探海+追影，威胁流量检测与文件深度分析的最佳实践

安天产品事业部

产品回顾

探海

- 安天自主研发的网络威胁检测设备
- 支持网络流量数据的协议解析与内容还原、全要素采集
- 从包、流、会话、文件、协议元数据、网络行为、文件　行为等多个层次进行全流量检测

探海威胁检测系统

追影

追影威胁分析系统

- 动静态揭示威胁行为
- 有效触发漏洞
- 支撑威胁情报生产

安天蝉联中国网络安全技术对抗赛第一名

長纓待展

CONTENTS

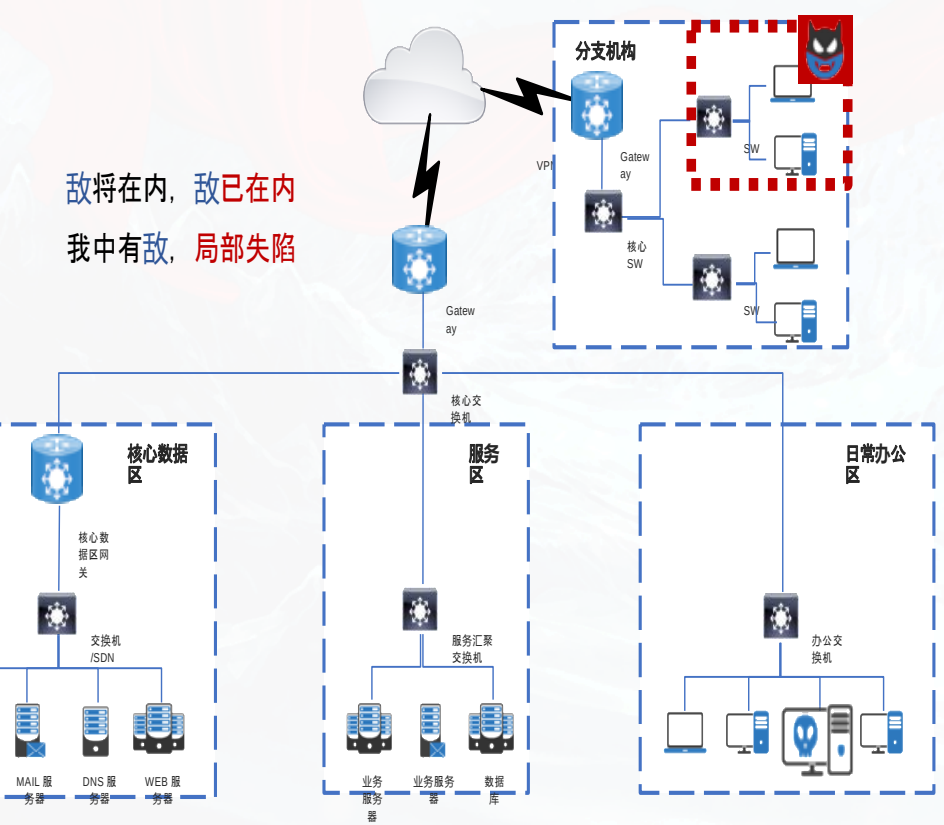
目 录

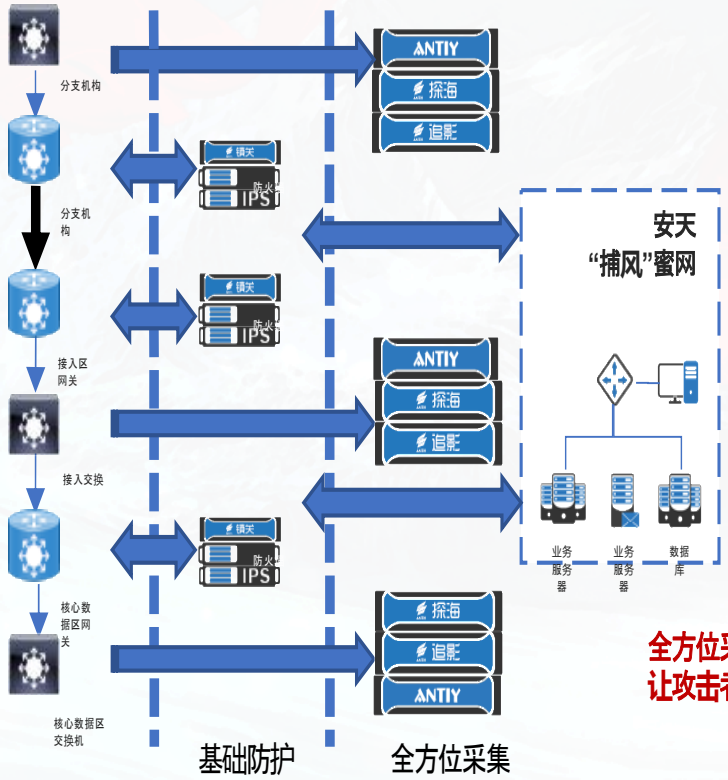
01 威胁监测需要两个基本能力：威胁检测与全要素记录

基于敌情假定，将检测能力部署在攻击者的必经之路

敌将在内，敌已在内

我中有敌，局部失陷

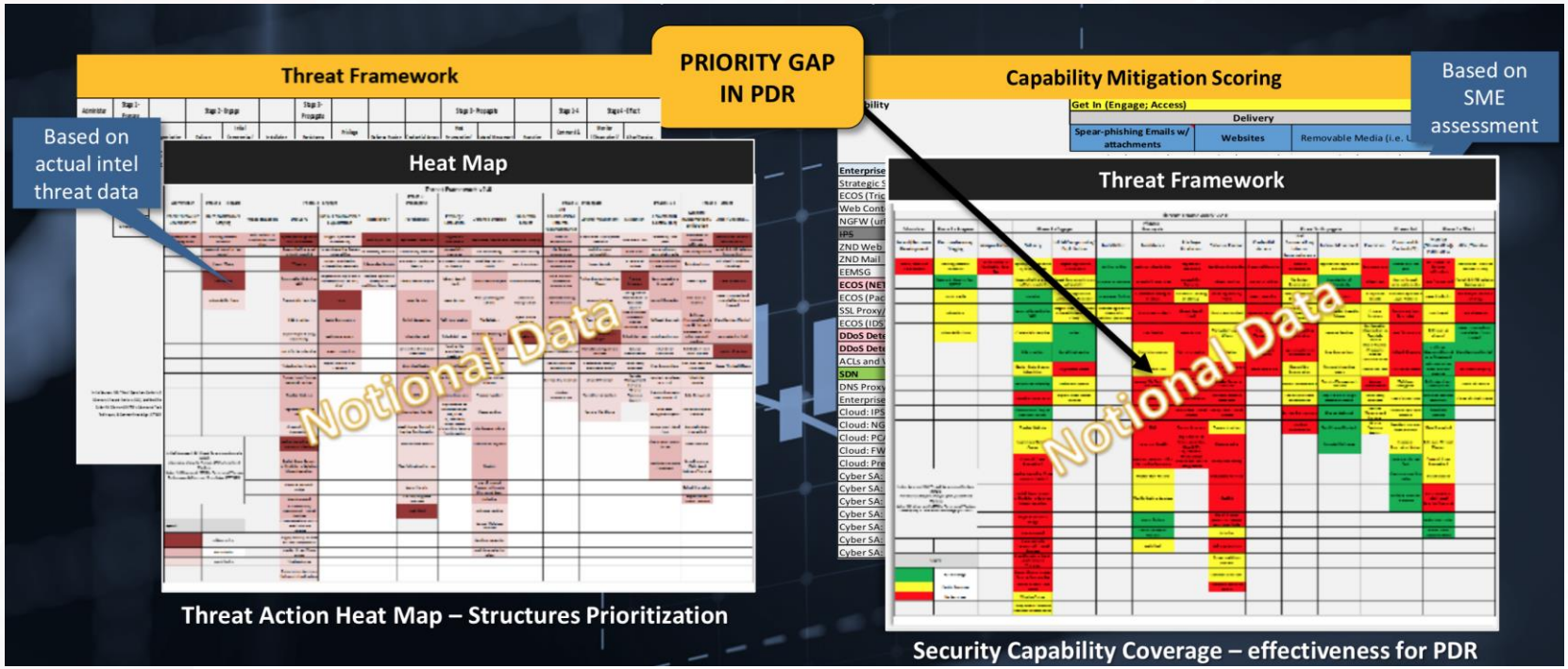




- 参考高价值目标构建合理分区
- 在抵达目标的路径上增加关隘
  - 业务路径
  - 数据路径
- 交叉火力**覆盖无死角**
  - **特别需要注意：设备管理流量**
  - **特别需要注意：包头记录**
- 被动防御能力是积极防御的基础

全方位采集、智能化响应
让攻击者无所遁行、无处可逃、无计可施

将实际威胁映射到框架，作为能力差距评估的依据



首要关注以下差距：

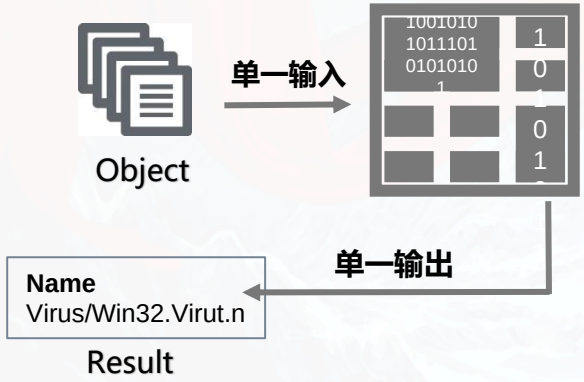
P 防御能力

D 检测能力

R 响应能力

引用自《DODCAR_-no class markings - Pat Arvidson.pdf》

威胁检测需要综合多个维度--多种输入输出对象

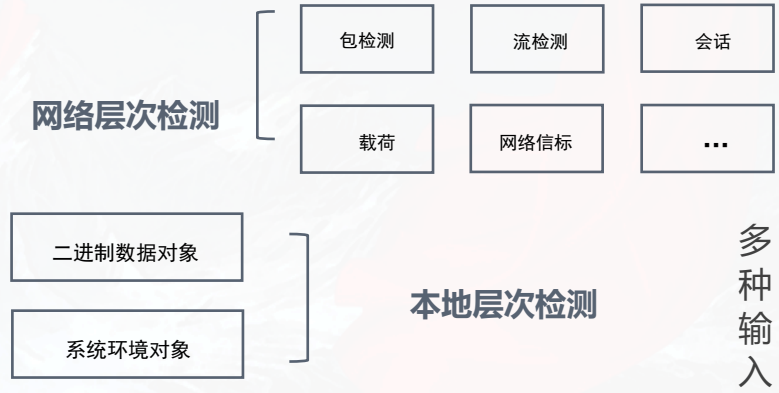


✓ **传统引擎**

主要是以单一对象为输入，以单一结果为输出。而随着威胁的进一步演进和泛化，威胁检测已不能仅仅停留在对单一对象进行鉴定上。

✓ **AVLSDK威胁检测引擎**

多种输入对象，多种输出结果。威胁检测多样化。



输出 1

- 黑白
  - 识别信息
  - 基础信息
- 多向量
  - 附加信息
  - 行为信息
- 核心行为
  - 远控 广告
  - DDOS 下载
  - 窃取
- 威胁行为
  - 传播 伪装
  - 隐蔽 对抗
  - 信息获取 攻击

输出 2

- 黑客组织名称
- 别名攻击目标
- 攻击领域
- 攻击方式
- 活跃时间
- 利用漏洞
- 组织简介

输出 3

ATT&CK框架信息

初始访问、执行、持久化、提权、防御规避、凭证访问、发现、横向移动、收集、命令控制、渗透

威胁分类的变化，从单一结果到融合信息

恶意代码分类
感染式病毒
蠕虫
木马
黑客工具
灰色软件
风险软件
垃圾文件
测试文件

2006 网络事件分类
扫描
攻击
溢出
植入
传输
控制
升级
失密
危险资源
应用

从简单的恶意代码分类到基础环境信息、协议信息、文件拆解、威胁框架与威胁情报融合的多维度结果

2007 网络事件分类
扫描
攻击
溢出
植入
传输
控制
升级
失密
危险访问
敏感应用
欺诈
欺骗
监听

2009 网络事件分类	二级分类
扫描	扫描.协议
攻击	攻击.效果
入侵	入侵.技术
传输	传输.恶意代码分类
控制	控制.控制命令
升级	升级.软件分类
窃密	窃密.技术
危险访问	访问.挂马/钓鱼/色情
敏感应用	敏感应用.应用类型
欺骗	欺骗.技术
监听	监听.技术
接入	接入.协议
原始协议事件	……

威胁情报
组织/行动名称
别名
攻击目标
攻击领域
攻击方式
活跃时间
利用漏洞
组织简介

ATT&CK 威胁框架
初始访问
执行
持久化
提权
防御规避
凭证访问
发现
横向移动
收集
命令控制
渗出
影响

MITRE ATT&CK™

NSA/CSS TCTF v2

2020

基于下一代威胁检测引擎

网络流量分类	行为标签	原始协议元数据	文件
16 种基础分类	74 种核心行为	289 种协议识别与解析	298 种格式识别与还原
16062 条规则		1853 种应用及行为识别	55 种包裹
		32 种远控木马协议	1660 维度元数据向量提取
		200万条 C2 规则	

