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

基于安全防御要素的检测及响应

以XDR为基础的管控协同体系

安天 | XDR产品中心

目 录

01 现状与挑战

现状与挑战

信息化发展带来新的安全场景与问题

随着信息化建设的开展和业务的增长，信息系统价值在不断提高，同时带来还有不断增加的网络复杂度、暴露面和脆弱点

为了解决各场景的问题，安全设备和系统也随之叠加堆砌

业务与数据	身份与凭证	网络与地形	应用与执行体	资产与系统
青竹WAF、UEBA、业务系统、日审、SIEM、诱捕	身份认证、UEBA、业务系统、ITDR	探海NDR、NTA、IPS、IDS、TID情报、NGFW、镇关FW、可管理网络设备、诱捕	智甲EDR、追影沙箱、TID情报、捕风诱捕、漏扫、情报、…	智甲EDR、EPP、CWPP、CMDB、…

现状与挑战

工程化 & 组织化的攻击模式

在信息化快速发展的同时，承载了高价值信息的系统显然成为了攻击者觊觎的目标，攻击者的攻击方式和手法也愈加工程化、组织化

强针对性与目的性

由于地缘因素和经济利益，攻击组织攻击的针对性和目的性也愈发增强
导致了以破坏、窃密、勒索等为目的进行的网络攻击的增多

长期潜伏瞬间爆发

攻击的持续性也在不断增加，攻击者在入侵后往往长期潜伏在信息系统中，基于特征检测或恶意行为检测很难发现
而真正攻击作业的爆发时间极短，靠人工处置和防御难以有效应对

混合攻击手法盛行

攻击者为了攻击的灵活性往往采用更加模块化和单元化的攻击工具和攻击资源
因此可以更加轻易的采用多种技术手段进行组合攻击

持续攻击成本低廉

而命令控制即服务(C2aaS)、恶意软件即服务(MaaS) 等攻击资源的基础设施化，也大幅降低了攻击成本
在持续的针对性的攻击中攻击方只要有任意一次攻击成功，即可成功渗透进入信息系统

现状与挑战

作为防守方我们堆砌的设备可以对一些明显特征的攻击进行防范，但是攻击的迭代周期往往会明显短于检测和防御能力更新周期，而面对更加复杂的组合手段攻击，单一的防御设备无法有效拦截，由于攻击的暴露面往往较广，也造成了响应周期极长

早期建设的soc/siem等往往仅能汇总数据或者对其格式进行简单处理，导致了其对第三方数据源很难做到真正的全局统筹理解和分析，因此在面对复杂攻击时各种问题便一一暴露出来

设备视角的局限性

- 单一设备囿于其所处位置和监测视角，仅能识别特定场景威胁
- 面对多场景组合的攻击方式以及长期潜伏的威胁无法有效发挥作用

设备间无法统筹分析

- 设备之间对信息的表述参差不齐，无法在全局视角有效地统筹分析

设备策略维护困难

- 环境的复杂化和设备增多导致了策略维护成本的陡增
- 策略下发后不知道有没有产生效果

整个防御体系无法有效地统筹和协调

需要全局性的监控及响应

需要统一的中枢分析调度和协调管控体系

以执行体等防御要素的细粒度采集与管控为基础，关注边界、流量、身份、终端、业务等场景下的异常行为。在全局视角下通过自动化上下文分析定位风险点，实现检测响应闭环，为用户的安全运营降本增效

通过安天威胁对抗运营**XDR**平台可以有效统筹各类设备，构建统一的网络安全防御体系

02 数据标准参差，需要互联互通

数据标准参差，需要规范互通

数据接入的目的不仅仅是将数据进行简单的留存，仅仅汇总数据是不够的，更需要格式的标准和内容的规范，通过两者的结合，才能为数据赋予含义，推动**数据到信息的转换**

而数据内容治理的成本高、短时间难以见效且需要持续的维护，所以市面上很多系统仅支持接入第三方设备数据但并未对第三方设备的内容进行规范，导致了数据分析时鸡同鸭讲应用困难

不仅要格式标准，更需要内容标准

安天在数据接入的基础上对数据进行重构和组合，**形成了可灵活拓展的数据和内容规范**，构建了**易拓展**的**可统筹第三方数据进行分析与关联的数据湖**，解决数据难以应用的问题

对象化的数据结构标准

安天根据数据产生原理及分析需要，将数据拆分理解、组合重构为数据对象

通过数据对象的组装，形成灵活可拓展的结构标准

基础信息 base	设备信息 dev							
通信节点 src dst	网络连接 net tunnel nat vpn	应用协议 http tls dns email ftp snmp	软件 app	文件 file	用户 user	网站 web	蜜罐 honey pot	终端类 host hard port service process Registry等
检测信息 risk attack intercept	信标检测 indicator	回连检测 c2	载荷 paylo ad	网页 web _risk	可用性 availa bility	脆弱性 wulner ability	弱口令 weak	补丁 patch

