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

内部资料

无所遁形——战术型态势感知的全方位流量监测

安天 网络监测产品中心

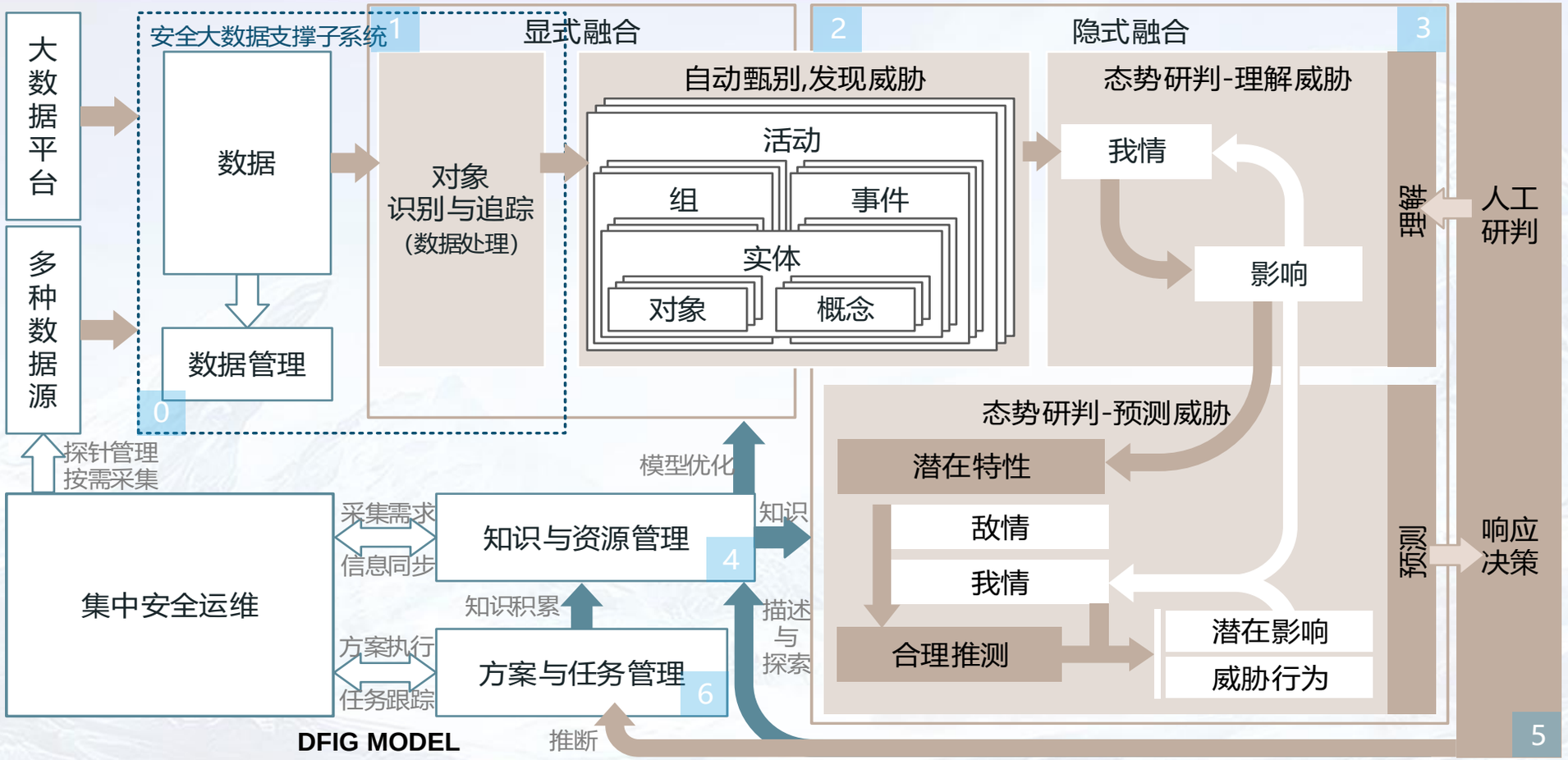
提纲

1. 战术型态势感知对流量监测的要求
2. 感知流量侧威胁，辅助态势理解威胁，预测威胁
3. 依托良好基础结构，发现安全措施失效
4. 接受指挥控制，协同进行响应与取证
5. 以敌情想定为核心，留存数据，进行威胁猎杀

探海高级威胁监测系统
追影高级威胁分析系统

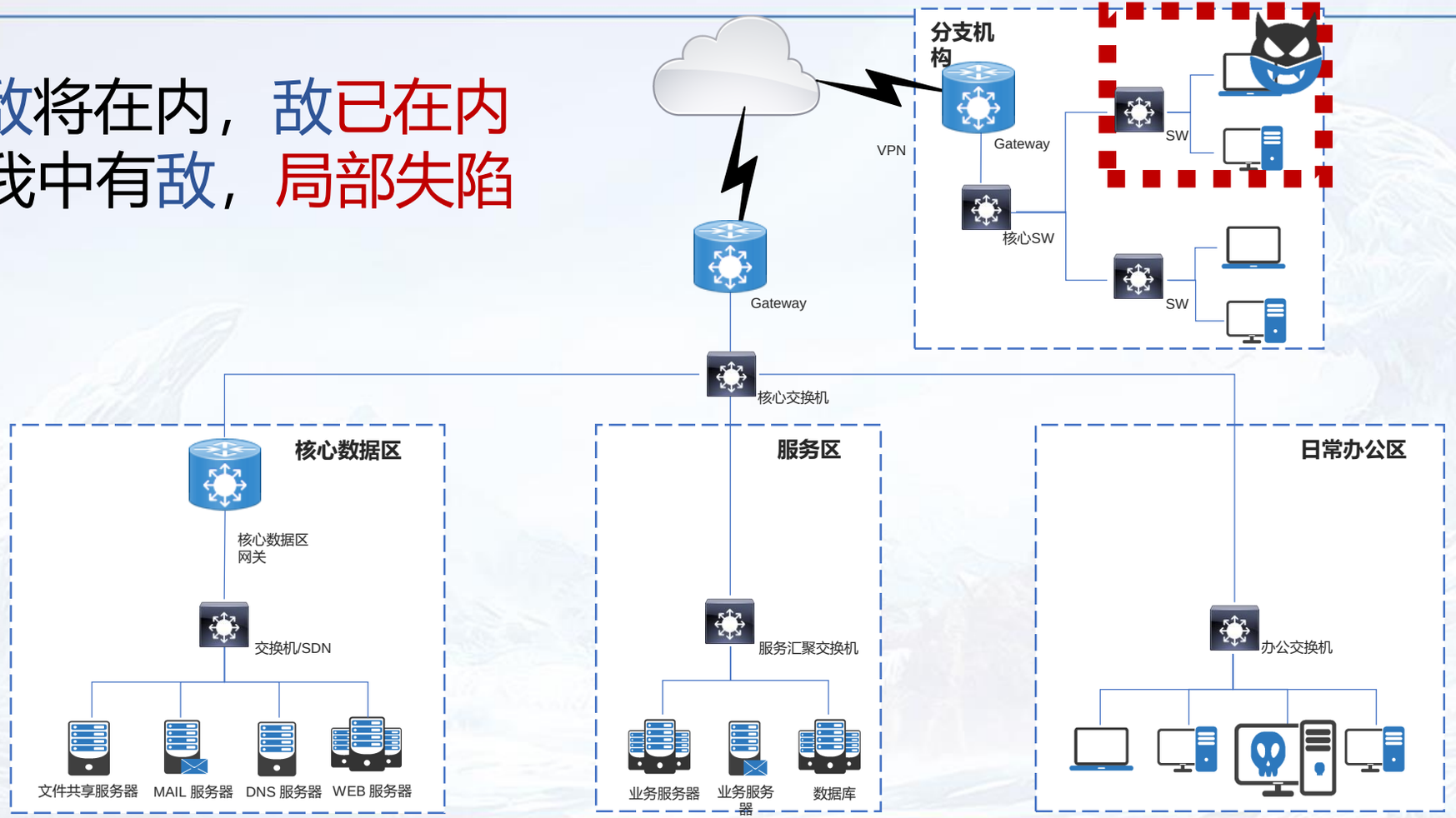
01 战术型态势感知对流量监测的要求

对威胁的识别、理解、预测是态势感知的目标

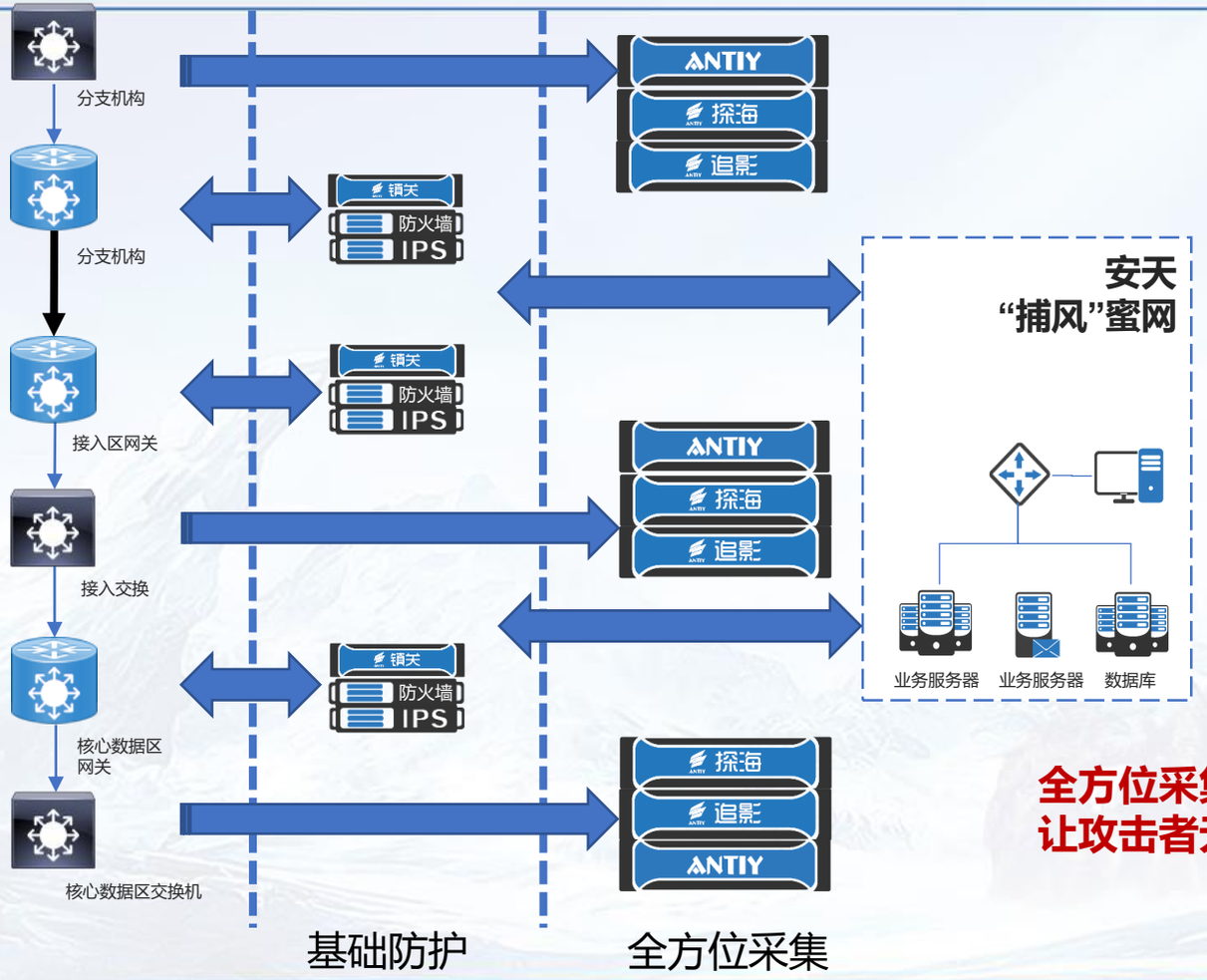


我中有敌、局部失陷是防护高价值目标的敌情想定

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

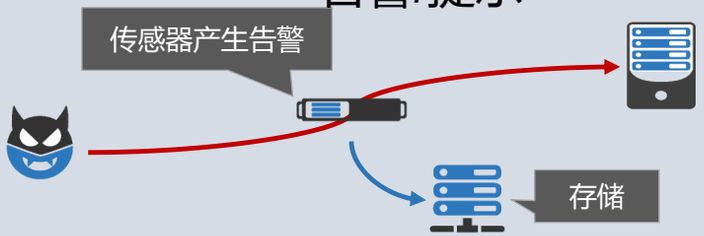


- 参考高价值目标构建合理分区
- 在抵达目标的路径上增加关隘
  - 业务路径
  - 数据路径
  - 控制路径
- 交叉火力**覆盖无死角**
  - **特别需要注意：设备管理流量**
- 被动防御能力是积极防御的基础

