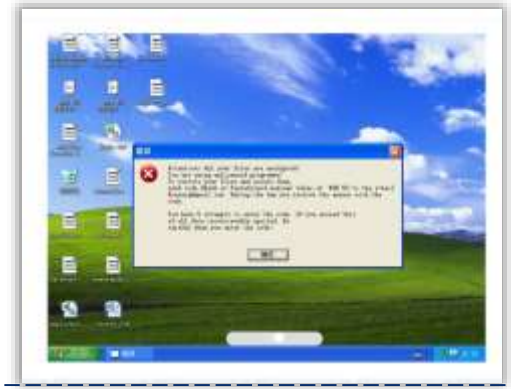
执行体情报输出案例—勒索

输出勒索相关的行为记录

创建勒索信息

移除源文件，新建加密文件

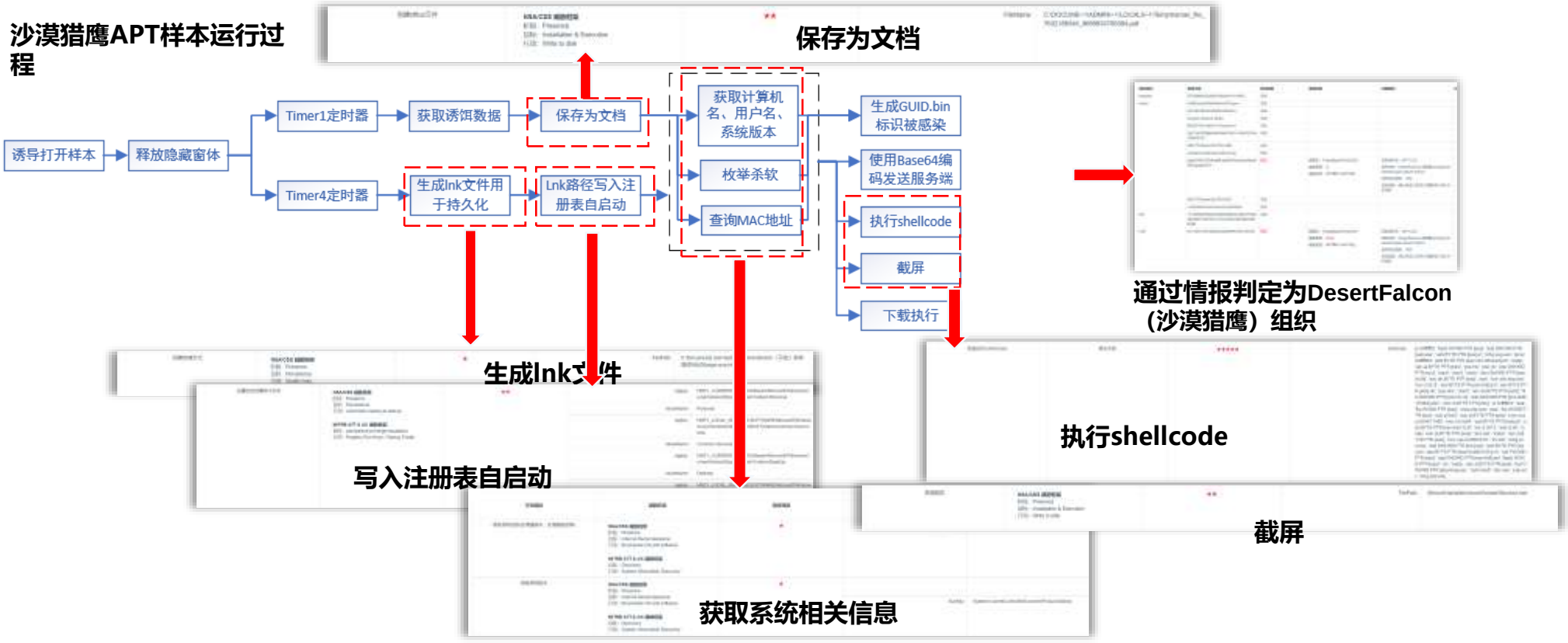
Windows弹出勒索信息



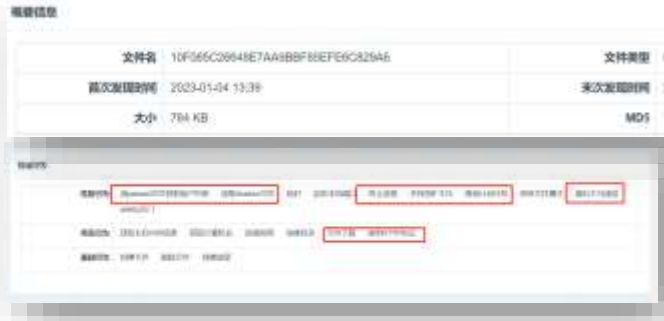
情报自动生产

执行体情报输出案例—APT

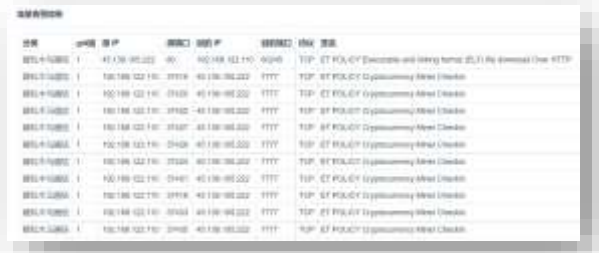
沙漠猎鹰APT样本运行过程



