网络空间威胁对抗防御技术研讨会
暨 第十届安天网络安全冬训营

沧海横流

执行体全量识别与精细管控

流量检测助力执行体治理

安天探海的实践

安天 | 流量安全产品中心

目 录

01

流量检测
执行体行为的网络投影

流量：攻击者载荷投放与控制实施的交火空间

侦查 → 定制 → 投放 → 利用 → 安装 → **控制** → 行动

侦查	定制	投放	利用	安装	控制	行动
分析攻击目标及攻击面	准备后门和渗入途径	发起攻击并注入后门	触发后门或漏洞利用	实现在受害机器的长期隐蔽	建立远程控制机制	执行预定行动，达成目标

命令与控制技战术遍历

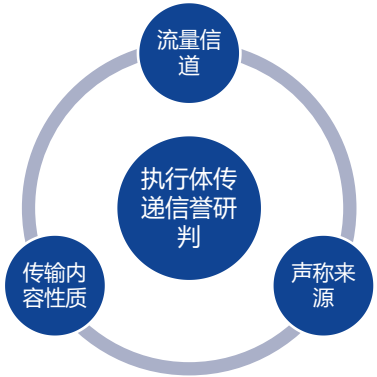
技术	使用应用层协议				通过可移动介质通信	编码数据		混淆数据			使用动态参数			使用加密信道		使用备用信道	使用入口工具传输	创建多级信道	使用标准非应用层协议	使用非标准端口	使用协议隧道	使用代理				利用远程访问软件	使用流量信令	利用合法Web服务		
子技术	使用Web协议	使用文件传输协	使用邮件协议	使用DNS协议		标准编码	非标准编码	使用垃圾数据	使用隐写术	模拟合法协议	使用域名生成算法(DGA)	使用Fast Flux DNS	使用DNS计算	使用对称加密算法	使用非对称加密算法								使用内部代理	使用外部代理	使用多跳代理	使用域名前置		端口敲门	C2情报传递点(DDR)	双向通信	单向通信

摸清家底：梳理执行体的网络行为底数

治理执行体行为

- 了解执行体传输行为
  - 细粒度识别流量与发起对象关系
- 识别执行体传输性质
  - 传输信息内容隐私检测
  - 升级动作及风险识别
  - 关联对象行为识别
- 控制执行体传输动作
  - 控制连接及内容
  - 防止过度收集信息

依托下一代引擎，对流量通道传递的执行体进行有效验证



➢根据归属信息构建证书链

➢根据证书链和可疑信息综合判断签名证书的权威性

➢综合时间戳和可疑信息（CRL撤销信息）判定签名是否存在密钥泄露等可疑点

➢综合身份信息判定是否被APT组织利用

➢判断签名是否被综合基本信息、可疑信息黑客组织利用

➢结合流量传递信道，确认执行体信誉

来源 | 信誉 | 动作 | 传输

密钥可信安全度

- 利用证书合法性常规验证及密钥算法特性，伪造可信根证书

离线场景限制证书可信度实时性

- 证书链构建需要在线构建
- 证书可信度需要在线验证

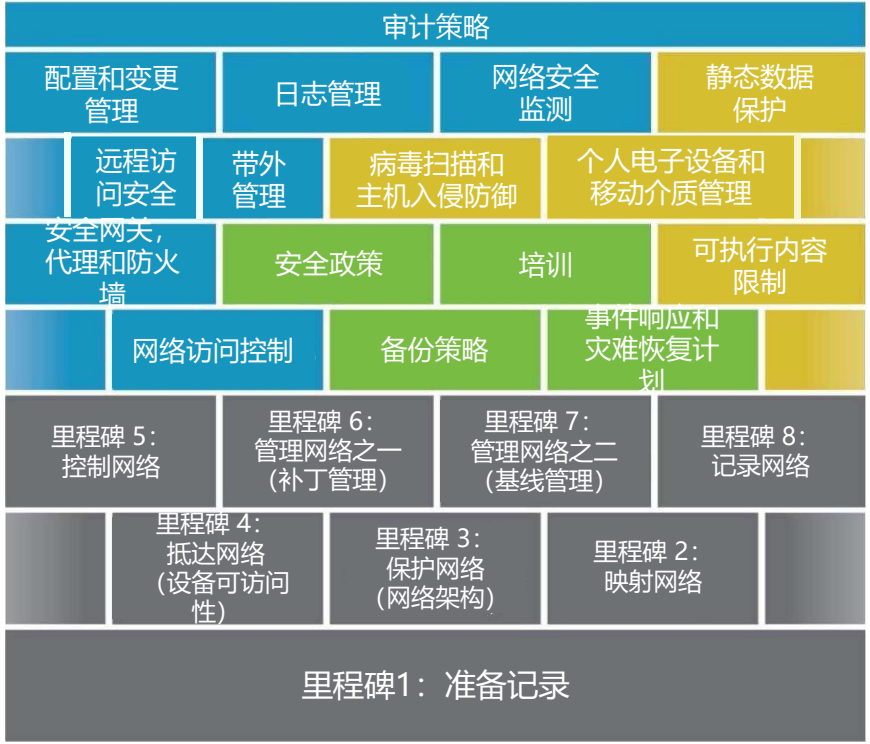
数字签名成为逃逸检测“保护伞”

- 执行体结构特性，数字签名机制成为逃避检测“帮凶”
- 无法保证执行体签名前是否恶意

平台成熟度

- PKI体系对国产操作系统与硬件平台的支持尚不成熟
- 传统哈希特征认证不可收敛

可管理网络对资产记录、网络了解的要求

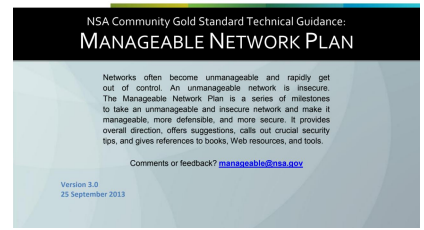


规划可管理网络的路线图[1]