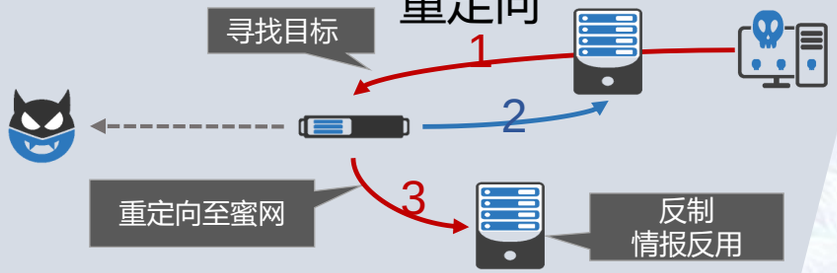
全方位采集、智能化响应
让攻击者无所遁行、无处可逃、无计可施

与态势感知的协同实现智能化响应能力

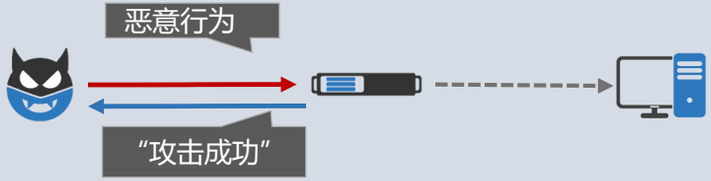
告警/提示



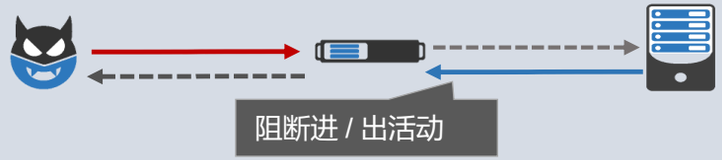
重定向



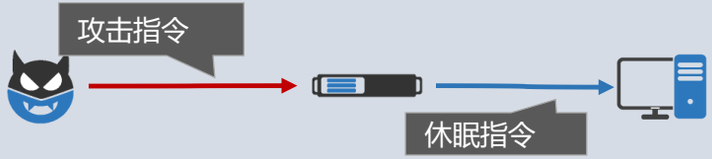
拦截



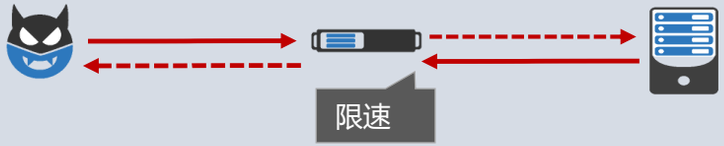
阻断



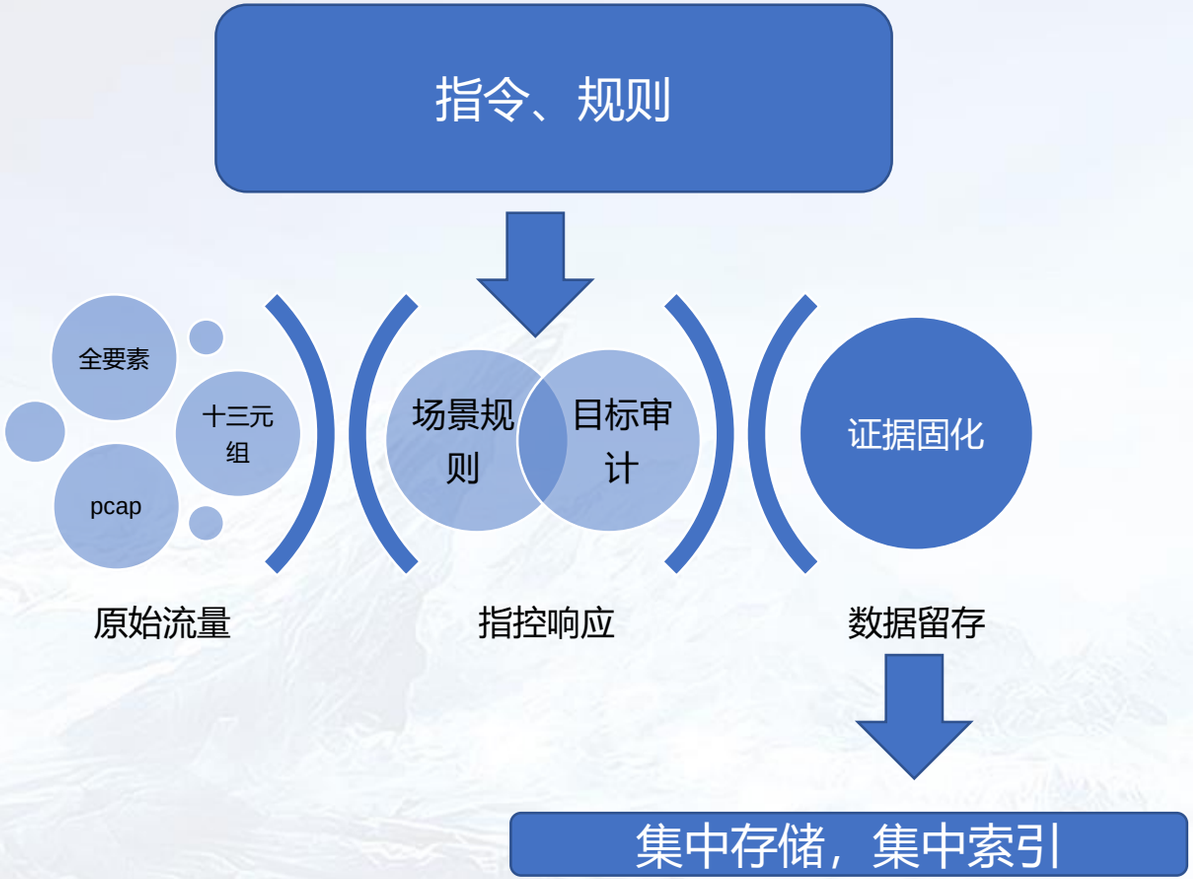
替换



延迟



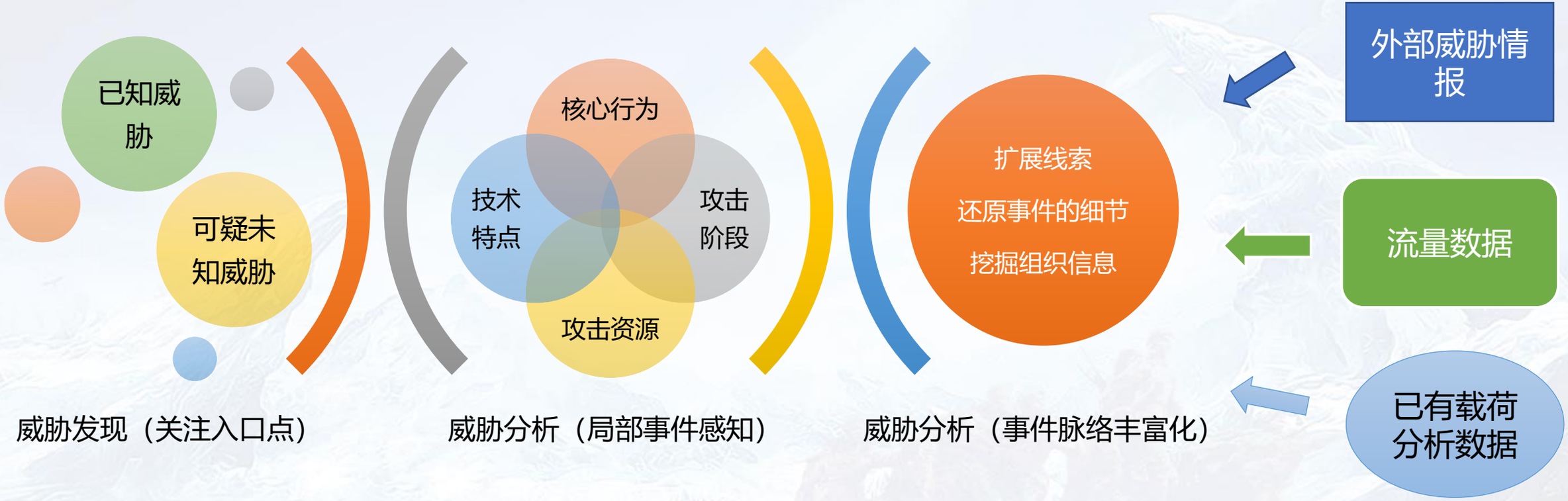
协同响应获取更多信息，固化证据



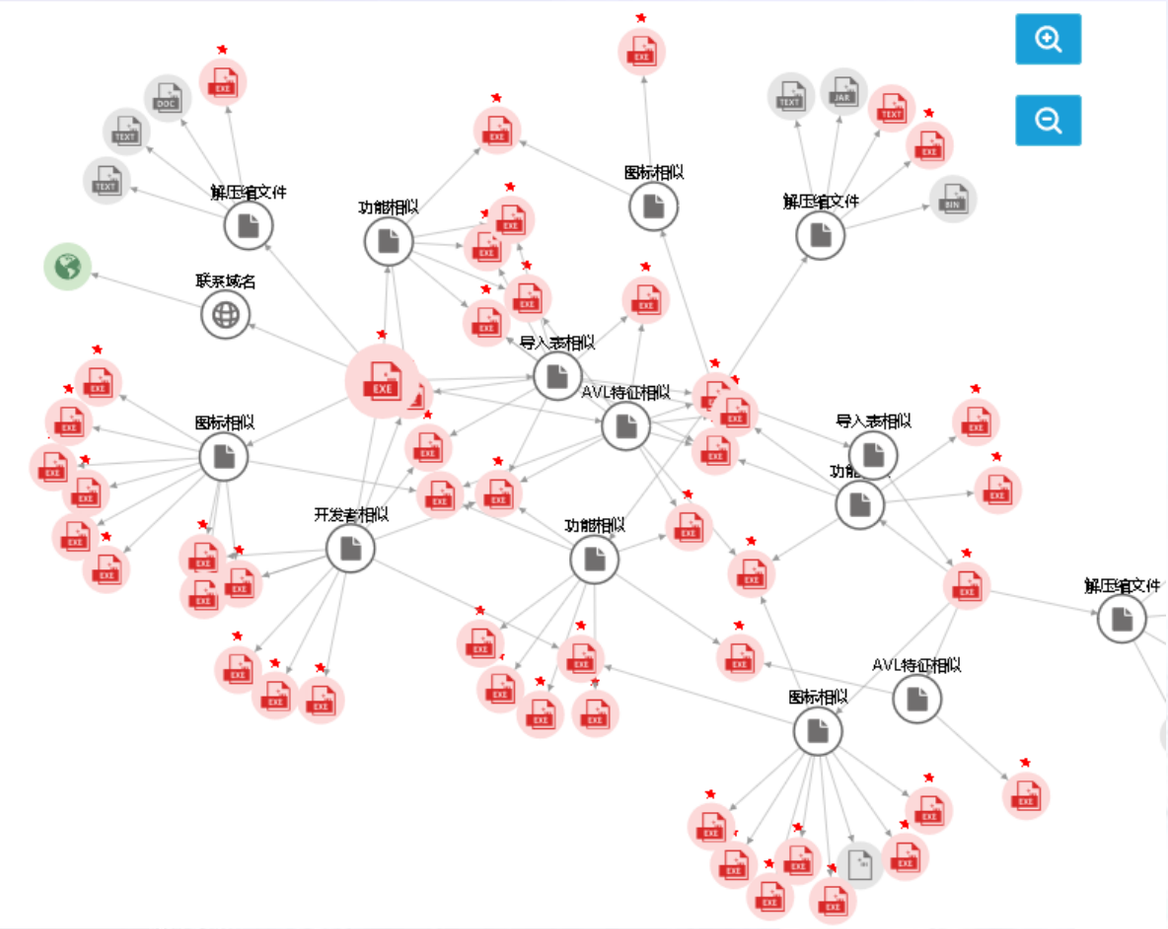
- 态势感知下发指令规则
- 使用场景规则和目标审计进行固化证据
  - 全要素
  - 十三元组
  - 流量pcap
- 固化的证据提供给态势感知集中存储
  - 作为case的一部分

