网络空间威胁对抗与防御技术研讨会
暨 第七届安天网络安全冬训营

流量全要素记录

融合细粒度威胁情报与威胁框架支撑威胁猎杀

安天监测分析产品子线

威胁框架：认知与实践

寒夜远征

寒夜迷径

CONTENTS

目 录

产品回顾

探海威胁检测系统

- 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

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


获奖证书

CNCERTICC 国家互联网应急中心 | 中国网络安全技术对抗赛

北京安天网络安全技术有限公司：

你公司 追影威胁分析系统与探海威胁检测系统 产品荣获

2019中国网络安全技术对抗赛

第一名

特发此证，以资鼓励！

国家计算机网络应急技术处理协调中心

二零一九年十二月

安天蝉联中国网络安全技术对抗赛第一名

寒夜速记

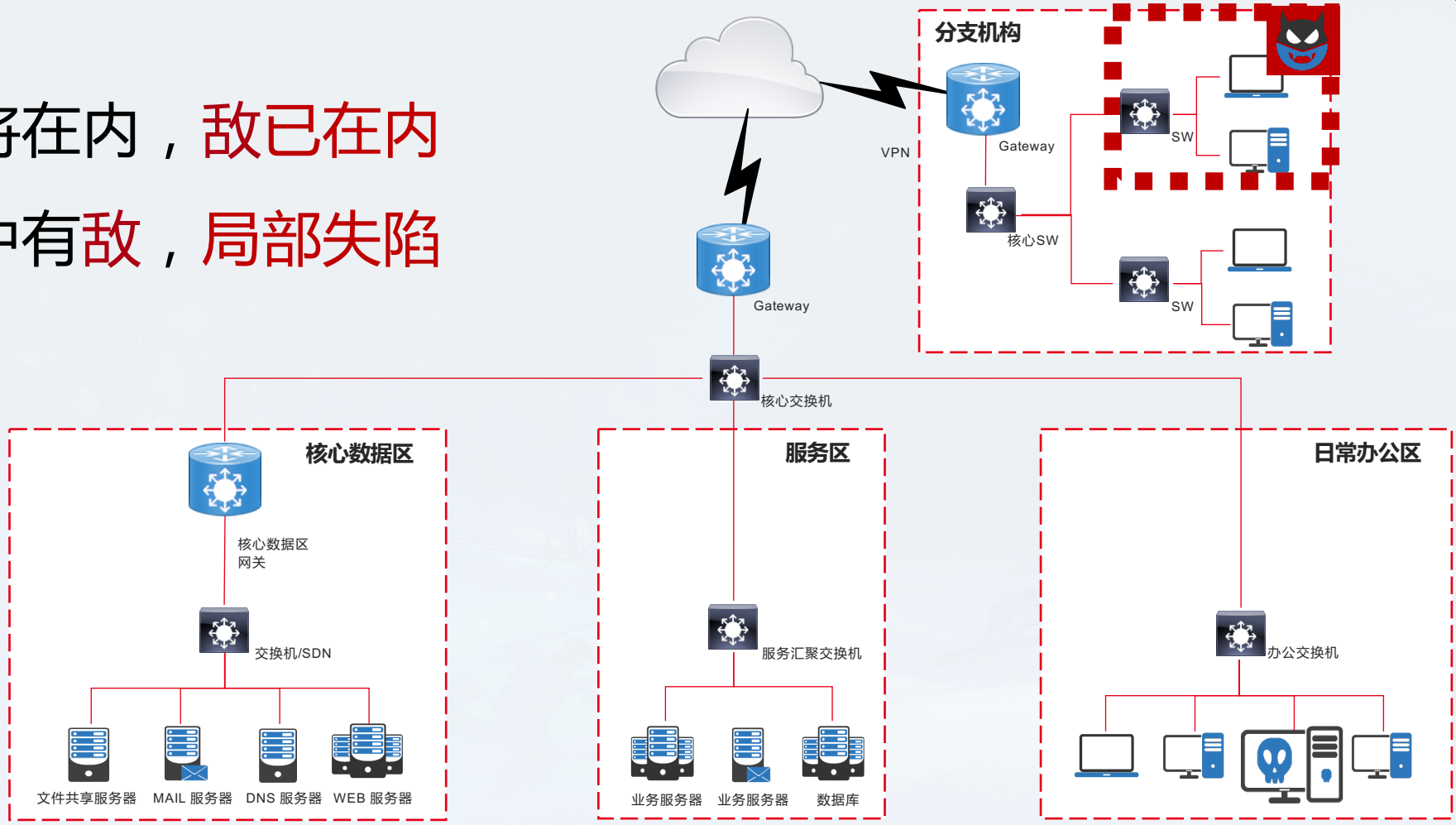
威胁框架：认知与实践

01 监测需要详尽长期的要素记录

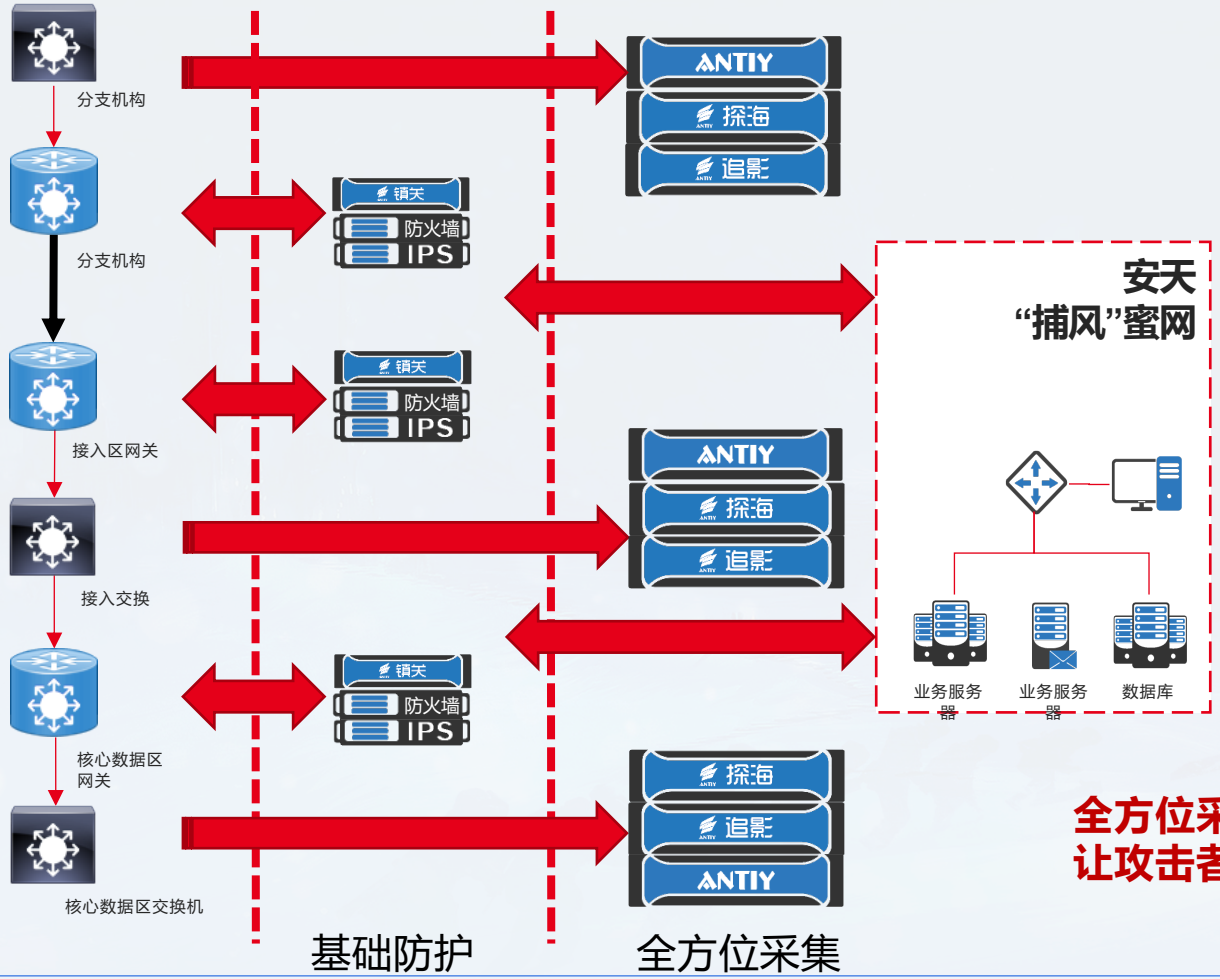