- ●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

National Security Agency/Central Security Service

INFORMATION ASSURANCE DIRECTORATE


NSA Community Gold Standard Technical Guidance:
MANAGEABLE NETWORK PLAN

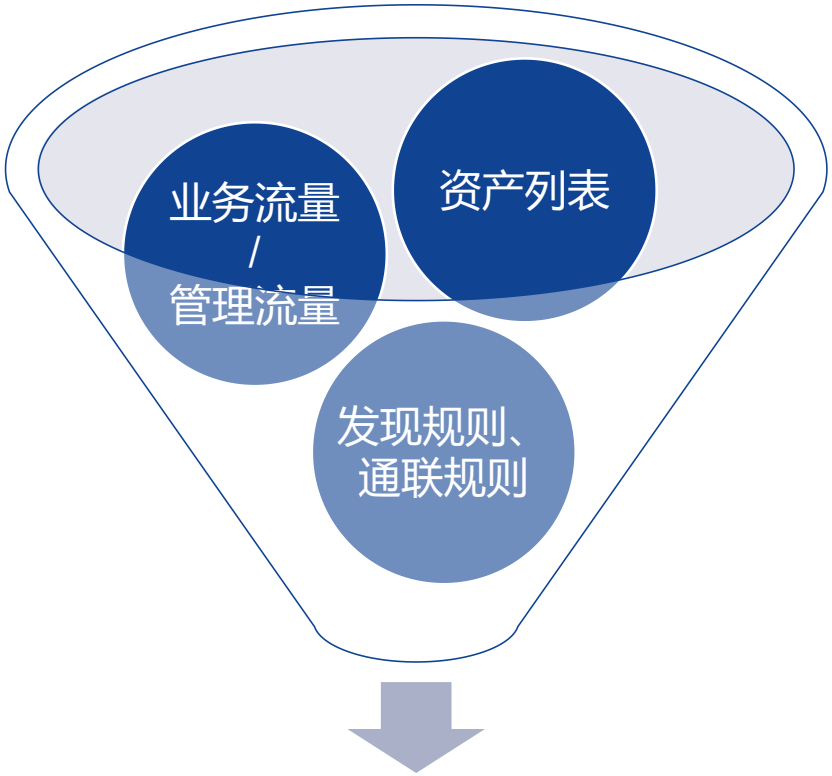
Networks often become unmanageable and rapidly get out of control. An unmanageable network is insecure. The Manageable Network Plan is a series of milestones to take an unmanageable and insecure network and make it manageable, more defensible, and more secure. It provides overall direction, offers suggestions, calls out crucial security tips, and gives references to books, Web resources, and tools.

Comments or feedback? manageable@nsa.gov

Version 3.0
25 September 2013

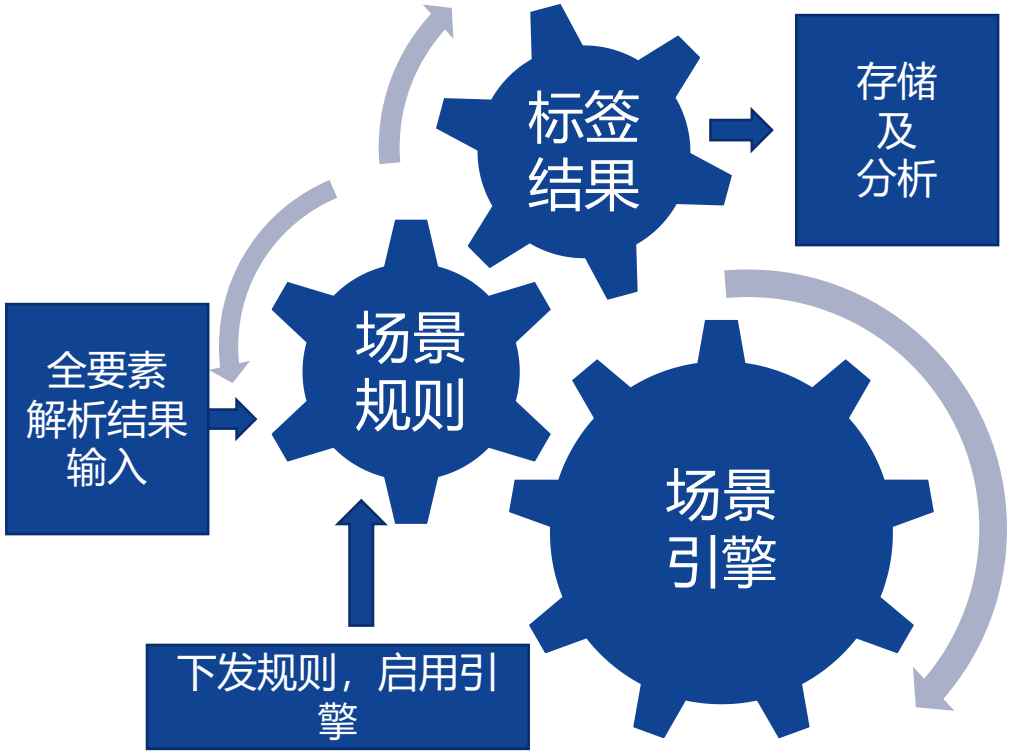
[1]：《可管理的网络计划指南V4.0》

摸清家底：网络暴露面梳理，收束端口、协议，支撑管控



- 发现
  - 非服务器区的开放端口
  - 协议与登记不一致
  - 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