- 当某IP/域名/URL被认为是C&C服务器时
  - 全网留存相关pcap
- 当某台主机被怀疑控制时
  - 留存一段时间内全部主机pcap
- 在进行特殊保障时
  - 全量采集流量日志

基于载荷的深度分析，结合外部情报、流量数据，理解威胁



基于载荷的情报生产挖掘，预测威胁



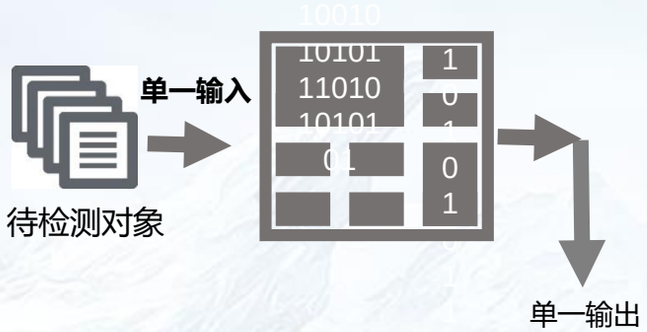
- 基于文件载荷，进行相似性计算
- 聚合攻击家族，发现攻击同源性
- 依托家族相似性，发现新的威胁载荷

02

感知流量侧威胁
辅助态势感知理解威胁，预测威胁

向量级的威胁发现能力

传统引擎



结果

单一名称

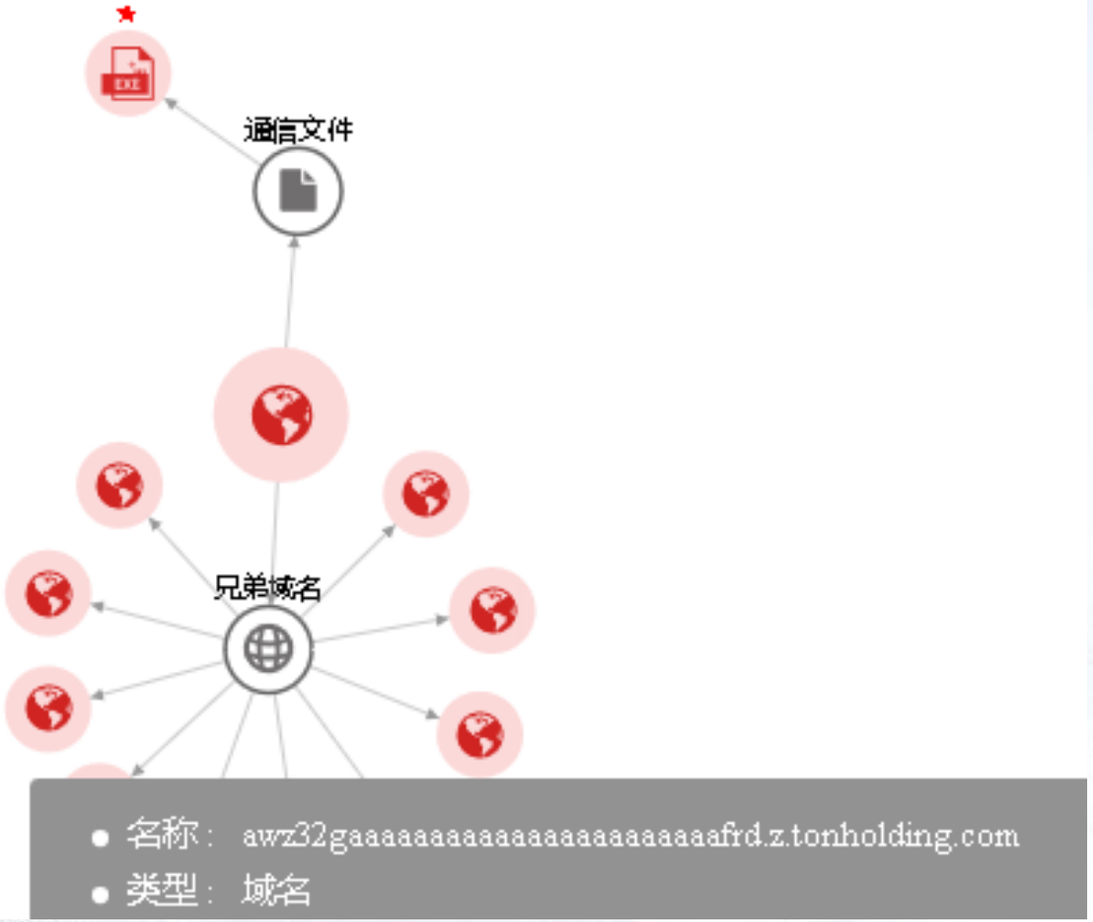
Trojan/Win32.Agent

以单一对象为输入，以单一结果为输

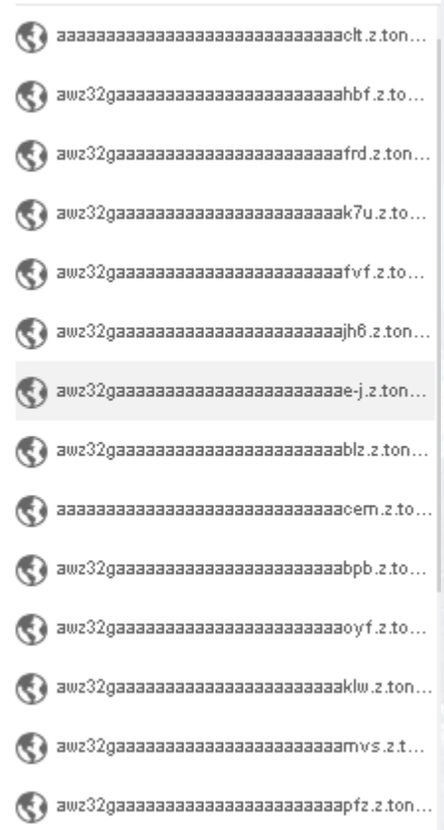
下一代威胁检测引擎

多种输入对象，多输出结果，威胁检测多样化。

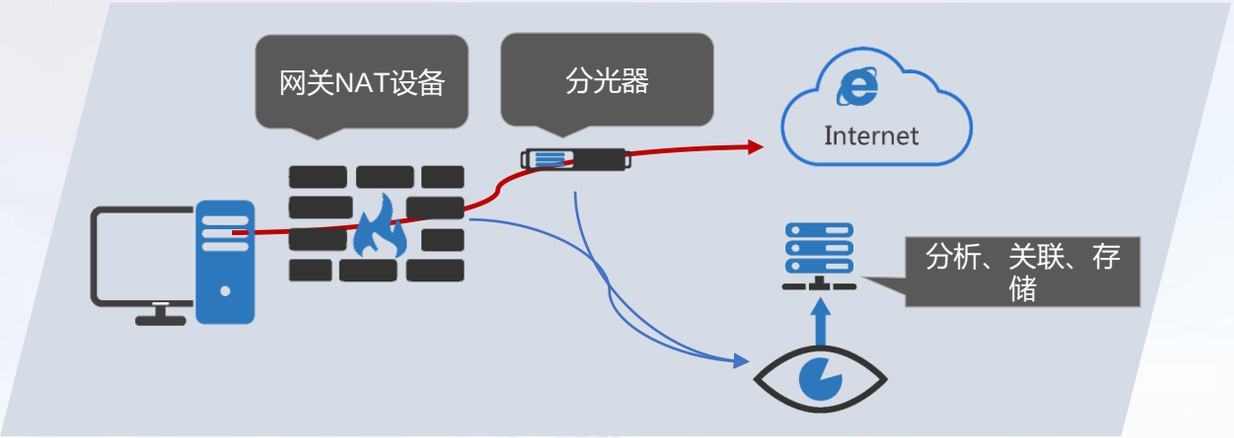
结合威胁情报，指导威胁搜寻和事件响应



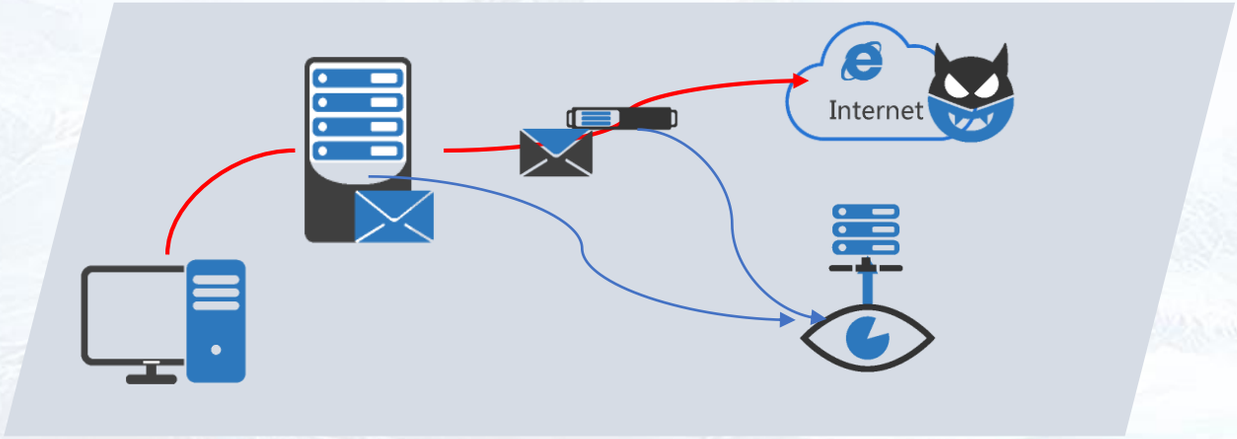
- 威胁情报生产过程中，发现DNS通联域名的特殊性
- 形成模式匹配方法
- 态势感知下发情报到设备，进行新的模式检测



