网络空间威胁对抗与防御技术研讨会
暨 第十一届安天网络安全冬训营

面向复杂网络的统一策略管理与自动化安全运营建设

安天通用平台产品中心

执行体治理赋能与大模型辅助

北向守望

01 **运营困境**/ 安全运营一直都在进行，但却收效甚微

02 **环境可见**/ 多层次信息融合与识别，提高网络可见性

03 **强化闭环**/ 聚焦威胁溯源处置闭环，释放人员压力

04 **动态适应**/ 使用XDR/MDR快速开始高效安全运营

01

运营困境

安全运营一直都在进行，但却收效甚微

直面产业问题——为什么安全建设未见成效

SIEM/态势/安管等传统管理平台，无法有效支撑安全运营

- 无法有效统一管理设备与系统
- 运营工作开展效率低下
- 无法达成防御所需的可见性

SIEM/态势/安管等传统管理平台，无法有效支撑安全运营

无法有效统一管理设备与系统

运营工作开展效率低下

无法达成防御所需的可见性

厂商对第三方只提供最小化能力对接，拒绝互相兼容，难以互相整合

徒有其表，面向无效的数据接入

- 声称适配了几千数据源，实际只是接过来放着
- 数据内容也没做转换，不同设备各说各的
- ……

各有心思，只提供最小转化

- 部分厂商的产品对第三方不提供完整数据
- 部分厂商的产品对第三方不提供明确格式
- ……

只玩封闭生态，拒绝互相兼容，缺乏灵活性

- 平台实际上只能集成自家产品,第三方依赖代码级定制
- 部分厂商的产品只对自家平台开放全量管理接口
- ……

呈现为主，忽略运营支撑

- 仪表盘地图炮做了很多种,但在运营效率上却少有增益
- 分析与处置要么流于形式,要么需要人持续或线下介入
- ……

SIEM/态势/安管等传统管理平台，无法有效支撑安全运营

无法有效统一管理设备与系统

厂商对第三方只提供最小化能力对接，
拒绝互相兼容，难以互相整合

运营工作开展效率低下

无法达成防御所需的可见性

运营过程处处离不开人， 占用运营人员大量精力且效率低下

信息归并差，导致事件淹没

- 设备逐渐增多数据量指数增加，信息归并却没自适应
- 缺乏归类，没有主次，无法使管理人员聚焦关键问题
- ……

以满足指标为目标建设,导致可用性差

- 检测分析能力几十种，实际上拆为了几十个页面
- 本应连续的业务流，被“解释”为离散的功能点
- ……

数据混乱存放，溯源工作开展困难

- 平台破碎零散的数据无法使用，仍要登陆产品去验证
- 关联分析流于形式，仅能单点链路还原
- ……

依靠人工开展运营，时效难以保证

- 事无巨细均需要人工参与和决策
- 应急响应/演练等场景对时效和溯源要求极高
- ……

SIEM/态势/安管等传统管理平台，无法有效支撑安全运营

无法有效统一管理设备与系统

厂商对第三方只提供最小化能力对接，
拒绝互相兼容，难以互相整合

运营工作开展效率低下

运营过程处处离不开人，
占用运营人员大量精力且效率低下

无法达成防御所需的可见性

网络环境不清不楚，要么不敢下策略，要么出问题时两眼一摸黑

网内资产盘不清，不知道有多少实际在用资产

- 不清楚有多少资产活跃在网内，不了解资产
- 不清楚资产由谁用，归谁管，是否符合安全策略
- ……

资产状况陈旧,不知道会不会遭受攻击

- 不清楚网络内有多少暴露的服务和应用
- 不清楚有多少漏洞，出现0DAY时更不知道如何排查
- ……

网络环境多变，不了解资产人员业务的关系

- 不清楚资产承载什么业务，攻击涉及的人员身份
- 发生威胁时不知道影响有多大
- ……

应急响应时，不清楚往哪里下策略

- 不清楚安全设备监控域，出问题时只能一刀切
- 不清楚策略怎么下，最后处置手段只有“拔网线”
- ……

高效开展运营需要建设敏捷平台

无法有效统一管理设备与系统

厂商对第三方只提供最小化能力对接，
拒绝互相兼容，难以互相整合

运营工作开展效率低下

运营过程处处离不开人，
占用运营人员大量精力且效率低下

无法达成防御所需的可见性

网络环境不清不楚，要么不敢下策略，
要么出问题时两眼一摸黑

需要在既有安全建设基础之上面向威胁对抗

叠加建设一个高效敏捷的安全运营平台

形成“管理+运营”双中心的模式

集成和盘活现有安全资源

在大规模运营基础上结合并盘
活现有的设备与系统，将他们
调度起来

加快闭环速度

增强分析与处置能力
提高自动化水平
降低人员要求和依赖

提高网络可见性

对网络环境进行全面持续监控
对不同体量不同结构不同信息化业
务场景的网络环境动态适配

02

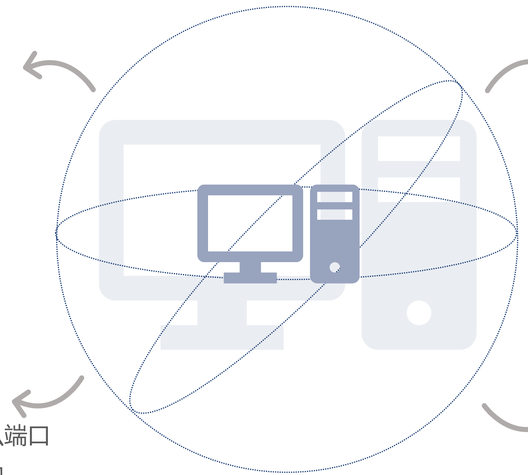
环境可见

多层次信息融合识别，提高网络可见性

环境可见性差，难以进行策略管理

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
- ……



资产现在状态如何

- 有多少资产在用
- 有没有关键设备挂掉

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
- 网内有没有新曝光的0DAY漏洞

资产会不会遭受攻击

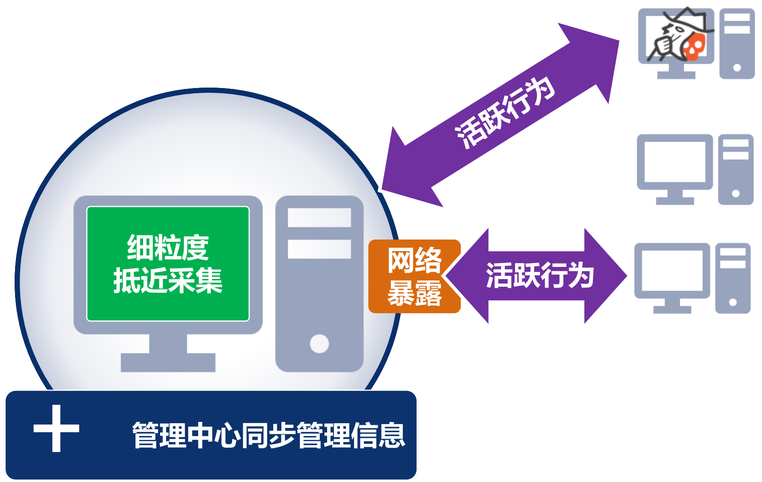
- 资产有哪些漏洞
- 配置有没有问题
- 设备和服务有没有弱口令

可见性是支撑安全运营和信息化管理的基础

有效开展安全运营首先需要明确防护目标，

结合其所处网空地形和环境信息，才能有效定位处置策略下发点

全面的资产信息采集，是构建可见性的基础



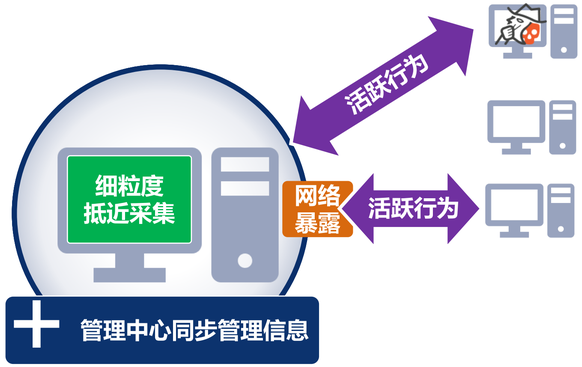
资产在不同环境可用监控方式不一

孤岛设备　生产设备　业务系统　...