我中有敌、局部失陷是基本的敌情假定

敌将在内，敌已在内

我中有敌，局部失陷



交叉火力部署在攻击者的必经之路，基于纵深发现失效



- 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

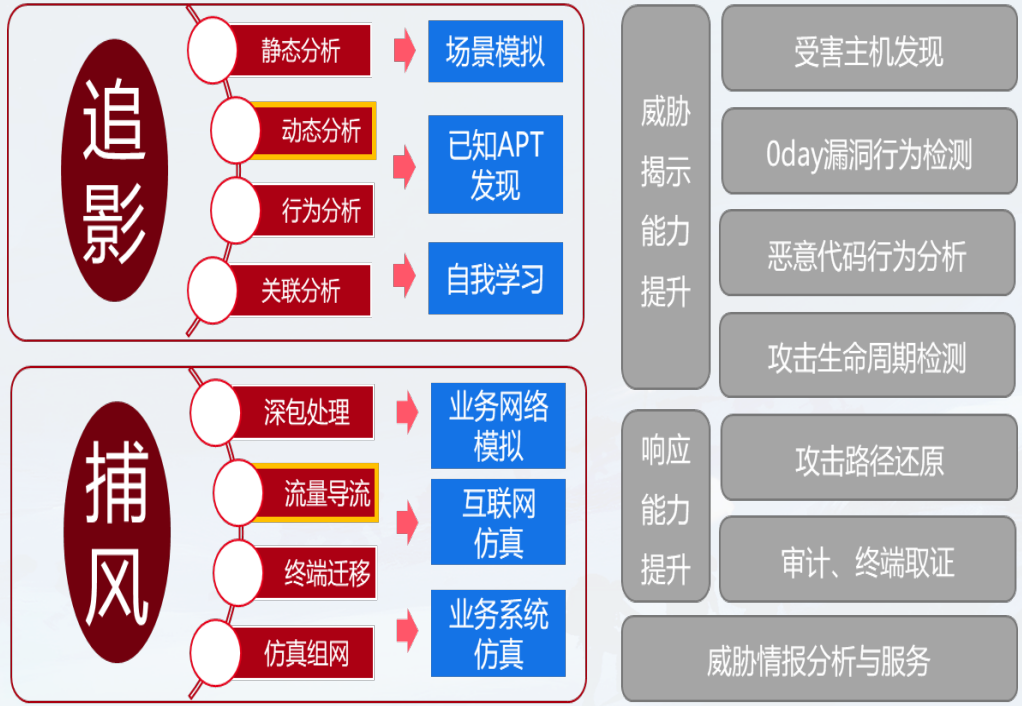
全方位采集、智能化响应
让攻击者无所遁行、无处可逃、无计可施

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



寒夜速记

威胁框架：认知与实践

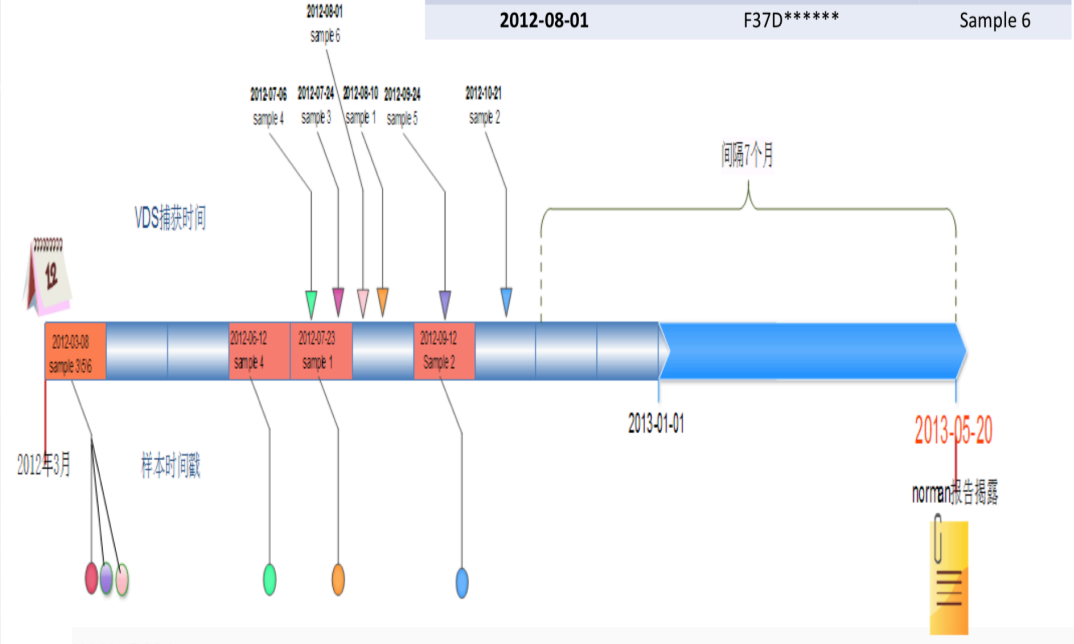
2.1 辩证地看全要素记录与分析

日益增长的流量记录分析诉求与有限的数据存储计算能力之间的矛盾

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；

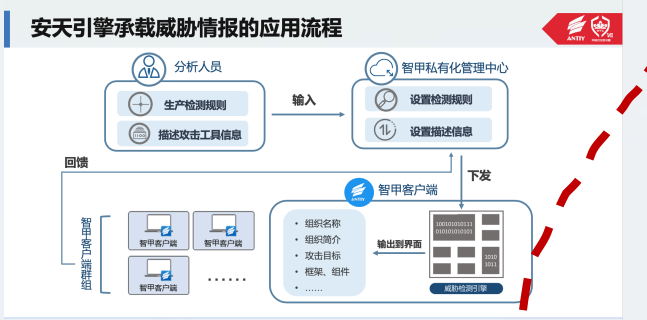
（三）采取监测、记录网络运行状态、网络安全事件的技术措施，并按照规定留存相关的网络日志不少于六个月；