基于运行场景规则，发现违反安全要求的情况

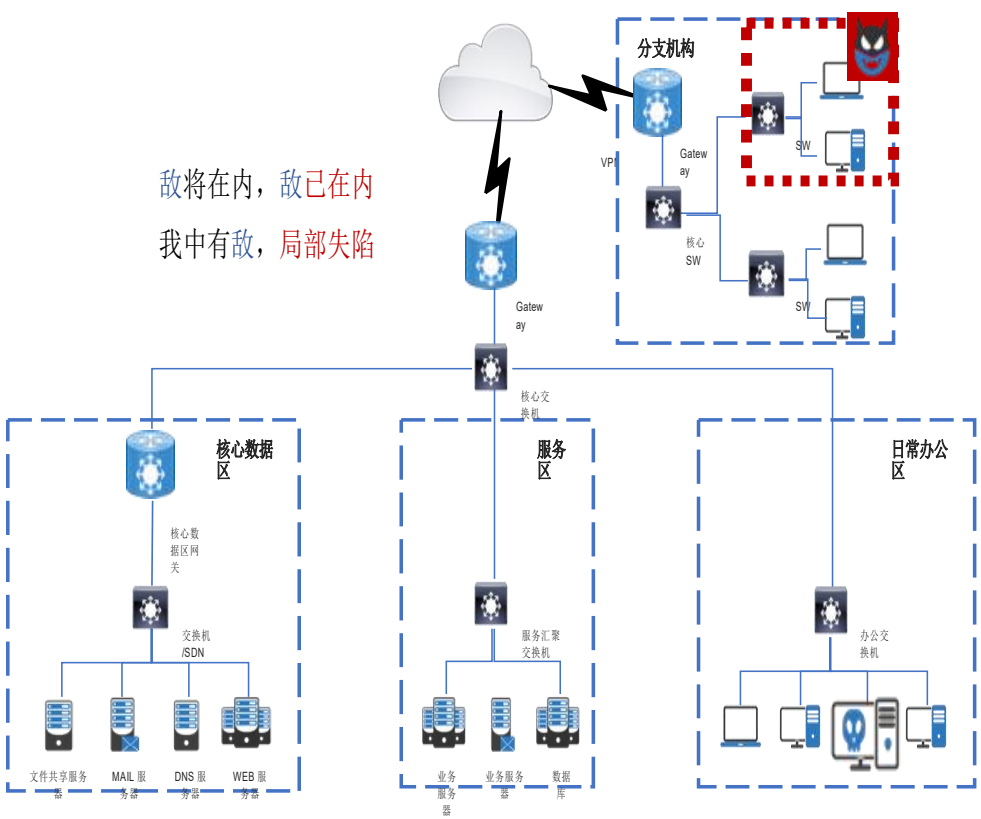


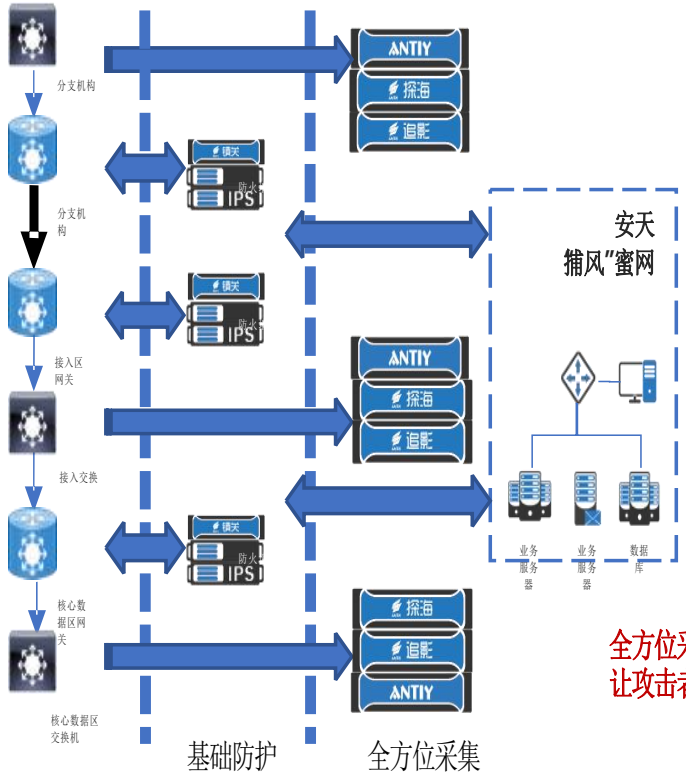
- 信息泄漏
- 明文管理协议
- 地址冲突
- 地址空间耗尽
- DNS服务器配置非正常DNS
- 具有没有登记的DHCP服务器
- 443端口上的HTTP流量
- 传递的PE文件具有非PE扩展名
- 传递的PE文件具有非PE的MIME
- 邮件中传递PE
- 非公司SMTP邮件服务器发送了邮件
- ……

应对攻击者的重要防线

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

02

全面掌握网络状况，服务威胁防御猎杀

多维度的基础检测能力

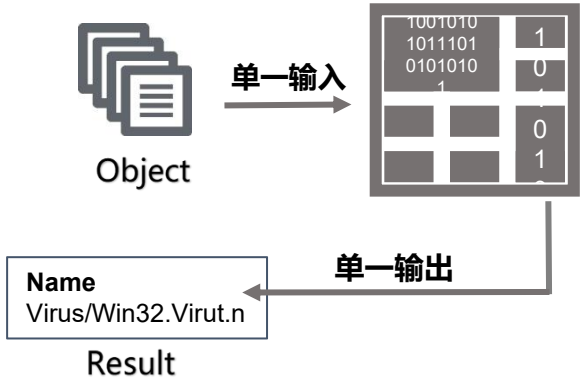
全要素采集（丰富的检测对象） → 多维度检测能力 → 威胁标注、追踪与响应

- 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；

- 获取载荷行为能力，形成对恶意代码的揭示能力，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；
- 深度定制规则，提供威胁的向前追溯和向后守候能力；