结合DNS数据、NAT数据、邮件发送数据等，完成受害主机定位

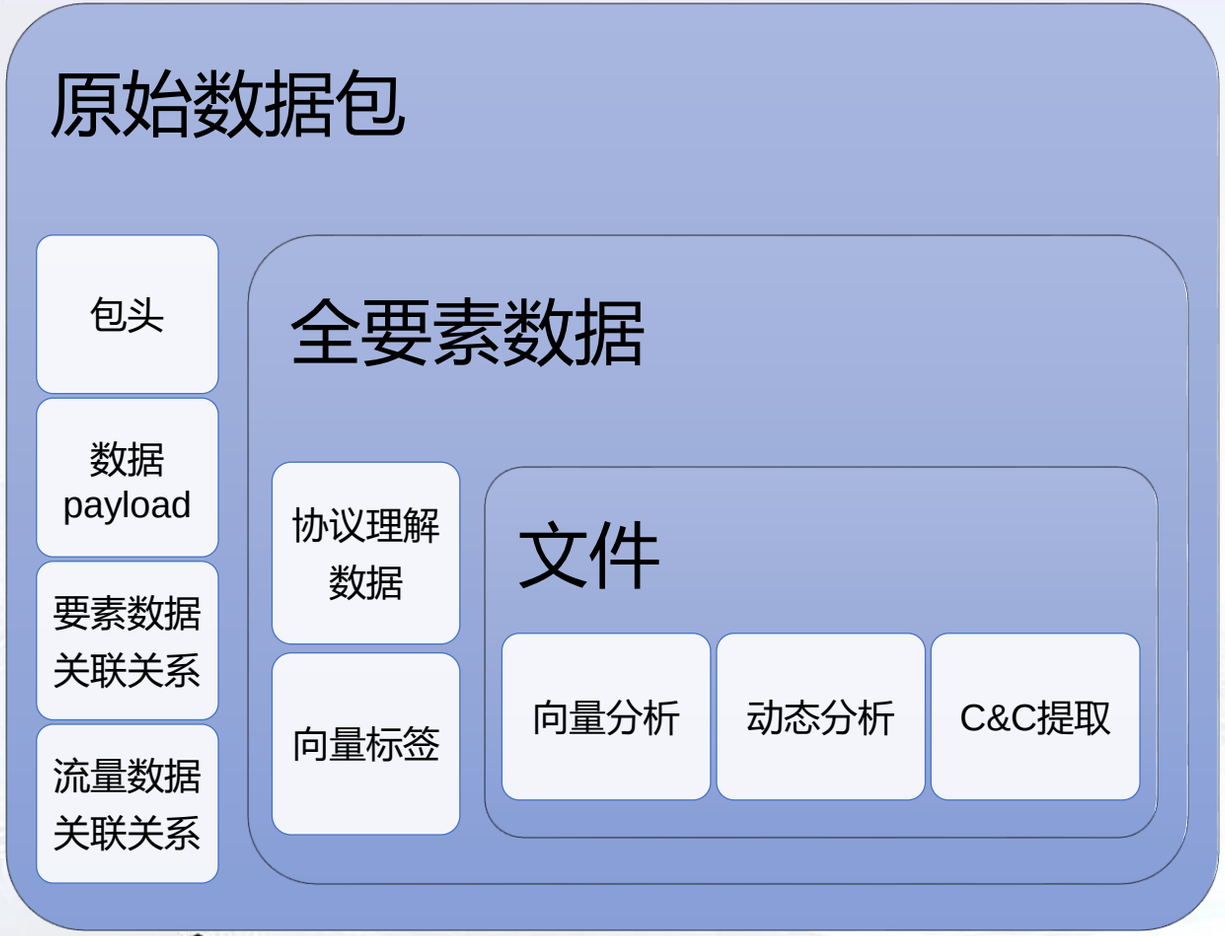


- 流量在不同位置会损失信息
- 链路抵近部署会带来融合问题
- 找到的威胁发起源可能是：
  - DNS服务器
  - NAT后的防火墙
  - 邮件MX解析记录的服务器
  - Web代理服务器



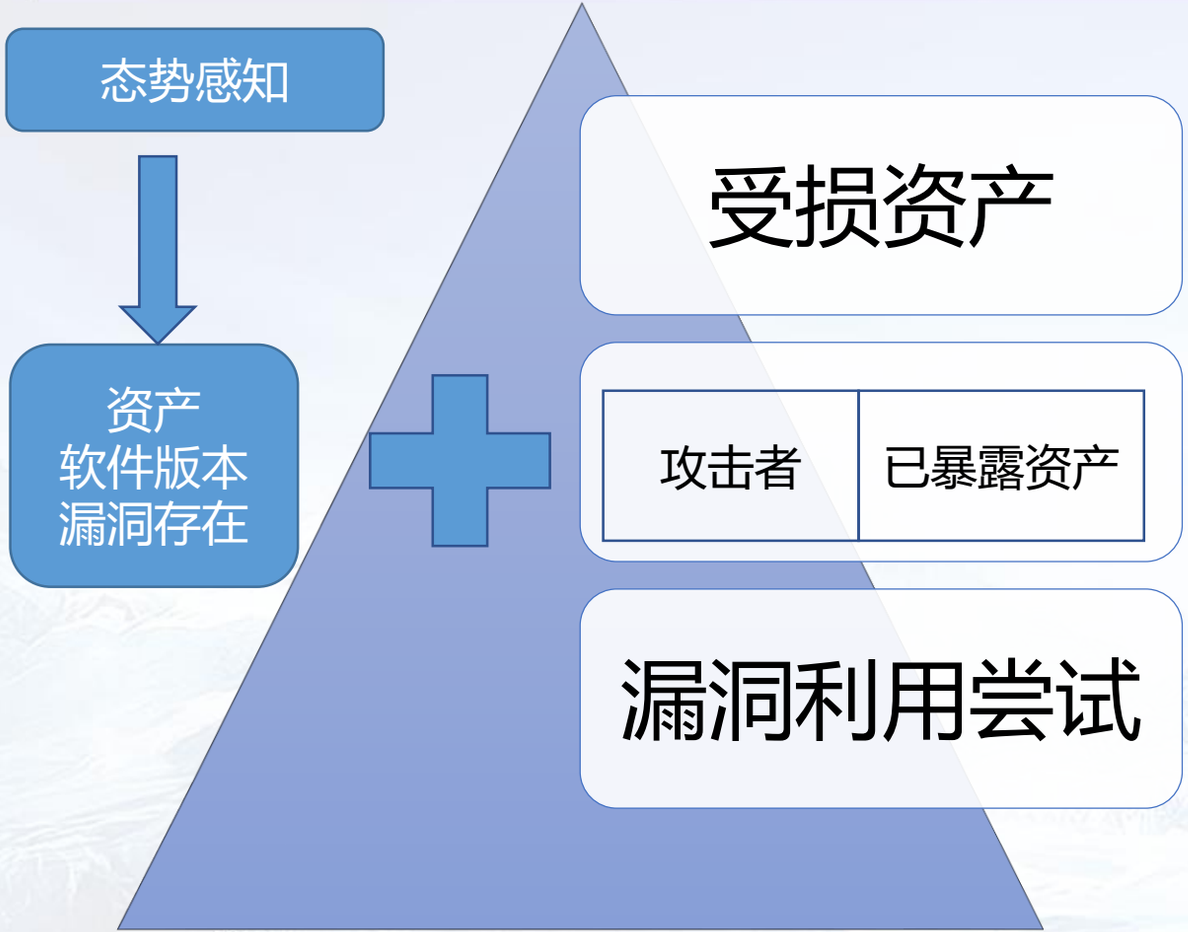
- 使用日志丰富化原始信息
- 多源日志融合，获知发起源
- 发现真实受害者
  - 谁发起了DNS解析?
  - 谁是NAT源
  - 谁发了这份邮件，导致MX解析
  - 谁在代理之后

依据威胁认知，留存证据



- 载荷传输，还原文件
  - 动态分析、向量分析
  - 必要时人工分析
  - 可用于产生情报
  - 情报反作用于系统
- 全要素数据
  - 理解协议，提取全部信息
  - 包含检测出的特征向量标签
  - 原始是哪台主机？初步的信息融合后结果。
- 原始数据包
  - 最全的数据
  - C&C通联：找到C&C相关数据包
  - 域名的C&C解析：连接的ip是啥？这个ip的数据包
  - 已知感染：感染主机一段时间的数据包

发现攻击尝试，结合资产脆弱性信息和场景，剔除无影响威胁



- 态势感知协同
  - 下发资产、软件版本、漏洞存在情况
  - 结合漏洞利用尝试，对比资产是否存在漏洞
  - 直接定位受损资产
  - 忽略无关警告
- 攻击者流量捕获
  - 用于关联payload，确认攻击者
  - 用于取证溯源
  - 提取攻击者意图，C&C服务器
- 已暴露资产流量重点关注
  - 是否有未被监测到的攻击成功威胁?
  - 是否有攻击行为，C&C服务器连接尝试?
- 受损资产弥补损失，响应处置

高度模拟业务，使用沙箱与蜜罐进行线索揭示

多来源输入 → 多重分析 → 丰富的虚拟环境 → 私有化威胁情报

结合追影，挖掘威胁情报，发现攻击者资源及手段，指导威胁猎杀

1 判断结果

文件被 网络威胁感知类设备 发现，经由YARA自定义规则鉴定器、静态分析鉴定器、动态行为（默认环境）鉴定器、智能学习鉴定器、安全云鉴定器等鉴定分析。

“安天追影高级威胁鉴定器”依据动态行为鉴定器最终将文件判定为 疑似高级威胁 。

根据动态行为（默认环境）得出该文件具有以下行为：利用漏洞释放PE文件、查找指定内核模块、创建特定窗体、获取计算机名称、获取驱动器类型、请求加载驱动的权限、获取主机用户名称、获取系统内存、查找特定窗体、释放PE文件、打开自身进程文件、访问文件尾部、独占打开文件、篡改系统文件创建时间、更新服务配置信息、自启动。

2 行为描述

行为描述：	利用漏洞释放PE文件	
附加信息：	FilePath	C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\2.tmp
	FilePath	C:\WINDOWS\system32\xpxpres.dll
	FilePath	C:\WINDOWS\system32\winHook.dll
	FilePath	C:\WINDOWS\system32\winOther.dll
	FilePath	C:\WINDOWS\system32\winScreen.dll
	FilePath	\??\C:\WINDOWS\system32\Rpcs4.dll
危险等级：	★★★★	

3 网络追溯

网络监控

UDP 信息

源 IP	源端口	目的 IP	目的端口
0.0.0.0	68	255.255.255.255	67
192.168.122.1	67	192.168.122.246	68
192.168.122.246	137	192.168.122.255	137
192.168.122.246	1025	192.168.122.1	53
192.168.122.1	53	192.168.122.246	1025
192.168.122.246	138	192.168.122.255	138

4 衍生关系

进程监控

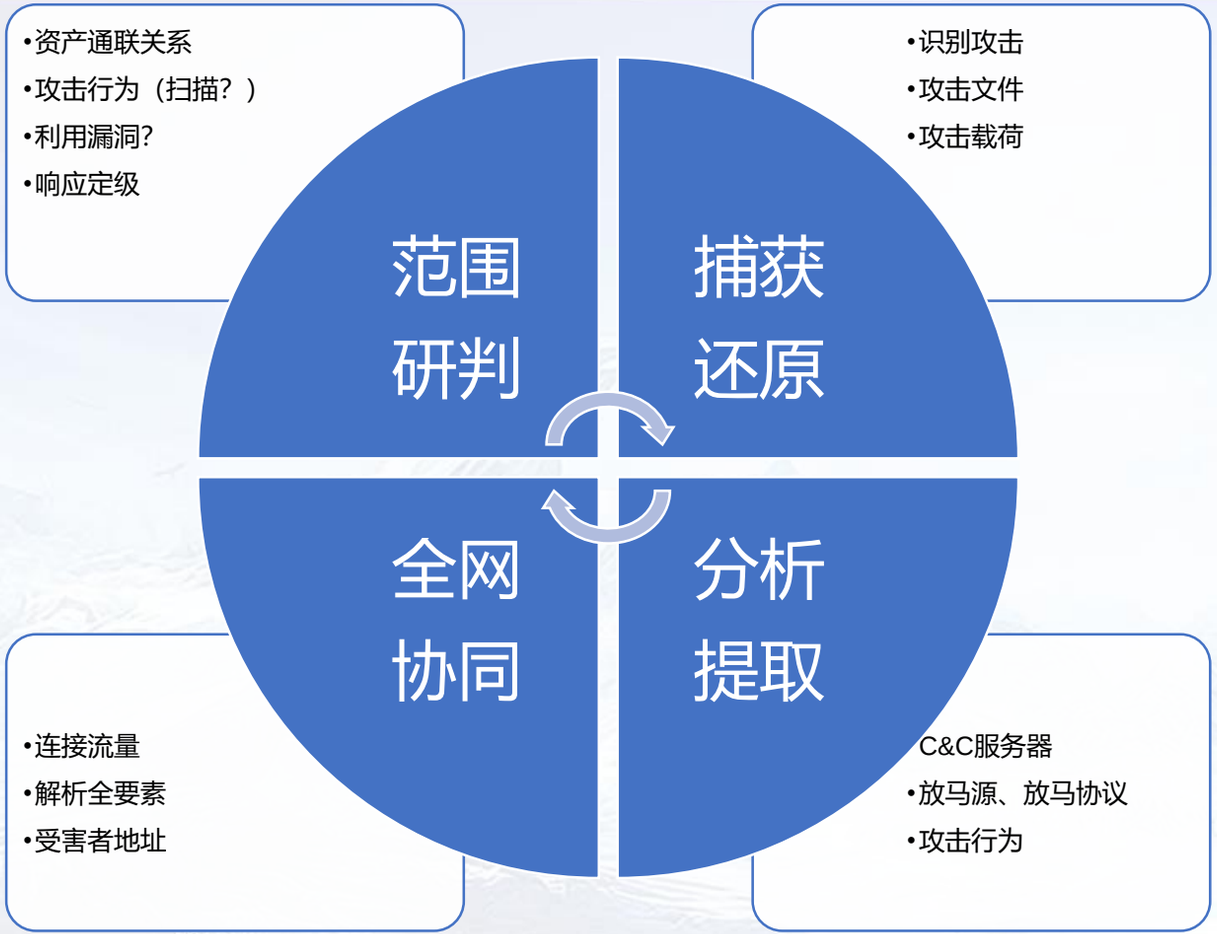
PID : 1136	创建：C:\Program Files\Microsoft Office\OFFICE11\POWERPNT.EXE
	命令行："C:\Program Files\Microsoft Office\OFFICE11\POWERPNT.EXE" "C:\a0912367fa814
PID : 1928	创建：rundll32.exe
	命令行：rundll32 xpxpres.dll,Colnstall C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\2.tmp
PID : 1692	创建：2.tmp
	命令行：C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\2.tmp
PID : 2004	创建：POWERPNT.EXE
	命令行：C:\Program Files\Microsoft Office\OFFICE11\POWERPNT.EXE "C:\DOCUME~1\ADMI