（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

C2服务器

暂存服务器

内网服务器

横向移动

数据资产

水坑攻击

鱼叉式钓鱼

内网主机

横向移动

内网主机

数据资产

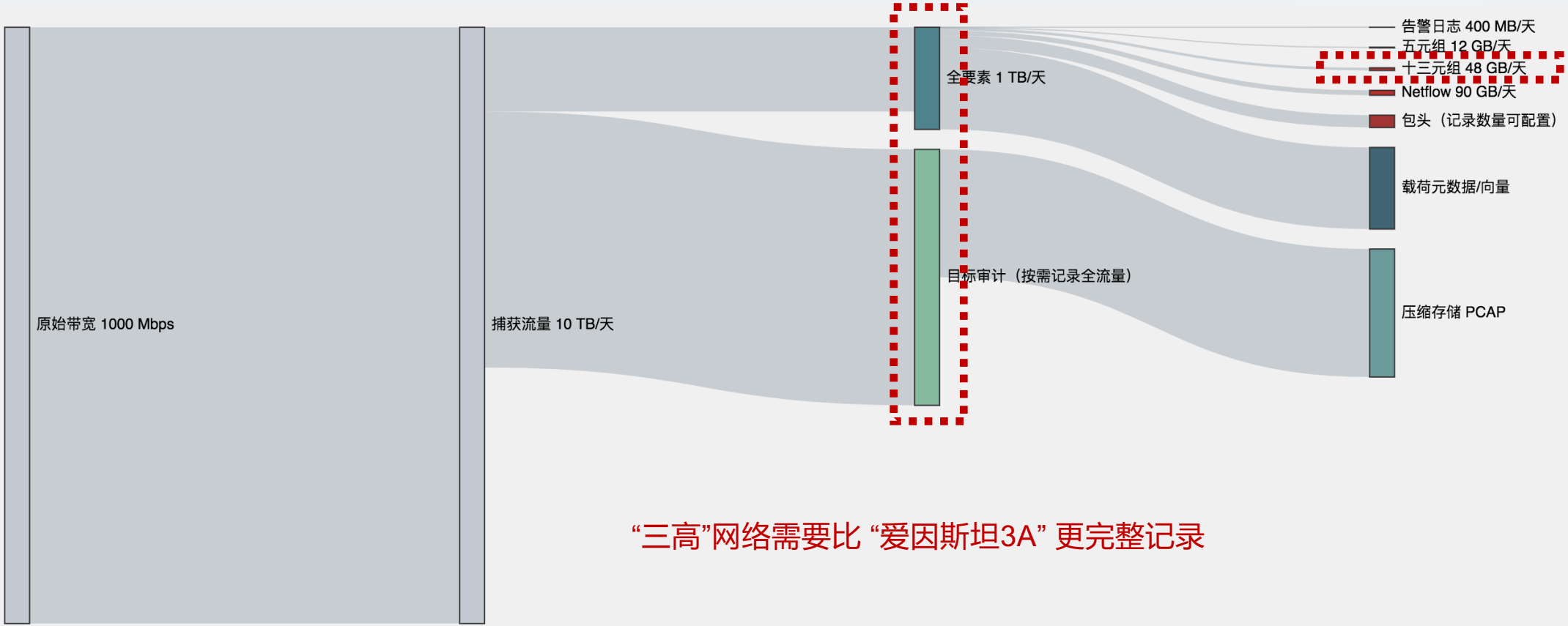
必经路径——全要素记录

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

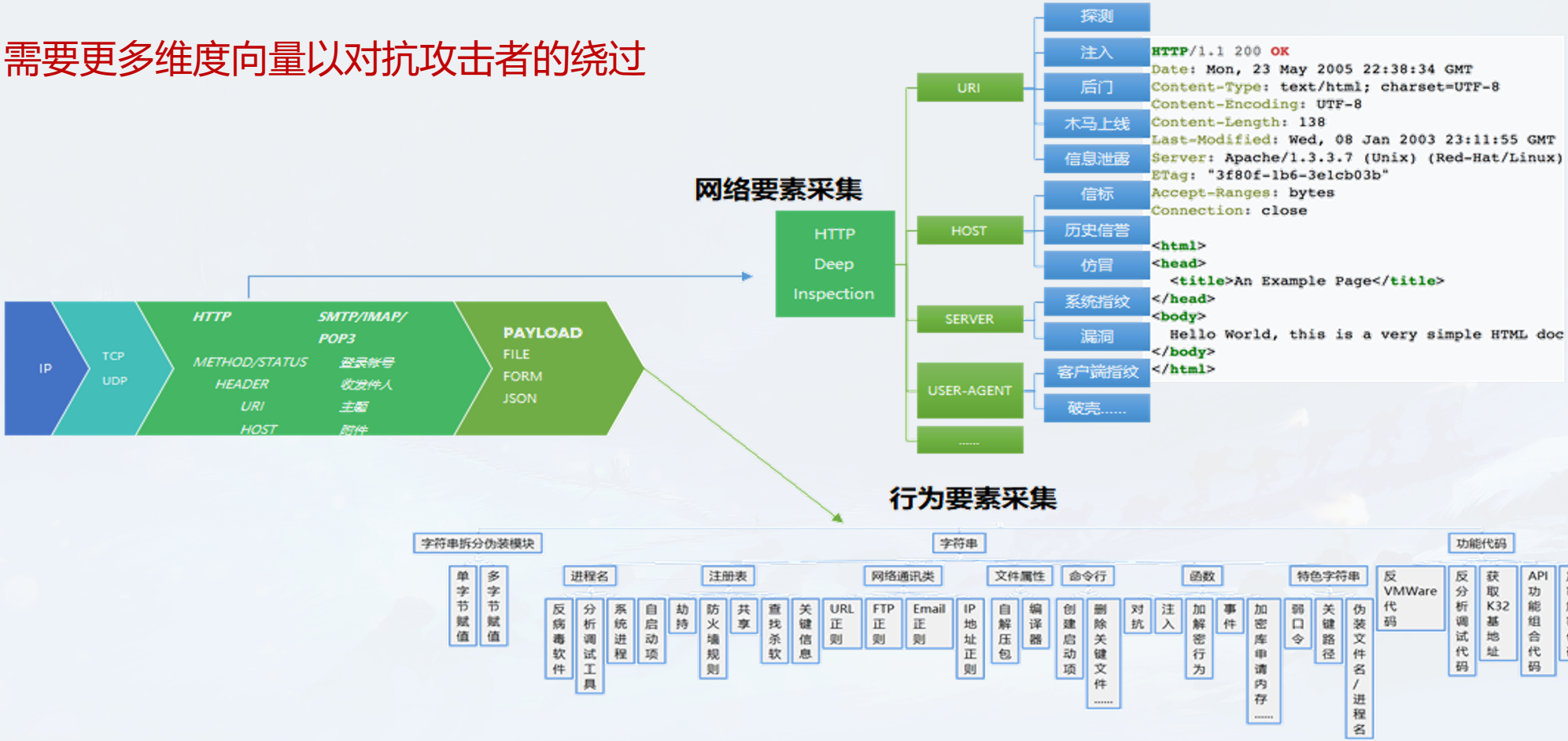
“探海”提供指引猎杀所需完整的要素采集



“三高”网络需要比 “爱因斯坦3A” 更完整记录

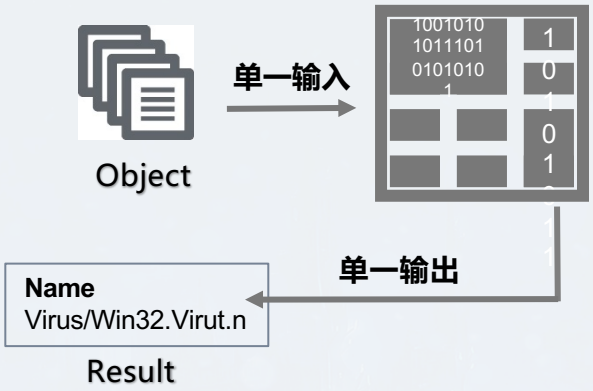
“探海”为融合威胁情报更丰富的要素采集

需要更多维度向量以对抗攻击者的绕过



安天探海威胁检测系统 - ATT&CK威胁框架覆盖度

引擎能力的维度--多种输入输出对象

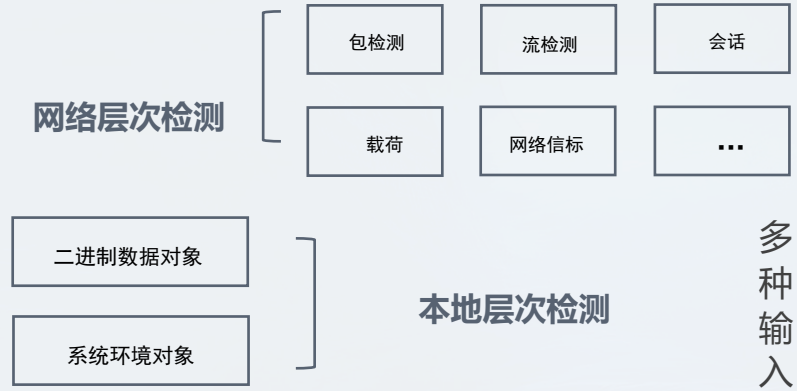


✓ **传统引擎**

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

引擎能力的维度—对ATT&CK框架的覆盖

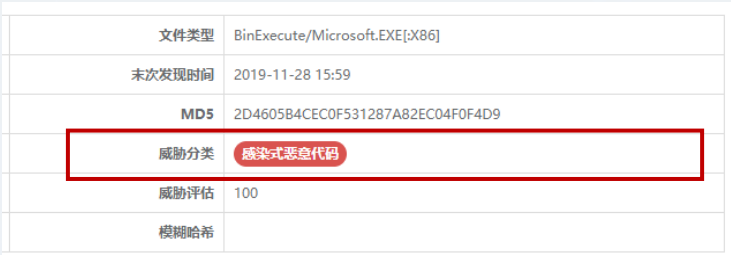
初始访问	执行		持久化			提权		防御规避			凭证访问	发现	横向移动	收集	命令与控制	渗出	影响
水坑攻击	利用AppleScript	利用签名的脚本代理...	利用.bash_profile和...	启动代理	利用服务器软件组件	操纵访问令牌	利用服务注册表权限...	操纵访问令牌	绕过Gatekeeper	Process Doppelgäng...	操纵账户	发现账户	利用AppleScript	捕获音频	利用常用端口	自动渗出数据	删除账户权限
利用面向公众的应用...	利用CMSTP	利用Source命令	利用辅助功能	启动守护进程	利用服务注册表权限...	借助辅助功能	利用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Windows时间服务	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Trap命令	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