威胁检测需要综合多个维度--多种输入输出对象

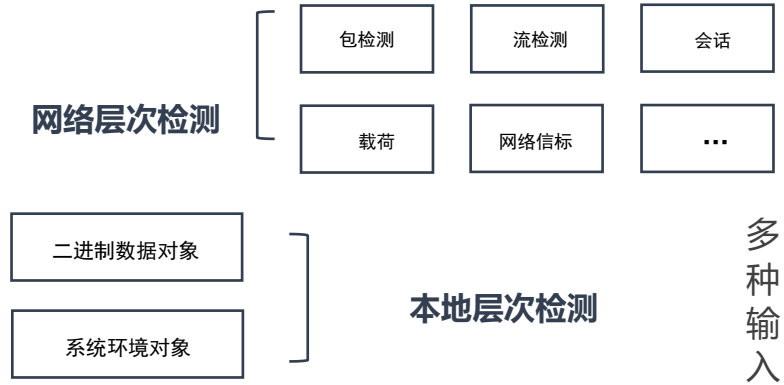


✓ **传统引擎**

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

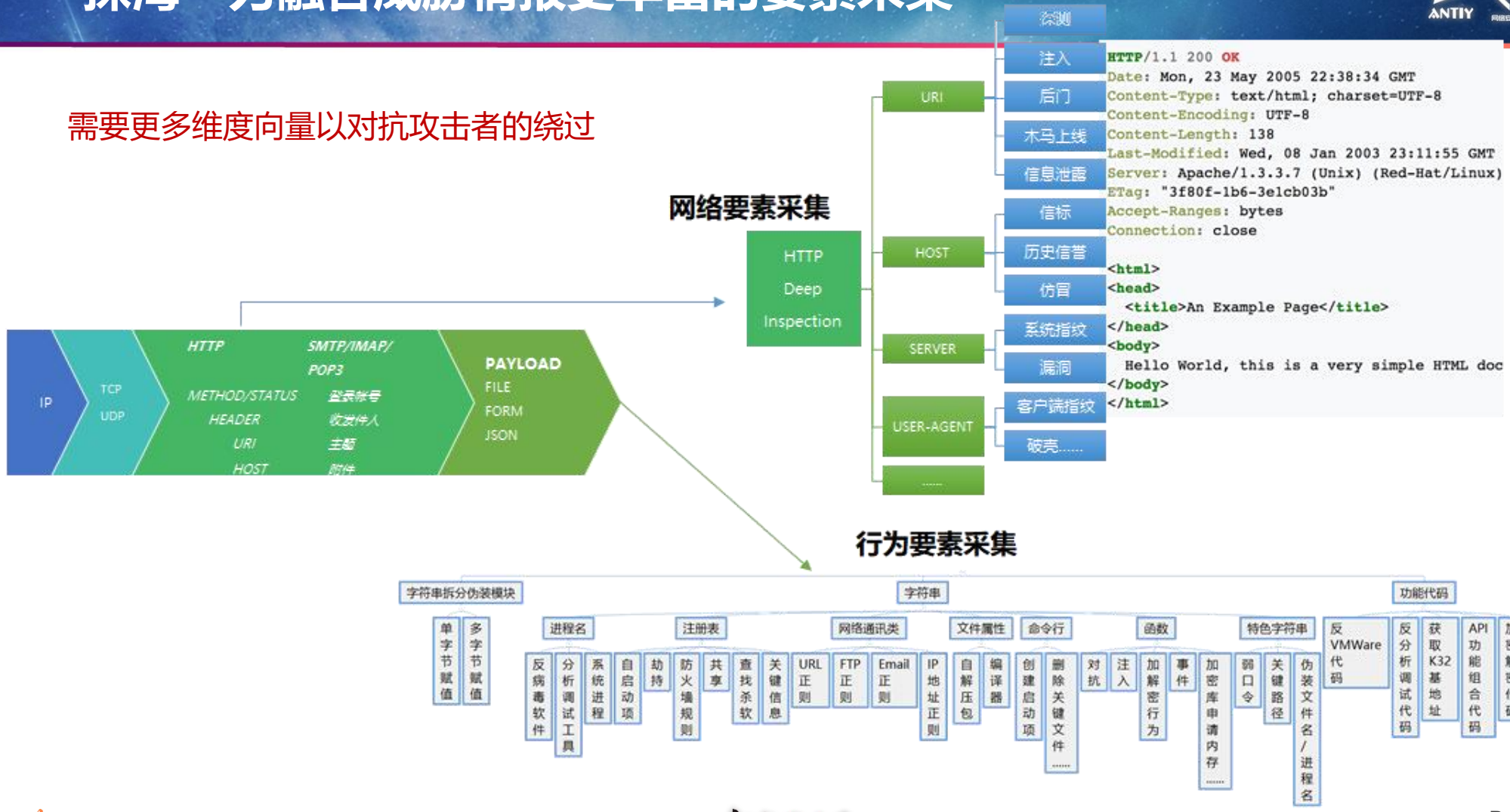
输出 3

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

“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



有效应用向量级威胁情报，进行丰富有效的威胁检测

安天威胁情报系统基于引擎覆盖全球**100万台**网络设备和超**28亿部**智能终端的感知数据。以及持续对捕获样本的进行动静态分析，已构建**超百亿级别**威胁知识图谱。经过安天**20年**分析能力积累，持续输出生产包括机读情报和向量情报2类**20余种**威胁情报类型，以及标识超过**30种**威胁类型情报。在高级威胁分析场景提供完整的运营级情报的同源关联分析能力。在威胁检测场景向全系统供应向量级威胁情报。