数据内容标准

统一度量标准

大多数设备检测后只会提供结论的信息，这些结论信息中不乏晦涩难懂和风险度量标准不一的问题，分析人员很难基于有限信息对检出的威胁进行度量和研判

安天通过专门的分析专家团队，面向第三方设备持续完善威胁认知，并定期更新

风险类型统一 | 风险名称翻译 | 技战术识别 | 攻击原理释义

处置建议 | 置信度评估 | 风险评级规范

在新威胁上报时，平台也会自动通过内置的机器学习算法自动识别攻击信息作为规则的补充

建设知识库

威胁分类库、威胁知识库、处置方案库、脆弱性知识库、脆弱性关联库、暴露面识别库、应用知识库等

提高整体防御认知，需要识别网空对象

数据本身是零散的缺乏上下文语义的，不利于理解和关联，为了有效的提升整体威胁的认知，需要通过网空对象的识别促进数据向信息的转化

网空对象识别

业务&数据

业务系统、API接口、关键业务节点、业务健壮性

身份&凭证

全局身份标识、主机账户标识、邮件账户标识、应用账户标识、外部身份标识等

网络&地形

系统连接点、路由连接点、服务连接点、外部连接点、通联过程

资产&系统

资产属性、配置与策略信息、日志和轨迹信息、接口和通道信息、端口和服务信息等

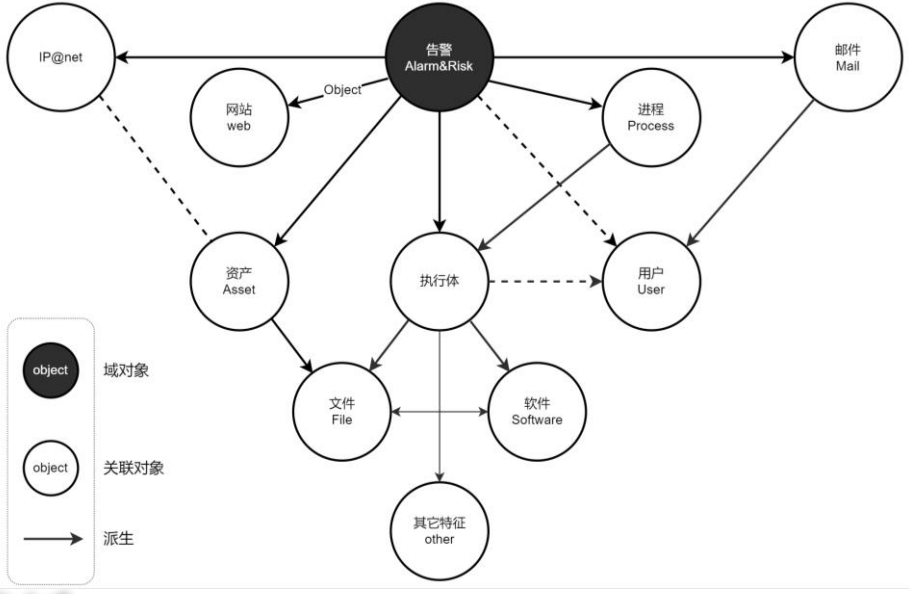
应用&执行体

可执行文件/脚本清单、软件清单、软件供应商清单、内部软件技术栈清单、执行器相关的重要向量清单

基于网空对象的统一风险描述形式

为对端/网/业务/身份等剖面的风险统一监控，需要对象化的风险描述和分析方法

安天采用了基于对象和作用关系统一风险描述形式，可以对攻击终端、威胁执行体、网站内容、用户行为等风险聚合和关联



03 网空环境多变，需要识别跟踪

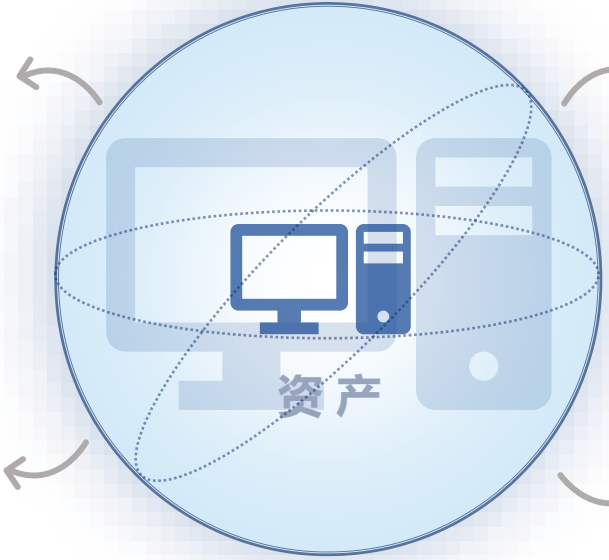
网空环境多变，需要识别跟踪

在分析和处置时，环境与地形尤为重要

资产是安全运营过程的核心保护目标，认清资产所处环境和地形是开展威胁对抗与防御工作的基础

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



资产现在状态如何

- 有多少资产在线
- 有没有关键设备宕机

有哪些暴露面

- 运行了哪些应用
- 开放了什么端口
- 哪些应用和服务暴露在互联网

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

面向各类安全场景提供对资产及其网络/应用/暴露面/脆弱性等环境信息的识别关联和风险治理能力

不止梳理资产名录，更需要摸清环境与地形

多渠道汇聚和融合环境与地形信息

运用多种手段全面、快速、准确的发现网络中的资产信息，通过对多源信息进行**融合**和统筹，识别资产**属性和用途**，动态发现更新资产的**环境和地形信息**，为进一步管理资产风险做好准备