外来设备　违规接入设备　人员/身份

需要运用多种手段全面、快速、准确的发现网络中的资产及其环境信息

全面的资产信息采集，需要不影响业务的无感识别发现活跃行为

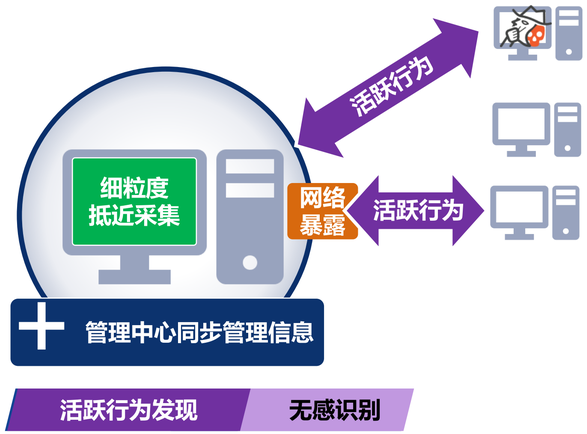


活跃行为发现 **无感识别**

面向未部署AGENT或无法部署AGENT的场景，提高对活跃节点的监测覆盖面

基于NDR等流量信源，在不影响业务的情况下无感识别，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**

全面的资产信息采集，需要主动探测暴露面

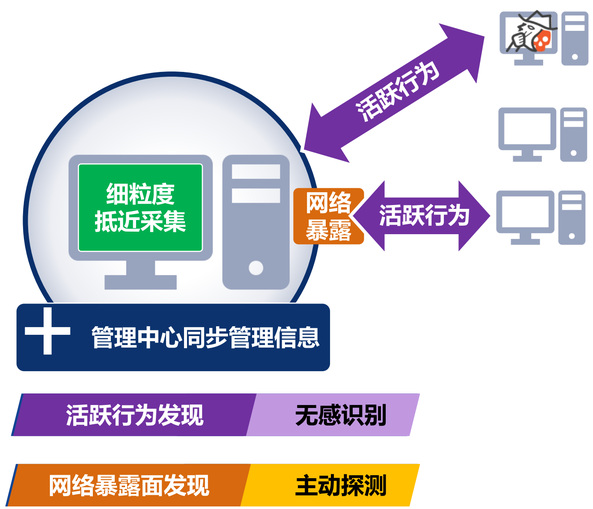


网络暴露面发现　主动探测

面向未部署AGENT或无法部署AGENT的场景，提高对暴露节点的监测覆盖面

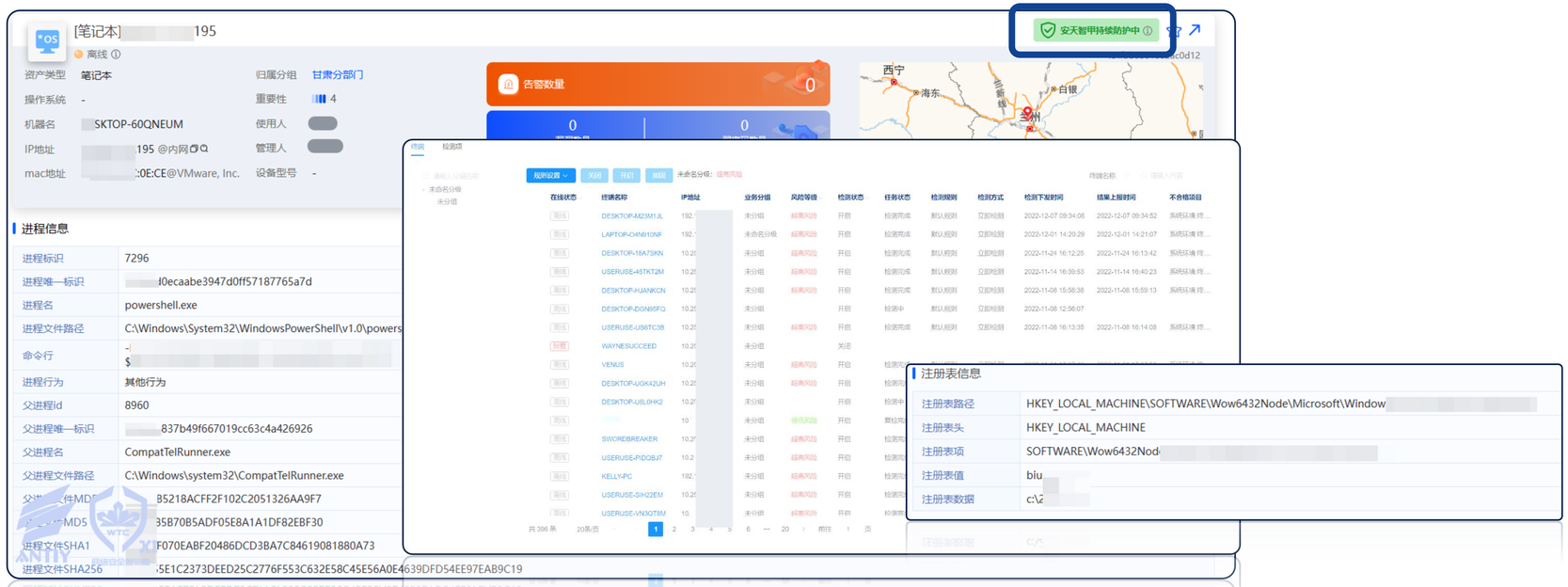
通过探测模块或协同扫描设备，更全面识别资产上运行的操作系统、中间件、应用软件、开放端口和服务等对象

全面的资产信息采集，需要抵近终端细粒度采集管控

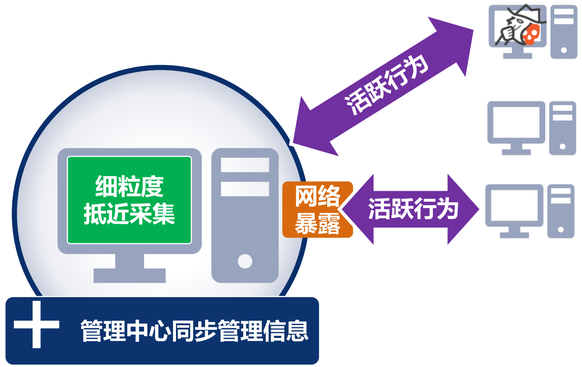


全面细粒度管控 **递近终端**

通过EDR/AGENT上报的终端资产信息同步用户资产，相较于活跃行为和网络暴露，可以全面的获取活跃和非活跃的全量执行体信息、软硬件、以及服务、注册表、启动项等配置信息