安天是国内完整具备全域威胁感知、自主情报生产、高级威胁情报分析的全能力型情报厂商。

支持输入数据源

- 静态分析数据
- 动态分析数据
- 多引擎分析数据
- 流量探针数据
- 端点感知数据

- 高级威胁情报
- 自主生产情报
- 开源情报

支持输出的情报类型

机读情报

- 文件情报
- 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

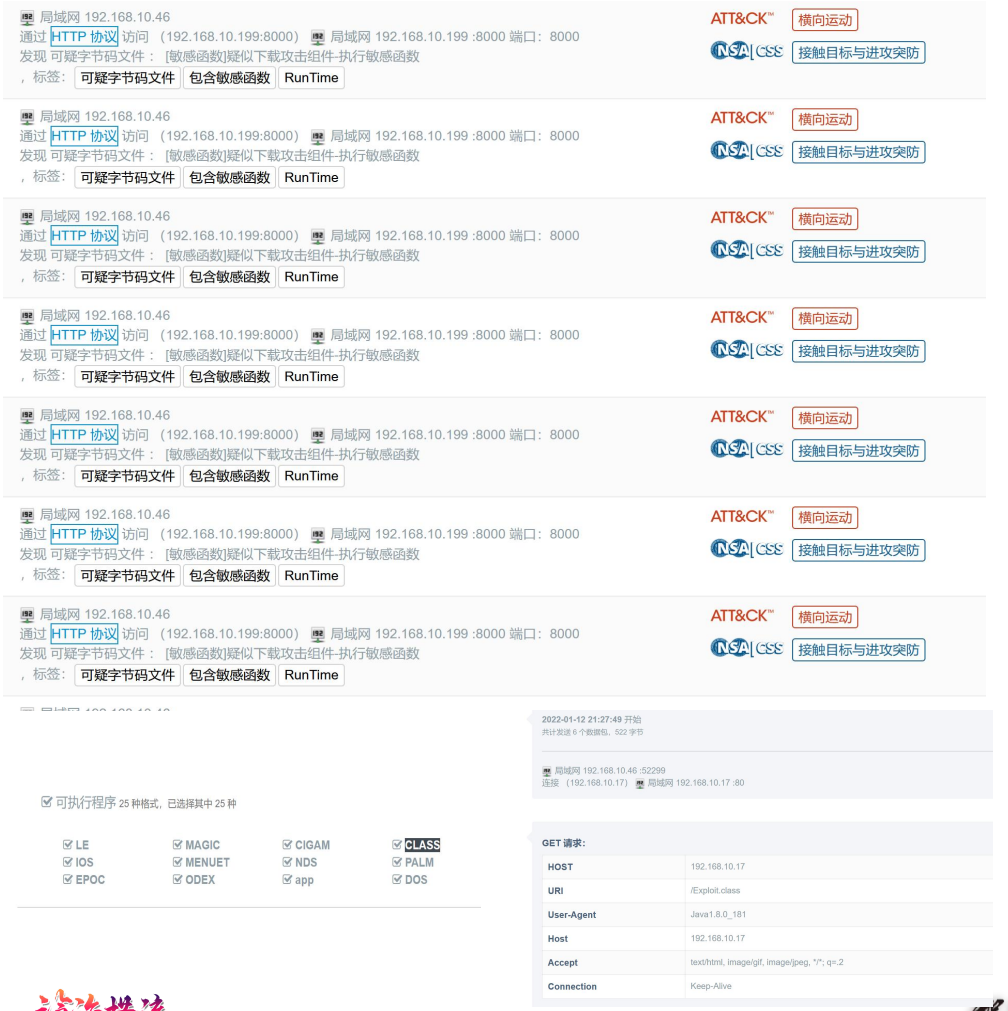
向量级情报

- **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**

需安天下一代威胁检测引擎支撑

- 注册表情报
- 互斥量情报
- 数字签名情报

持续将经验转换为标签规则，打造攻击者无法预测的防线



行为向量 + 标签

多维度呈现

- **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

通过识别class文件传输

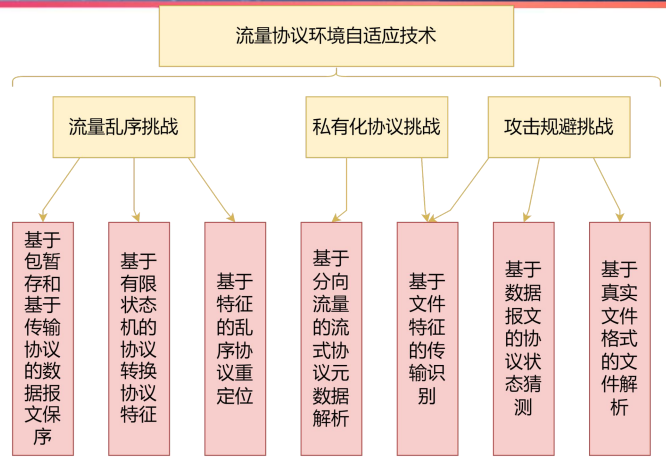
探海可直接发现Log4j漏洞利用成功事件

基础数据标签化、场景化，构建定制化威胁守候能力

流量协议环境自适应，广泛适配流量环境，支撑治理

问题与挑战

- 流量中的乱序、重传、分片、聚合问题
- 旁路处理时上游报文镜像报文丢失、路由牵引导致的流量分向处理问题
- 恶意流量对监测的规避问题
- 影响报文的监测留存质量，从而影响对内容的检测定性



解决要点

流量分向提取聚合

- 对请求向、响应向、控制流、数据流进行分别识别、分别提取元数据和识别威胁。
- 在较少的内存占用的情况下，允许超大文件留存，无数据包丢失容忍，乱序包整理，MTU变化自适应等功能。

解决要点

乱序协议，重新定位

- 有限的内存对应无限的乱序
- 基于对协议的了解，寻找报文中可用于标志处理协议状态的位置
- 基于标志位置进行重新定位。
- 无回溯，效率提升显著

解决要点

协议转换特征，抗压界

- 当在攻击者使用较小MTU、IP分片或巨型帧的情况以规避协议分析的情况下，依然可以取得较好的协议识别效果
- 基于对各可能协议上下文的理解，智能判断是否应当暂存数据报文，并在允许范围内等待后续报文。

解决要点

识别私有协议中的文件传输

- 基于对文件特征的理解，从流量中寻找文件的传输迹象，并尝试从文件头开始直接剥离文件内容
- 对Metasploit等常见攻击平台进行恶意控制木马载荷传输时，对载荷的剥离和识别也能取得较好的效果。