无感识别 活跃

基于探海NDR全要素日志等流量信息结合发现规则识别资产，确定资产的归属网络/分组/位置/用途等资产信息，同时无感发现终端活跃的应用软件和中间件

主动发现 开放

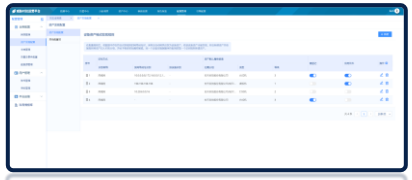
通过平台的探测模块或协同扫描设备，可以更全面的识别资产上运行的操作系统、中间件、应用软件、开放端口和服务等对象

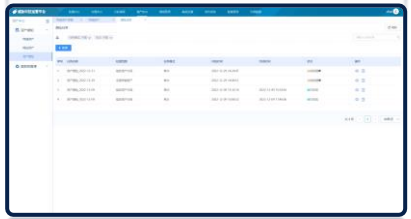
终端采集 全面

通过智甲EDR上报的终端资产信息同步用户资产，除前述内容外，可以全面的获取终端的执行体信息、软硬件、以及服务、注册表、启动项等配置信息

主动同步 拓扑

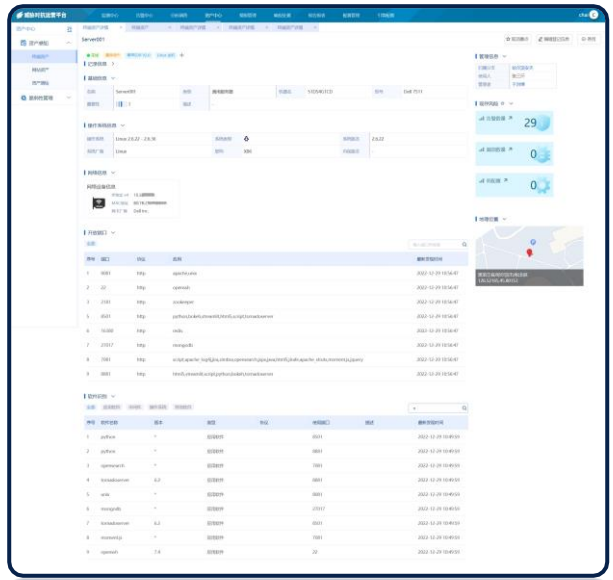
通过协同SNMP、网管系统等设备或系统进行同步获取资产信息，动态构建资产拓扑关系





多来源信息融合

多来源信息在融合后统一汇总和监控，形成统一的资产环境状态画像



不止梳理资产名录，更需要摸清环境与地形

主被动结合发现脆弱点

威胁总是利用资产脆弱性来提权和横移扩散，通过分析资产脆弱性，结合资产的价值、综合评估脆弱程度和攻击影响，然后据此选取合适的安全保护措施，降低网络资产的风险

漏洞风险识别

在融合漏扫和EDR等多来源数据的基础上，**平台基于漏洞关联库对应用软件、中间件、和硬件信息的关联，强化漏洞识别能力**

基于漏洞知识库对已知的漏洞风险进行评估，对风险控制措施做出建议，帮助用户建立对漏洞的全面认识，正确完成弱点修复工作

口令风险

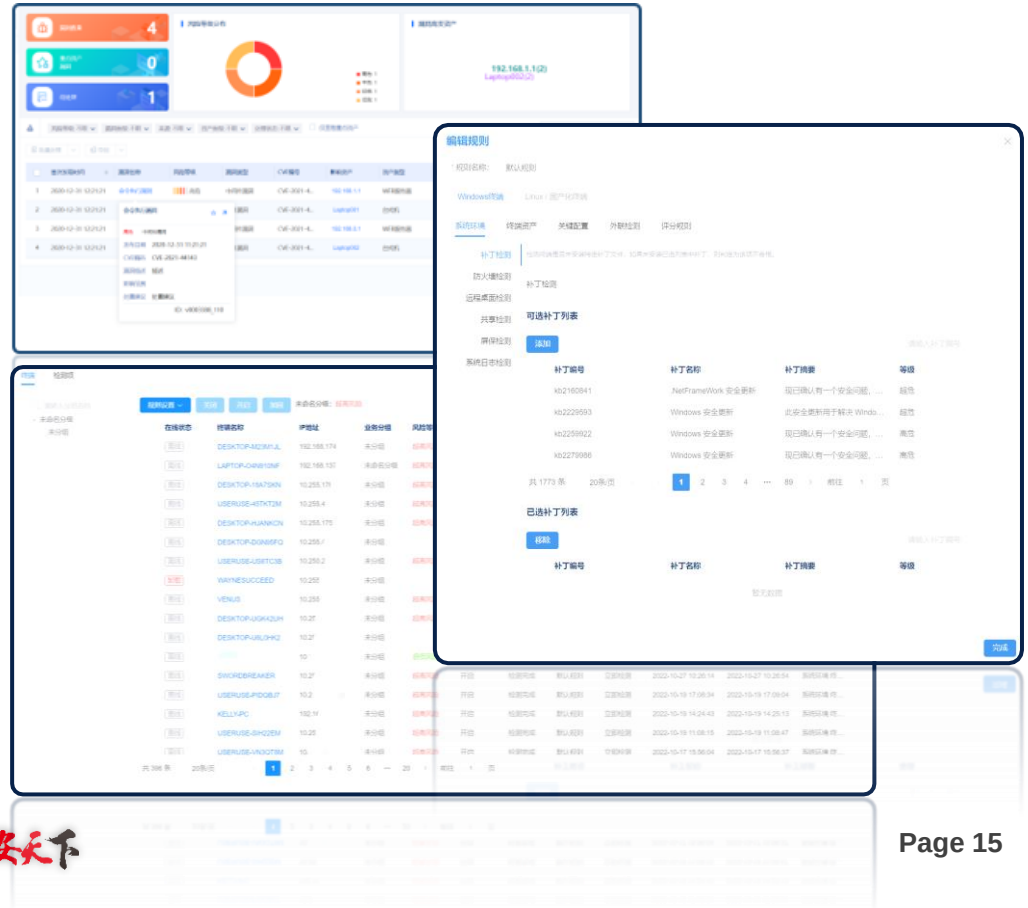
建立弱密码知识库和弱密码检测规则，基于NDR的全要素感知能力和探测模块，实现弱密码检测的能力，对明文和密文的弱密码进行识别