全面的资产信息采集，需要结合业务信息



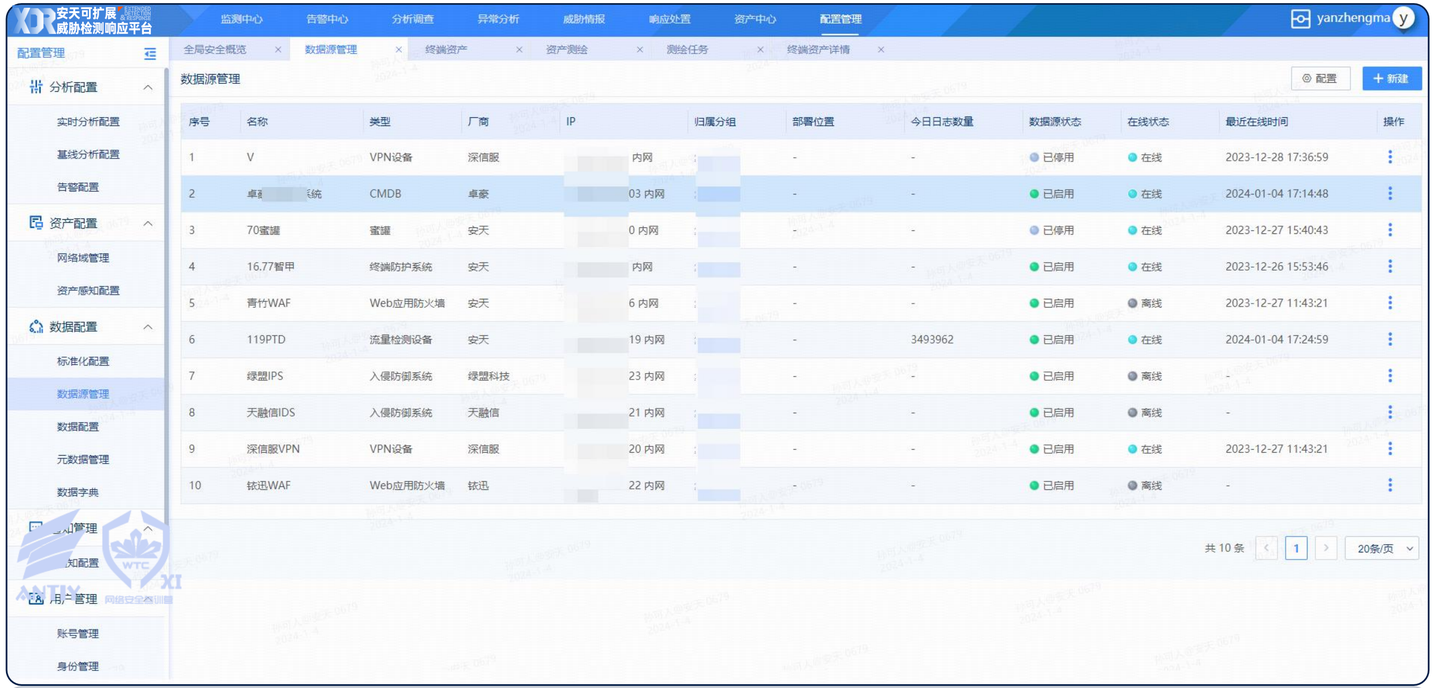
活跃行为发现　无感识别

网络暴露面发现　主动探测

全面细粒度管控　递近终端

业务管理信息　**主动同步**

通过SNMP、网管(CMDB)等设备或系统进行同步，获取资产的业务管理信息，动态构建资产拓扑关系



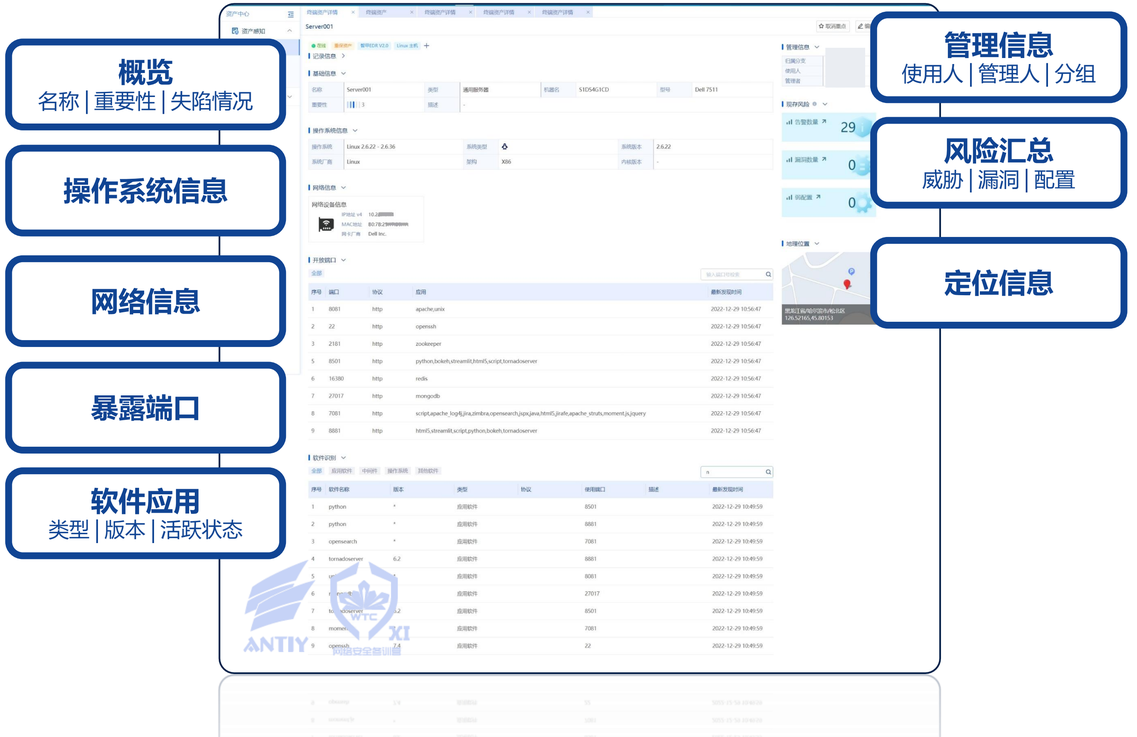
融合与识别资产信息，构建资产画像

在不同维度识别网空对象

- 活跃行为发现 | 无感识别
- 网络暴露面发现 | 主动探测
- 全面细粒度管控 | 递近终端
- 业务管理信息 | 主动同步

融合环境与地形信息

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



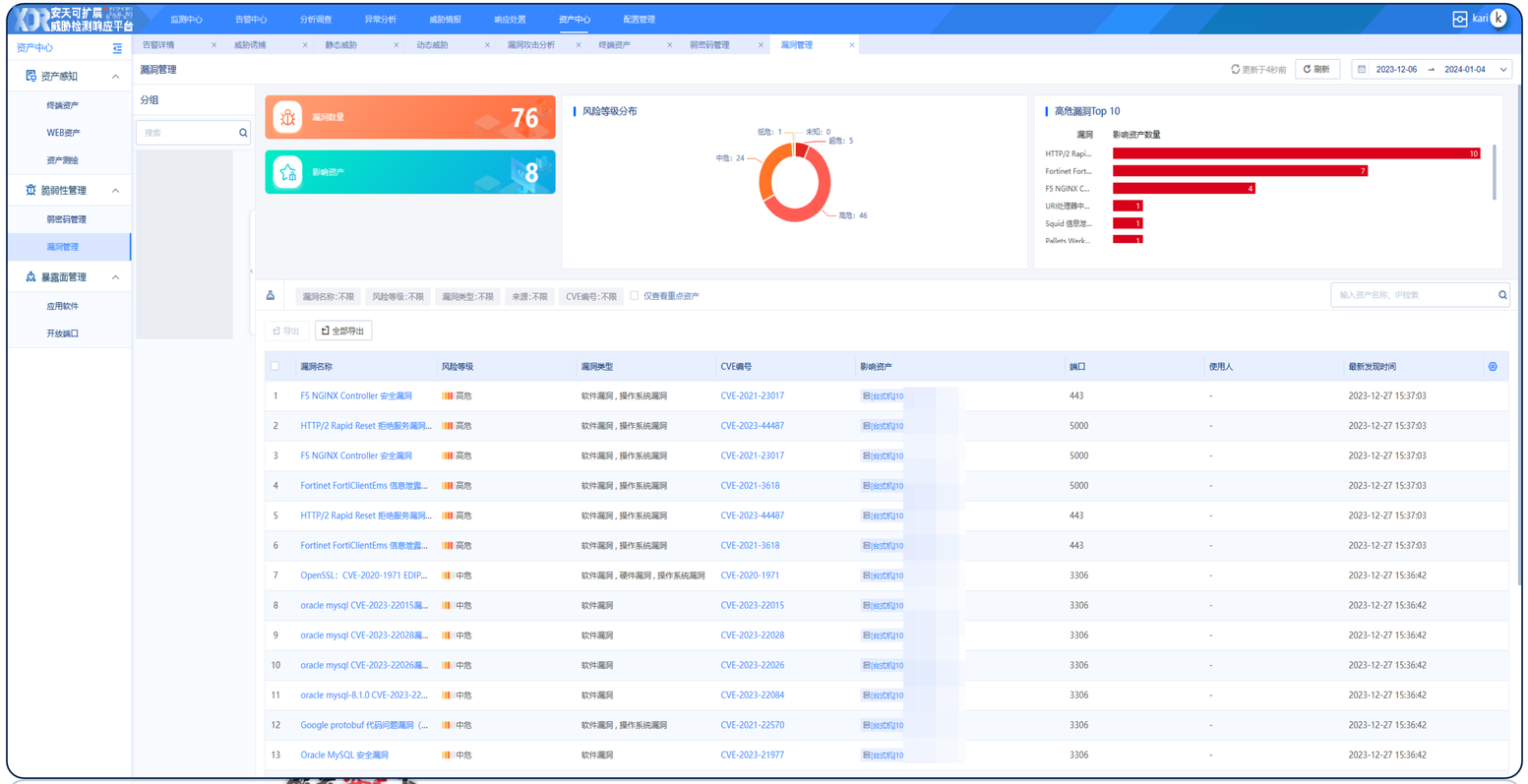
通过暴露面和脆弱性检测，进一步强化资产的可见性

在识别网空对象的基础上，需要进一步确认每类对象存在的脆弱点和暴露风险

漏洞风险识别 业务/身份层、终端/系统层、应用/执行体层

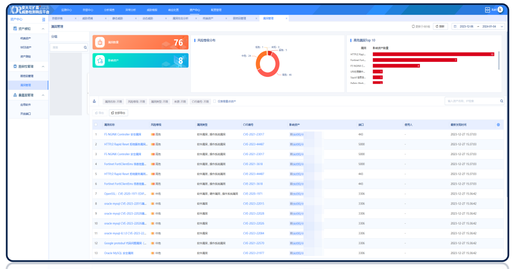
在融合漏扫和EDR等多来源数据的基础上，**平台基于漏洞关联库通过对应用软件、中间件、和硬件信息的关联，强化漏洞识别能力**

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。如加固建议、补丁下载参考链接等，帮助用户建立对漏洞的全面认识，正确完成弱点修复工作



通过暴露面和脆弱性检测，进一步强化资产的可见性

在识别网空对象的基础上，需要进一步确认每类对象存在的脆弱点和暴露风险



漏洞风险识别 业务/身份层、终端/系统层、应用/执行体层