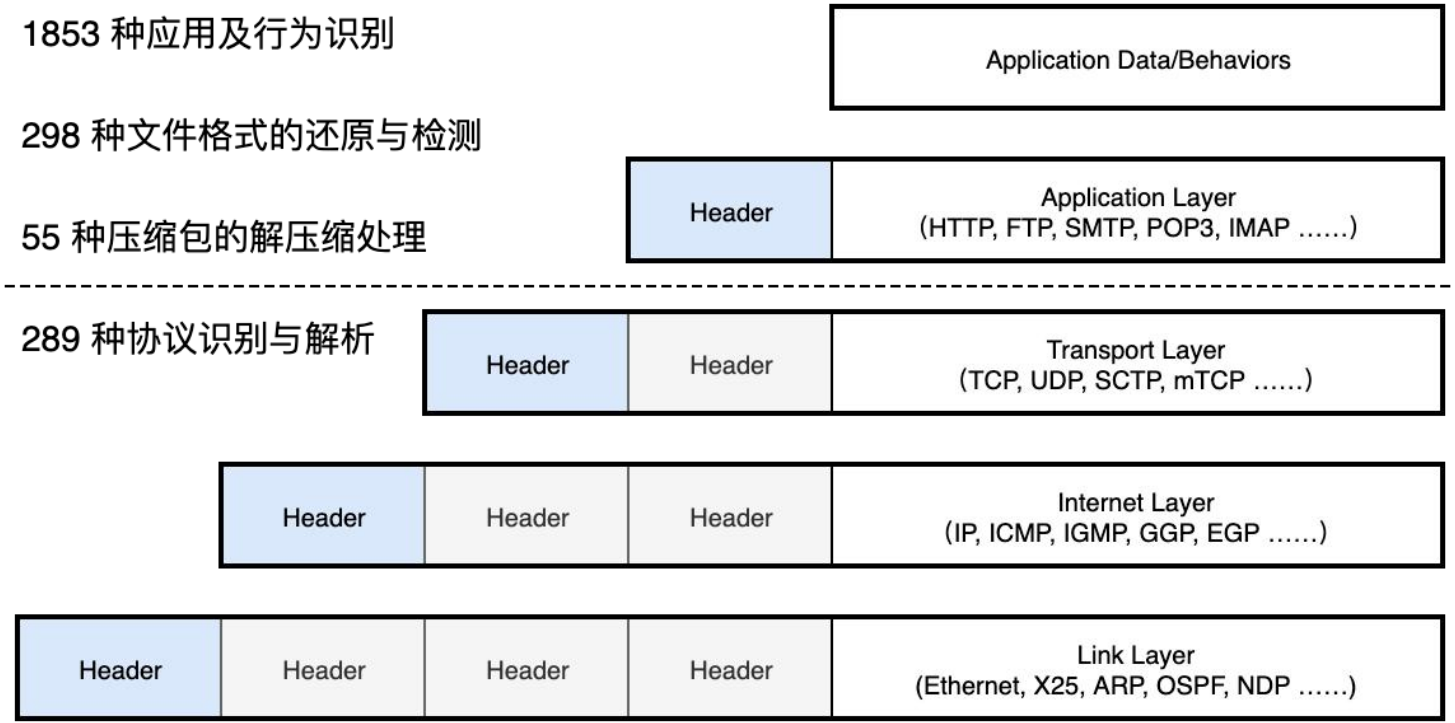
“探海”支持的协议识别、元数据化与要素提取能力

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

自动流量特征收集，细粒度识别应用流量行为

证书号第3686173号

发明专利证书

发明名称：一种基于探针的自动流量特征收集方法及系统

发明人：李林哲;张浩;关墨辰;张栗伟

专利号：ZL 2017 1 0224478.6

专利申请日：2017年04月07日

专利权人：北京安天网络安全技术有限公司

地址：100195 北京市海淀区闵庄路3号清华科技园玉泉慧谷一期1号楼

授权公告日：2020年02月07日　　授权公告号：CN 108366042 B

国家知识产权局依照中华人民共和国专利法进行审查，决定授予专利权，颁发发明专利证书并在专利登记簿上予以登记。专利权自授权公告之日起生效。专利权期限为二十年，自申请日起算。

专利证书记载专利权登记时的法律状况。专利权的转移、质押、无效、终止、恢复和专利权人的姓名或名称、国籍、地址变更等事项记载在专利登记簿上。

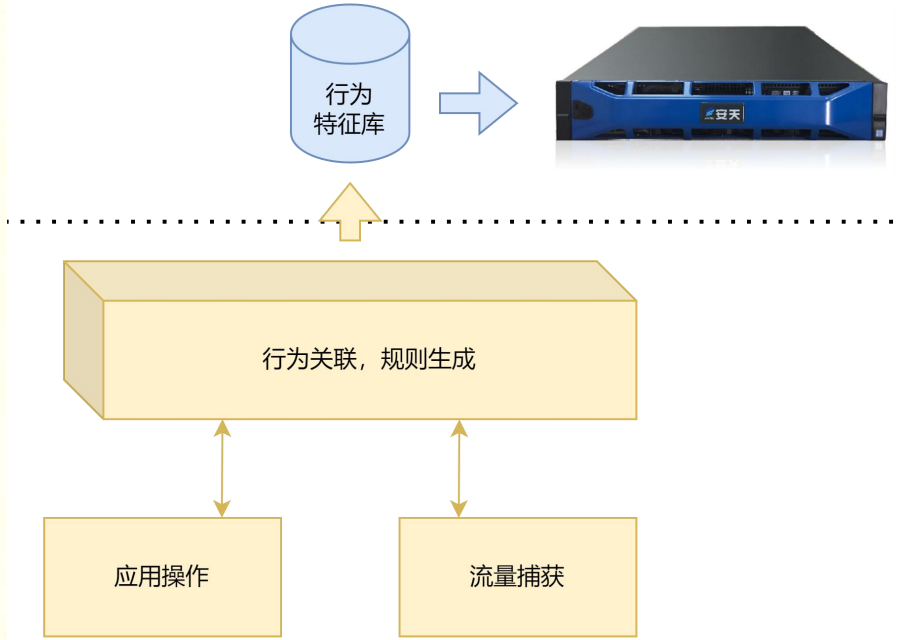
局长
申长雨

国家知识产权局

2020年02月07日

第1页(共2页)