执行体情报输出案例—挖矿



输出挖矿相关行为汇总



流量告警揭示挖矿通信行为

文件和进程操作记录

基于计划任务进行持久化

终止其他种类挖矿进程

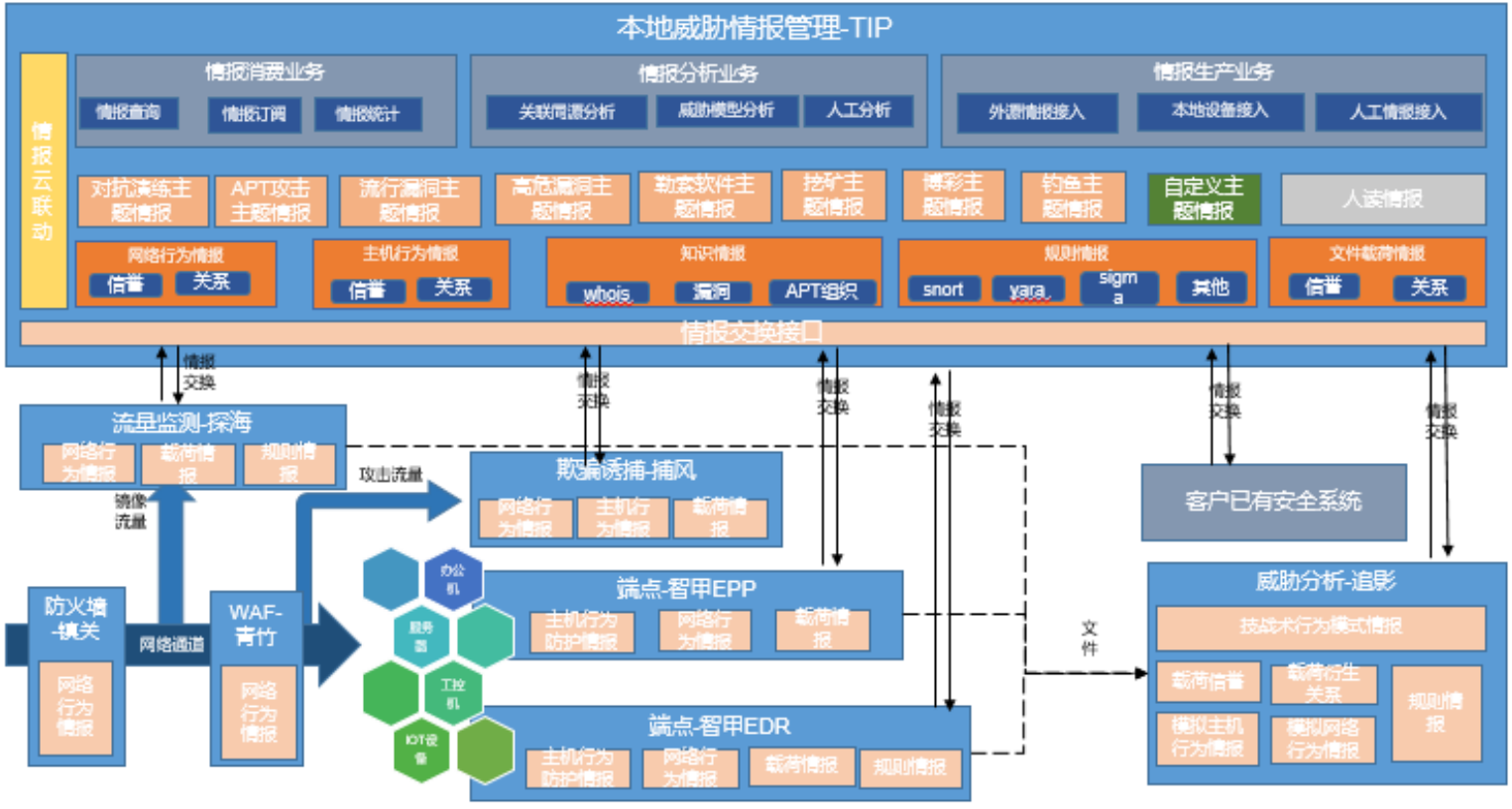
TCP五元组通信细节

http通信细节

http外联下载可执行文件

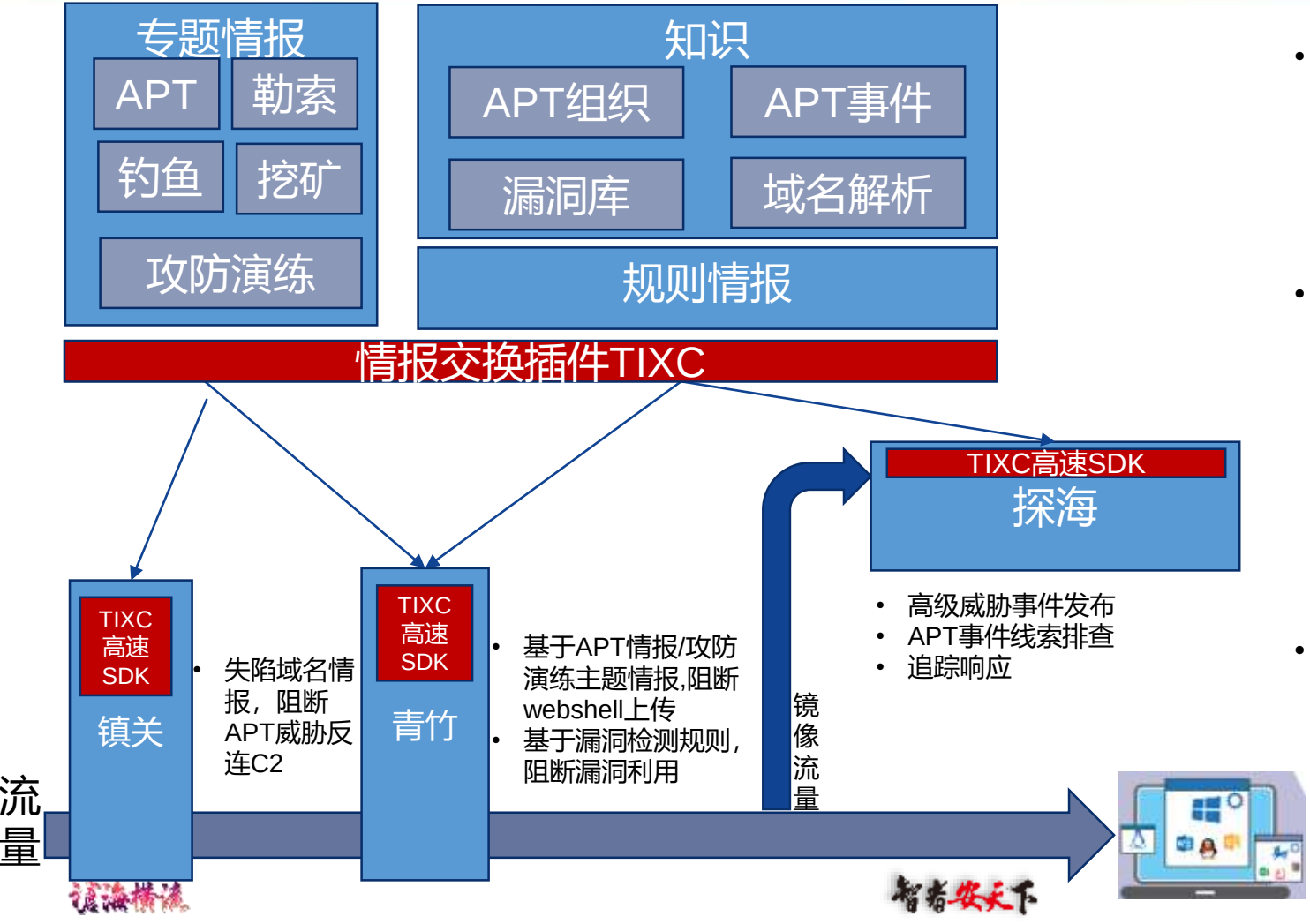
03 执行体情报管理与应用

一切安全设备，皆可生产威胁情报，皆可消费威胁情报



- 追影——文件载荷深度分析，威胁情报生产