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通过对应用软件、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。如加固建议、补丁下载参考链接等，帮助用户建立对漏洞的全面认识，正确完成弱点修复工作

配置风险识别 终端/系统层

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

通过暴露面和脆弱性检测，进一步强化资产的可见性

在识别网空对象的基础上，需要进一步确认每类对象存在的脆弱点和暴露风险

漏洞风险识别 业务/身份层、终端/系统层、应用/执行体层

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通过对应用软件、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。如加固建议、补丁下载参考链接等，帮助用户建立对漏洞的全面认识，正确完成弱点修复工作

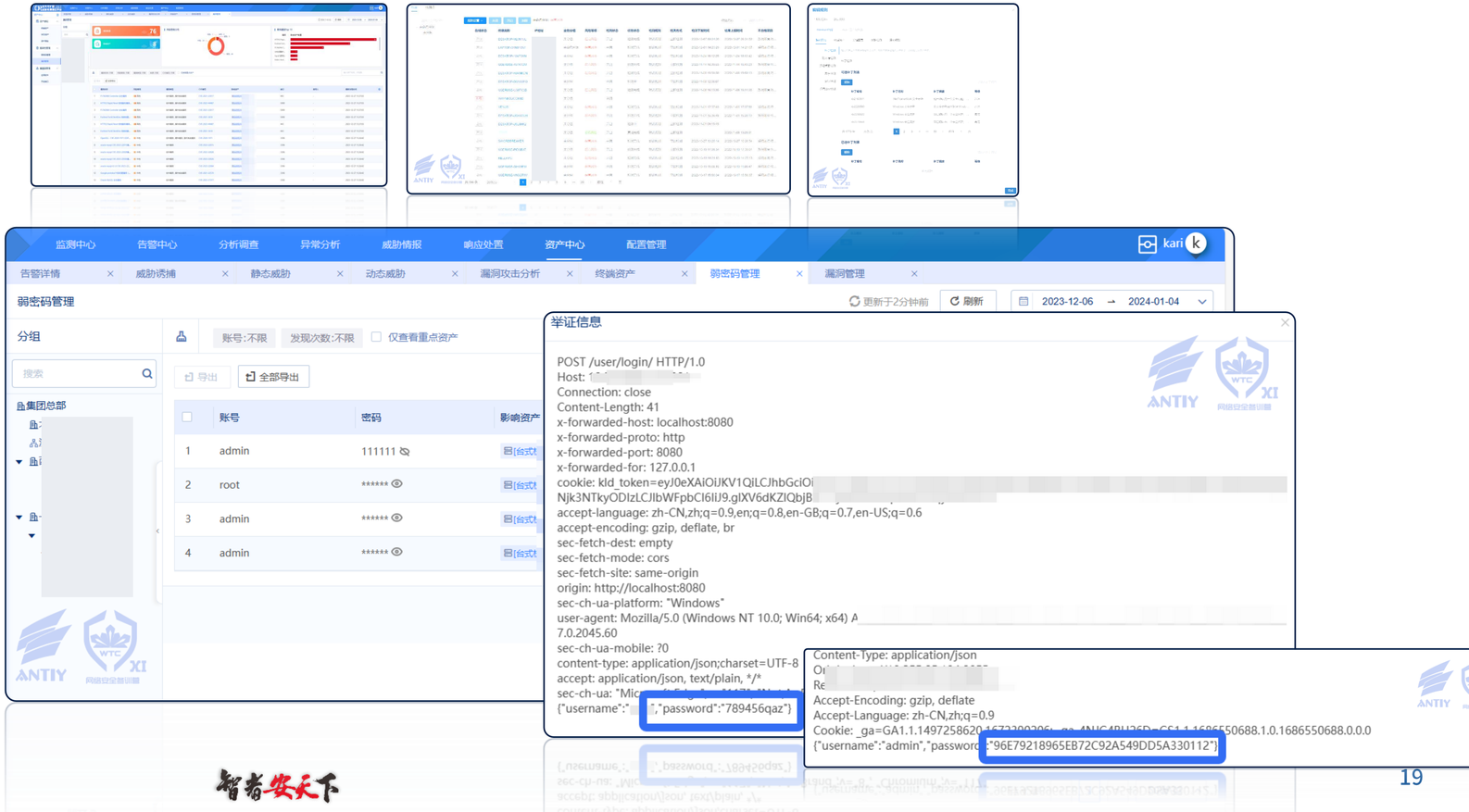
配置风险识别 终端/系统层

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

口令风险识别 业务/身份层、终端/系统层

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，

实现弱密码检测的能力，实现对明文和密文的弱密码进行识别



通过暴露面和脆弱性检测，进一步强化资产的可见性

在识别网空对象的基础上，需要进一步确认每类对象存在的脆弱点和暴露风险

漏洞风险识别 **业务/身份层、终端/系统层、应用/执行体层**

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通过对应用软件、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。如加固建议、补丁下载参考链接等，帮助用户建立对漏洞的全面认识，正确完成弱点修复工作