访问风险

通过遥测数据分析资产的互访情况，以便于对访问情况进行控制，通过指定时间窗口可快速对资产通信情况进行溯源

配置风险

能够监控资产的应用配置和策略配置情况，对其中违规配置或异常配置进行处置



04 威胁长期潜伏，需要主动发现

不止是设备警报，更需要异常识别

单一设备和系统对威胁的识别往往是有局限的，而威胁往往会采用绕过防御设施、且长期潜伏的特点，因此需要在更上层的视角识别威胁和异常

通过融合端点、流量、用户行为等数据，面向各类典型安全场景，对行为特征、离群行为、生僻对象以及行为上下文进行检测以识别异常

身份异常场景检测

虚拟专用网（VPN）是近几年网络攻击和攻防演练重点关注的安全点，而大多问题都出现在身份的盗用和滥用

平台提供对账号泄露、账号滥用、暴力破解、业务异常等细分场景的多类检测识别手段

流量威胁及异常场景检测

以流量检测设备基础上提供全局视角的流量检测能力，如分布式扫描、可疑外联、弱口令攻击、漏洞攻击等，强化流量侧识别能力

网站及业务系统场景检测

网站和业务系统的内容安全和数据安全尤为重要，对路径遍历/WEB漏洞攻击/路径穿越等风险检测，且融合WEB扫描设备对网站安全全方位监控

终端场景检测

面向Windows等办公PC环境，基于系统日志的检测分析，对内网穿透、横向渗透等异常违规或安全威胁进行持续监控

服务器场景检测

面向Linux等服务器环境，基于系统日志的威胁和异常检测能力，对异常命令执行和命令注入进行检出

可灵活拓展++++

平台具备良好的可拓展性，可通过在线配置或规则包导入的形式动态拓展新规则

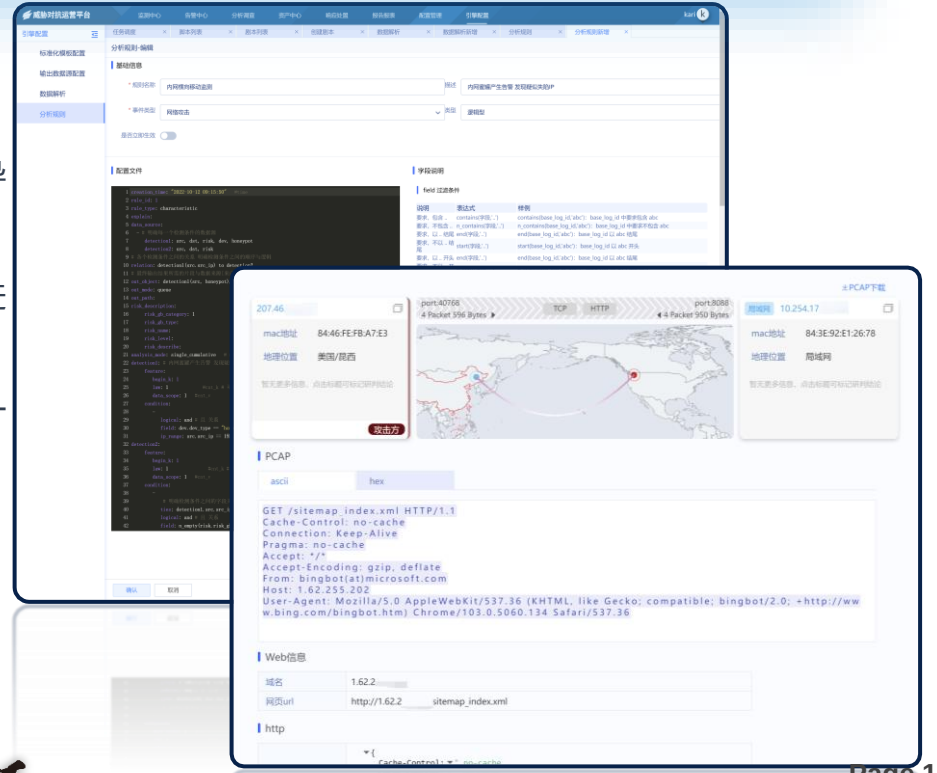
不止是设备警报，更需要异常识别

攻击方在攻击时总会根据防御方的实际情况调整策略，而防守方如果仅采用被动的防守策略，在长期的对抗过程中势必会出现能力差距，因此必须需要能够根据实际环境、遭受威胁情况、威胁趋势、动态拓展和调整策略的分析能力