- 探海——流量情报生产和消费
- 青竹——web情报生产和消费
- 镇关——流量情报消费
- 捕风——威胁诱捕，威胁情报生产
- 智甲——端点情报生产和消费
- TIP——情报管理及关联分析

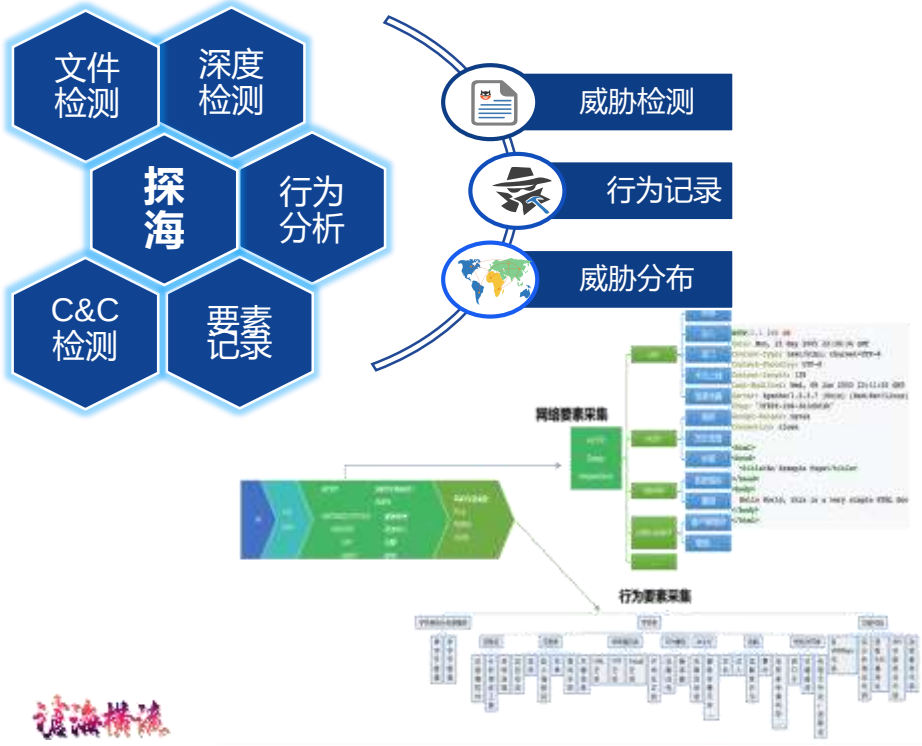
网络侧：情报驱动拒止威胁，事前阻断，事中定位，事后响应溯源



- 事前：在威胁进入网络之初即阻断传播
  - 钓鱼邮件发件人情报
  - 勒索威胁分发url情报
  - 挖矿威胁情报
  - 攻防演练攻击源IP情报
- 事中：基于情报，定位异常节点，阻断网间传播，缩小危害
  - 对于漏洞情报和资产信息，识别利用漏洞的蠕虫威胁的分布，隔离相关网段
  - 基于端点异常线索，一键搜索专属情报命中的网内同源威胁，还原事件全貌
- 事后：情报驱动，对高级威胁回溯分析与响应
  - 基于安全厂商发布的APT组织报告，进行网内痕迹排查
  - 基于泄露的网络军火库情报，进行历史筛查

网络侧：记录威胁流动与活跃痕迹，生产威胁情报

- 全量采集威胁要素，捕获高级威胁攻击中载荷高度定向、一次性投放
- 多维度检测，获取载荷行为能力，并对关键威胁信息进行留存
- 通过威胁样本追溯威胁源和传播路径