全要素与行为揭示结合，支撑检测与响应，扩展事件线索

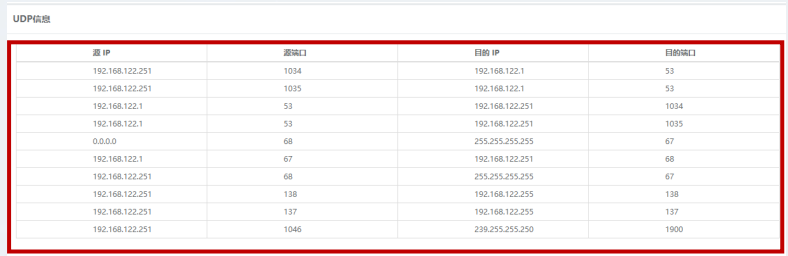
威胁情报输出能力：发现攻击者资源及手段，联动响应与防御设备；

1 判断结果



文件类型	BinExecute/Microsoft.EXE[:X86]
末次发现时间	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	

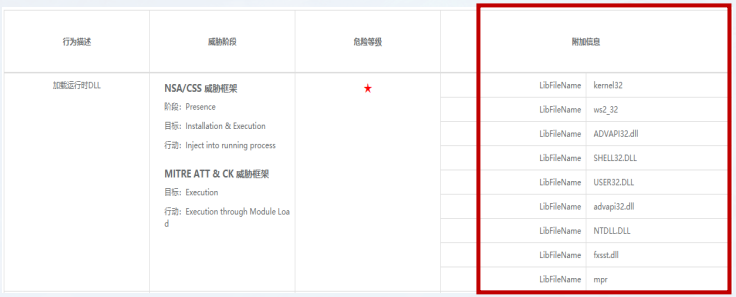
3 网络追溯



UDP信息

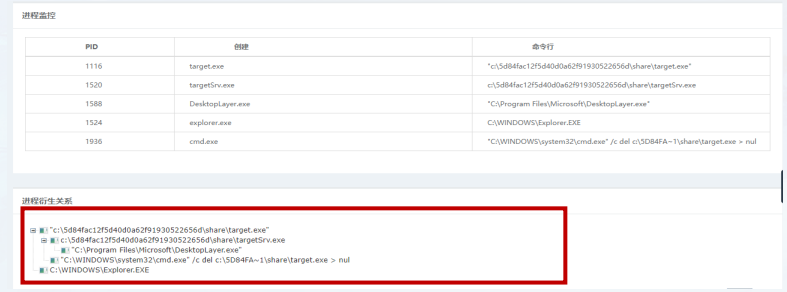
源 IP	源端口	目的 IP	目的端口
192.168.122.251	1034	192.168.122.1	53
192.168.122.251	1035	192.168.122.1	53
192.168.122.1	53	192.168.122.251	1034
192.168.122.1	53	192.168.122.251	1035
0.0.0.0	68	255.255.255.255	67
192.168.122.1	67	192.168.122.251	68
192.168.122.251	68	255.255.255.255	67
192.168.122.251	138	192.168.122.255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

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

4 衍生关系



进程监控

PID	创建	命令行
1116	target.exe	"c:\5d84fac12f5d40d0a62f9193052656d\share\target.exe"
1520	targetSrv.exe	c:\5d84fac12f5d40d0a62f9193052656d\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:\5d84fac12f5d40d0a62f9193052656d\share\target.exe"
  - c:\5d84fac12f5d40d0a62f9193052656d\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.bash_profile和...	操纵访问令牌	操纵访问令牌	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	利用辅助功能	借助辅助功能	填充二进制文件	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	操纵账户	利用AppCert DLL(注...	利用BITS服务	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AppCert DLL(注...	利用AppInit DLL(注册...	绕过用户账户控制(UAC)	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	网页内容篡改攻击
通过可移动介质复制	利用组件对象模型(C...	利用AppInit DLL(注...	利用Windows应用程...	清除命令历史	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Windows应用程...	绕过用户账户控制(U...	利用CMSTP	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...	利用认证包	DLL搜索顺序劫持	代码签名	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BITS服务	Dylib劫持	投递后编译	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	使用Bootkit	提示用户输入合法凭...	利用HTML编译文件	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	添加浏览器扩展插件	利用事件监控守护进程	利用组件固件	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	利用漏洞提权	组件对象模型(COM)劫持	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	额外窗口内存注入(E...	利用连接代理	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)...	利用文件系统权限漏洞	利用控制面板项	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	利用Hook	使用DCShadow技术	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	映像劫持	反混淆/解码文件或信息	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	启动守护进程	禁用安全工具	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	新建服务	DLL搜索顺序劫持	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	伪造父进程	DLL旁路加载	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	路径拦截	按条件执行	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	修改属性列表	利用漏洞规避防御	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	端口监控	额外窗口内存注入(EW...	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PowerShell配置...	修改文件和目录权限		发现系统时间			利用Web服务		
	利用windows服务	映像劫持	进程注入	删除文件		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	利用计划任务	文件系统逻辑偏移							