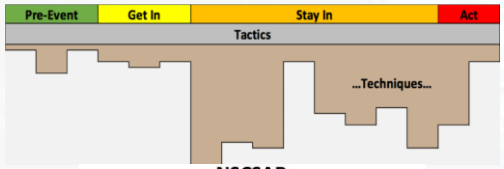
安天探海威胁检测系统 - ATT&CK威胁框架覆盖度

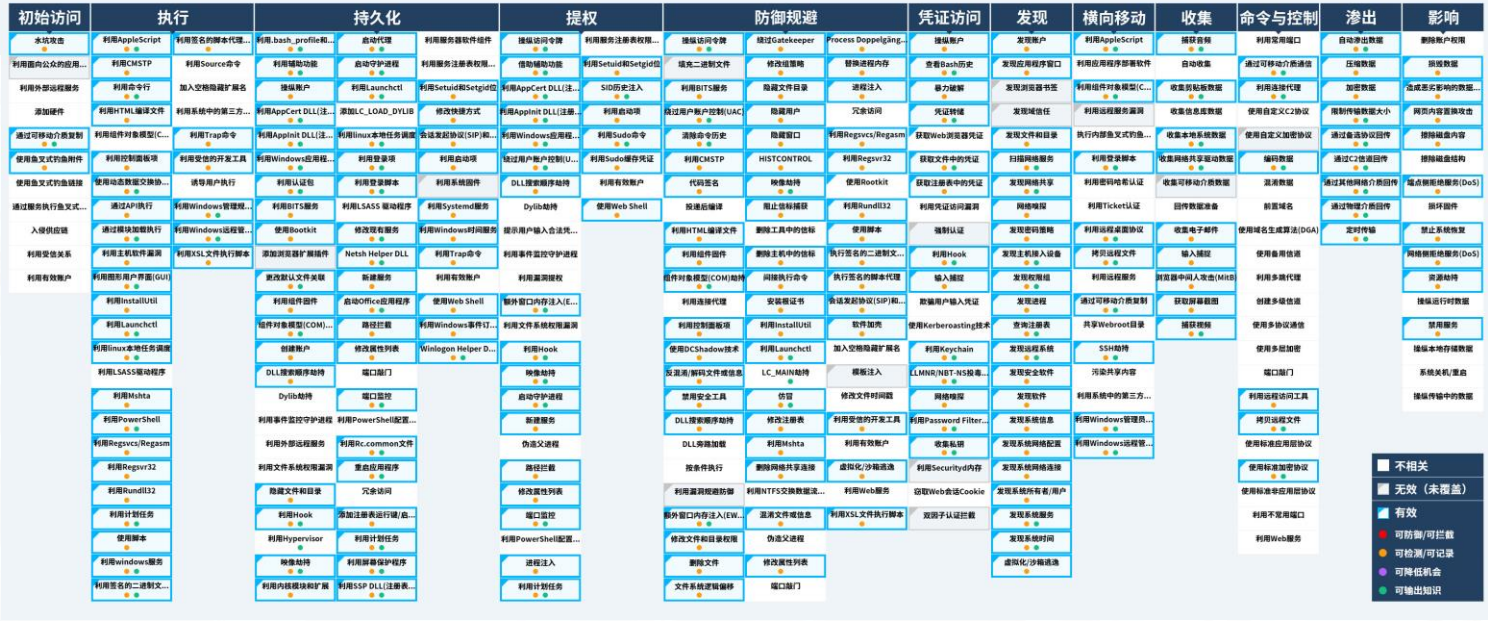
智者安天下

威胁框架：细粒度对抗

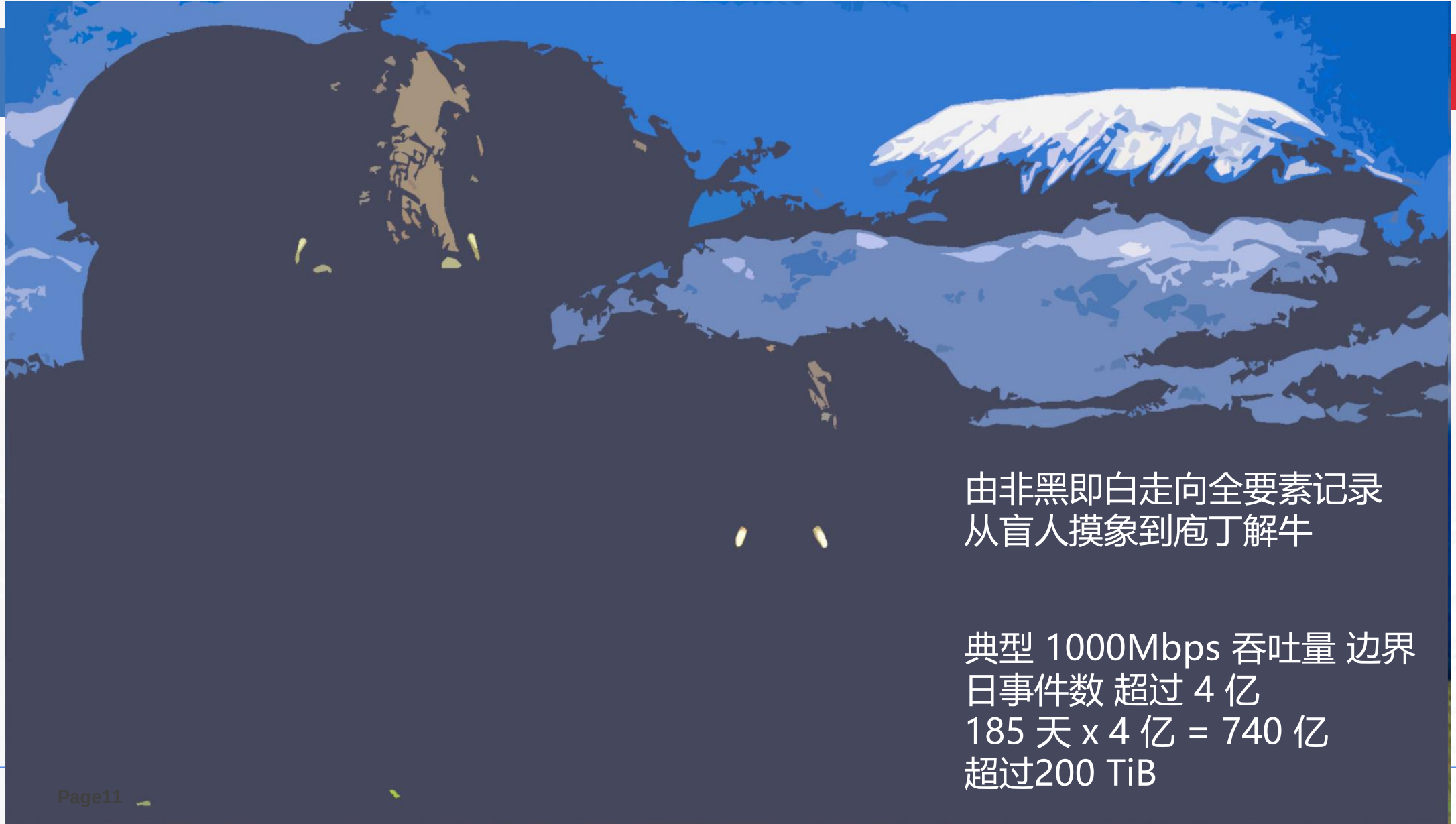
安天探海威胁检测系统 - ATT&CK威胁框架覆盖度

基于对载荷文件的检测
可以大幅度的提升威胁框架的覆盖度





智者安天下



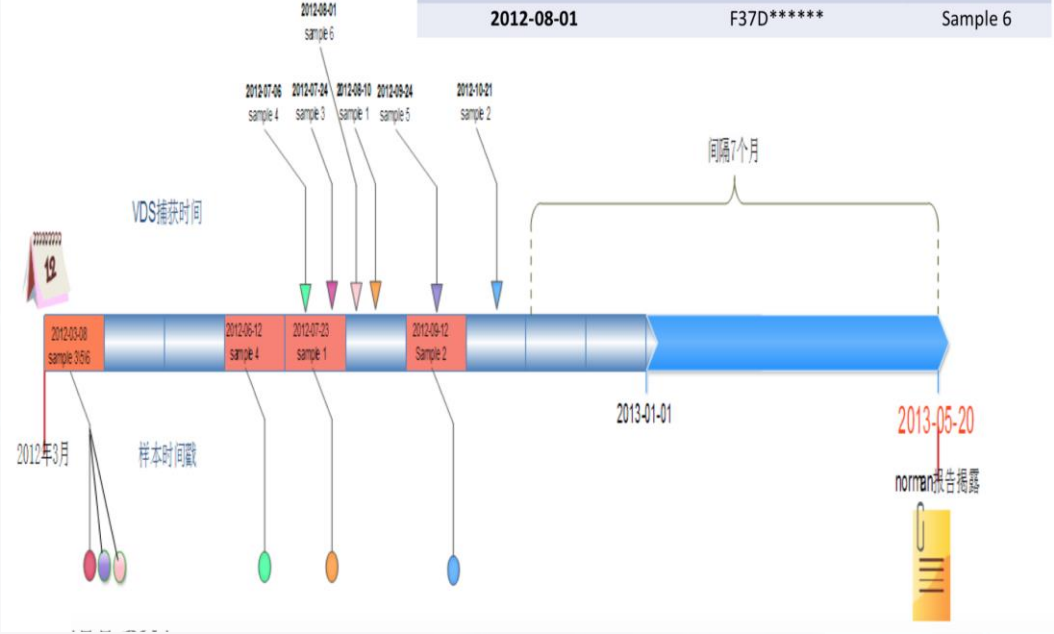
由非黑即白走向全要素记录
从盲人摸象到庖丁解牛

典型 1000Mbps 吞吐量 边界
日事件数 超过 4 亿
185 天 x 4 亿 = 740 亿
超过200 TiB

采集的要素需要长期留存（6个月的日志还远远不够）

- “白象”对中国的攻击时间链——超过1年

捕获时间	样本hash列表	代号
2012-08-10	0D46******	Sample 1
2012-10-21	734E******	Sample 2
2012-07-24	9A20******	Sample 3
2012-07-06	CE00******	Sample 4
2012-09-24	DE81******	Sample 5
2012-08-01	F37D******	Sample 6



- 网络安全法要求日志保存六个月

中华人民共和国
网络安全法
含草案说明

第三章　网络运行安全

第一节 一般规定

第二十一条　国家实行网络安全等级保护制度。网络运营者应当按照网络安全等级保护制度的要求，履行下列安全保护义务，保障网络免受干扰、破坏或者未经授权的访问，防止网络数据泄露或者被窃取、篡改：

（一）制定内部安全管理制度和操作规程，确定网络安全负责人，落实网络安全保护责任；

（二）采取防范计算机病毒和网络攻击、网络侵入等危害网络安全行为的技术措施；

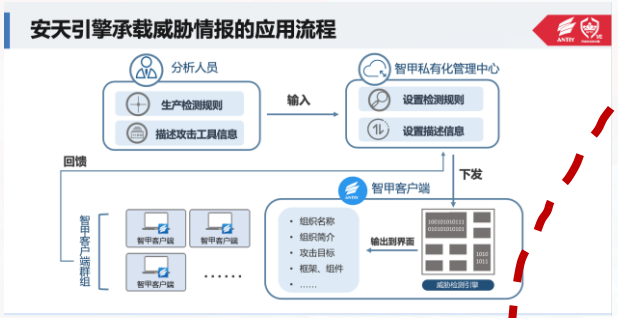
（三）采取监测、记录网络运行状态、网络安全事件的技术措施，并按照规定留存相关的网络日志不少于六个月；