进程衍生关系

- POWERPNT.EXE
  - C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\2.tmp
  - C:\Program Files\Microsoft Office\OFFICE11\POWERPNT.EXE "C:\DOCUME~1\ADMINI~1\LOCA

- 样本定性，寻找高危载荷
- 行为列表，揭示载荷功能
  - 规避方式
  - 行为能力
- 行为描述，定位终端呈现
  - 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

通过对攻击者掌握资源的监控，协助理解受害范围



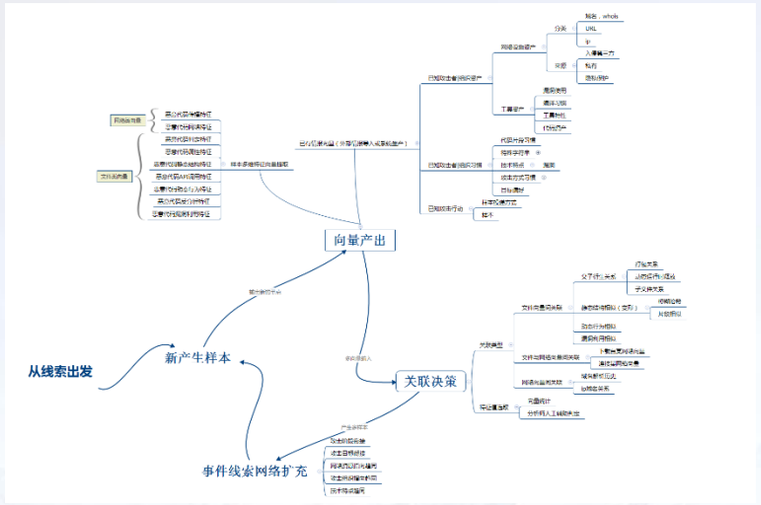
- 捕获还原识别威胁，获取攻击向量
  - 用于本地化的产生情报
  - 获取文件、流量payload
- 分析提取分析威胁，产生情报
  - 动态分析、向量分析
  - 产生C&C服务器
  - 产生放马源
  - 产生攻击行为
- 态势感知全网协同
  - 寻找那些主机连接这些地址
  - 寻找互斥量、文件的存在
- 态势感知结合通联关系和行为研判范围

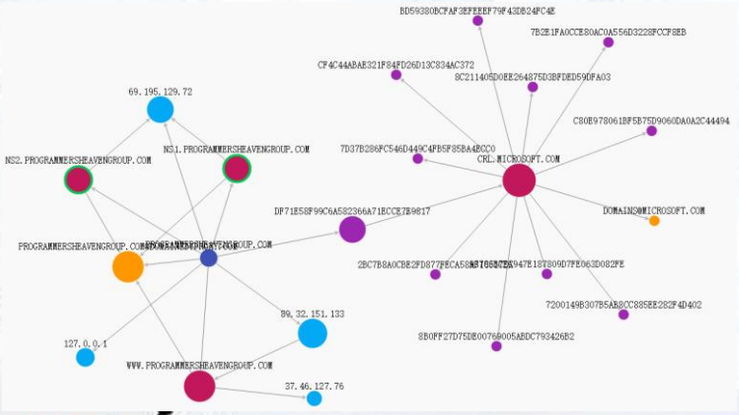
结合追影，发现恶意代码的行为和攻击阶段，指导人工处置

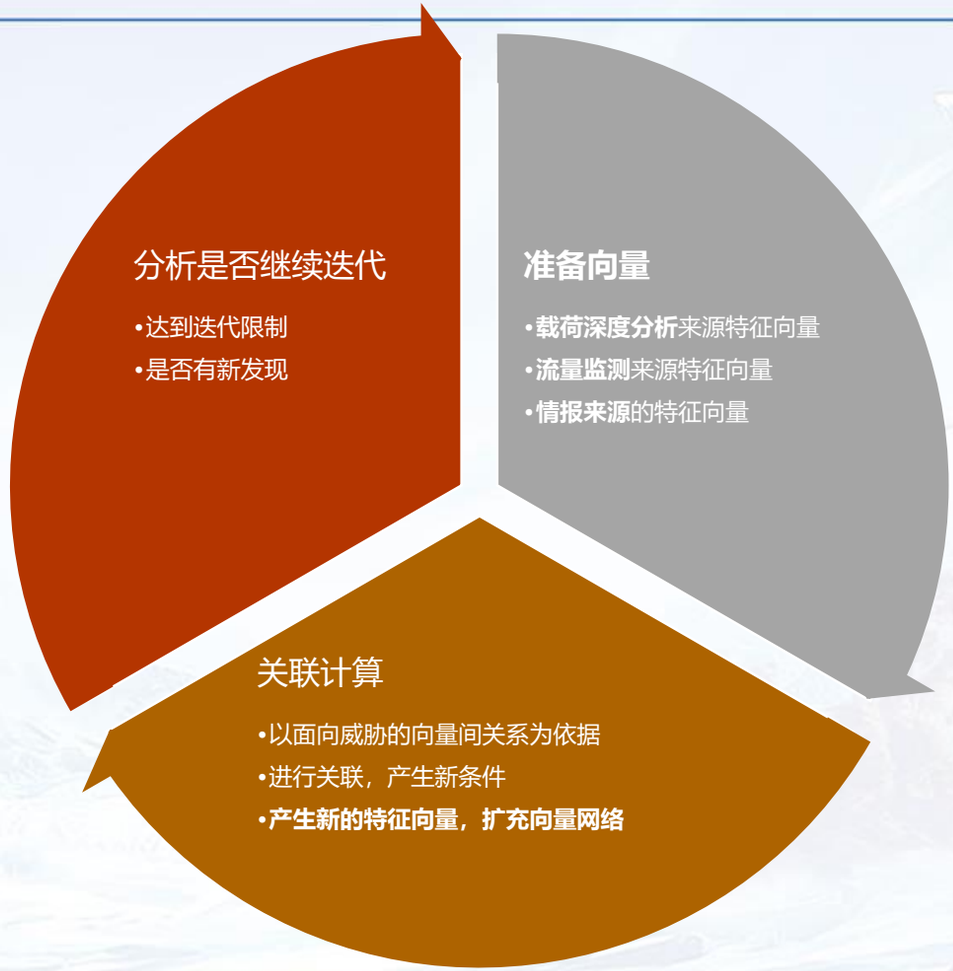
交互		存在					
投放	利用	安装/执行	内部侦察	提权	凭证访问	横向移动	持久化
带有附件的鱼叉式钓鱼邮件	应用程序本地漏洞利用	磁盘写入	账户枚举	使用合法凭证	凭证转储	应用部署软件	利用合法凭证
带有恶意链接的鱼叉式钓鱼邮件	操作系统漏洞利用	内存中执行代码	文件系统枚举	辅助功能	网络嗅探	应用程序本地漏洞利用	辅助功能
网站	应用程序远程漏洞利用	解释脚本	组权限枚举	系统启动时自动加载	键盘记录	操作系统漏洞利用	系统启动时自动加载
可移动介质	社会工程学	二进制文件替换	本地网络连接枚举	库搜索劫持	社会工程学	采用登录脚本	库搜索劫持
SQL注入	虚拟化攻击	命令行	本地网络设置枚举	创建新服务	密码破解	利用对等连接	创建新服务

- 对应：NSA/CSS中，安装执行和保持存在的阶段
- 发现行为，逆转行为，指导处置。
- 威胁保持存在的位置，进行杀除
- 威胁横向移动的方法，进行阻抑

结合追影，输出多维线索，帮助关联挖掘，揭开事件全貌与预测态势







核心：

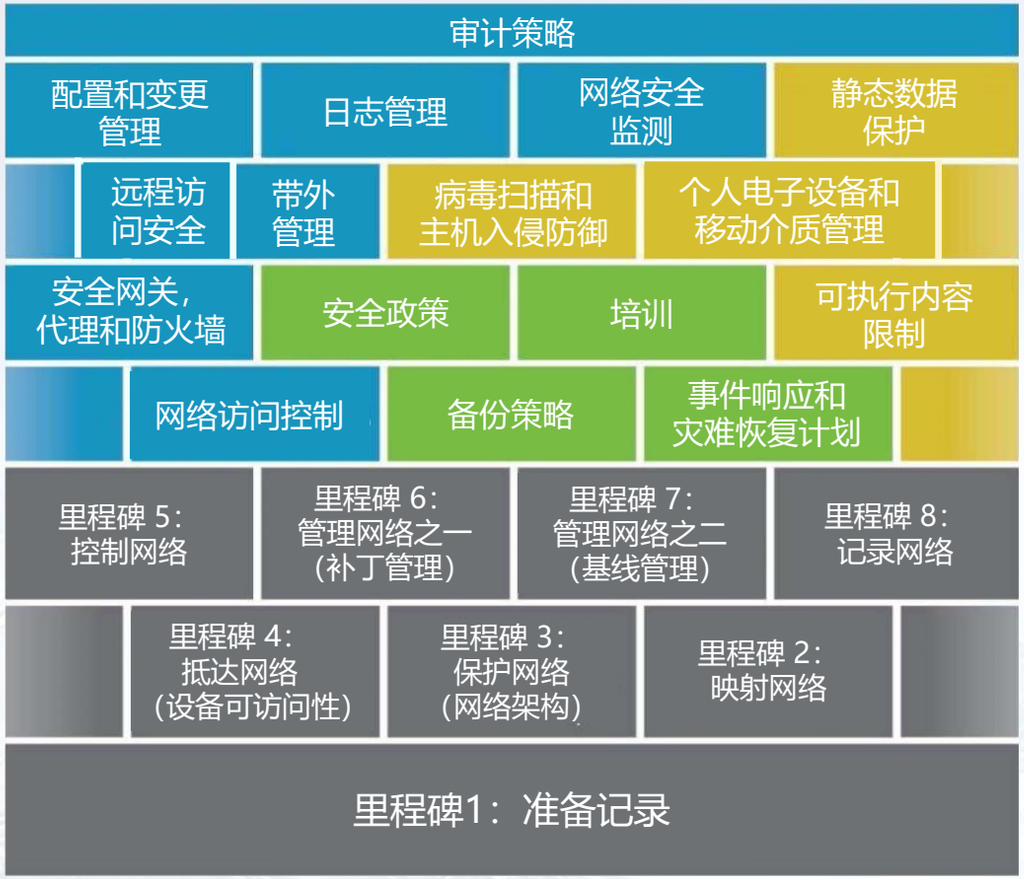
- 生产多维线索
- 迭代运行，

丰富化事件脉络，

逐步了解威胁全貌

03 依托良好基础结构，发现安全措施失效

可管理网络对资产记录、网络了解的要求



规划可管理网络的路线图[1]