配置风险识别 **终端/系统层**

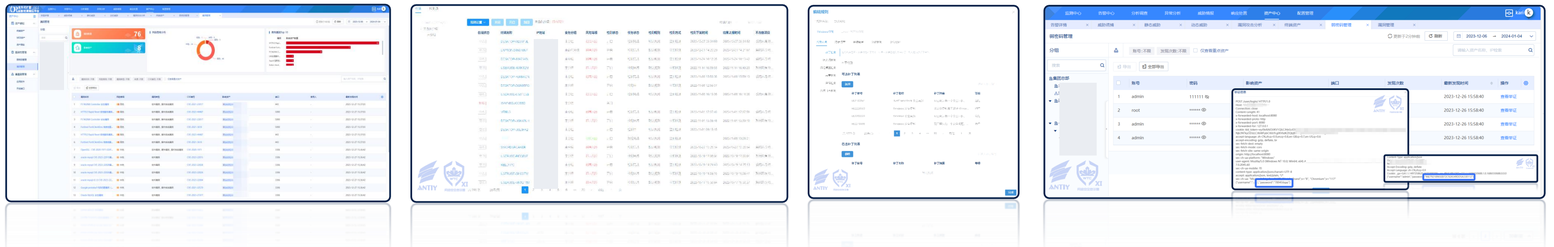
监控资产的应用配置和策略配置情况， 对其中违规配置或异常配置进行处置

口令风险识别 **业务/身份层、终端/系统层**

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，实现弱密码检测的能力，实现对明文和密文的弱密码进行识别

暴露面识别 **业务/身份层、终端/系统层**

在状态方面监控活跃的服务；在行为方面监控通信和互访情况，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