（四）采取数据分类、重要数据备份和加密等措施；

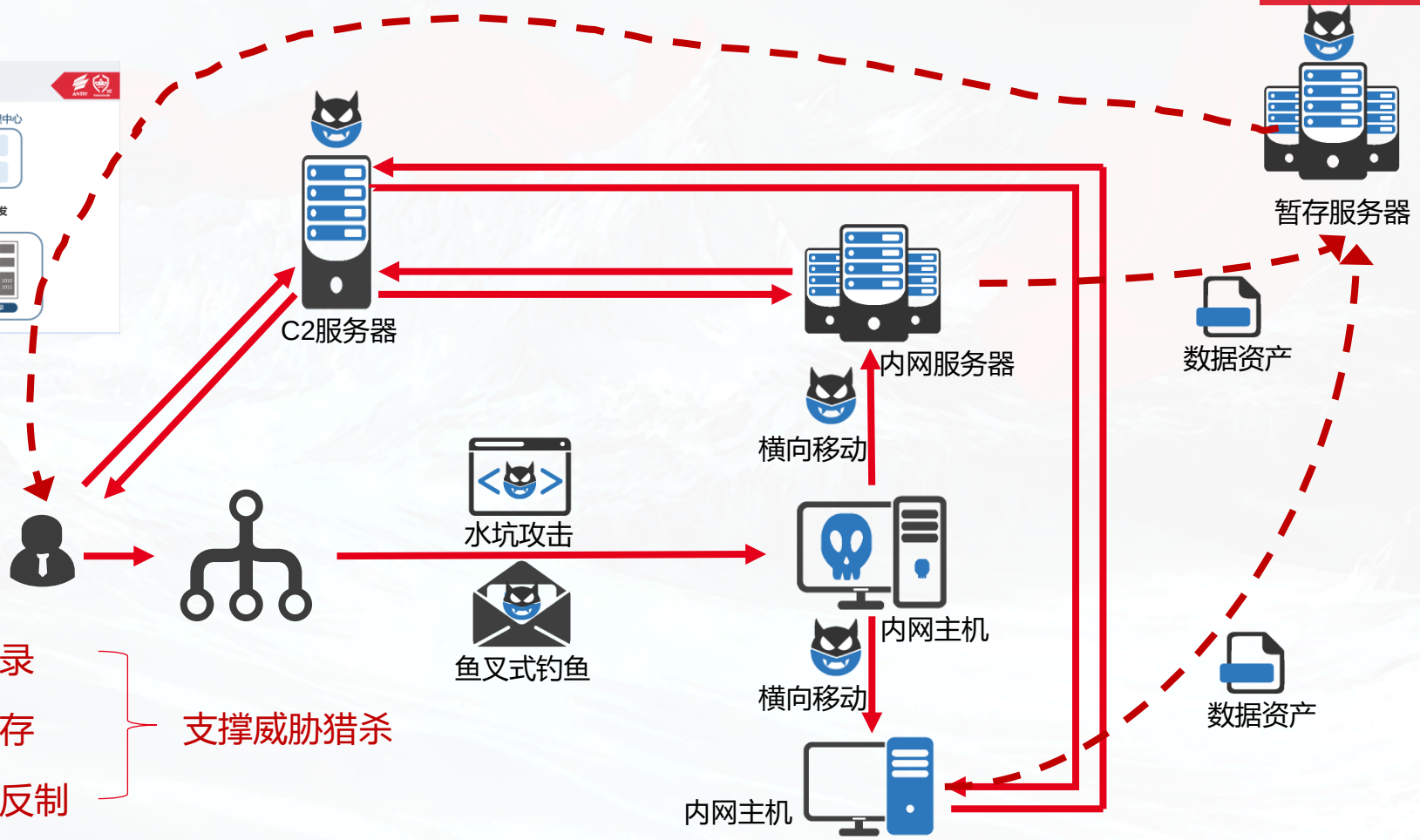
（五）法律、行政法规规定的其他义务。

第二十二条　网络产品、服务应当符合相关国家标准的强制性要求。网络产品、服务的提供者不得设置恶意程序；发现其网络产品、服务存在安全缺陷、漏洞等风险时，应

潜伏者被激活，内部威胁更需要全方位无死角的采集



基于场景，对威胁情报进行适配



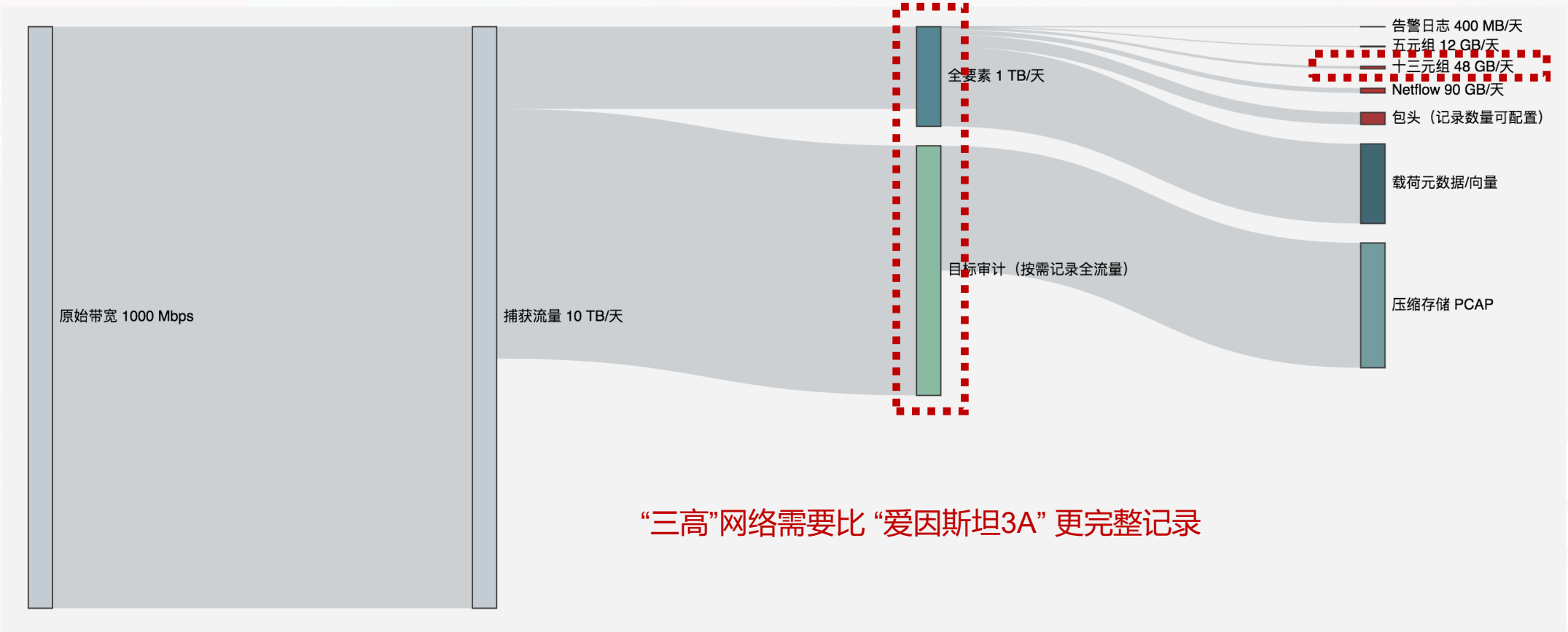
必经路径——全要素记录

失陷节点——全流量留存

信标触发——导入蜜网反制

支撑威胁猎杀

“探海”提供指引猎杀所需完整的要素采集



“三高”网络需要比 “爱因斯坦3A” 更完整记录

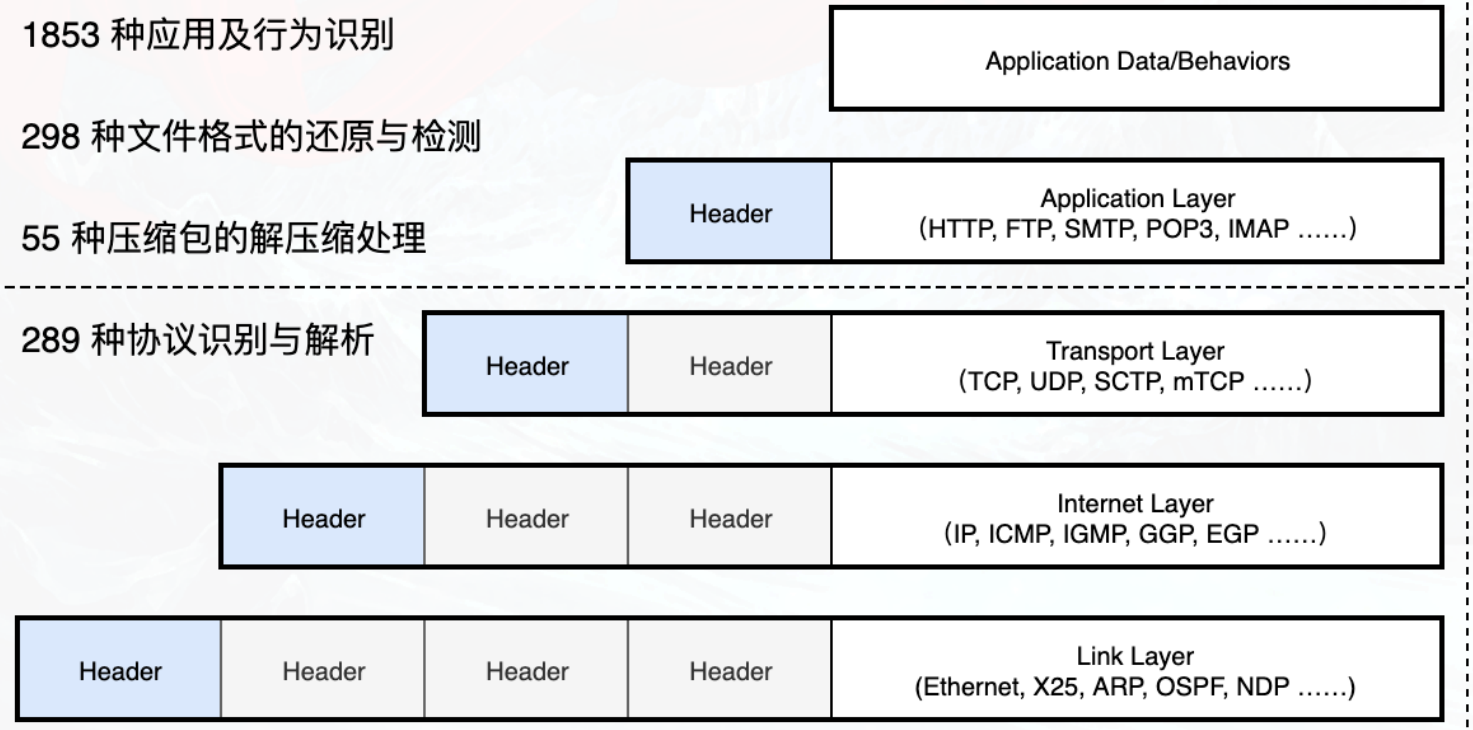
“探海”支持的协议识别、元数据化与要素提取能力

1853 种应用及行为识别

298 种文件格式的还原与检测

55 种压缩包的解压缩处理

289 种协议识别与解析



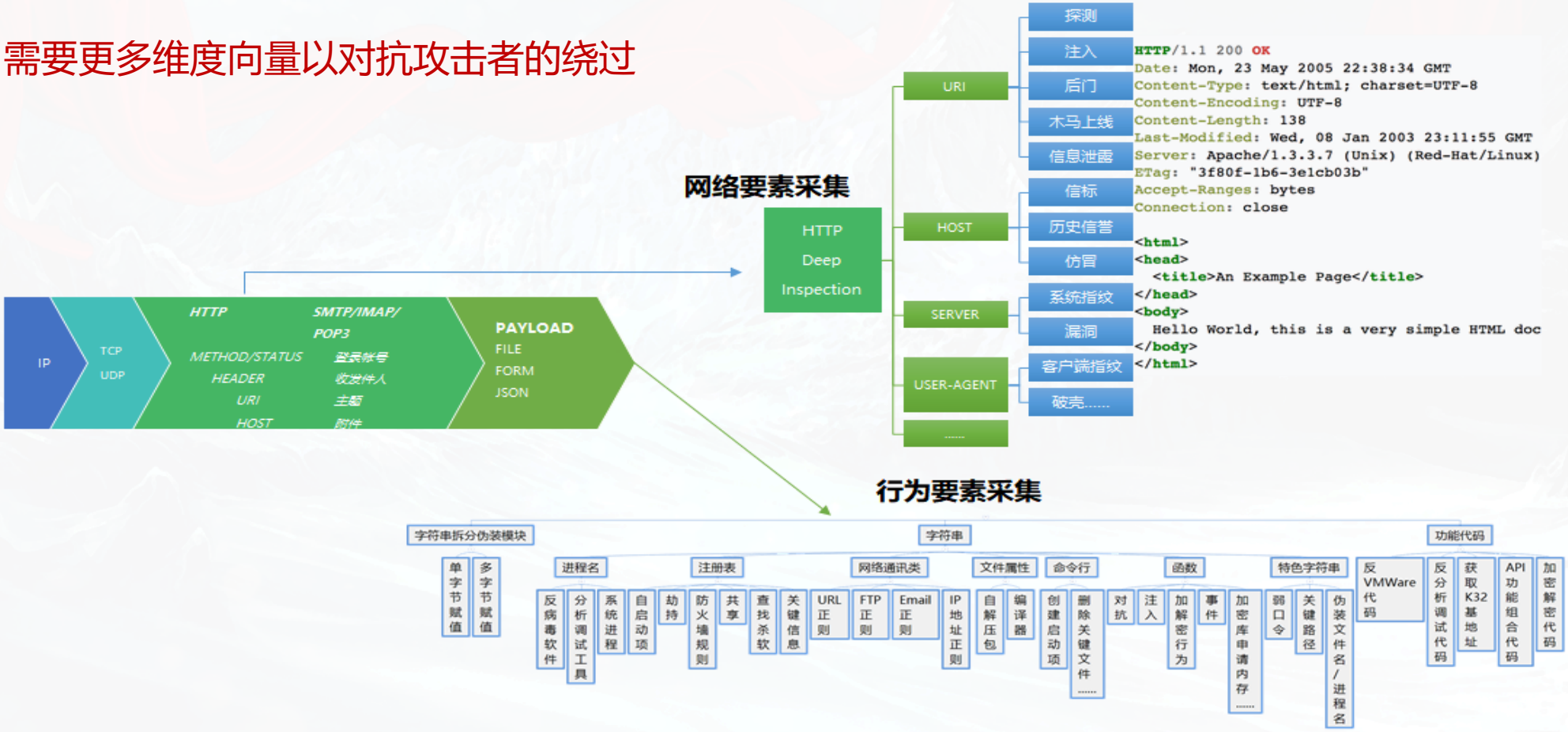
协议识别能力与开源项目对比

产品名称	协议/应用数量
探海	**2142**
OpenAppID	1464
nDPI	248
libprotoident	474

*所有开源项目基于 11 月 3 日版本统计

“探海”为融合威胁情报更丰富的要素采集

需要更多维度向量以对抗攻击者的绕过

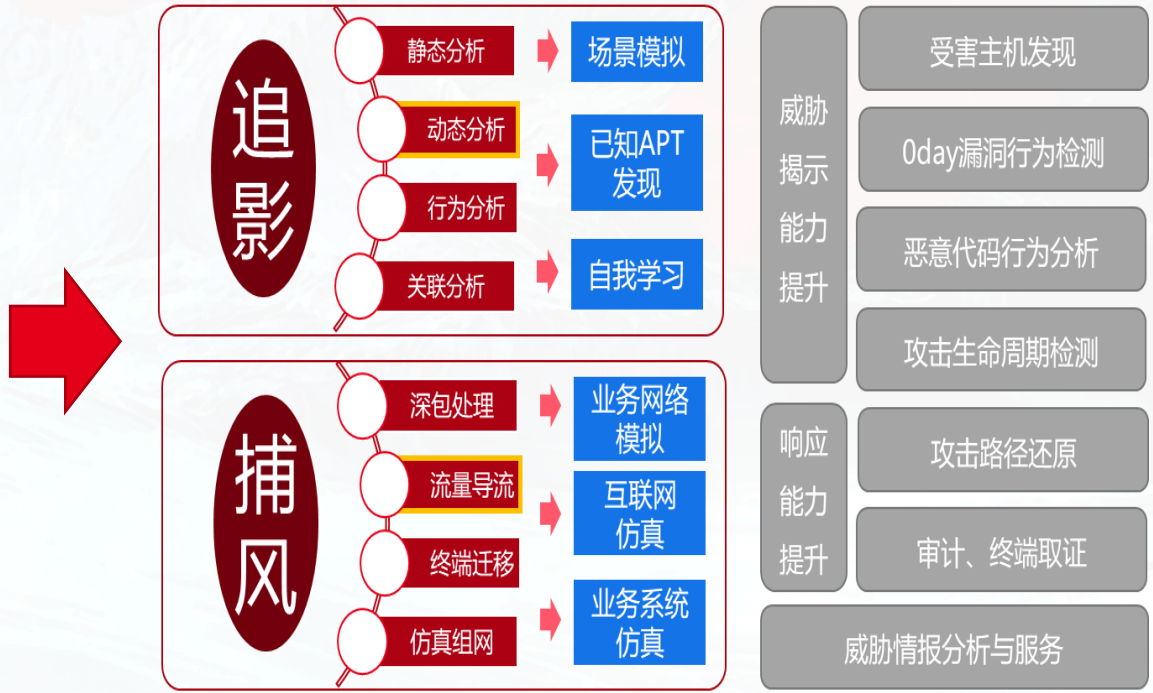


全面掌握资产、实现实体分析需要全要素支撑

- 全面掌握资产以支撑场景化的分析

业务还原	•资产画像 •业务活动画像 •资产-业务活动链条 •设备资产拓扑
资产、业务活动元原数据提取	•可识别、可分析流量类型扩展 •可提取资产、业务元数据扩展 •构建资产、业务元数据模型的场景化应用
从流量中提取协议要素	•虚拟化流量识别和分析 •标准网络流量识别和分析； •业务流量（网络主流应用）特征识别；分类分析和属性标记； •用户的行为元数据提取及分析

- 构建基于我情的沙箱与蜜网



02 更深刻的揭示和理解威胁需要结合威胁框架、融合威胁情报

日趋复杂的威胁、海量的数据与人的心智负荷之间的矛盾

威胁发生

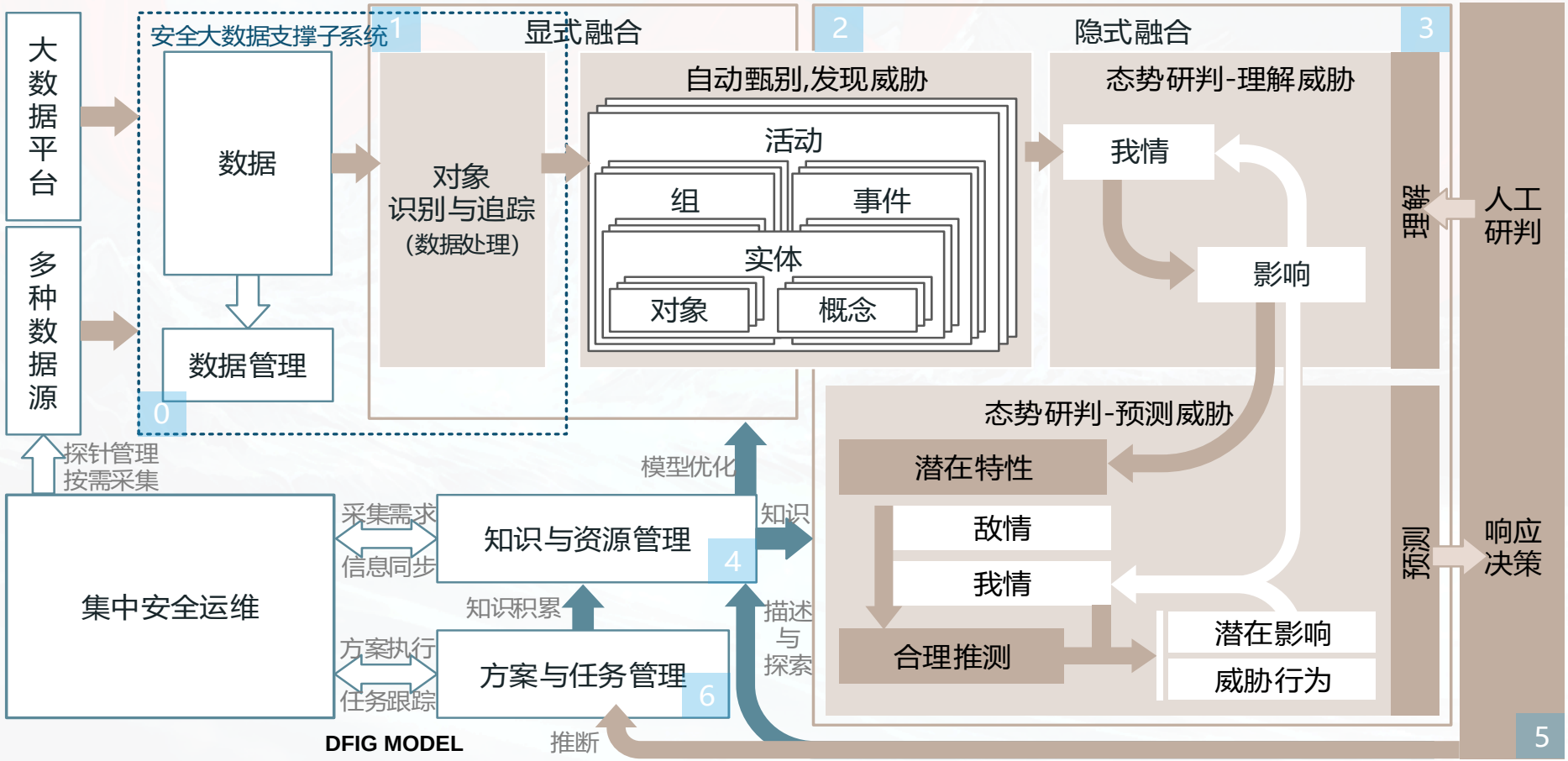
分析

响应

Observe → Orient → Decide → Act

描述	情报分析	攻击阶段
局域网 192.168.18.160 通过 POP 协议 访问 局域网 192.168.18.61 端口：110		ATT&CK 初始访问 执行 持久性
APT 海莲花 木马程序 跨域邮件		NSA CSS 行动管理与资源保障
局域网 192.168.18.186 通过 SMTP 协议 访问 局域网 192.168.18.61 端口：25		ATT&CK 初始访问 执行 持久性
蠕虫程序 Spread Email 跨域邮件		NSA CSS 行动管理与资源保障
局域网 192.168.18.186 通过 SMTP 协议 访问 局域网 192.168.18.61 端口：25		NSA CSS 行动管理与资源保障
APT 白象 木马程序 隐匿程式		
局域网 192.168.18.160 通过 POP 协议 访问 局域网 192.168.18.61 端口：110		ATT&CK 初始访问 执行 持久性
木马程序 邮件通讯		NSA CSS 行动管理与资源保障
局域网 192.168.18.186 通过 SMTP 协议 访问 局域网 192.168.18.61 端口：25		ATT&CK 初始访问 执行 持久性
木马程序 溢出代码		

数据融合是为了支撑人的态势感知



基于确定线索的组织同源关联能力

基于向量揭示攻击技术、攻击资源、攻击工具、攻击行为等

样本

格式文档　可执行文件

压缩文件　脚本文件

图片　……

格式识别、脱壳、解包

静态向量

远控配置解密

数字证书与签名