持久化		提权		防御规避		
启动代理	利用服务器软件组件	利用服务注册表权限...	Process Doppelgäng...	绕过Gatekeeper	利用签名的脚本代理...	
启动守护进程	利用服务注册表权限...	利用Setuid和Setgid位	替换进程内存	修改组策略	利用Source命令	
利用Launchctl	利用Setuid和Setgid位	SID历史注入	进程注入	隐藏文件目录	加入空格隐藏扩展名	
添加LC_LOAD_DYLIB	修改快捷方式	利用启动项	冗余访问	隐藏用户	利用系统中的第三方...	
利用linux本地任务调度	会话发起协议(SIP)和...	利用Sudo命令	利用Regsvcs/Regasm	隐藏窗口	利用Trap命令	
利用登录项	利用启动项	利用Sudo缓存凭证	利用Regsvr32	HISTCONTROL	利用受信的开发工具	
利用登录脚本	利用系统固件	利用有效账户	使用Rootkit	映像劫持	诱导用户执行	
利用LSASS 驱动程序	利用Systemd服务	使用Web Shell	利用Rundll32	阻止信标捕获	利用Windows管理规...	
修改现有服务	利用Windows时间服务		使用脚本	删除工具中的信标	利用Windows远程管...	
Netsh Helper DLL	利用Trap命令		执行签名的二进制文...	删除主机中的信标	利用XSL文件执行脚本	
新建服务	利用有效账户		执行签名的脚本代理	间接执行命令		
启动Office应用程序	使用Web Shell		会话发起协议(SIP)和...	安装根证书		
路径拦截	利用Windows事件订...		软件加壳	利用InstallUtil		
修改属性列表	Winlogon Helper D...		加入空格隐藏扩展名	利用Launchctl		
端口敲门			模板注入	LC_MAIN劫持		
端口监控			修改文件时间戳	仿冒		
利用PowerShell配置...			利用受信的开发工具	修改注册表		
利用Rc.common文件			利用有效账户	利用Mshta		
重启应用程序			虚拟化/沙箱逃逸	删除网络共享连接		
冗余访问			利用Web服务	利用NTFS交换数据流...		
添加注册表运行键/启...			利用XSL文件执行脚本	混淆文件或信息		
利用计划任务				伪造父进程		
利用屏幕保护程序				修改属性列表		
利用SSP DLL(注册表...				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