暴露在网络中的应用软件 / 中间件 / 编程语言

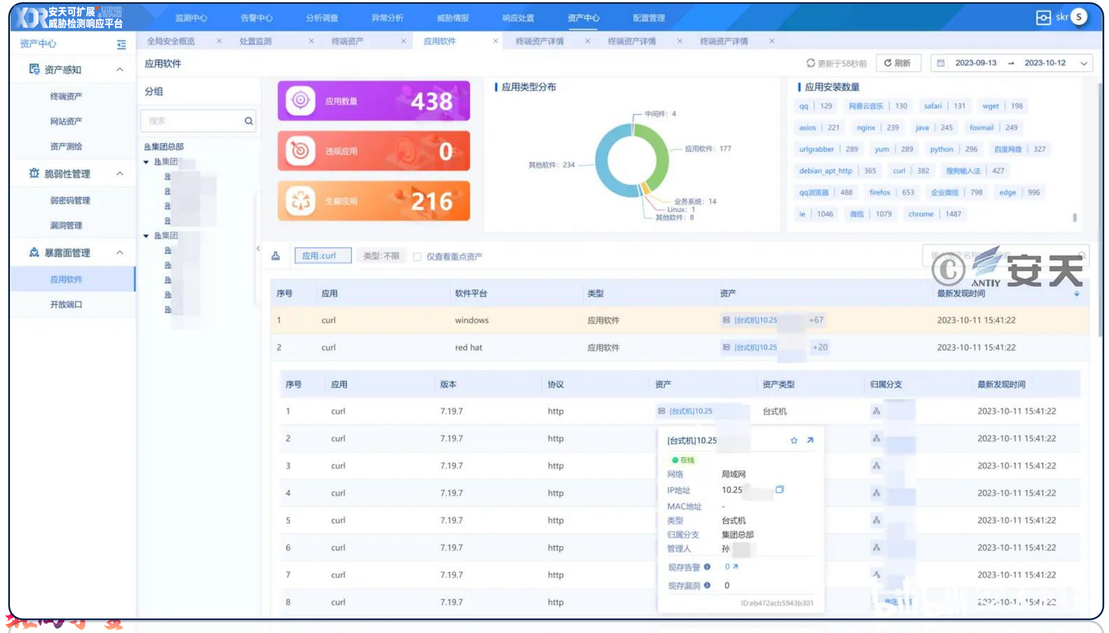
暴露在网络中的端口和服务

通过构建资产可见性，高效且准确的支撑对潜在和违规风险的筛查

快速排查新兴漏洞

CURL-0DAY漏洞影响范围排查

在CURL 0DAY漏洞爆出时可以立即排查网内使用CURL的终端快速确定影响范围，针对暴露资产、重点资产可明显快速标定



发现违规执行体部署

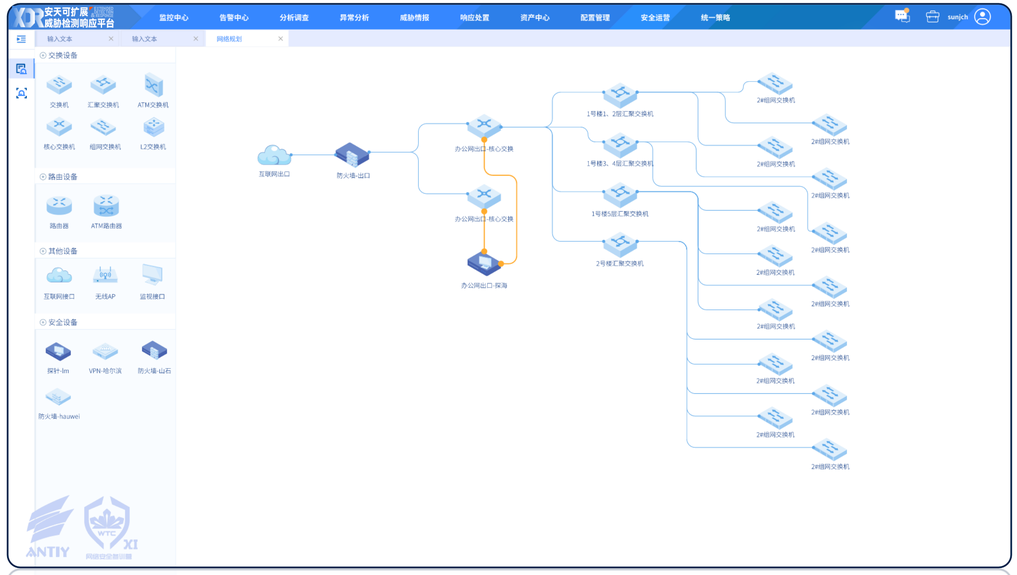
自动发现活跃远控程序 隔离网场景

发现违规开放服务 业务网场景

构建拓扑关系以保障策略的有效性

逻辑拓扑

自动化构建逻辑拓扑为主，以管理员手动调整和绘制为辅，基于拓扑对网络节点进行监控



设备监控域

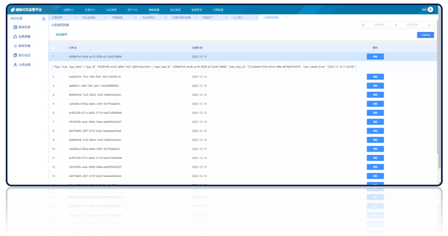
针对每个设备节点可以基于数据识别或手动设置其监控域，保证处置策略的有效下达

基于地形自动关联策略降低心智负担、为高效运营提供基础能力支撑

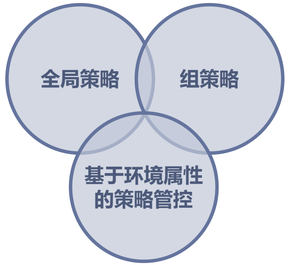
确定处置对象

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及其逻辑编排

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	……

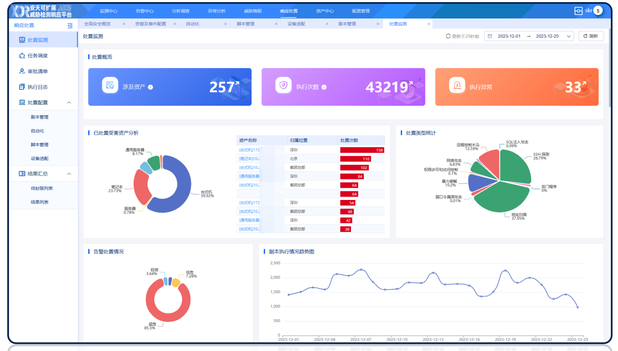
定位执行单元

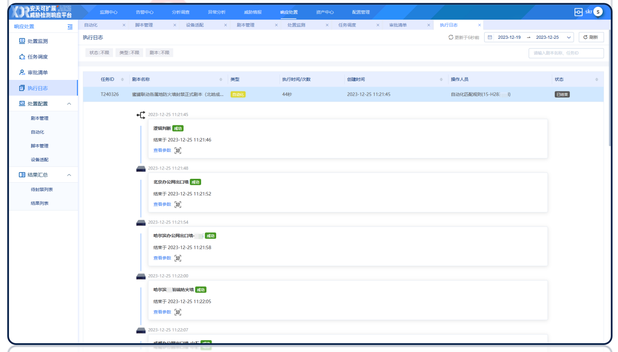
快速定位到可有效执行处置策略的执行单元

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		

执行过程持续监控

通过仪表盘和任务调度持续监控和管理策略



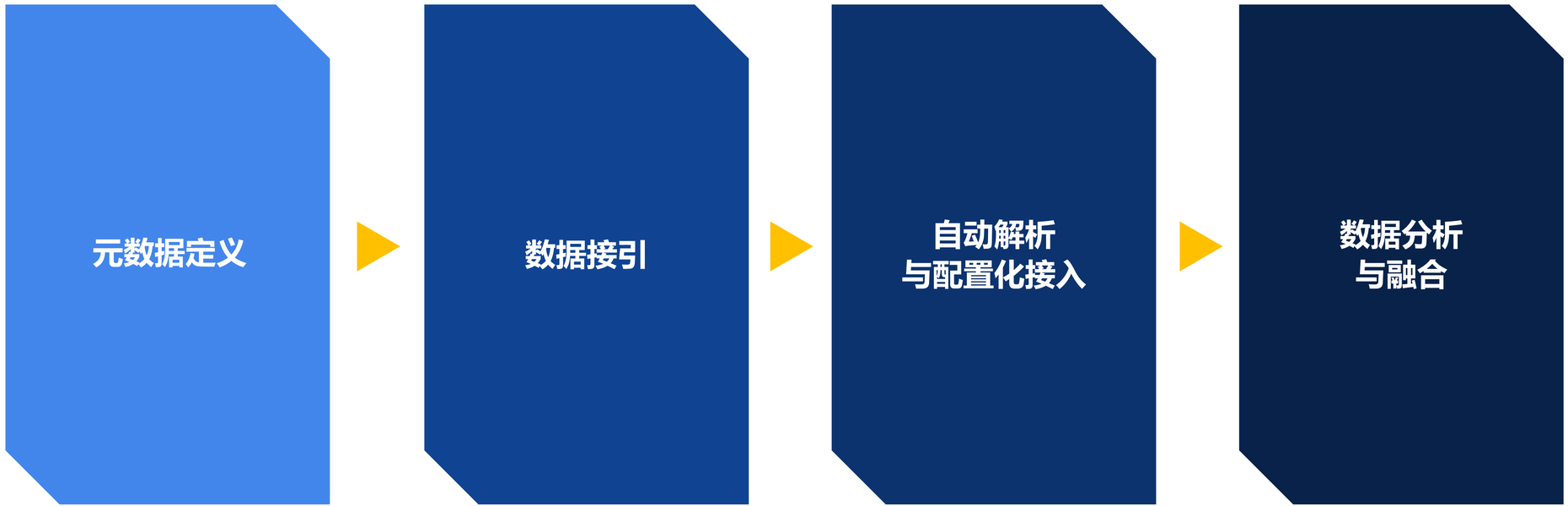


03

强化闭环