行为

IP，URL，自启动
信息获取，对抗
传播，控制，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
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

- 攻击技术揭示
- 攻击资源揭示
- 攻击工具揭示
- 攻击行为揭示

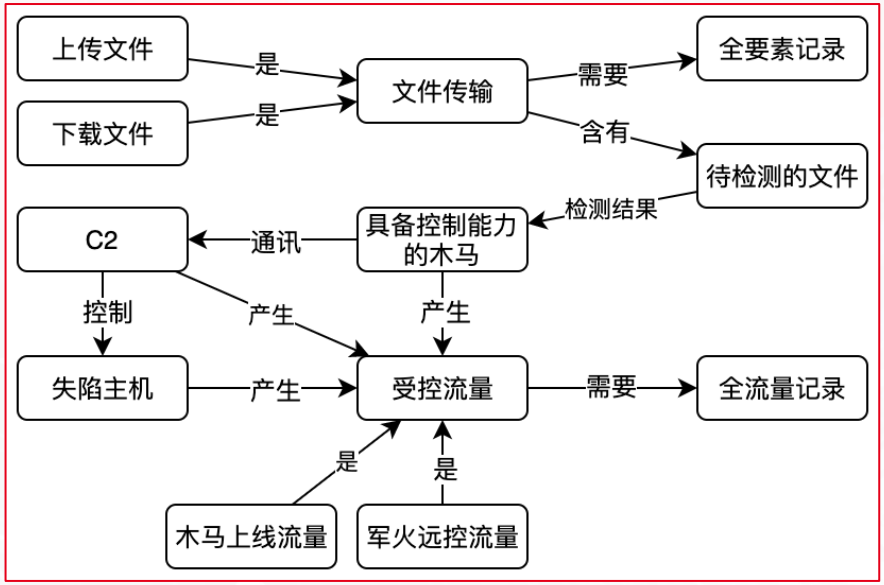
提取时间戳

样本开发者时间分组统计

时区

攻击者所在区域或国家

基于本体模型的产出/推荐新线索的能力



产生受控流量的域名 -> 新 C2

下载木马的来源 -> 新放马源/水坑

借助威胁框架实现系统的威胁分析与响应

APT攻击组织"方程式"情报分析报告

组织信息　意图及目标　攻击活动　技术战术过程

①组织信息

方程式(Equation Group)

性质：超高能力国家/地区行为体　　别名：Equation/方程式/方程式集团/EquationGroup

归属地：美国　　成员：未知

首次公开：2015-02-16 00:00:00　　最后活跃：2019-12-20 14:48:20

组织描述：方程式组织是具有美国背景的超高能力国家/地区行为体，又名Tilded Team、Equation Group等，由卡巴斯基于2015年2月16日首次披露，是一个活跃了近20年的攻击组织。该组织主要针对伊朗、中东、中国、印度、俄罗斯、德国、西班牙、韩国等国家/地区，针对工业控制系统、SWIFT服务提供商、核工业、教育、政府、金融、科研、运营商、网络安全等行业进行破坏、修改、窃密、监视等攻击行动。该组织主要采用零日漏洞利用、U盘摆渡攻击、数十种常见品牌硬盘固件修改、攻击载荷原子化、多种加密算法、安全软件规避、持久化等攻击手法，利用的漏洞涉及CVE-2010-2568、CVE-2011-3402、CVE-2015-2360、打印机后台程序服务漏洞（MS10-061）、快捷方式文件解析漏洞（MS10-046）、RPC远程执行漏洞（MS08-067）等，使用EquationLaser、EquationDrug、DoubleFantasy、TripleFantasy、Fanny、GrayFish等攻击装备。

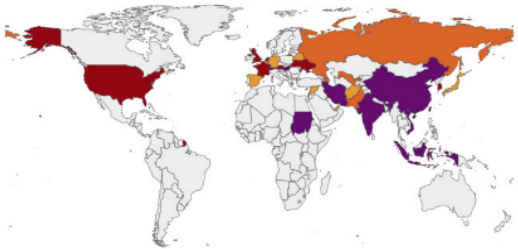
标签：方程式　APT

研究报告：2019-06-01　"方程式组织"攻击SWIFT服务提供商FastNets事件复盘分析报告　https://www.antiy.cn/research/notice&report/research_report/20190601.html

2017-01-26　安天图解方程式组织和木式主机作业　https://www.antiy.cn/research/notice&report/research_report/663.html

②意图及目标

"方程式"组织主要针对伊朗、中东、中国、印度、俄罗斯、德国、西班牙、韩国等国家/地区，针对工业控制系统、SWIFT服务提供商、核工业、教育、政府、金融、科研、运营商、网络安全等行业进行破坏、修改、窃密、监视等攻击行动。其攻击意图包括窃密、破坏、获取系统信息、系统破坏、修改可编程逻辑控制器（PLC）的代码、窃取机密信息、修改数据、物理影响、收集信息、修改硬盘固件、隐藏、窃取信息、修改PLC、监视、控制、间谍、间谍活动、收集受害主机信息、获取基础设施等。



③攻击活动

研究人员发现了2014年出现的恶意软件Stuxnet新组件，这揭示了参与Stuxnet恶意软件的早期开发的第四个组织。此次发现的Stuxshop新模块与另一种名为Flowershop的恶意软件家族与存在关联，Stuxshop是一个旨在提供基本C＆C和登记计划功能的模块，此外所发现的新版本Stuxnet的Duqu 1.5、Flame 2.0也与Flowershop存在关联。Flowershop于2015年被发现，它与泄露方程式工具Territorial Dispute（TeDi）有关。