其他事项参见背面

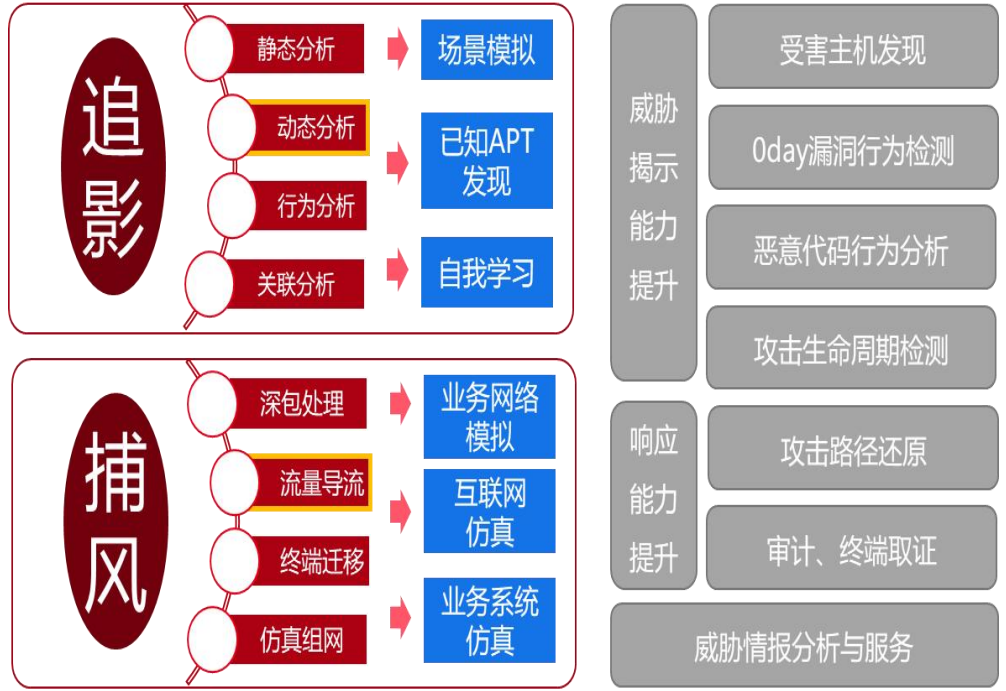


- 了解执行体传输行为
  - 细粒度识别流量与对象关系
- 识别执行体传输性质
  - 传输信息内容检测
  - 升级动作及风险识别
  - 关联对象行为识别
- 控制执行体传输动作
  - 控制连接及内容
  - 防止过度收集信息

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

- 构建基于我情的沙箱与蜜网



03 联动闭环，完善治理能力

依据防御框架，发挥部署位置优势，组合达成关键防御动作

指挥、决策与控制

汇聚、关联、统计、分析模型与呈现

关键防御动作矩阵

识别	塑造	防护	检测	响应
系统环境识别	系统环境策略塑造	资源访问拒止	系统环境检测	缓解
网络环境识别	网络管控策略塑造	连接拒止	流量环境检测	固证
业务识别	配置加固	创建拒止	应用环境检测	主机环境处置
用户识别	加密环境塑造	写入拒止	数据体检测	网络侧处置
配置识别	欺骗环境构造	执行拒止	用户行为检测	环境与数据恢复
暴露面/脆弱性识别		加载拒止		策略调整
活动识别		……		

作用对象

网络类	用户类	应用类	信息类	执行体类
内容	用户	DNS	配置	载荷
地址	帐户	TLS	补丁	进程
协议	身份	VPN	脆弱点	内存
端口	权限	邮件	……	服务
……		WEB		……
		……		