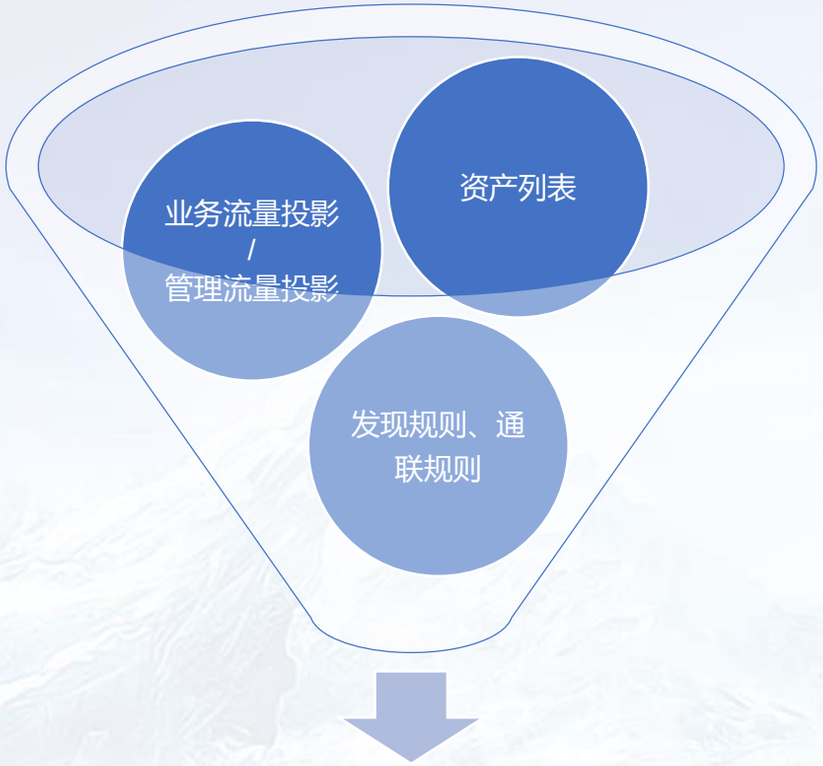
- 难以管理的网络是不安全的[1]
- 可管理网络的特点
  - 完整准确记录网络及其中的设备、协议、配置等信息并保持持续更新
  - 具有健全的网络安全架构、访问控制规程、设备管理流程及用户权限约束
  - 具备完善的补丁管理流程和基线状态管理措施等

[1]：《可管理的网络计划指南V4.0》

利用流量监测，完善网空地形绘制

	人工记录	主机Agent获取	扫描发现	流量监测发现
成本	高	中	低	低
完整性	同步建设时可达成完整记录。否则限于重要网络节点	限于重要网络节点	限于开放设备及端口	限于网络流量及通联关系
网络拓扑记录	同步建设完整记录逻辑拓扑和物理拓扑	一般，难以发现物理拓扑，逻辑拓扑依靠推测	一般，难以发现物理拓扑，逻辑拓扑依靠推测	一般，难以发现物理拓扑，逻辑拓扑依靠推测
新主机发现	难以及时更新	难以及时更新	周期性发现	迅速
不活跃主机发现	难以及时更新	迅速	周期性发现	限于算法发现
软件资产发现	难以及时更新	准确度高	限于提供服务的软件	可发现提供服务的软件和发起通联的软件
协议通联关系	定义规则，依托技术手段强制	发现通联事实	-	发现通联事实
配置管理	经审核的配置，依靠技术手段强制	作为技术强制手段	-	-

依托业务在流量的投影，协助发现违反可管理网络要求的资产

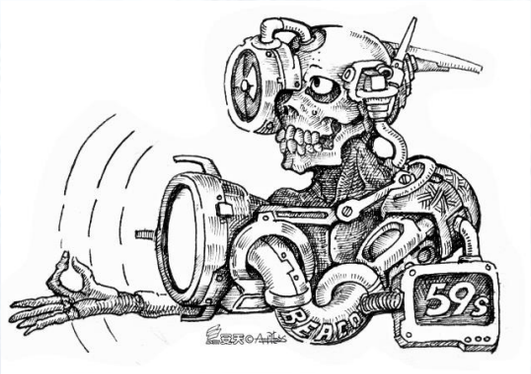


- 可管理网络的要求：
  - 完整准确记录网络及其中的设备、协议、配置等信息，并保持持续更新
  - 具有健全的网络安全架构，访问控制规程、设备管理流程及用户权限约束
- 发现
  - 久未活跃资产/未登记资产
  - 协议信息记录不准确
  - 管理网络非带外管理情况
  - 访问控制规程违例
  - 用户权限约束不准确
  - ……
- 持续更新网络记录

依托流量，接受威胁场景规则，发现违反最佳安全实践的情况

- 信息泄漏
- 明文管理协议
- 地址冲突
- 地址空间耗尽
- DNS服务器配置非正常DNS
- 具有没有登记的DHCP服务器
- 443端口上的HTTP流量
- 传递的PE文件具有非PE扩展名
- 传递的PE文件具有非PE的MIME
- 邮件中传递PE
- 非公司SMTP邮件服务器发送了邮件
- ……

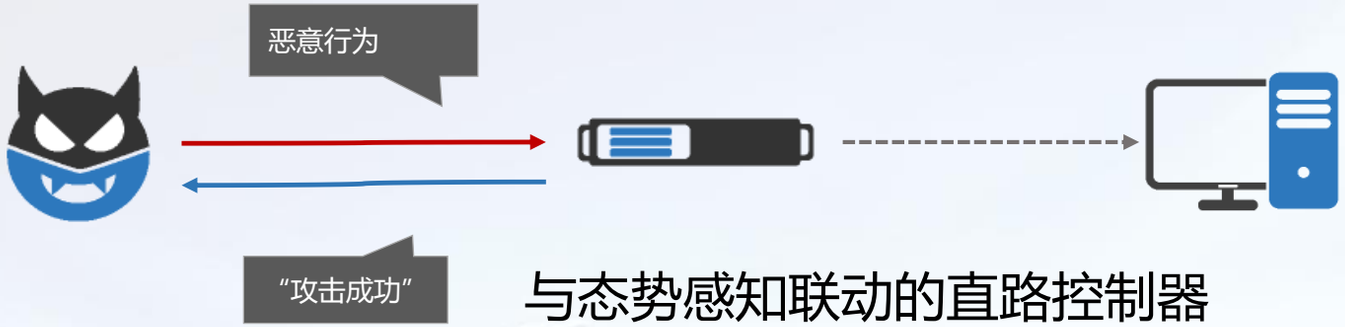
通过对异常流量的调查，发现安全机制失效节点



- DGA检测
  - 海莲花APT木马
- 弱口令登录
  - IoT的蠕虫化传播
- DDoS行为
- ICMP隐秘信道
- 端口扫描
  - 445的端口扫描：永恒之蓝，双脉冲星？
  - 其他蠕虫化传播？
- 网络流量检测与终端检测不一致
  - 终端没有查到恶意连接
  - 暗云3：bootkit