寒夜速记

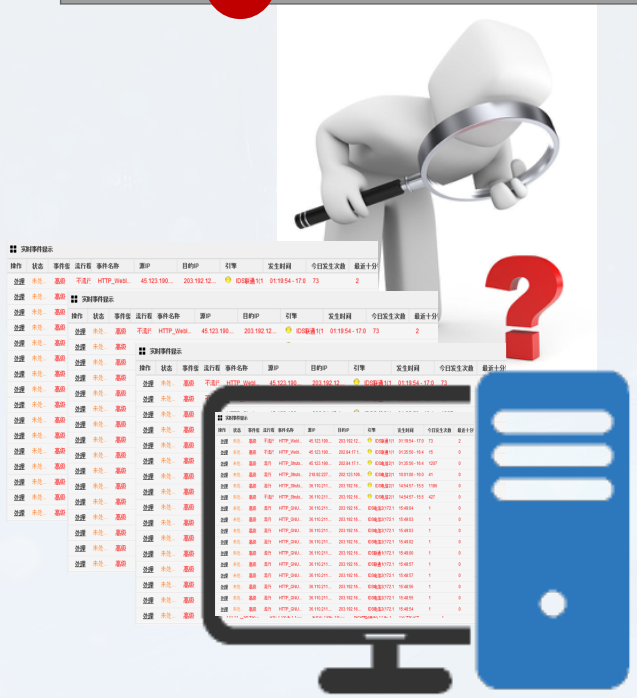
威胁框架：认知与实践

2.2 辩证地看全要素记录与分析

日趋复杂的威胁、海量的数据与人的心智负荷之间的矛盾

日趋复杂的威胁、海量的数据与人的心智负荷之间的矛盾

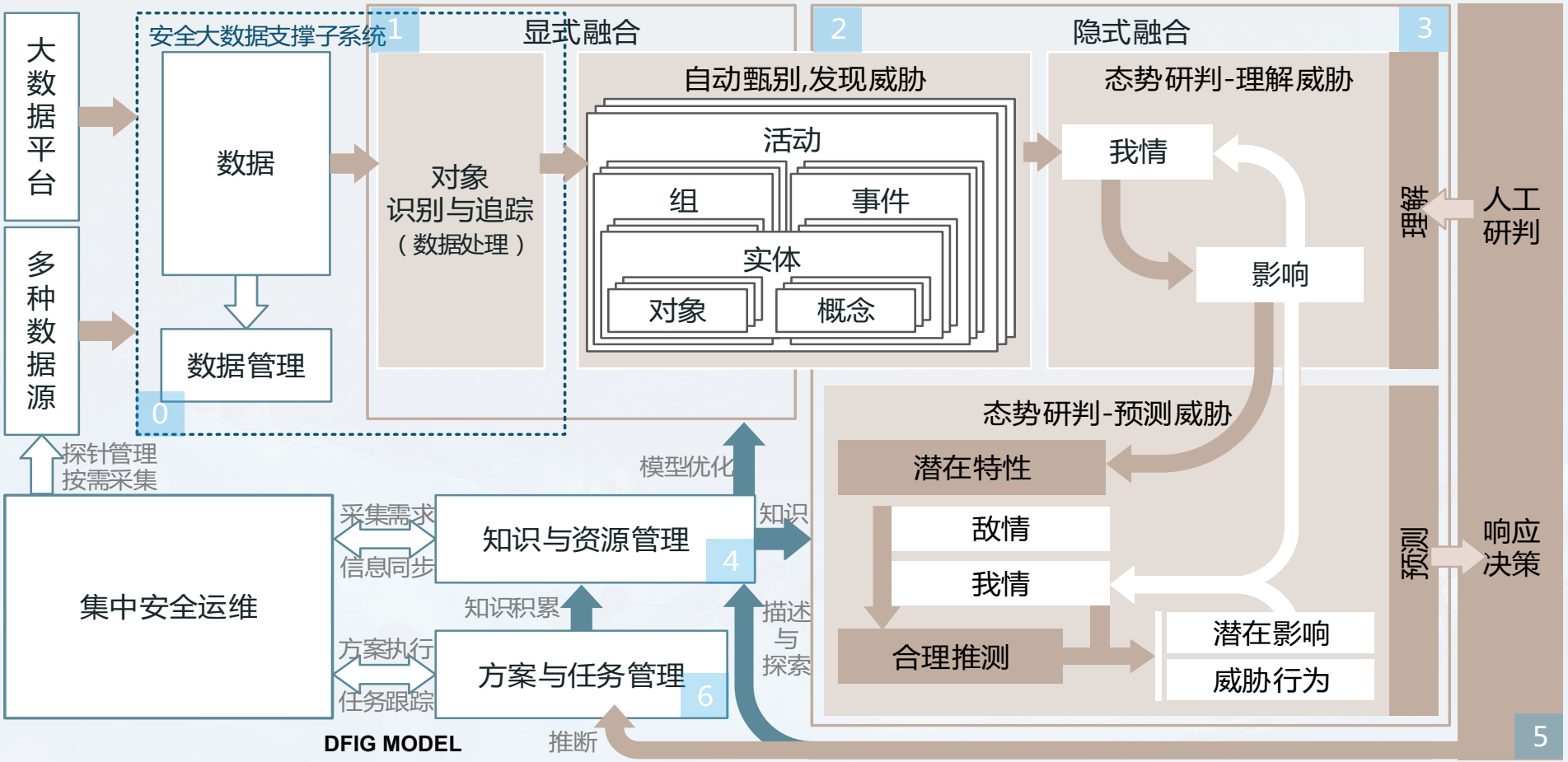
威胁发生　　分析　　响应



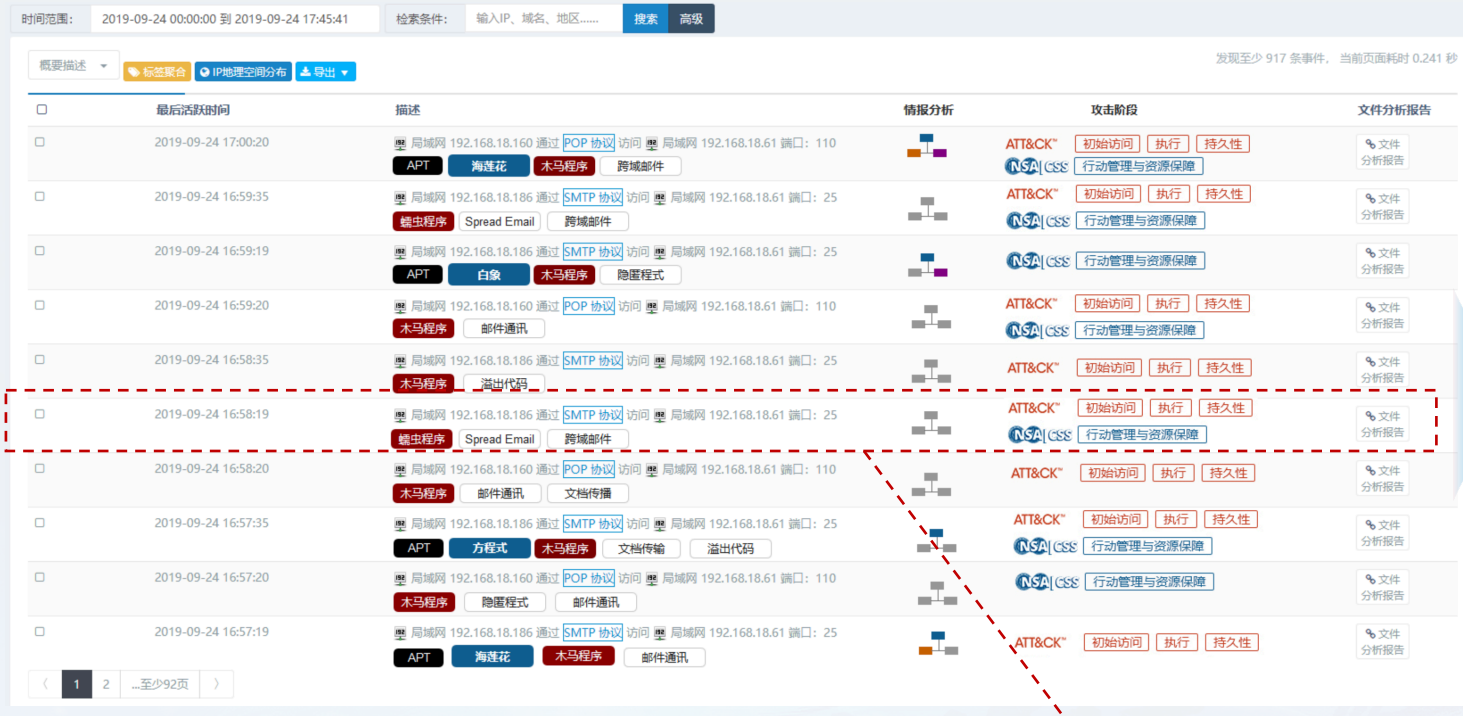
Observe → Orient → Decide → Act