④威胁分析

MD5:	2BDA3159666B29BF6F912A69B9325435	威胁名称：	Worm/Win32.Stuxnet
组织信息：	方程式 方程式组织是一个美国的超高能力国家行为体，又名Tilded Team、Equation Group等，由卡巴斯基于2015年2月16日首次披露，是一个活跃了近20年的攻击组织。该组织主要针对伊朗、中东、中国、印度、俄罗斯、德国、西班牙、韩国等国家/地区。		
框架信息：	Tided	工具组件：	Stuxnet Dropper
威胁描述：	需网Dropper样本，搜索.stub节，解密并执行,该节包含Stuxnet DLL文件，该节包含Stuxnet DLL文件，这个DLL包含了stuxnet的所有功能。同时，该文件还被用作用户模式rookit，用于隐藏stuxnet文件。具有挂钩API行为。		
标签：	Stuxnet　APT　Dropper　Equation　释放文件　Rootkit　Hook　Shellcode		
情报向量拓展：	关键字：Dropper 其他：.stub		

⑤战术技术过程

战术技术过程

MITRE ATT&CK

初始访问	执行	持久化	提权	防御规避	凭证访问	发现	横向运动	收集	命令控制	渗漏	对抗
		T1179 挂钩	T1179 挂钩	T1140 反混淆/解码文件或信息 T1014 Rootkit	T1179 挂钩					T1022 数据加密	

安天 智者安天下

智者安天下

威胁框架：细粒度对抗

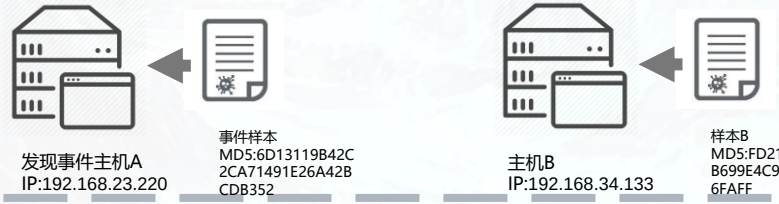
全要素支撑多设备间联合分析也需要对威胁细致的揭示

03 应对高级威胁需要文件深度分析能力来补足的缺口

以 Cobalt Strike 为例，威胁检测仅有流量是不够的

影响分析

事件发现



利用已提取的向量检索其它主机，发现主机B中存在哈希不同于原事件样本A的样本B

向量提取

加密解密	网络通讯	进程操作	反调试	提权	获取信息	服务操作
•RSA加密 **•AES加密**	•HTTP通讯 **•IP:146.0.XX.107**	•枚举进程 **•进程注入**	**•检测调试器** •显示调试字符串	**•查看系统权限的特权值** **•启动或禁止权限**	**•获取机器名称** **•获取用户名称**	•创建服务 •打开服务 •启动服务

事件分析：Cobalt Strike v2.4（后门的商用平台）

高仿真沙箱环境模拟能力，提升漏洞触发效果

主机环境仿真

- 操作系统仿真：已有默认种类超过11种，包括windows（7种，包括xp、win7、winx64、win8、win10等）、**linux（2种，包括centos、ubuntu）、国产沙箱系统（2种,包括中标麒麟、银河麒麟)。**
- 主机环境软件栈仿真类型：默认软件环境覆盖软件类型大于30种，范围涵盖常用办公软件、浏览器、解压软件、运行时环境等；
- 环境定制伪装：诱饵文件动态生成及投放、注册表标识伪装、随机化分析起始路径等
- 可定制化提供指定主机环境组合。

网络环境仿真

- 支持3种网络连接模式切换：隔离局域网仿真连接、模拟网络连接、真实互联网连接
- 模拟网络环境支持10种默认网络协议模拟，包括: TCP、UDP、DNS、FTP、HTTP、HTTPS、IRC、POP3、SMTP、TFTP 等等
- 支持自定义HTTP、TCP网络模拟响应。

行为触发仿真

- 交互仿真类型：智能鼠标移动及点击、智能按钮识别与点击、基于脚本的交互仿真、基本远程窗口的人工交互仿真等

动态分析支持格式

- 默认支持30种文件格式的动态分析还可根据需要进行格式支持扩充。包括可执行文件5种、压缩文件9种，文档文件13种，脚本类6种，其他4种。

全面监控分析,揭示威胁细节：

行为监控API 监控点

- 监控点总数423。
- 涵盖文件（58）、进程（52）、注册表（41）、网络 (104)、服务（18）、系统（43）、反调试（3）、证书（5）、剪贴板（5）、加解密（23）、设备（3）、浏览器（9）、office（11）、内存（3）、网络管理（10）、flash（3）、其他（32）

其他数据输出支持

- 支持API调用日志、截图、衍生文件、进程内存DUMP等的输出

行为分析规则及敏感行为提取能力

- 行为分析规则1115条，覆盖网络类（52）、注册表类（322）、进程类（288）、文件类（84）、其他（369）等类别。
- 支持识别564种敏感行为（危险行为及其他行为）

对抗行为揭示

- 规则总数：100+
- 类别：反虚拟机、反调试、反沙箱等

漏洞利用发现

- 采用shellcode识别、缓冲区溢出行为识别、软件异常行为监控等手段
- 发现堆栈异常操作、DEP绕过、ASLR绕过等典型漏洞利用特征。

内置威胁情报关联

- 支持基于内置威胁情报库，可关联识别APT攻击事件150+；可检测超过600种远控程序；对域名的检测特征数量超过160万，对IP的检测特征超过10万，对URL的检测特征超过20万

满足私有的威胁情报输出需要细粒度的揭示

基本对象信息

- 文件名、大小、哈希、模糊哈希、文件格式、分析时间相关信息等

威胁判定信息 【赋能威胁检测；支撑威胁猎杀】

- 病毒名（威胁分类、核心行为、运行平台、变种号、漏洞号等）
- 病毒百科知识、漏洞相关知识

关联信息 【用于扩线分析；支撑威胁猎杀】

- 文件衍生关系
- 信标关联关系

感染指标（IoC） 【赋能威胁检测；支撑威胁猎杀】

- 网络信标：IP、域名、URL等
- 主机信标：mutex、注册表路径、文件路径等

威胁行为体归属标签

自定义规则命中标签【赋能威胁检测；支撑威胁猎杀】

- Yara鉴定器匹配特征
- 自定义信标匹配特征

战术技术过程（TTPs）标签 【用于威胁理解、扩线分析；支撑威胁猎杀】

- ATT&CK 战术名称、技术名称、对应行为、参数细节等
- TCTF 战术名称、技术名称、对应行为、参数细节等


```
{
    "behaviorsequence": [
    "mal_info": {
    "relation": {
    "danger_behavior": [
    "other_behavior": [
    "file_monitor": [],
    "network_monitor": {
    "mutex": [],
    "process_monitor": [
    "reg_monitor": {},
    "genesummary": [
}
```


动态类向量：总计大于500种

基础行为信息【赋能威胁检测；用于扩线分析；支撑威胁猎杀】

- 文件信息（文件操作，行为，文件路径等）
- 进程信息（进程衍生关系，进程行为）
- 注册表信息（注册表操作）
- 网络行为（TCP UDP HTTP DNS等细节）
- 其他

敏感行为信息【威胁理解；用于扩线分析；支撑威胁猎杀】

- 常见行为列表及动作细节
- 危险行为列表及动作细节

不同主机环境样本行为对比【威胁理解】

扫描判定【用于扩线分析；支撑威胁猎杀】

- yara ， 家族信息扫描
- 字符串扫描信息
- 衍生文件判定信息

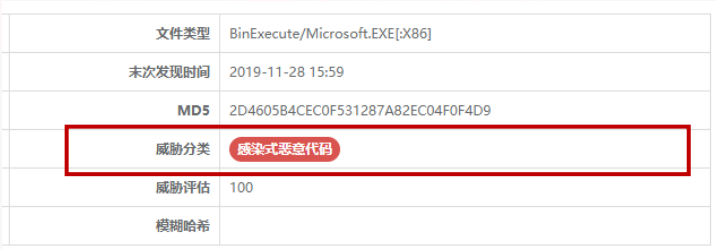
动态截屏【威胁理解】

Pcap文件、内存dump文件【支撑威胁猎杀】

全要素与行为揭示结合，完成私有化的威胁情报生产

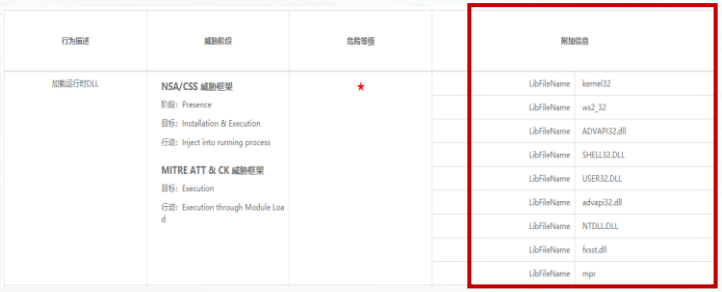
威胁情报输出能力：发现攻击者资源及手段，联动响应与防御设备；

1 判断结果



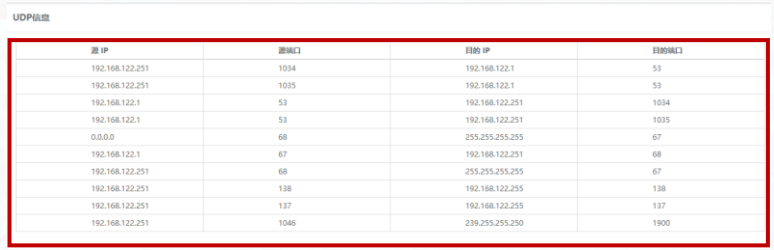
文件类型	BinExecute/Microsoft.EXE[:X86]
未次发现时间	2019-11-28 15:59
MD5	2D4605B4CEC0F531287A82EC04F0F4D9
威胁分类	感染式恶意代码
威胁评估	100
模糊哈希	

2 行为描述



行为描述	威胁阶段	危险等级	附加信息	
加载运行时DLL	NSA/CSS 威胁框架 阶段：Presence 目标：Installation & Execution 行动：Inject into running process MITRE ATT & CK 威胁框架 目标：Execution 行动：Execution through Module Load	★	LibFileName	kernel32
			LibFileName	ws2_32
			LibFileName	ADVAPI32.dll
			LibFileName	SHELL32.DLL
			LibFileName	USER32.DLL
			LibFileName	advapi32.dll
			LibFileName	NTDLL.DLL
			LibFileName	fxsst.dll
			LibFileName	mpr

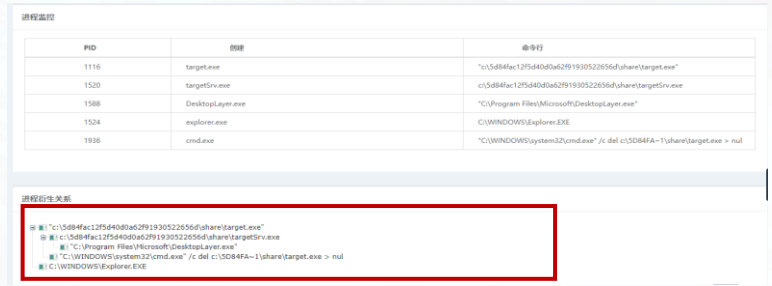
3 网络追溯



UDP信息

源 IP	源端口	目的 IP	目的端口
192.168.122.251	1034	192.168.122.1	53
192.168.122.251	1035	192.168.122.1	53
192.168.122.1	53	192.168.122.251	1034
192.168.122.1	53	192.168.122.251	1035
0.0.0.0	68	255.255.255.255	67
192.168.122.1	67	192.168.122.251	68
192.168.122.251	68	255.255.255.255	67
192.168.122.251	138	192.168.122.255	138
192.168.122.251	137	192.168.122.255	137
192.168.122.251	1046	239.255.255.250	1900

4 衍生关系



进程监控

PID	创建	命令行
1116	target.exe	"c:\5d84fac12f5d40d0a62f91930522656d\share\target.exe"
1520	targetSrv.exe	c:\5d84fac12f5d40d0a62f91930522656d\share\targetSrv.exe
1588	DesktopLayer.exe	"C:\Program Files\Microsoft\DesktopLayer.exe"
1524	explorer.exe	C:\WINDOWS\Explorer.EXE
1936	cmd.exe	"C:\WINDOWS\system32\cmd.exe" /c del c:\5D84FA~1\share\target.exe > nul

进程衍生关系

- "c:\5d84fac12f5d40d0a62f91930522656d\share\target.exe"
  - c:\5d84fac12f5d40d0a62f91930522656d\share\targetSrv.exe
  - "C:\Program Files\Microsoft\DesktopLayer.exe"
  - "C:\WINDOWS\system32\cmd.exe" /c del c:\5D84FA~1\share\target.exe > nul
  - C:\WINDOWS\Explorer.EXE

- 样本定性，寻找高危载荷
- 行为列表，揭示载荷功能
  - ✓行为能力
  - ✓规避方式
- 行为描述，用于关联扩线
  - ✓释放文件
  - ✓Mutex
  - ✓注册表
- 网络监控，发现攻击设施
  - ✓IP、域名、URL
  - ✓是否为定向攻击
- 衍生关系，提供防御手段
  - ✓阻断进程创建