聚焦威胁溯源处置闭环，释放人员压力

面向闭环运营，多信源的复杂度需要规范和统一

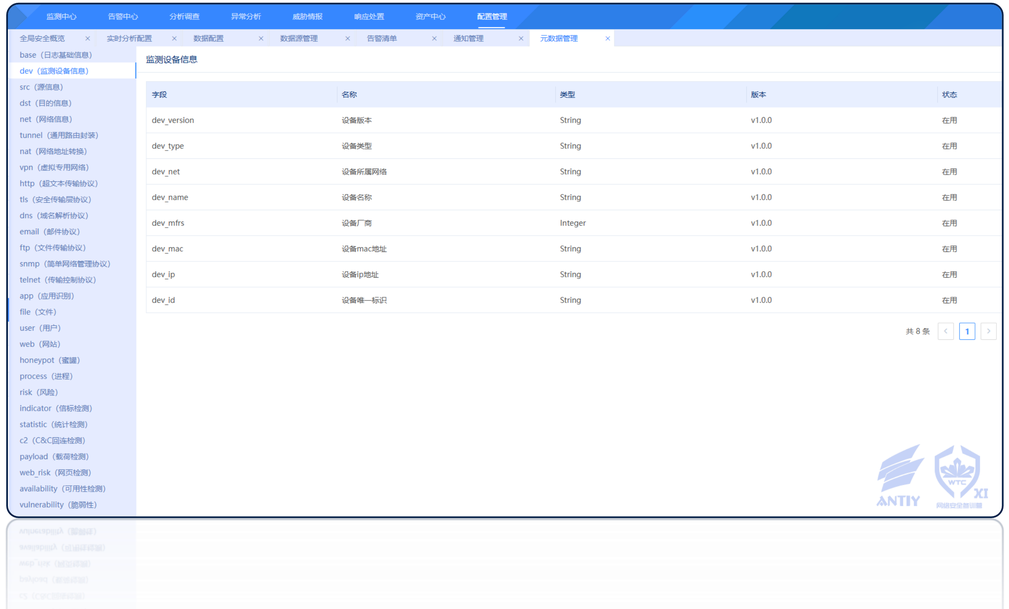


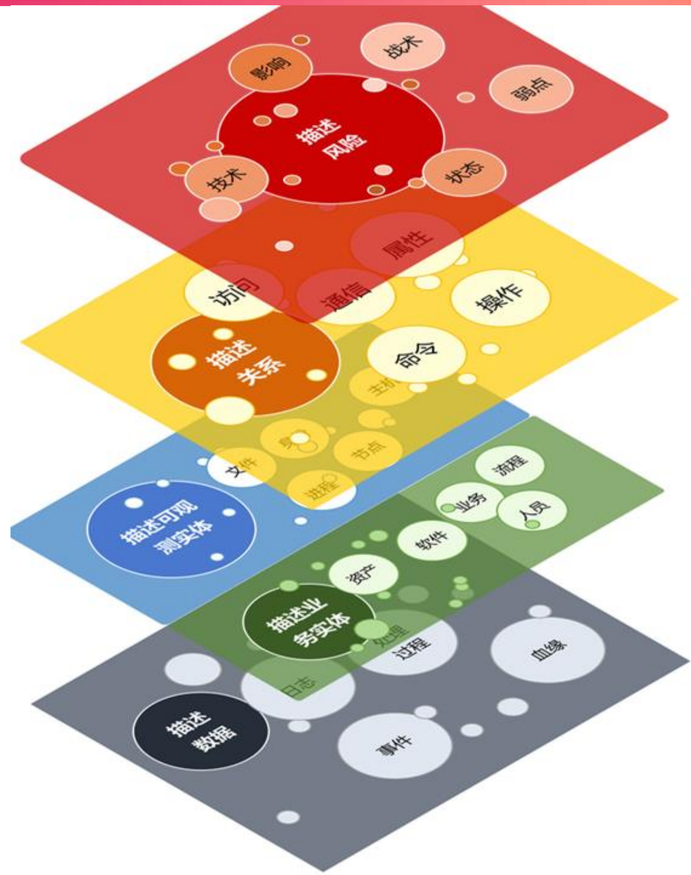
基于数据原理分层的元数据定义，为数据赋予含义

元数据定义 **基于数据原理分层**

对各类遥测数据进行统一汇总和分析需要对数据进行充分的理解，需要形成可机读的数据定义

在实践中，基于数据原理，对各类数据进行抽象，形成了分层的对象定义模式，在数据、实体、关系、风险几个层面定义不同的数据对象，每类对象自身声明其数据的定义，也可以通过声明衍生的子对象实现在更细分场景下的应用





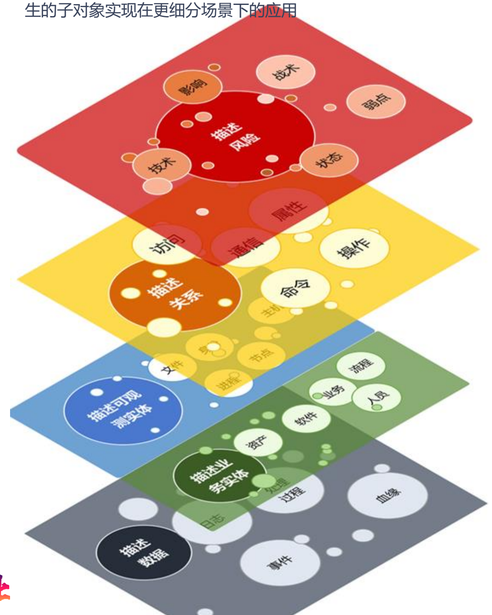
网络内各种复杂环境的数据都需要接引

元数据定义

基于数据原理分层

对各类遥测数据进行统一汇总和分析需要对数据进行充分的理解，需要形成可机读的数据定义

在实践中，基于数据原理，对各类数据进行抽象，形成了分层的对象定义模式，在数据、实体、关系、风险几个层面定义不同的数据对象，每类对象自身声明其数据的定义，也可以通过声明衍生的子对象实现在更细分场景下的应用



数据接引

应接尽接

在安全治理中，数据接引的覆盖面要足够广，才能有效的对全网进行监控，受限于带宽和算力，很多场景下也需要针对性的对大范围覆盖面按需遥测采集或进行部分分析能力的下沉

- 被动采集
- 主动采集
- 外置采集器
  推模式/拉模式
- 数据同步

\+

前置
预处理

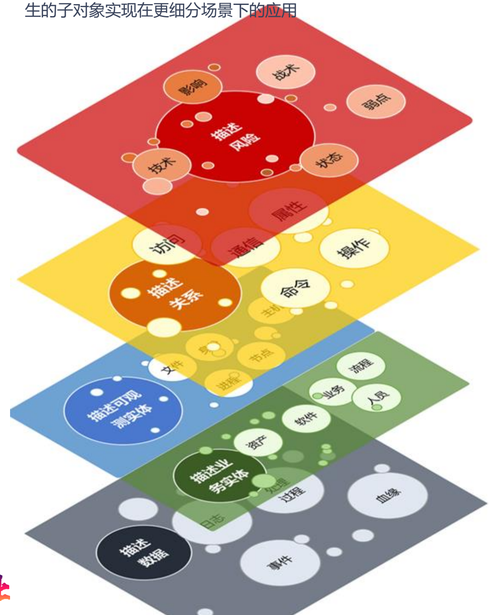
杂乱的数据需要规范和自适应

元数据定义

基于数据原理分层

对各类遥测数据进行统一汇总和分析需要对数据进行充分的理解，需要形成可机读的数据定义

在实践中，基于数据原理，对各类数据进行抽象，形成了分层的对象定义模式，在数据、实体、关系、风险几个层面定义不同的数据对象，每类对象自身声明其数据的定义，也可以通过声明衍生的子对象实现在更细分场景下的应用