04 接受指挥控制，协同进行响应与取证

作为网络基础设施，接受指挥控制，欺骗威胁，化被动为主动



与态势感知联动的直路控制器

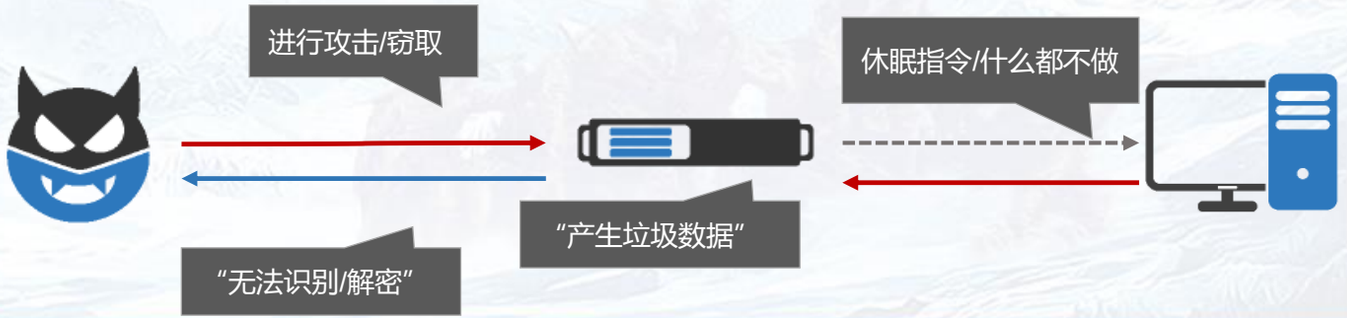
- 动态重定向网络流量
- 修改入站/出站报文
- 插入/删除报文

透明的干涉对手行为，告知对手其行动已完成，而不暴露目标未被攻陷的事实。

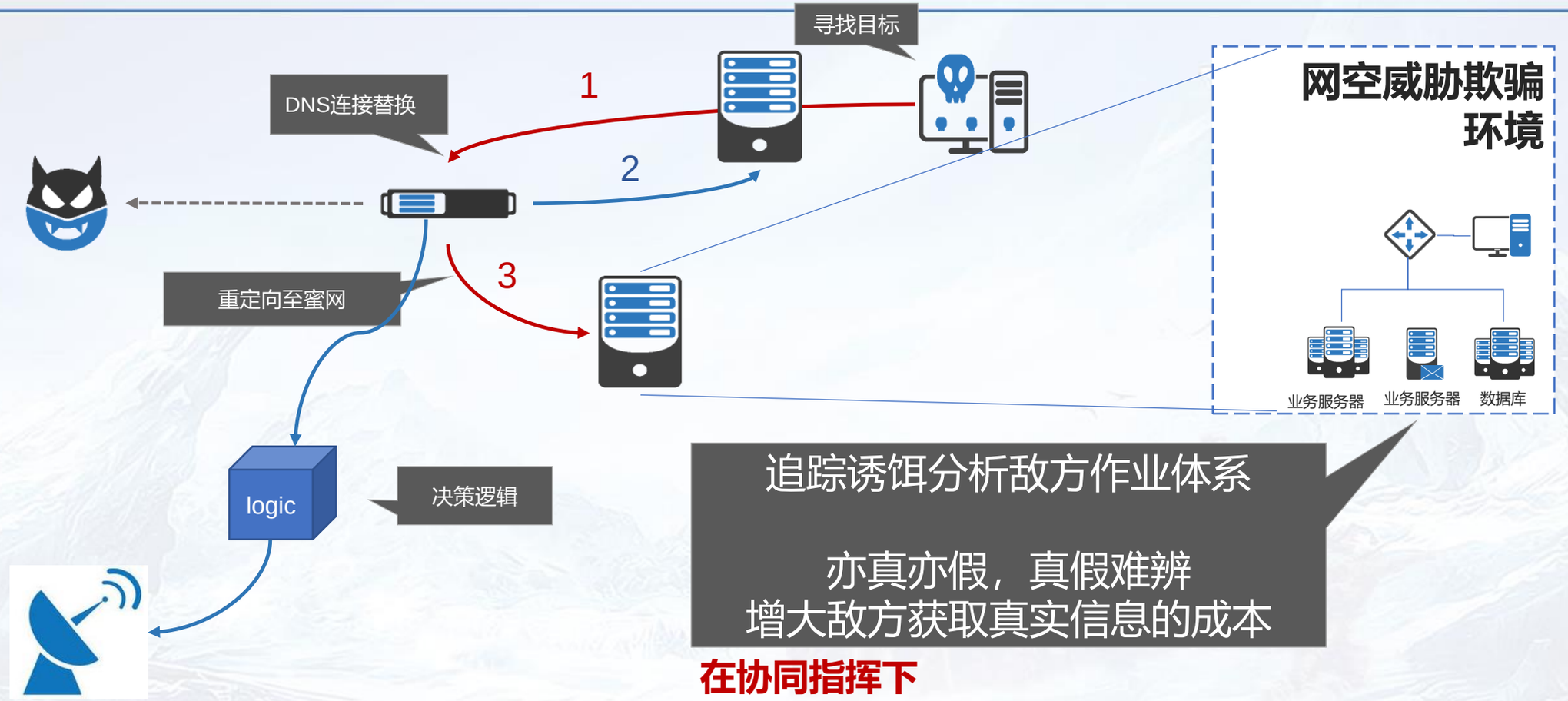
（导入蜜网，占据优势）

- 拦截替换

  基于远控协议回应（＞30种）



作为网络基础设施，接受指挥控制，欺骗威胁，化被动为主动



追踪诱饵分析敌方作业体系

亦真亦假，真假难辨
增大敌方获取真实信息的成本

在协同指挥下
让攻击者无处可逃、无计可施

协同指挥，同铸网络防线；众志成城，攻击无处可逃

Orient

场景关联检测引擎

基于威胁认知的告警合并

多标签组合事件分析

Observe

沙箱

脆弱性监测

C&C 检测

文件检测

资产识别

自定义检测

细粒度解析与还原

向量提取

协议识别

包、流 特征检测

全要素记录

场景化 13 元组 记录

Act

高性能流量捕获

目标审计（全流量记录）

光纤分光

交换机镜像

协同日志

资产状态

场景规则

情报

取证

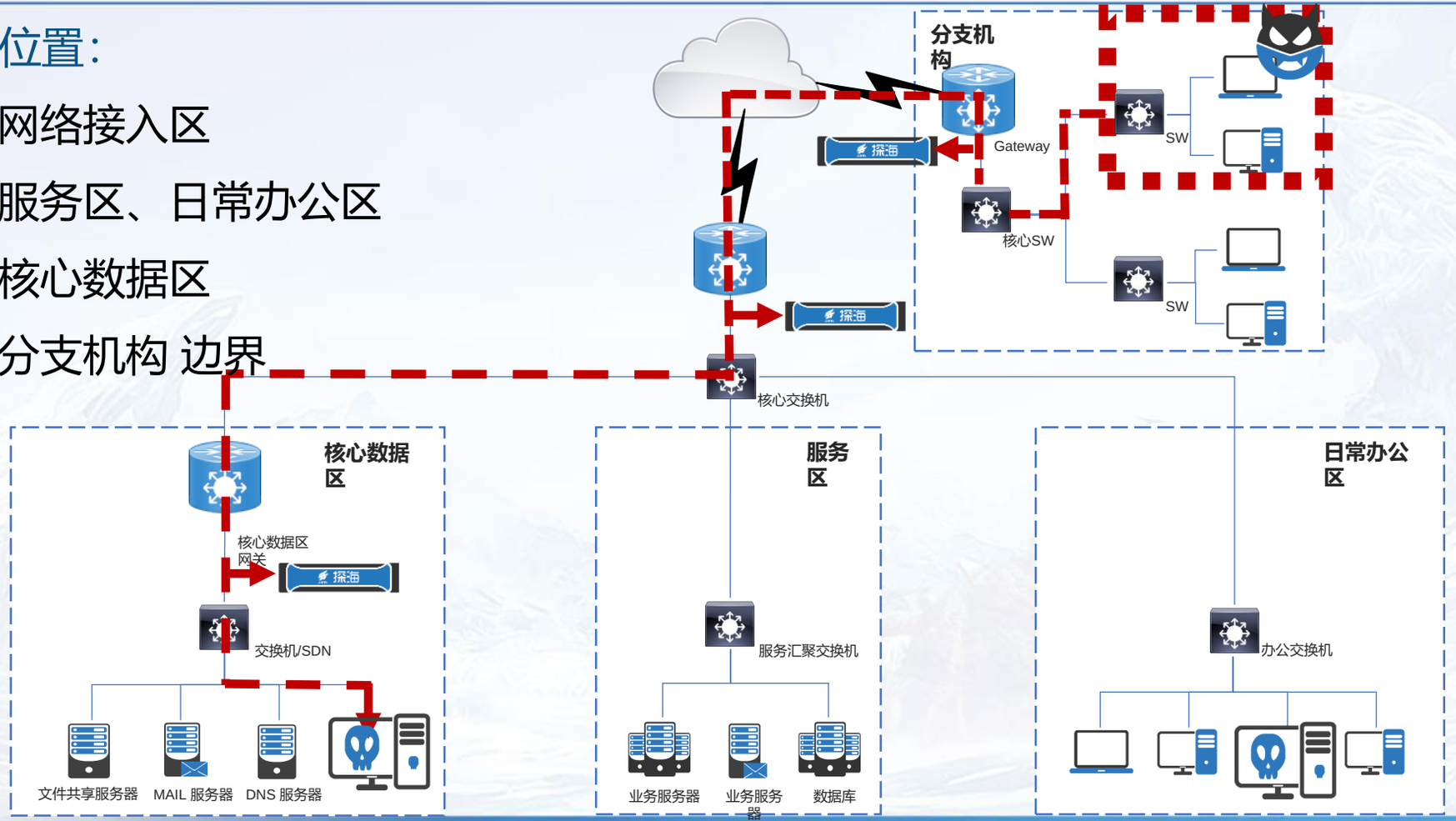
态势感知

05 以敌情想定为核心 留存数据，进行威胁猎杀

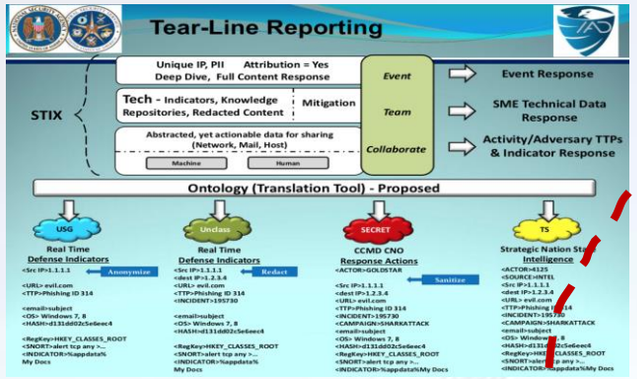
敌方突破防御时，威胁猎杀需要全方位的数据留存

部署位置：

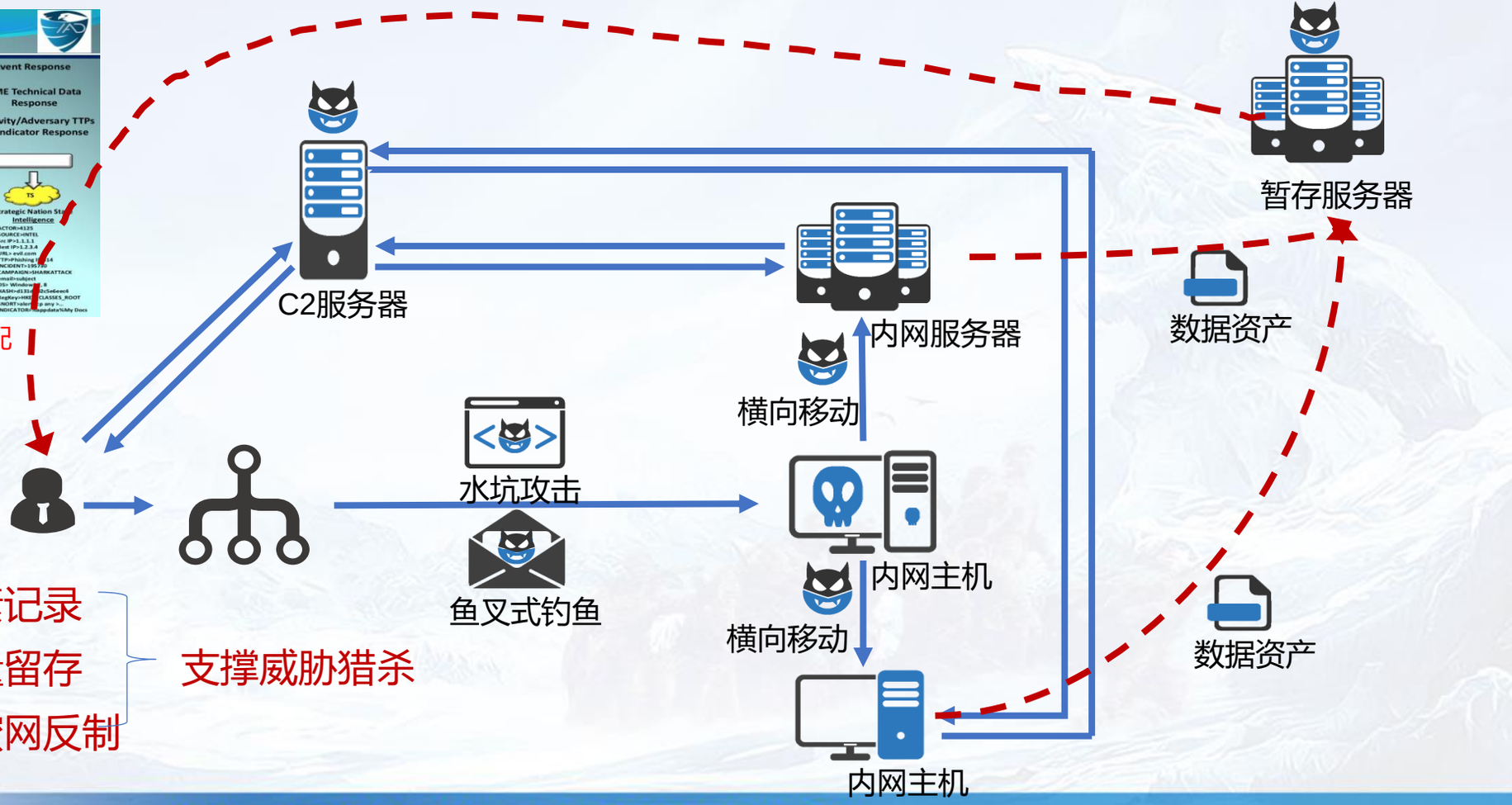
1. 网络接入区
2. 服务区、日常办公区
3. 核心数据区
4. 分支机构 边界



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



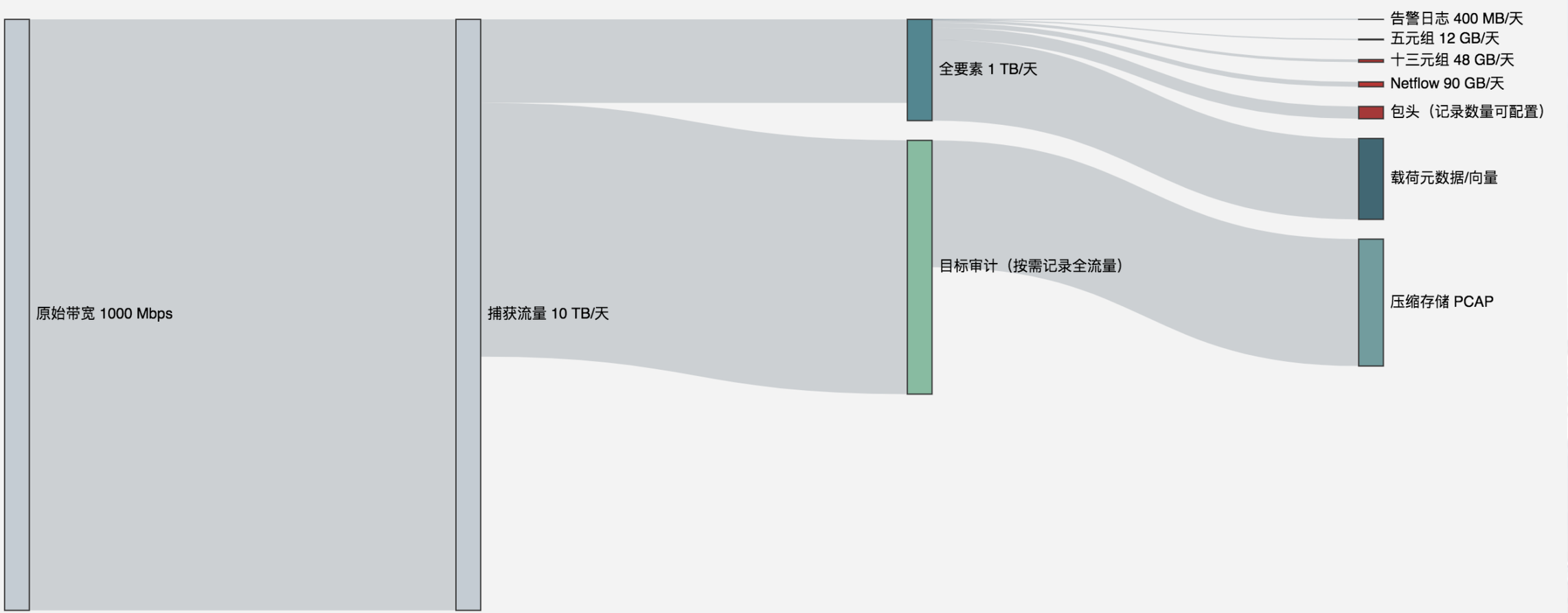
必经路径——全要素记录

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

海量数据带来的挑战


原始带宽 1000 Mbps
捕获流量 10 TB/天
全要素 1 TB/天
目标审计（按需记录全流量）
告警日志 400 MB/天
五元组 12 GB/天
十三元组 48 GB/天
Netflow 90 GB/天
包头（记录数量可配置）
载荷元数据/向量
压缩存储 PCAP