“追影”借助动态分析能力进一步提升对威胁框架的覆盖

初始访问	执行		持久化			提权		防御规避			凭证访问	发现	横向移动	收集	命令与控制	渗出	影响
水坑攻击	利用AppleScript	利用签名的脚本代理...	利用.bash_profile和...	启动代理	利用服务器软件组件	操纵访问令牌	利用服务注册表权限...	操纵访问令牌	绕过Gatekeeper	Process Doppelgäng...	操纵账户	发现账户	利用AppleScript	捕获音频	利用常用端口	自动渗出数据	删除账户权限
利用面向公众的应用...	利用CMSTP	利用Source命令	利用辅助功能	启动守护进程	利用服务注册表权限...	借助辅助功能	利用Setuid和Setgid位	填充二进制文件	修改组策略	替换进程内存	查看Bash历史	发现应用程序窗口	利用应用程序部署软件	自动收集	通过可移动介质通信	压缩数据	损毁数据
利用外部远程服务	利用命令行	加入空格隐藏扩展名	操纵账户	利用Launchctl	利用Setuid和Setgid位	利用AppCert DLL(注...	SID历史注入	利用BITS服务	隐藏文件目录	进程注入	暴力破解	发现浏览器书签	利用组件对象模型(C...	收集剪贴板数据	利用连接代理	加密数据	造成恶劣影响的数据...
添加硬件	利用HTML编译文件	利用系统中的第三方...	利用AppCert DLL(注...	添加LC_LOAD_DYLIB	修改快捷方式	利用AppInit DLL(注册...	利用启动项	绕过用户账户控制(UAC)	隐藏用户	冗余访问	凭证转储	发现域信任	利用远程服务漏洞	收集信息库数据	使用自定义C2协议	限制传输数据大小	网页内容置换攻击
通过可移动介质复制	利用组件对象模型(C...	利用Trap命令	利用AppInit DLL(注...	利用linux本地任务调度	会话发起协议(SIP)和...	利用Windows应用程...	利用Sudo命令	清除命令历史	隐藏窗口	利用Regsvcs/Regasm	获取Web浏览器凭证	发现文件和目录	执行内部鱼叉式钓鱼...	收集本地系统数据	使用自定义加密协议	通过备选协议回传	擦除磁盘内容
使用鱼叉式钓鱼附件	利用控制面板项	利用受信的开发工具	利用Windows应用程...	利用登录项	利用启动项	绕过用户账户控制(U...	利用Sudo缓存凭证	利用CMSTP	HISTCONTROL	利用Regsvr32	获取文件中的凭证	扫描网络服务	利用登录脚本	收集网络共享驱动数据	编码数据	通过C2信道回传	擦除磁盘结构
使用鱼叉式钓鱼链接	使用动态数据交换协...	诱导用户执行	利用认证包	利用登录脚本	利用系统固件	DLL搜索顺序劫持	利用有效账户	代码签名	映像劫持	使用Rootkit	获取注册表中的凭证	发现网络共享	利用密码哈希认证	收集可移动介质数据	混淆数据	通过其他网络介质回传	端点侧拒绝服务(DoS)
通过服务执行鱼叉式...	通过API执行	利用Windows管理规...	利用BITS服务	利用LSASS 驱动程序	利用Systemd服务	Dylib劫持	使用Web Shell	投递后编译	阻止信标捕获	利用Rundll32	利用凭证访问漏洞	网络嗅探	利用Ticket认证	回传数据准备	前置域名	通过物理介质回传	损坏固件
入侵供应链	通过模块加载执行	利用Windows远程管...	使用Bootkit	修改现有服务	利用Trap命令	提示用户输入合法凭...		利用HTML编译文件	删除工具中的信标	使用脚本	强制认证	发现密码策略	利用远程桌面协议	收集电子邮件	使用域名生成算法(DGA)	定时传输	禁止系统恢复
利用受信关系	利用主机软件漏洞	利用XSL文件执行脚本	添加浏览器扩展插件	Netsh Helper DLL	利用有效账户	利用事件监控守护进程		利用组件固件	删除主机中的信标	执行签名的二进制文...	利用Hook	发现主机接入设备	拷贝远程文件	输入捕捉	使用备用信道		网络侧拒绝服务(DoS)
利用有效账户	利用图形用户界面(GUI)		更改默认文件关联	新建服务	利用有效账户	利用漏洞提权		组件对象模型(COM)劫持	间接执行命令	执行签名的脚本代理	输入捕捉	发现权限组	利用远程服务	浏览器中间人攻击(MitB)	利用多跳代理		资源劫持
	利用InstallUtil		利用组件固件	启动Office应用程序	使用Web Shell	额外窗口内存注入(E...		利用连接代理	安装根证书	会话发起协议(SIP)和...	欺骗用户输入凭证	发现进程	通过可移动介质复制	获取屏幕截图	创建多级信道		操纵运行时数据
	利用Launchctl		组件对象模型(COM)...	路径拦截	利用Windows事件订...	利用文件系统权限漏洞		利用控制面板项	利用InstallUtil	软件加壳	使用Kerberoasting技术	查询注册表	共享Webroot目录	捕获视频	使用多协议通信		禁用服务
	利用linux本地任务调度		创建账户	修改属性列表	Winlogon Helper D...	利用Hook		使用DCShadow技术	利用Launchctl	加入空格隐藏扩展名	利用Keychain	发现远程系统	SSH劫持		使用多层加密		操纵本地存储数据
	利用LSASS驱动程序		DLL搜索顺序劫持	端口敲门		映像劫持		反混淆/解码文件或信息	LC_MAIN劫持	模板注入	LLMNR/NBT-NS投毒...	发现安全软件	污染共享内容		端口敲门		系统关机/重启
	利用Mshta		Dylib劫持	端口监控		启动守护进程		禁用安全工具	仿冒	修改文件时间戳	网络嗅探	发现软件	利用系统中的第三方...		利用远程访问工具		操纵传输中的数据
	利用PowerShell		利用事件监控守护进程	利用PowerShell配置...		新建服务		DLL搜索顺序劫持	修改注册表	利用受信的开发工具	利用Password Filter...	发现系统信息	利用Windows管理员...		拷贝远程文件		
	利用Regsvcs/Regasm		利用外部远程服务	利用Rc.common文件		伪造父进程		DLL旁路加载	利用Mshta	利用有效账户	收集私钥	发现系统网络配置	利用Windows远程管...		使用标准应用层协议		
	利用Regsvr32		利用文件系统权限漏洞	重启应用程序		路径拦截		按条件执行	删除网络共享连接	虚拟化/沙箱逃逸	利用Securityd内存	发现系统网络连接			使用标准加密协议		
	利用Rundll32		隐藏文件和目录	冗余访问		修改属性列表		利用漏洞规避防御	利用NTFS交换数据流...	利用Web服务	窃取Web会话Cookie	发现系统所有者/用户			使用标准非应用层协议		
	利用计划任务		利用Hook	添加注册表运行键/启...		端口监控		额外窗口内存注入(EW...	混淆文件或信息	利用XSL文件执行脚本	双因子认证拦截	发现系统服务			利用不常用端口		
	使用脚本		利用Hypervisor	利用计划任务		利用PowerShell配置...		修改文件和目录权限	伪造父进程			发现系统时间			利用Web服务		
	利用windows服务		映像劫持	利用屏幕保护程序		进程注入		删除文件	修改属性列表			虚拟化/沙箱逃逸					
	利用签名的二进制文...		利用内核模块和扩展	利用SSP DLL(注册表...		利用计划任务		文件系统逻辑偏移	端口敲门								