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



“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

寒夜速记

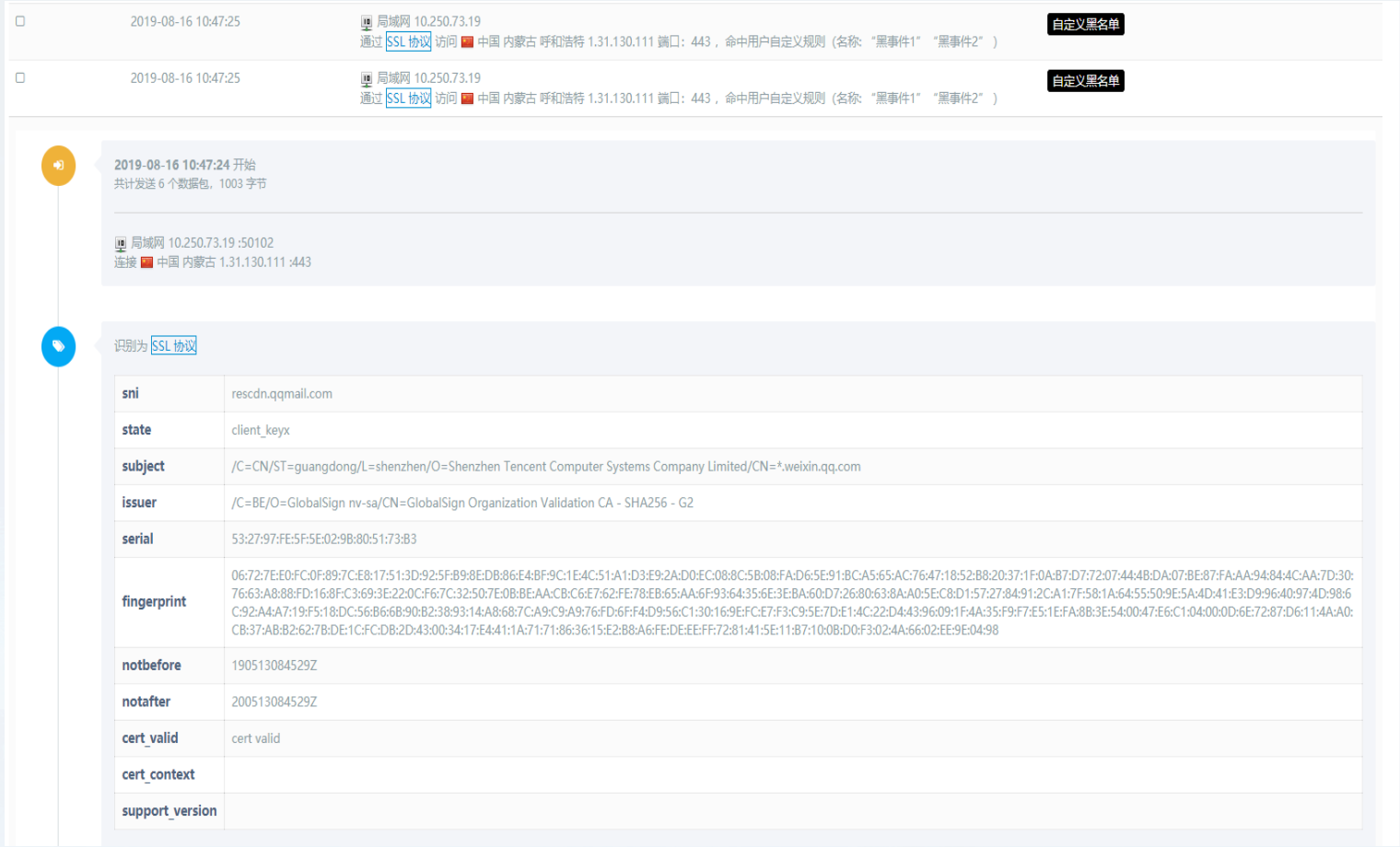
威胁框架：认知与实践

2.3 辩证地看全要素记录与分析

流量加密与监管需要之间的矛盾

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