可动态拓展规则与模型的分析引擎

平台具备良好的可拓展性，可随时通过在线配置或规则包导入的形式动态拓展新规则

得益于对象化基础，在分析配置时可以融合多种数据类型进行检测，无需进行过多复杂配置即可快速开始检测及识别，在大多数情况下也无需重复定义后续业务流程即可进行统一告警和自动化处置

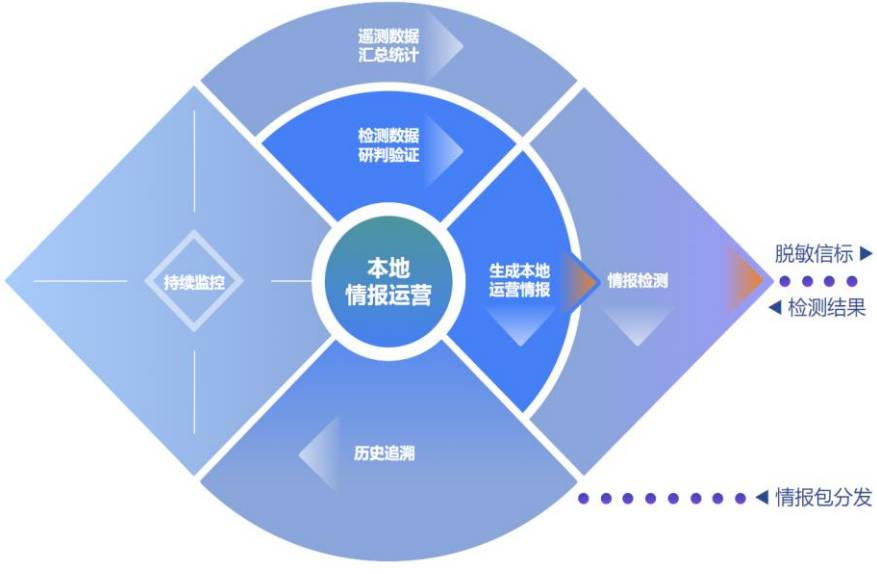


不止是设备警报，更需要异常识别

威胁情报可以有效提高风险识别能力，借助**安天TID情报平台**，可以有效赋能威胁识别和异常发现；

同时在安全运营过程中监测响应的知识经验也是需要固化的，XDR平台能够将其固化形成**本地运营情报**，形成可迭代可演进的威胁识别能力

安天威胁对抗运营平台能够结合**本地运营情报**/**安天威胁情报平台/第三方情报平台**，融合传统威胁情报的**广度和预见性**与运营情报的**强针对性、高命中率、高客户价值**对网内发现的远控终端、网站域名/地址、执行体等风险对象进行持续检测和监控，发现威胁并形成高置信/高风险告警，有效提升网空威胁感知能力



兼容第三方情报

安天情报平台

T.I.Data

支持本地化

05 事件零散分布，需要理清脉络

事件零散分布，需要理清脉络

设备上报的事件和分析模型输出的事件如果仍然零散的分散于多个模块内的话，在多个页面来回的切换显然会占用分析人员大量的时间和记忆成本，难以为分析人员提供快速的洞察，无法有效驱动威胁的监控和响应

通过安天的威胁对抗运营平台，可以有效提取事件中涉及的对象识别其行为，通过决策模型形成统一告警
通过上下文的自动循线调查和多渠道拓线分析，串接威胁活动链路，还原威胁全貌