自动化生产情报

自动化提取C&C情报

- 基于恶意代码精确分类的C&C静态提取
- 联动沙箱进行动态分析，获取C&C地址
- 基于流量规则的C&C服务器识别

探海支持输出的情报类型

传统机读情报

- 文件hash情报
- 域名情报
- IP情报
- URL情报
- 邮箱情报
- IP/域名端口情报

威胁类型

- APT情报
- 僵尸网络情报
- C&C情报
- 勒索情报
- DDOS情报
- 挖矿情报

向量级情报

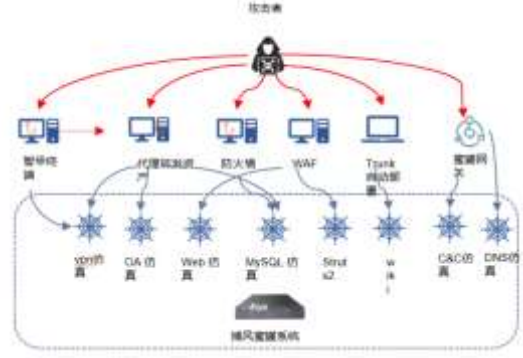
- **指令级向量情报**
- **API级向量情报**
- **功能级向量情报**
- **静态引擎输出情报**
- 互斥量情报
- 数字签名情报