- 不相关
- 无效（未覆盖）
- 有效
  - 可防御/可拦截
  - 可检测/可记录
  - 可降低机会
  - 可输出知识

智者安天下

威胁框架：细粒度对抗

文件深度分析进一步补充威胁框架的映射威胁分析与响应

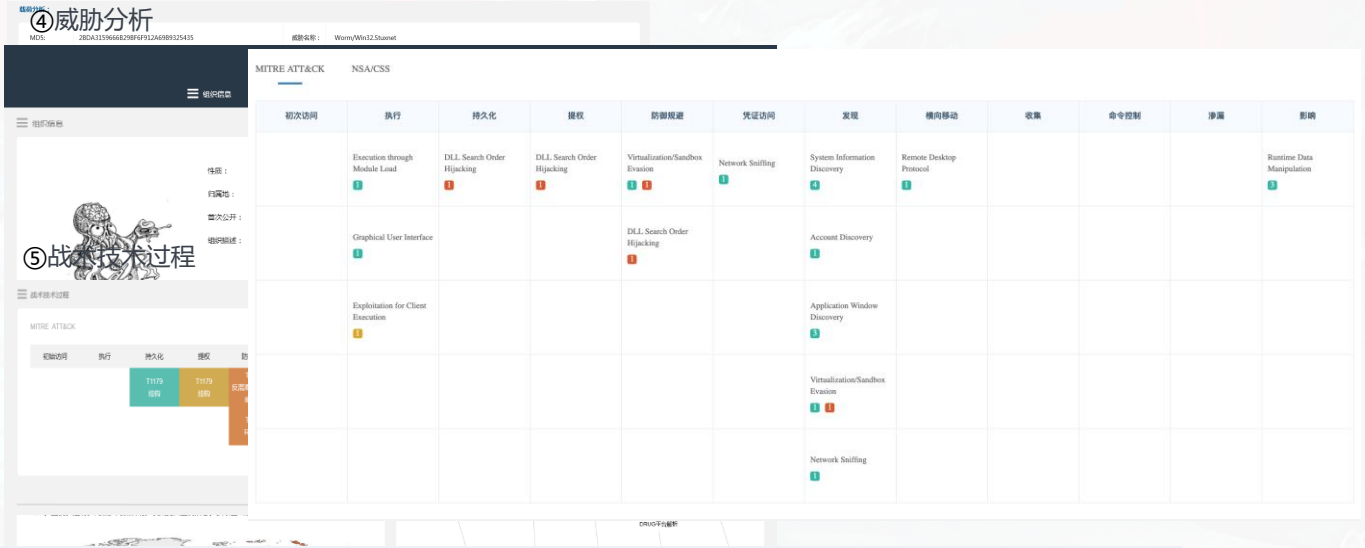
①组织信息

②意图及目标

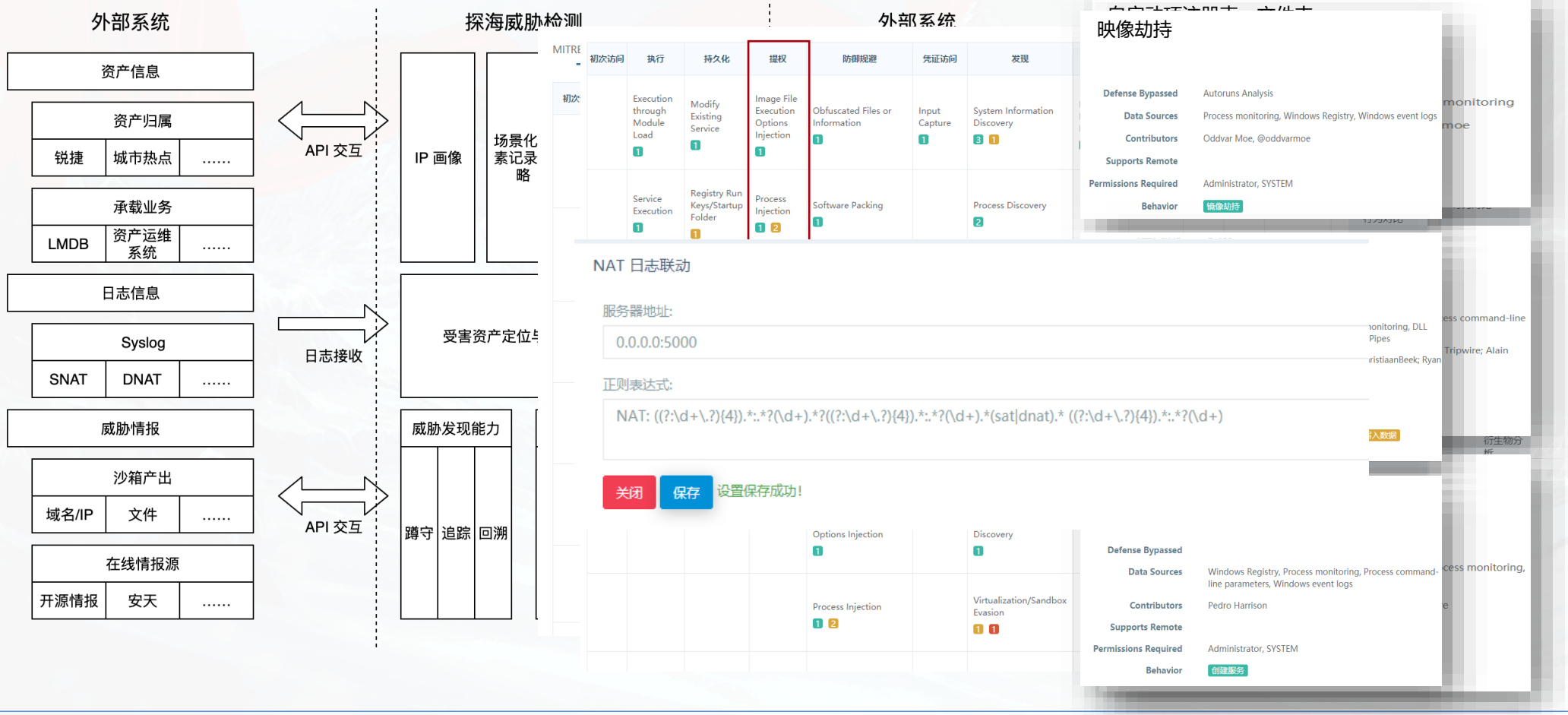
③攻击活动

④威胁分析

⑤战术技术过程



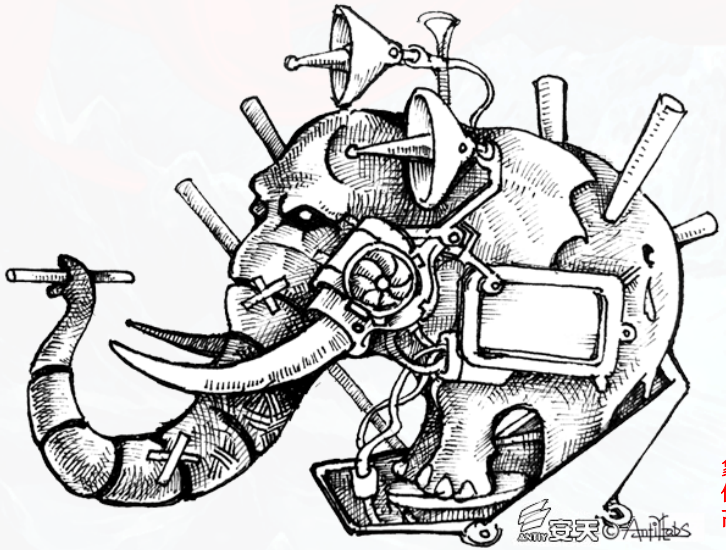
多设备间联合分析的缺失，可以借助深度分析得到补足

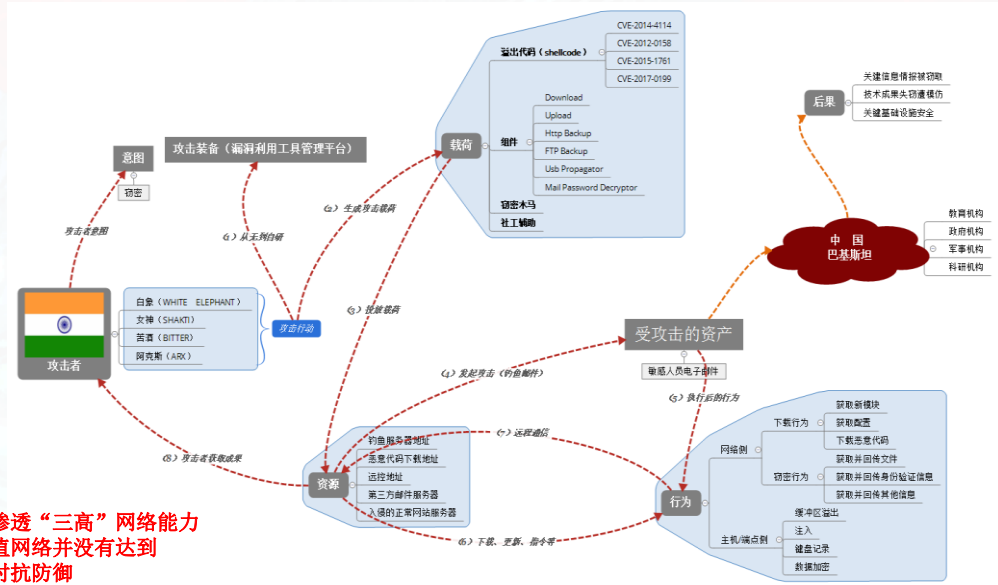


威胁框架：细粒度对抗

04 加密流量与威胁的长尾化需要产品能够支撑持续运营

高级威胁使用一次性载荷，并采用加密通讯投递

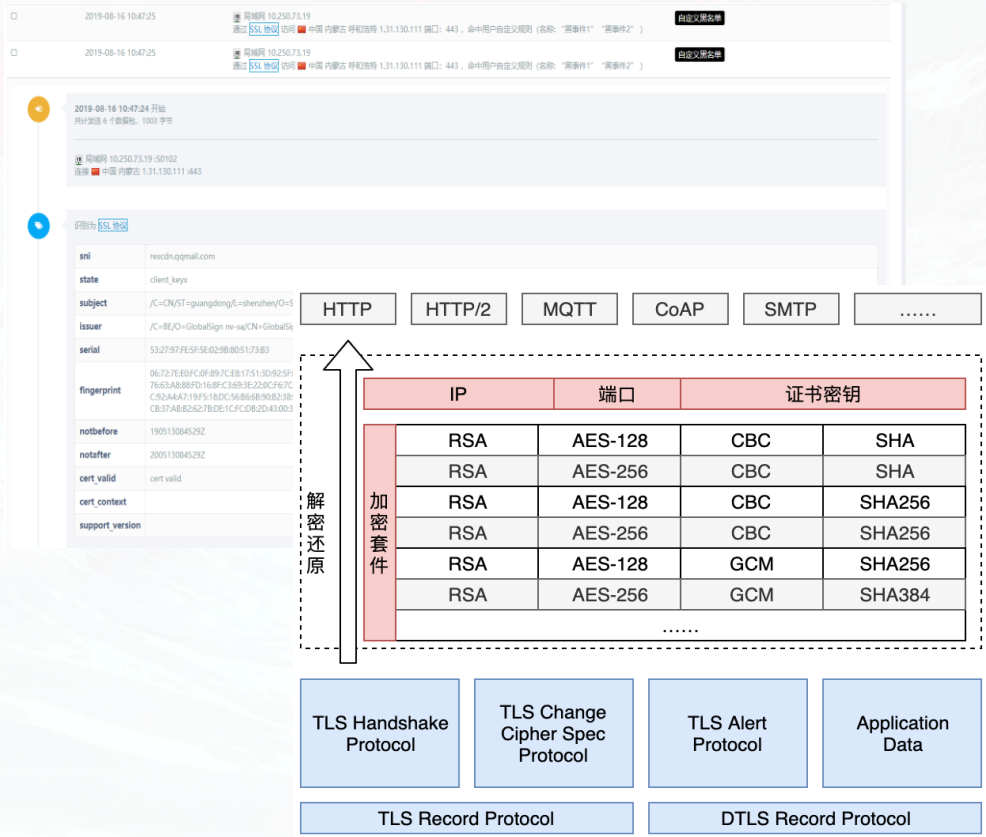




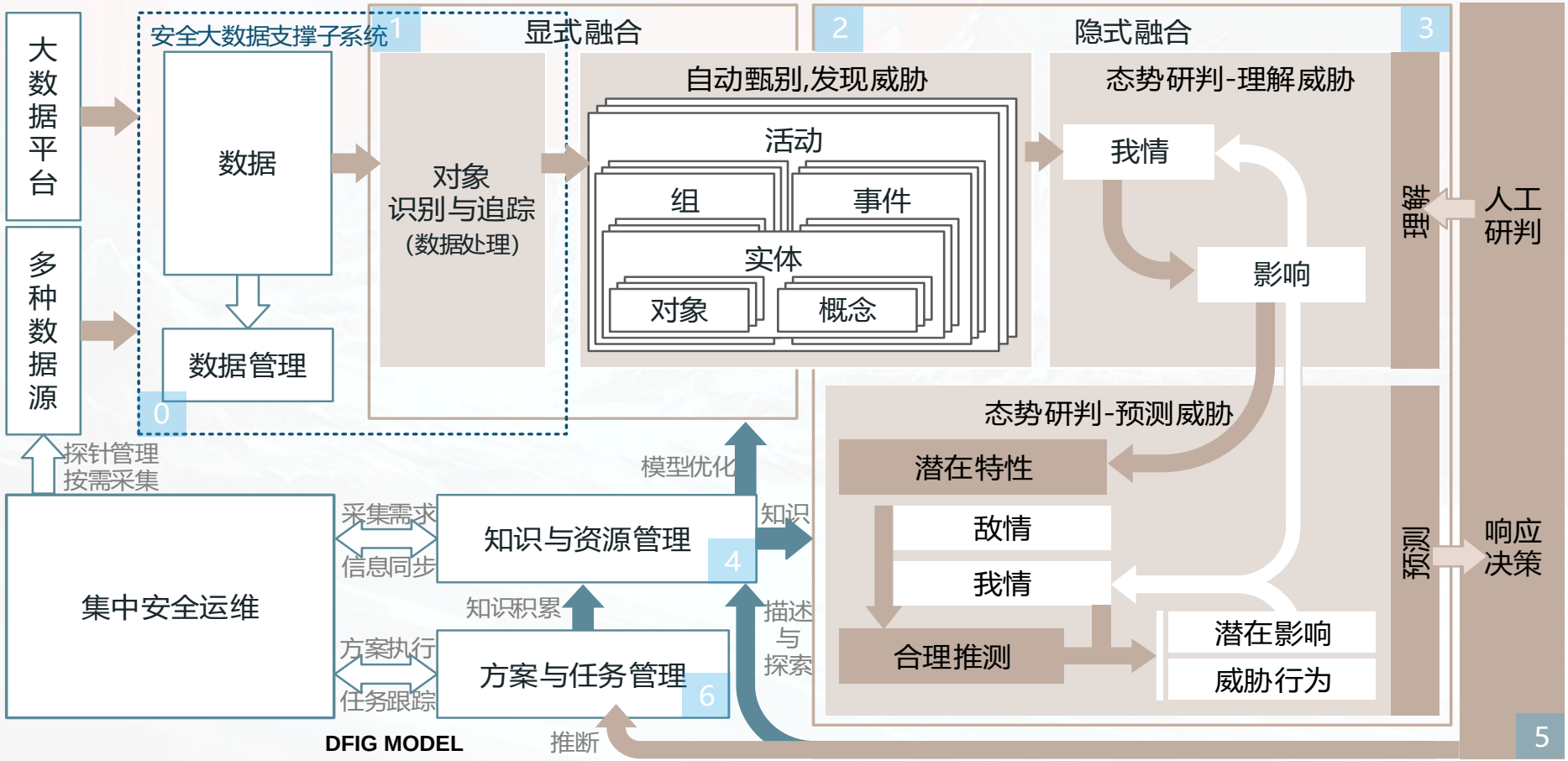
象群作业能力达不到渗透“三高”网络能力
但目前很多高信息价值网络并没有达到
高防护等级和高信息对抗防御

加密流量需要提取更丰富的要素

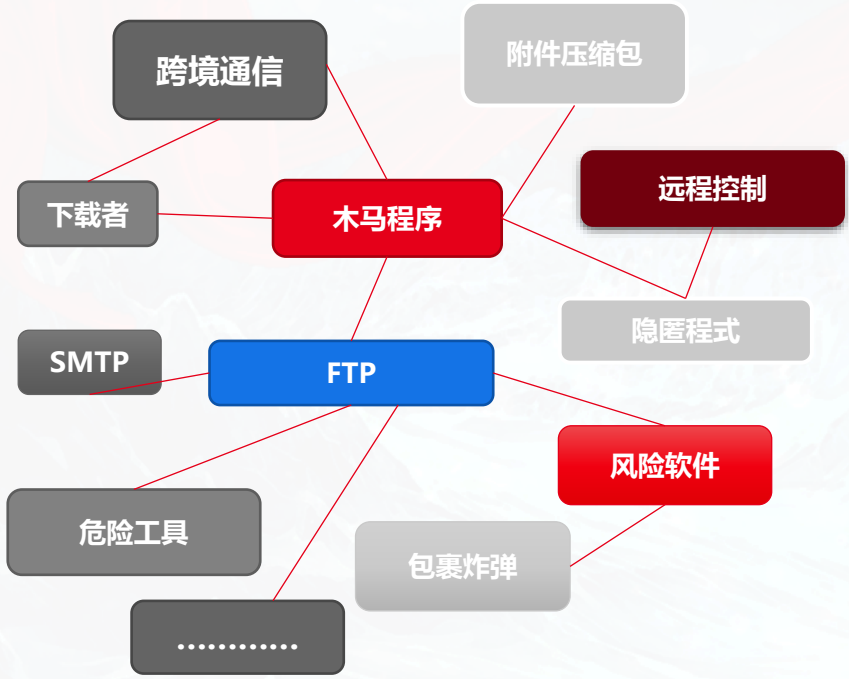
- IP 层
- TCP/UDP 层
- 应用层
  - DNS
  - DNS over TLS
  - DNS over HTTPS
  - HTTPS
  - QUIC
  - TLS/SSL
  - ……