事件零散分布，需要理清脉络

安天采用了基于对象和作用关系的统一风险描述形式，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

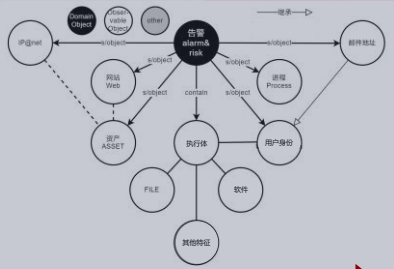
在真实环境下可降低98%以上重复或相似告警

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

流量威胁抽取示意

协议信息
DNS　MAIL　…

环境信息 & 检测信息 & …
Domain　M-Dst　N-Src

文件信息 & 证书信息
Mal　Cert　Mal

告警策略&白名单规则

归类告警

统一告警监控

告警将涉及对象按攻击方、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

得益于对象化的基础平台对各类对象形成了本地知识库和信息卡，记录对象信息、活动情况、涉及资产情况以及风险情况，以便于快速追溯

事件零散分布，需要理清脉络

单一的威胁点不易于理解且缺少上下文，在高威胁对抗的场景下仍然会导致信息过载。因此需要基于对象进行关联，按需调度设备和系统辅助分析和溯源，以便于快速还原事件链路

不止关注单一威胁，更需要关联全局数据

依据事件中涉及对象及其之间的作用关系，关联串接事件链路

端点 定位执行体及其活动链

基于安天EDR的环境引擎可以有效识别进程风险，串接执行体的本地和网络活动链路

执行体 关注生僻/可疑执行体

在全局、业务分组内关联生僻和可疑行为的执行体信息，例如生僻应用、生僻签名等，串接多端，确定影响范围。

流量 串接端与端的通信链路

基于地形通联情况和安天NDR的全要素信息留存，能够有效串接端与端之间的可疑和恶意通信链路

身份&业务 溯源定位/串接行为链

基于统一身份认证和业务系统的身份信息关联串接行为链路

不止关注已知表象，更需要挖掘潜在问题

通过全局的对象知识、结合分析资源调度，拓展线索

执行体鉴定 调度分析资源

沙箱：动态鉴定、静态鉴定…

情报：本地情报、TID威胁情报、第三方情报…

远端主机鉴定 调度分析资源

情报：本地情报、TID威胁情报、第三方情报…

沙箱：动态鉴定…

相同相似属性的对象

- 执行体特征：相同签名、相同编译路径…
- 账号身份特征：相似用户名、相同平台…
- 通信地址特征：相似网络地址、相同运营商…
- 业务特征：相似域名、亲属域名

同时间窗内相似可疑行为

依托于全要素流量信息和系统的遥测数据，对相同时间窗口内的威胁进行关联

- 执行体行为特征：相似命令行……
- 流量特征：相似参数…
- 系统特征：敏感路径操作…

事件零散分布，需要理清脉络

通过多种方式串接事件链的基础上，结合空间和时间维度对事件链路进行切片，通过威胁对象百科和ATT&CK威胁框架为对威胁进行多维度的诠释，形成对系列事件链路的深度洞察

关联全局数据

端点　流量　身份

挖掘潜在问题

执行体　相同相似属性的对象

远端主机鉴定　同时间窗内相似可疑行为

威胁研判定性

向前追溯历史威胁

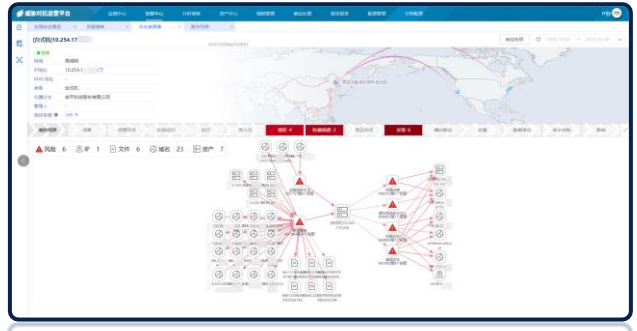
支持根据对象快速检索历史数据，研判后平台会向前自动化追溯历史

固化知识向后监控

固化研判知识为本地情报，平台会向前自动化进行追溯、向后持续监控恶意或可疑对象的活动

自动化下发处置策略

能够自动化地或人工执行处置策略，及时对威胁进行处置



06 设备系统众多，需要统筹策略

设备系统众多，需要统筹策略

策略管理的困境

- 不知道这个终端是做什么的，承载了什么业务，封这个端口会不会把业务宕机
- 3个隔离网、划了10个网络分区，20个墙，发现了攻击终端不知道给谁下策略
- 设备报了漏洞攻击，不知道终端实际有没有漏洞

策略管理必须结合环境和地形

策略管理必须结合网空地形和环境信息，才能有效定位处置策略下发点，高效准确的分析和处置威胁

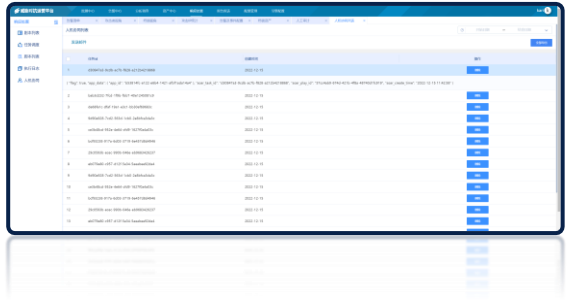
通过安全编排与自动响应模块可有效解决风险治理的抵近问题，结合对环境的识别，能够为用户提供可拓展的自动化威胁分析和响应能力，提高安全运营效率

以地形为基础，对全局安全策略进行管控

确定处置对象

动态生成待处置对象的任务队列

网站域名	执行体(静态)	启动项	向量特征
远端终端	执行体(动态)	资产	服务
业务身份	注册表	签名供应商	……



基于资产及环境的批量策略管理

确定处置策略

基于地形信息自动化确定可用的处置策略

执行体动态分析	网络封堵
执行体静态分析	身份停用
执行体多引擎鉴定	权限限制
执行体情报鉴定	重定向
信标向量情报鉴定	流量限制
环境仿真	业务仿真
执行体全网追溯	执行体定点查杀
隔离执行体等	停止进程
拦截/限制行为	暴露面管控
应用管控	脆弱性管控
隔离终端	……