由安天下一代威胁检测引擎支撑

网络侧：捕风蜜罐——欺骗式防御与网络情报生产

捕风蜜罐

- 多层次仿真
- 全链路采集
- 强威胁检测

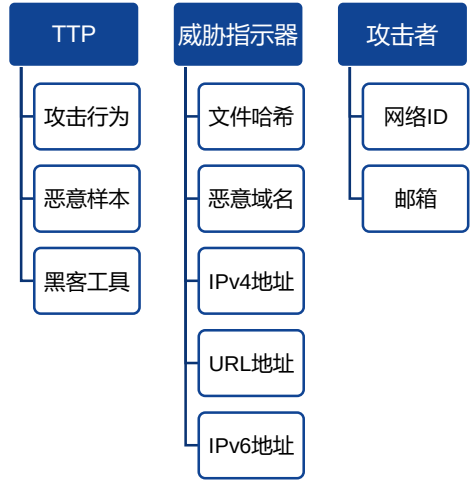


攻防演练
渗透攻击
捕获

DNS隧道
攻击捕获

捕获远控
窃密样本

威胁情报生产



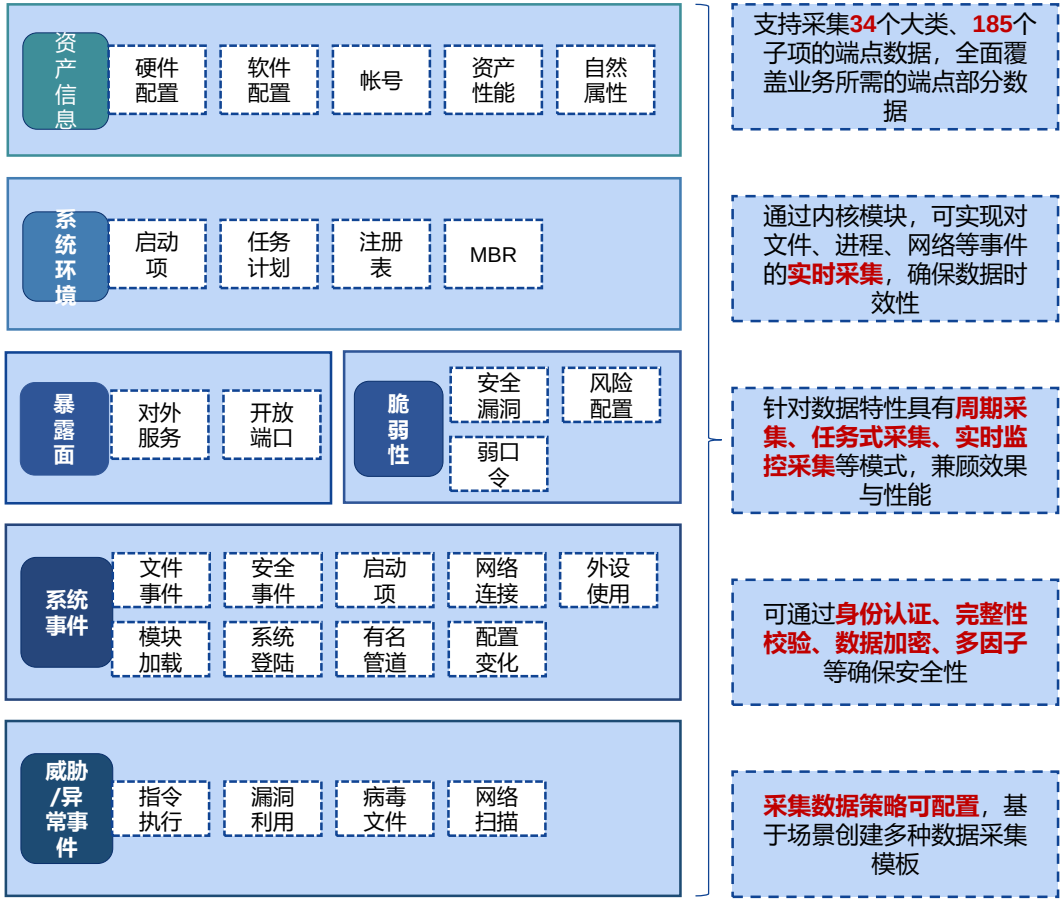
端点侧：情报赋能防御、检测、响应闭环

智甲EDR：帮助企业构建自适应的**安全运营防护能力**和**响应体系流程**

可执行体	定向攻击	非定向攻击
•文件格式：可执行程序(exe,dll,elf等)、脚本、复合文档等 •威胁类型：木马、蠕虫、感染式病毒、黑客工具、灰色软件、高级威胁	•获利：定向勒索 •破坏：勒索、加密 •窃密 •权限维持：后门主流与启动持久化 •初始访问：定向钓鱼邮件、水坑攻击、U盘感染、移动设备突破	•获利：挖矿获利、无差别勒索获利、欺诈获利、广告流量获利 •权限控制：僵尸网络、后门驻留 •无控制：炫技型蠕虫传播

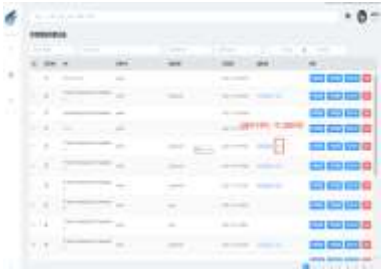
- 威胁防护环节
  - 基于漏洞利用缓解情报，官方补丁下发前执行临时缓解措施
  - 基于漏洞补丁情报、软件配置情报，实现已知漏洞的提前预防攻击
- 威胁检测环节
  - 已知流行威胁检测
    - 恶意邮件发件人情报：邮件落地时进行检出，阻止运行
    - 文件哈希、c2域名等情报：告警并处置
  - 免杀对抗木马、商用渗透工具等的高级威胁检测
    - 进程情报：父子关系及命令行参数识别，阻止可疑进程运行
    - 注册表情报：发生危险动作，阻止创建
    - 互斥量情报：检测并阻止相关进程运行
    - 自启动、服务等主机情报：检测阻断
    - PE数字证书情报：**证书盗用签名、利用签名漏洞生成证书、低信誉广告件签名**，阻止虽然签名验签通过但是不符合场景需求，存在风险的执行体的运行
    - 文件未知壳、编译器情报：检测阻断
- 实时响应环节
  - APT主题情报：终端事件与情报命中情况排查，用户、文件、进程、注册表、服务、内存和网络事件
  - 漏洞情报：调查受影响端点情况，进行回滚，修复，删除，阻止

端点侧：精细化数据采集，生成本地端点情报



- 基于端点的精细化采集能力，可提供独有的端点视角情报
  - 异常事件线索情报
    - 漏洞利用事件、恶意文件下载、恶意文件运行、网络扫描事件、异常指令运行
  - 执行体载荷情报
    - 文件格式、壳、编译器的统计分布
    - PE数字证书情报
  - 执行体的主机行为情报
    - 执行体注册表行为数据，生成专属情报
    - 执行体的进程行为异常数据，生成专属情报
    - 执行体网络行为情报
  - 软件资产情报
    - 软件版本情报
    - 脆弱配置情报