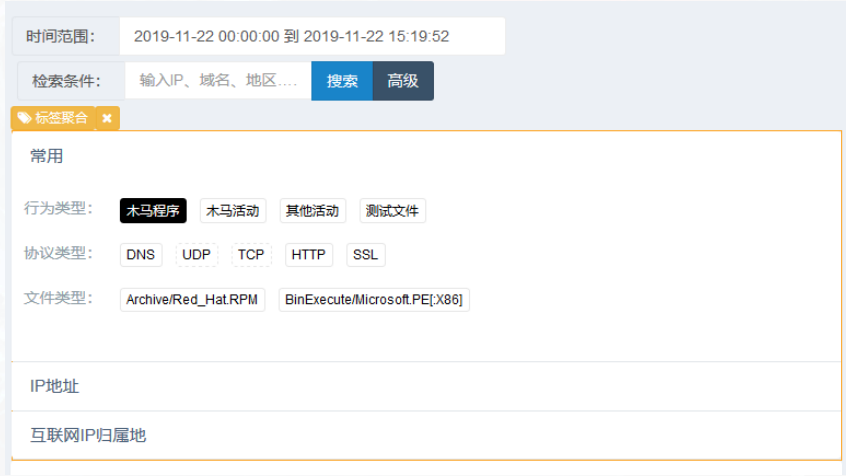


数据融合是为了支撑人的态势感知



检测结果标签化，威胁框架标注，辅助人员筛选关键威胁

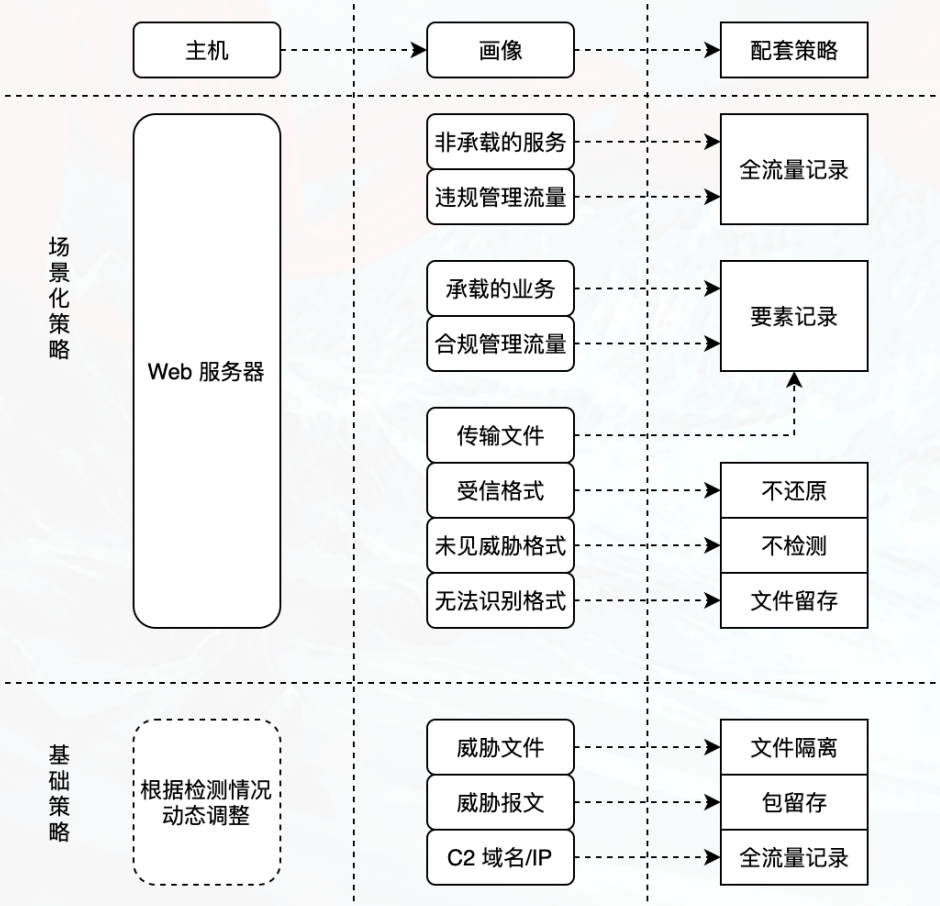




1. 减少用户需要关注的信息量
2. 传递标签背后的知识

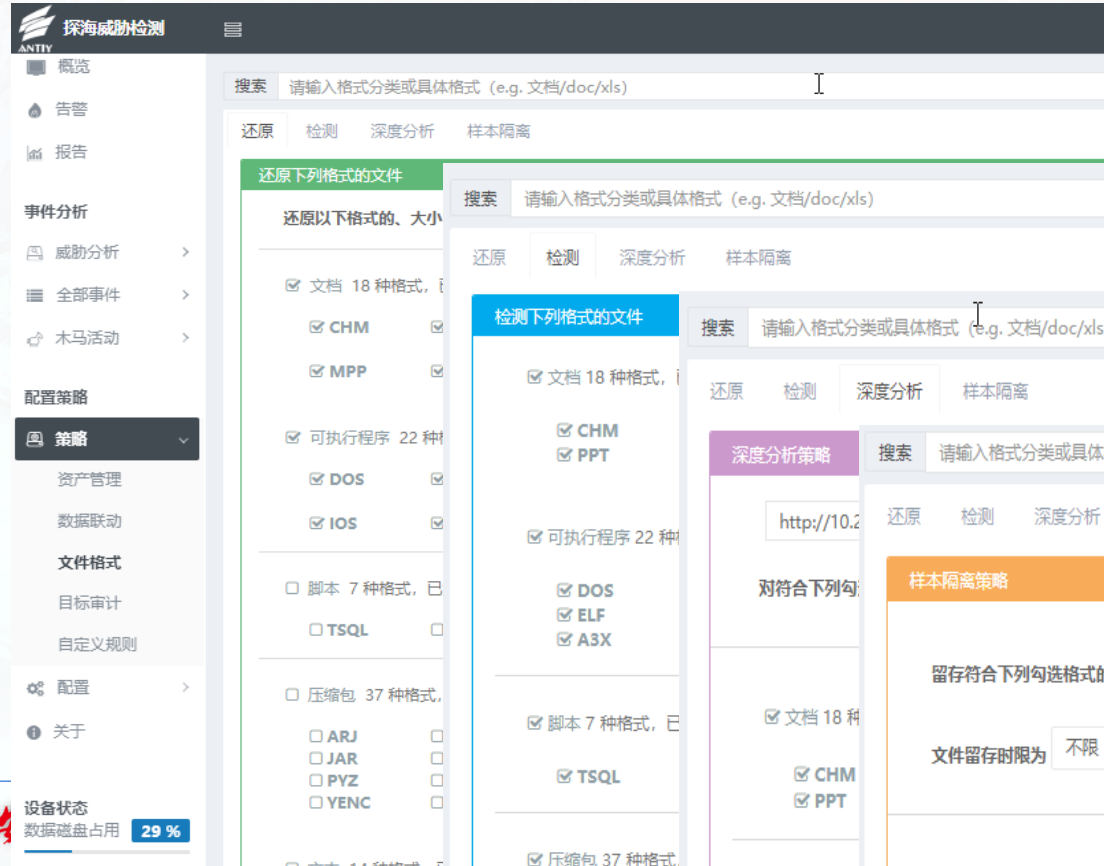
通过标签聚合和IP聚合可快速定位威胁事件，提升威胁揭示能力及威胁响应速度，避免受到高级威胁的侵害

威胁情报指引、场景触发的不同粒度记录能力

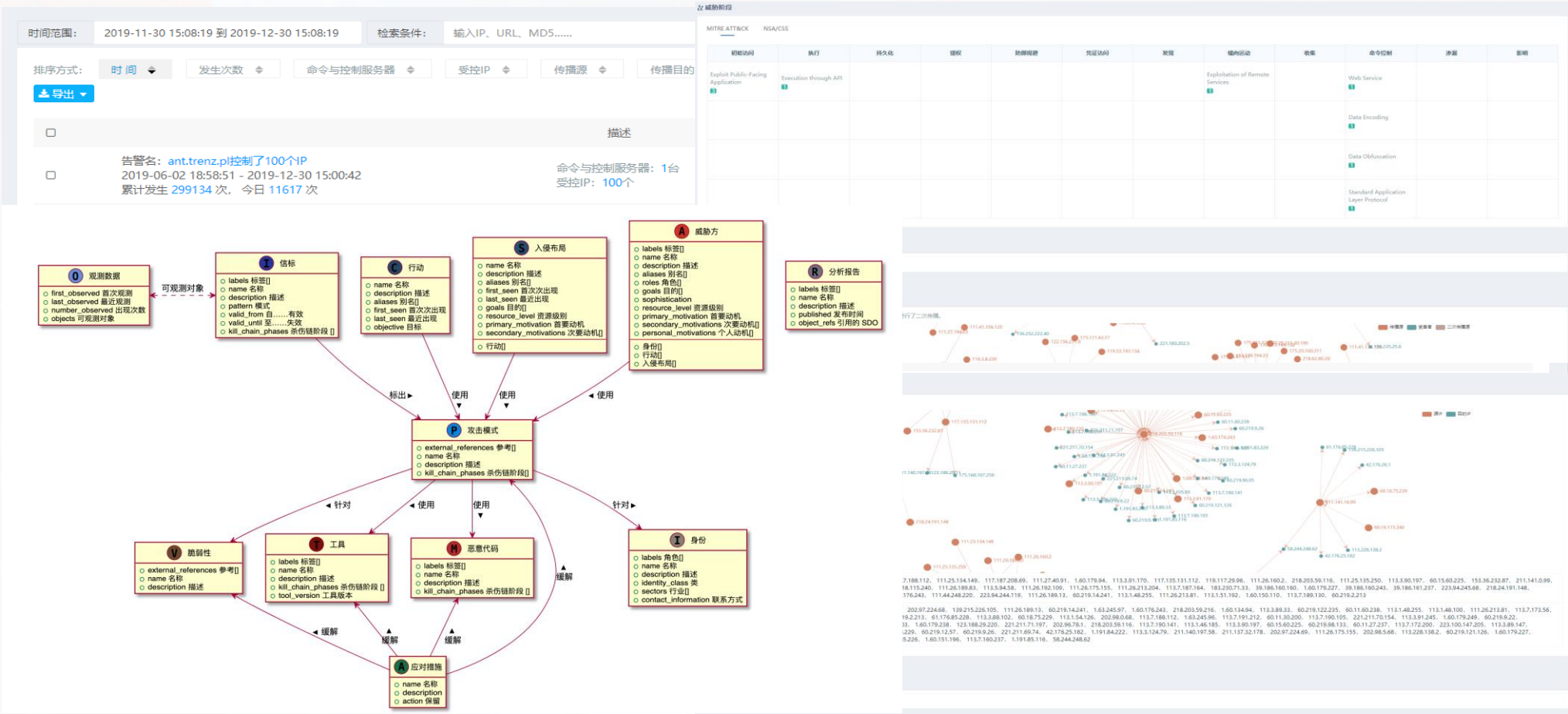


以威胁发现为目标的基础记录策略+场景化策略

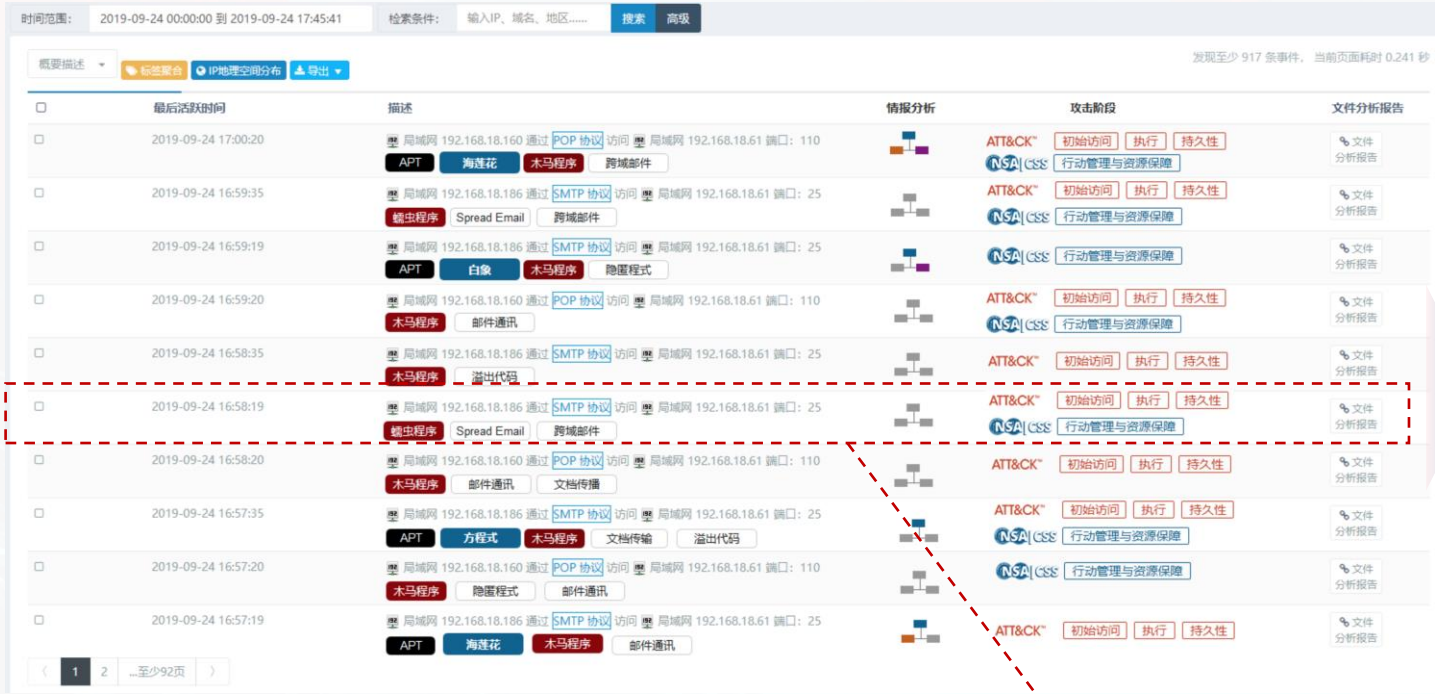
优化需要记录的数据、提升人员分析效率



基于本体模型自动合并告警，降低分析人员负荷



“探海”支持持续将经验转换为标签规则、场景规则



- **行为向量提取+标签化**

1. 减少用户需要关注的信息量
2. 传递标签背后的知识

- **场景化**

1. 多个标签恰好构成了不同的场
2. 自定义条件规则构成场景

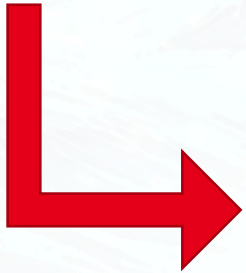
- **威胁情报共享**

1. 将威胁情报线索应用为检测规则

【示例】识别特定攻击

跨境通讯、邮件通讯、压缩包、包含脚本

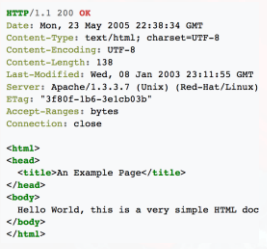
“探海”支撑态势感知所需的流量监测预处理能力



结合下发的预处理规则
降低威胁感知的负荷，提升高威胁发现时效

充分利用流量全要素，结合威胁框架
融合威胁情报与资产信息，形成可持续运营的威胁检测能力

细粒度解析、全要素采集、真实格式识别



流式协议解析

280+文件格式

全要素采集

多层次，多维度的精准检测

多维度全向量检测

AVSDK

Since 2000

自主研发的检测引擎

开放式引擎，构建场景，赋能用户

场景化检测

SNORT

SURICATA

规则兼容

快速集成情报

威胁视角和资产视角的关联分析

威胁画像

路径呈现

谢谢大家