定位执行单元

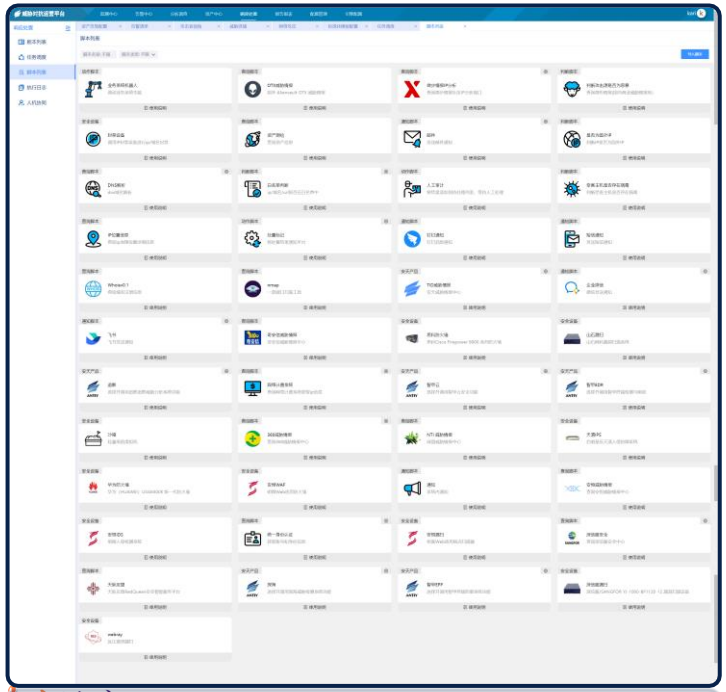
快速定位到可有效执行处置策略的执行单元

网络	流量采集和元数据化单元	应用层边界	链路层边界	业务层边界	通讯层边界
终端	主机侧采集和元数据化单元	执行控制单元	介质管控单元	主机侧防火墙单元	修复与更新单元
	对象处置单元	策略调整单元	主机应用行为管控单元	日志提取单元	
诱捕	场景模拟构建单元	端口和业务仿真单元	情报生产单元		
分析	执行体静态分析单元	执行体动态分析单元	执行体多引擎鉴定单元	信标/向量查询单元	
探测	重载扫描单元	爬取单元	分布式轻载扫描/无损扫描单元		