海量数据带来的挑战及我们的应对

威胁发生

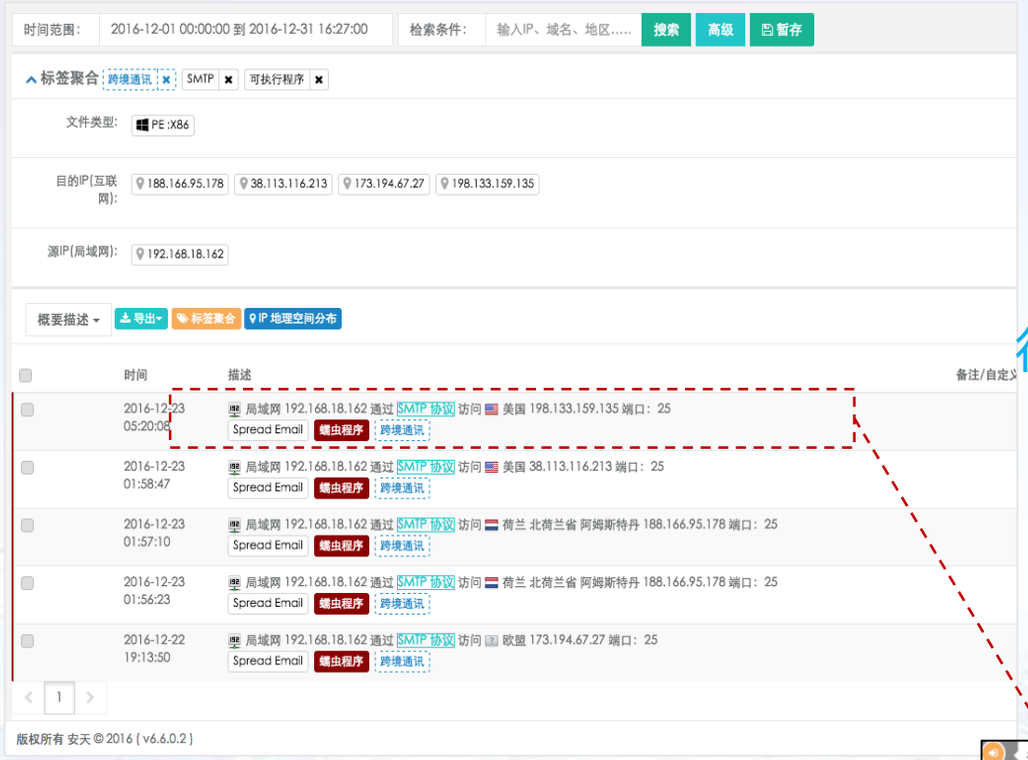
分析

响应

Observe → Orient → Decide → Act

2016-12-23 05:20:08	局域网 192.168.18.162 通过 SMTP 协议 访问 美国 198.133.159.135 端口：25 Spread Email 蠕虫程序 跨境通讯
2016-12-23 01:58:47	局域网 192.168.18.162 通过 SMTP 协议 访问 美国 38.113.116.213 端口：25 Spread Email 蠕虫程序 跨境通讯
2016-12-23 01:57:10	局域网 192.168.18.162 通过 SMTP 协议 访问 荷兰 北荷兰省 阿姆斯特丹 188.166.95.178 端口：25 Spread Email 蠕虫程序 跨境通讯
2016-12-23 01:56:23	局域网 192.168.18.162 通过 SMTP 协议 访问 荷兰 北荷兰省 阿姆斯特丹 188.166.95.178 端口：25 Spread Email 蠕虫程序 跨境通讯
2016-12-22 19:13:50	局域网 192.168.18.162 通过 SMTP 协议 访问 欧盟 173.194.67.27 端口：25 Spread Email 蠕虫程序 跨境通讯

持续将经验转换为标签规则、场景规则



行为向量 + 标签

多维度呈现

【示例】识别特定攻击

跨境通讯、邮件通讯、文档、启动powershell

- **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**

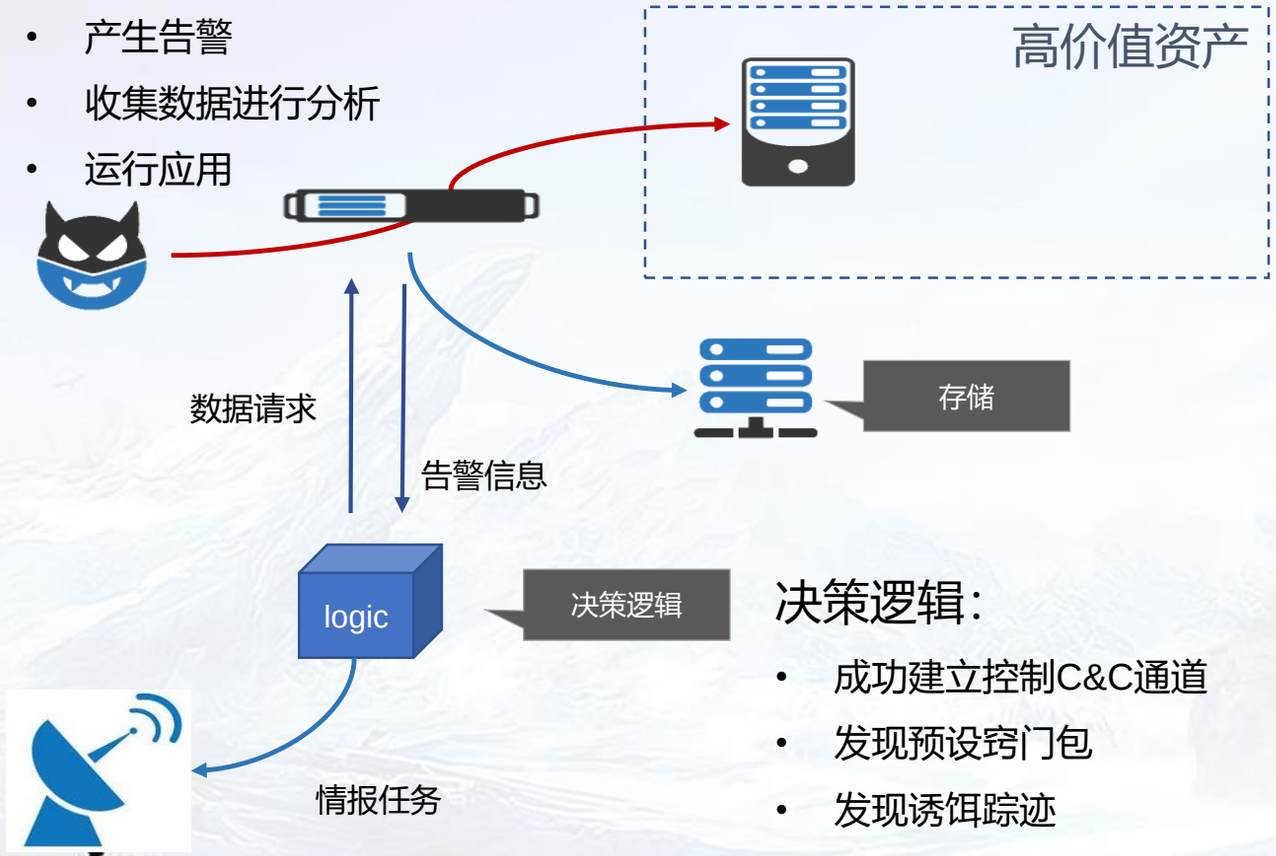
1. 多个标签恰好构成了不同的场景

2. 自定义条件规则构成场景

接受指挥控制，边缘分布式计算，减轻态势负担

传感器：

- 产生告警
- 收集数据进行分析
- 运行应用



决策逻辑：

- 成功建立控制C&C通道
- 发现预设窃门包
- 发现诱饵踪迹
- ……

告警指示恶意活动存在，并将数据提供给态势感知，配置的条件和决策逻辑决定数据是否存储。

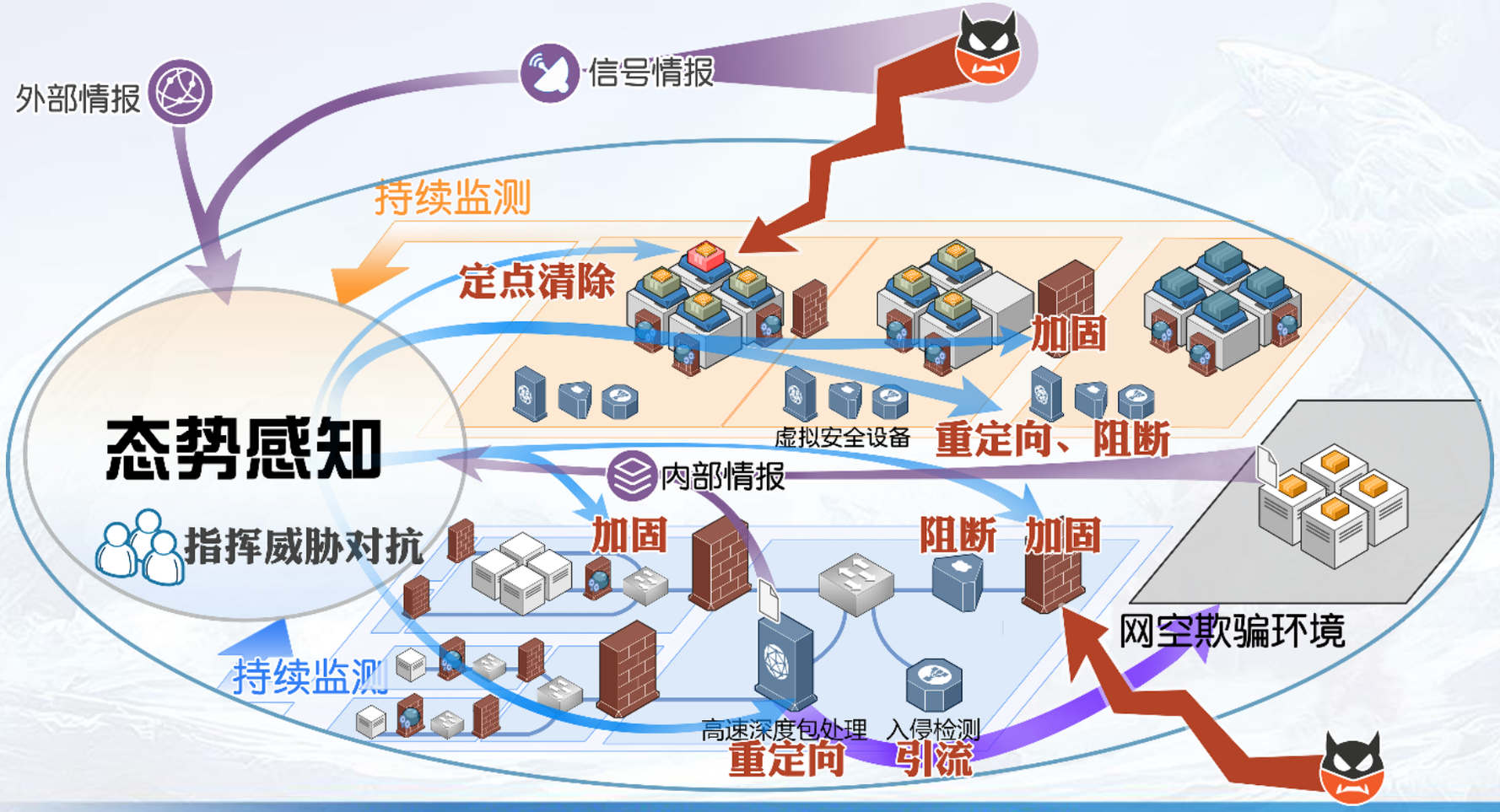
综合分析(态势感知)的预处理环节

充分利用边缘计算的分布优势

提升态势感知的数据处理能力

在协同指挥下
让攻击者无所遁行、无处可逃、无计可施

网络监测与响应能力是全方位态势感知的基础



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