  - ……

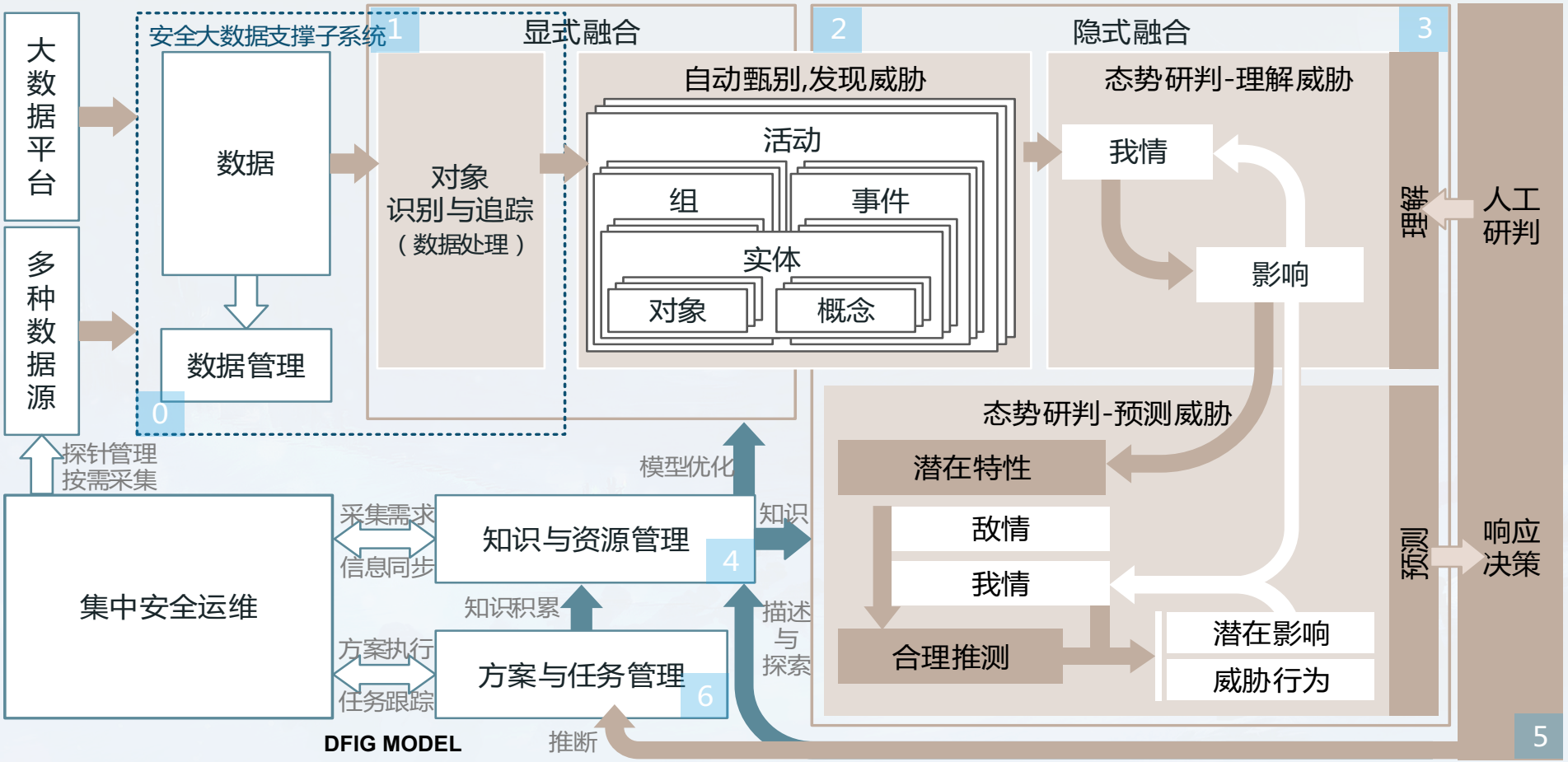


寒夜速记

威胁框架：认知与实践

03 全要素与威胁情报、框架融合

融合威胁情报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

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

网络空间威胁对抗与防御技术研讨会
暨 第七届安天网络安全冬训营

恳请批评指正

寒夜远征

威胁框架：认知与实践