不止联动下发策略，更需要精细化处置

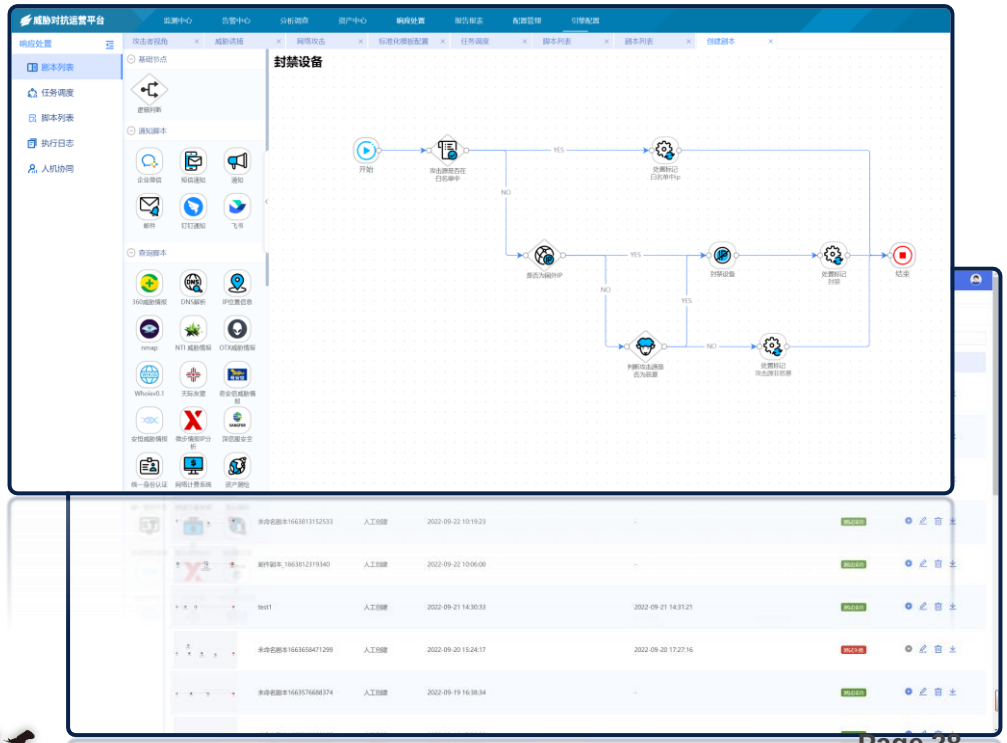
可拓展处置脚本

为了降低用户的使用成本，采用了开箱即用、轻量化参数配置的案例式的脚本设计，覆盖大多数场景，对于无法覆盖的场景，可以自定义编辑导入脚本实现灵活拓展



可自定义的场景化处置剧本

可根据业务场景灵活自定义处置剧本，剧本支持查询、调度、策略下发等能力



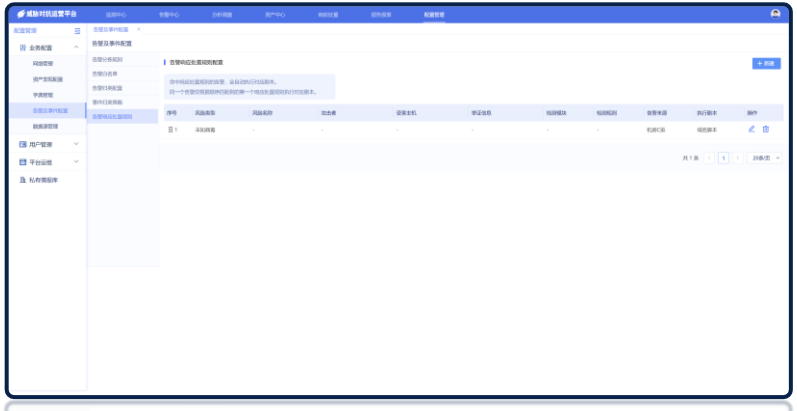
不止联动下发策略，更需要精细化处置

分析研判与响应剧本案例

不止联动下发策略，更需要精细化处置

通过自动化提高运营效率

剧本支持自动化执行、自动生成策略人工审批、手动执行。自动化执行或生成策略时会通过策略为告警自动匹配剧本，以便于自动化处理高置信度的风险，可将威胁的平均响应时间(MTTR)缩短95%以上

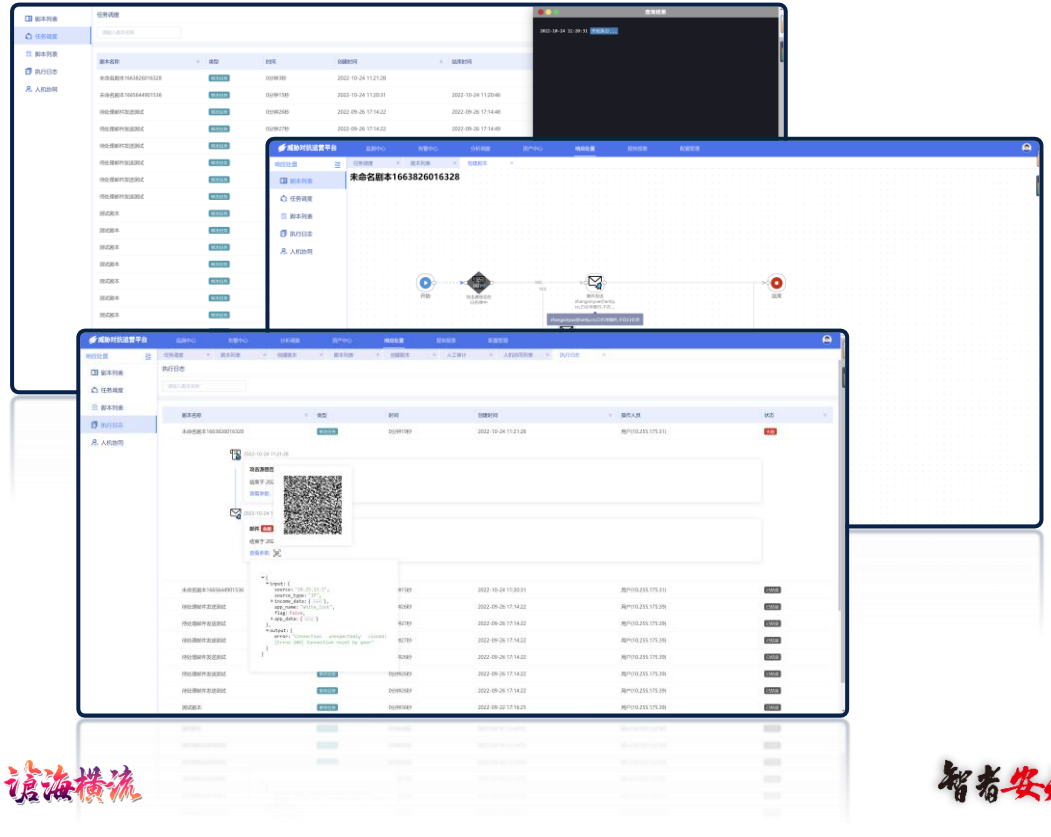


不止联动下发策略，更需要精细化处置

任务执行过程透明可视

剧本执行会形成任务，可以随时查看任务中各脚本执行情况及过程中的参数

执行参数支持生成二维码，以便于隔离环境下远程问题排查



执行结果可跟进验证

支持通过多种方式组合验证策略执行情况

下发成功性验证

通过管理接口查询策略是否下发成功

行为仿真验证

通过模拟行为验证策略是否有效，例如通过发包验证封堵策略是否有效、通过探活验证端口是否成功关闭

存在性验证

通过抵近验证对象实体是否存在，例如通过EDR验证执行体实体是否仍然存在或扩散、通过POC验证漏洞缓解措施是否生效等

结语

安天威胁对抗运营XDR平台以数据和资产的认知为基础

通过跨设备的**风险识别**、**关联调度**、**协同处置**与**策略验证**形成威胁对抗运营闭环

提高威胁对抗和安全运营的自动化水平，为安全治理降本增效

感谢大家的关注

安天冬训营 wtc.antiy.cn