作用位置

主机　边界

流量　应用

流程

部署方式　与被保护对象原生融合/安装 | 基于载体设备部署 | 基于虚拟化资源部署

管理模式　单点管控/集中管控 | 无管控

认知威胁	攻击者	意图	装备	载荷	行为	被攻击者	脆弱性	检测结果	后果

保护目标	硬件资产	软件资产	外设资产	数据资产	仿真资产

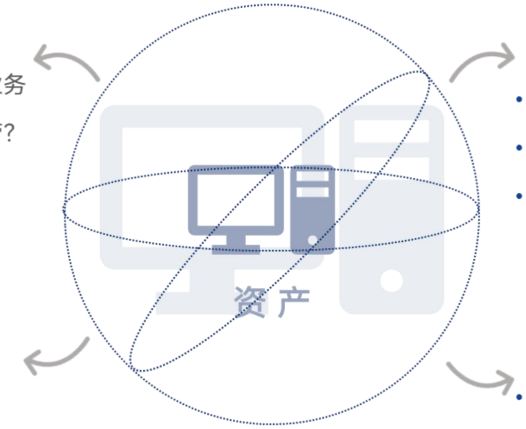
流量检测支撑基于可管理网络的资产安全治理

我有哪些资产

- 有哪些资产？承载什么业务
- 这些资产由谁用？归谁管？
- 会造成什么影响后果
- ……

有哪些暴露面

- 运行了哪些应用
- 哪些应用和服务暴露在互联网
- 开放了什么端口

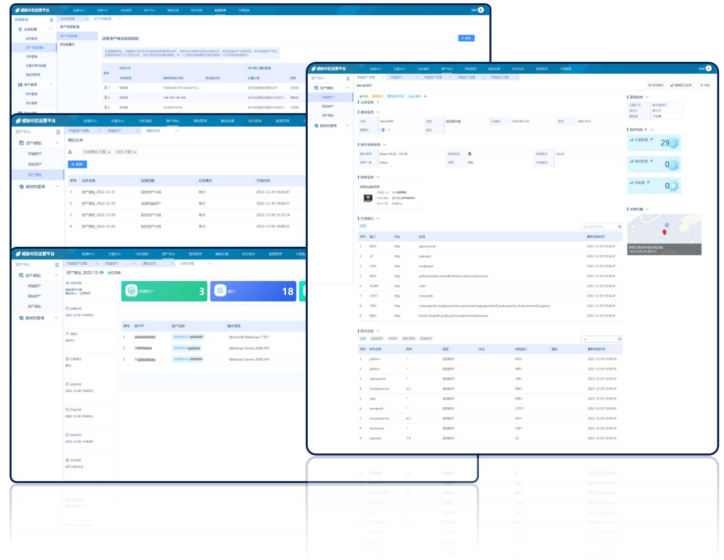


资产现在状态如何

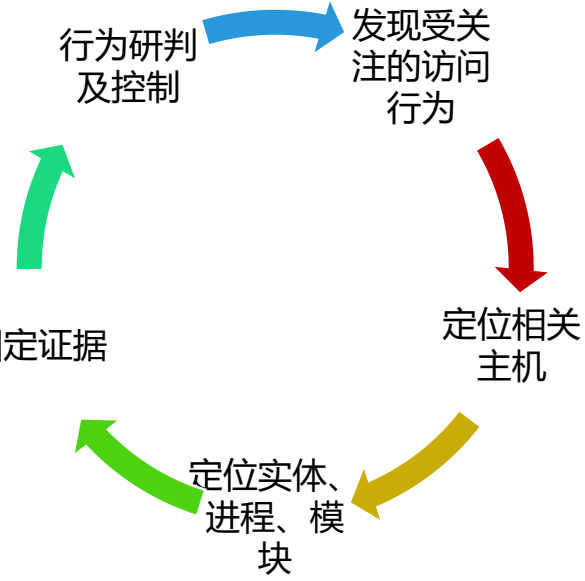
- 有多少资产在用
- 有没有关键设备挂掉
- ……

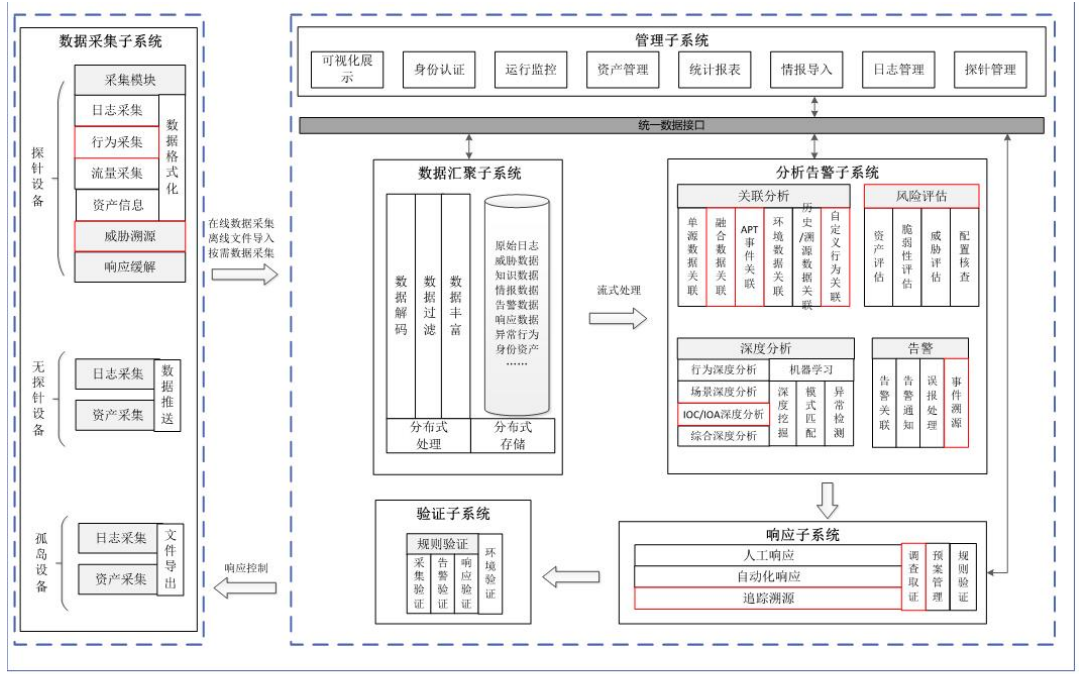
资产会不会遭受攻击

- 资产有哪些漏洞
- 配置有没有问题
- 设备和服务有没有弱口令



联动智甲，基于流量行为发现，支撑执行体治理控制





流量检测支撑威胁追溯、猎杀

安天采用了基于对象和作用关系统一风险描述形式，通过提取事件中涉及的对象，标识其攻击方/影响方等风险作用关系，对同类事件归类去冗余，实现对网络攻击、网站内容、用户行为等风险的统一呈现和关联

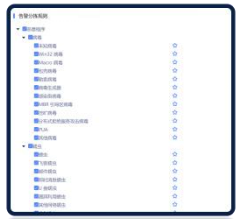
在真实环境下可降低98%以上重复或相似告警

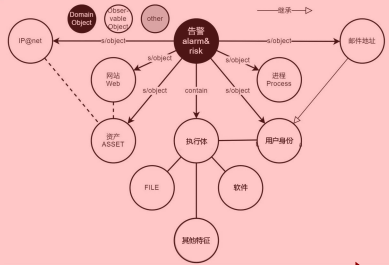
分析模型发现事件

安天通过数据标准预定义事件结构及依赖字段，分析模块可自由定义输出内容，只要满足基础依赖要求即可录入对应事件

设备检出事件复验与分拣

用户可以自行配置哪些风险类型进行告警、调整告警归并周期，也可以通过组合条件的白名单策略进行细粒度过滤





基于对象化风险描述形式
通过决策模型抽取对象

统一告警监控

告警对涉及对象按攻击方、受害方、攻击工具/载荷的维度进行描述和归类，覆盖对象类型包括：邮件地址、用户、通信节点(IP)、终端资产等，对象类型且可以灵活拓展，其中IP、域名、文件、资产、组织机构形成了本地知识库和信息卡，便于快速追溯

全天候、全方位持续监控网络威胁，建立实战化的防御体系

感谢大家的关注

安天冬训营 wtc.antiy.cn