情报管理平台：提供情报消费与情报生产管理服务

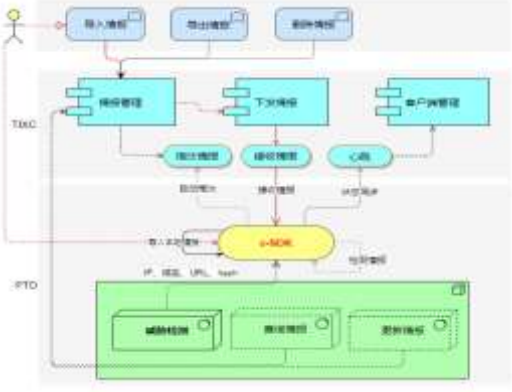


TIP情报消费记录图

外源情报接入

TIP情报生产记录

人工情报接入



C-sdk运转流程图

- 情报消费服务，联动接入设备
  - 精准情报检测
    - 内置外源情报接入（安天情报云平台， VT，AlienVault等），提供多源交叉验证能力
    - 支持自定义接入外部情报
    - 内置安天主题情报
  - 主题情报订阅
    - 云端协作响应，主题订阅
    - 针对网关类设备，提供基于C的情报交换SDK，利用缓存设计提高检测速度
  - 生产情报命中查询
    - 用于关联分析场景与溯源
- 情报生产接口，为本地情报消费提供素材
  - 本地设备情报生产接入
    - 本地设备通过情报交换组件（TIXC）接入
    - 支持向量级威胁情报接入
  - 人工情报生产接入
    - 现场运营人员手工加入情报

情报管理平台：支持高级安全研究成果、开源规则接入

基于STIX2记录IOC情报

基于snort表示流量行为情报

疑似Lazarus组织针对韩国的攻击活动分析

https://www.antiy.cn/research/notice&report/research_report/20221101.html

基于sigma规则记录行为情报

基于yara规则记录载荷向量情报

情报管理平台：具备关联分析与情报自动编排能力

TIP 具备基于ioc和样本同源特征的关联分析能力

TIP 基于自动编排的情报生产能力

- **简化分析师的“机械重复”的情报挖掘分析工作**
  - 图模型关联拓线
  - 同源溯源分析

- 对**情报消费的场景需求**的敬畏，支持用户对情报内容的再编排
  - 网关流量监测设备，低误报容忍度：**多来源交叉验证（本地+云端）**
  - 威胁狩猎与调查系统，看重线索丰富度：**配置为宽松的线索收集条件**
  - 低硬件配置安全设备：**可设定的数量限制、关注的情报主题、淘汰规则**

向量级威胁情报应用——APT攻击检测

攻击过程

1. 钓鱼链接诱导点击
2. 含漏洞诱饵文档运行
3. 释放专有BADNEWS木马
4. 执行专有BADNEWS木马

- 释放到C盘某文件夹下
- 通过注册表创建自启动
- 含有数字签名5Y TECHNOLOGY LIMITED

- 隐藏窗口
- 创建互斥体
- 收集受害者信息
- 使用自定义算法加密流量，发送收集的信息至C2
- 接收进一步控制指令并行动

情报内容

类别	情报名称	情报值
哈希	木马MD5	1e788e54f67fa64af39005af106567b0 8328a66d974a5a4aca475270b94a428a
网络环境	下载地址	https://***.org/magzine/zhongguo/
	回连IP	74.**.**.**
	回连C2	http://74.**.**.**/e3e7e71a0b28b5e96cc492e636722f73/4sVKAOvu3D/BDyot0NxyG.php http://74.**.**.**/e3e7e71a0b28b5e96cc492e636722f73/4sVKAOvu3D/UYEfgEpXAOE.php
主机环境	文件路径	C:\\ProgramData\\Microsoft\\DeviceSync\\mcods.exe
	注册表键值	HKCU\Software\Microsoft\Windows\CurrentVersion\Run\OneDrive
	互斥量	rendumm
工具载荷	算法加密密钥	37FF8272C0EEBC0AE1D90382847618DD
	数字证书	使用者：5Y TECHNOLOGY LIMITED 指纹： 0b26d02a94f4c8e14222a966b005bb7d30b45786 有效期从：2022年3月31日 8:00:00 有效期到：2023年3月16日 7:59:59 序列号：25ba18a267d6d8e08ebc6e2457d58d1e

生产情报

达成效果

追影

- 基于执行体静态分析与动态虚拟执行，生产**工具载荷类情报、主机环境类情报、c2回连情报**

消费情报

生产情报

镇关FW

青竹WAF

探海NDR

- 消费网络环境类情报
- 生产网络侧看到的事件线索

消费情报

生产情报

智甲EPP

智甲EDR

- 消费主机环境类情报
- 生产端点侧看的事件线索

感谢大家的关注

安天冬训营 wtc.antiy.cn