数据接引

应接尽接

在安全治理中，数据接引的覆盖面要足够广，才能有效的对全网进行监控，受限于带宽和算力，很多场景下也需要针对性的对大范围覆盖面按需遥测采集或进行部分分析能力的下沉

被动采集

主动采集

外置采集器
推模式/拉模式

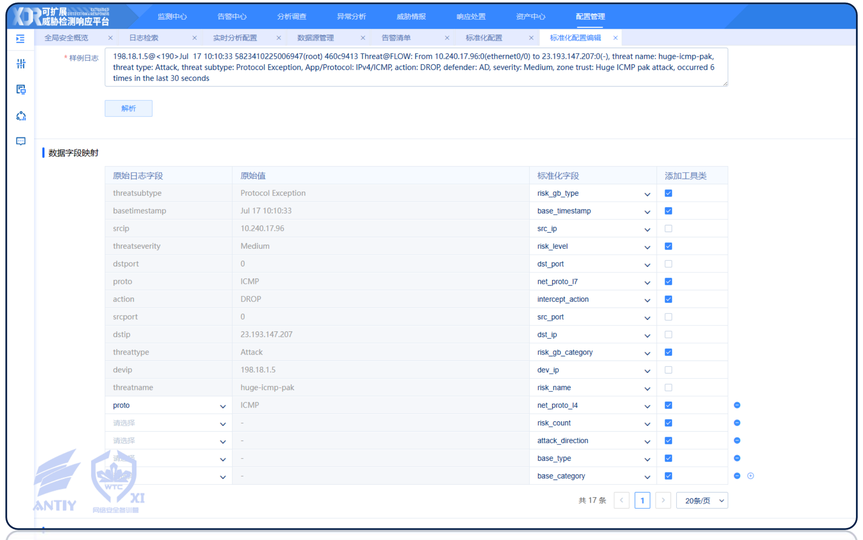
+ 前置预处理

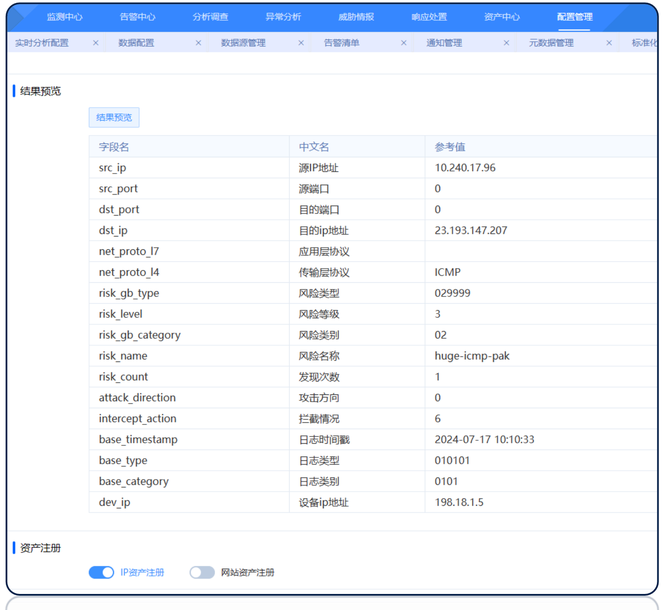
数据同步

自动解析与配置化接入

广度适配

信源的广度势必会使数据格式和数据内容的混乱度加大，这在后续安全治理中会带来指数级的复杂度上升，需要对数据进行规范





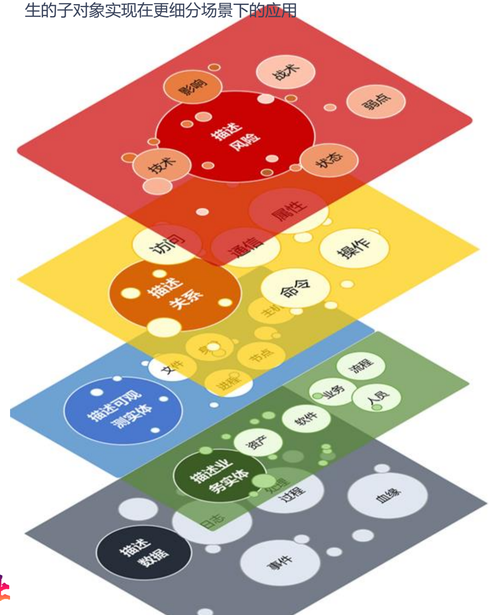
不局限于设备警报，需要进一步的进行数据分析和丰富

元数据定义

基于数据原理分层

对各类遥测数据进行统一汇总和分析需要对数据进行充分的理解，需要形成可机读的数据定义

在实践中，基于数据原理，对各类数据进行抽象，形成了分层的对象定义模式，在数据、实体、关系、风险几个层面定义不同的数据对象，每类对象自身声明其数据的定义，也可以通过声明衍生的子对象实现在更细分场景下的应用



数据接引

应接尽接

在安全治理中，数据接引的覆盖面要足够广，才能有效的对全网进行监控，受限于带宽和算力，很多场景下也需要针对性的对大范围覆盖面按需遥测采集或进行部分分析能力的下沉

被动采集

主动采集

外置采集器
推模式/拉模式

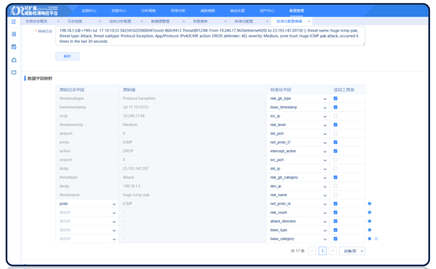
数据同步

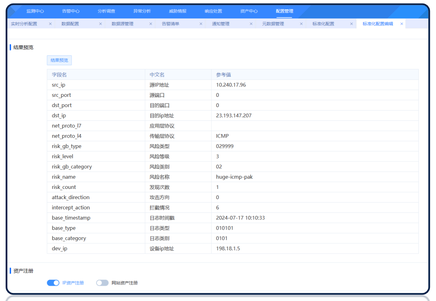
\+ 前置预处理

自动解析与配置化接入

广度适配

而信源的广度势必会使数据格式和数据内容的混乱度加大，这在后续安全治理中会带来指数级的复杂度上升，需要对数据进行规范





数据分析与融合

统一度量衡

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

业务分析与丰富	环境信息	管理属性	影响情况	……
情报分析与丰富	实体	关系	行为	……
专家知识库分析	风险分类	技战术识别	置信度评估	……

智者安天下

主动识别威胁-分层检测与关联分析

主动检测和分析威胁

单一设备和系统仅能针对所在范围内的威胁行为或主体进行识别，由于网内不同区域信息化业务各异，通用的识别方式往往是有局限的，规则严格了很难检出率就很低，规则宽松了误报率又居高不下，而高级威胁往往会采用绕过防御设施、伪装行为且长期潜伏的特点，很难通过设备直接发现

因此需要在设备基础上形成更上层的视角，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，差异化的识别威胁和异常点

身份异常场景

近几年网络攻击和攻防演练重点关注的安全点之一就是身份的盗用和滥用

针对身份安全方面，以统一身份认证、OA、业务系统日志为基础

形成了对账号泄露、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

需要以流量检测设备基础上形成全局视角的流量检测能力，强化流量侧识别能力

叠加业务场景和环境信息，使攻击的分析更加有效

网站及业务系统场景

网站和业务系统往往承载了管理或生产的业务信息，因此其内容安全、数据安全、可用性等均尤为重要

在实践中，通过平台内置的扫描器进行了网站的系列监控，协同扫描设备和网络侧告警综合评估网站的风险和影响

终端场景

面向办公PC环境，问题主要聚焦在违规行为和恶意软件相关风险

需要根据业务分区进行差异化分级管控

例如对于关键业务分区，基于进程及相关日志的检测分析，对内网穿透、横向渗透、文件外发等异常违规或安全威胁等场景进行持续监控

服务器场景

面向服务器环境，根据不同业务用途划定不同分区，基于分区进行差异化的监控和检测

例如针对运维场景的违规外联、异常命令执行等风险持续监控

灵活拓展++++

攻击方往往会根据防御情况动态调整策略，防守方如果仅采用静态防守策略，在长期对抗中势必会出现安全能力差距

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

主动识别威胁-分层检测与关联分析

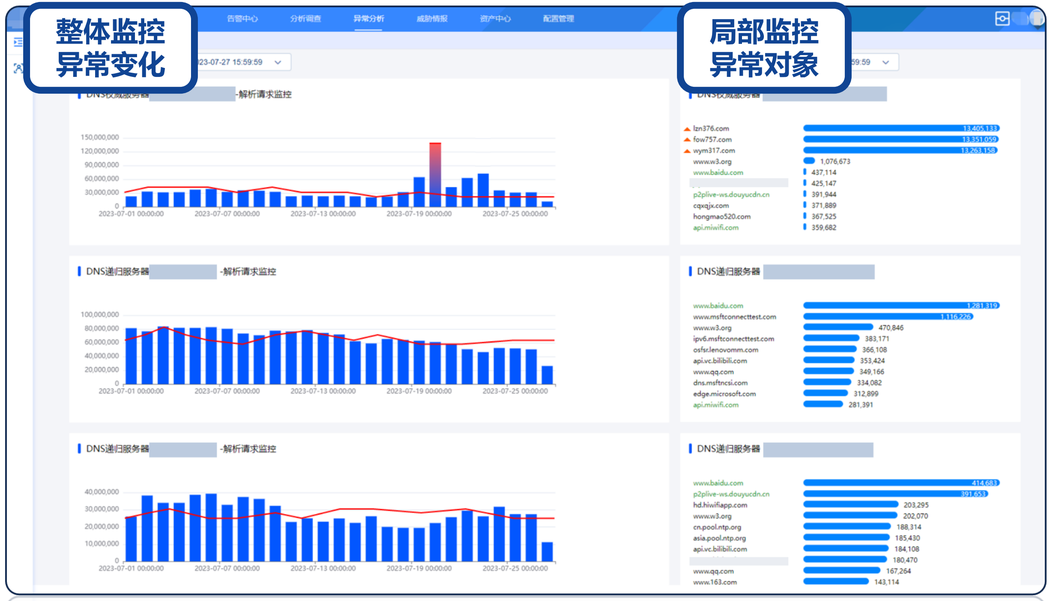
主动识别威胁网内威胁

拒绝服务攻击

2023年7月 多家高校DNS服务器遭受来自互联网的拒绝服务攻击，威胁分析引擎自动发现和预警威胁， 安天MDR/MSS团队监测的第一时间协同封禁设备进行自动化处理，保障校园网的正常使用

整体监控
异常变化

局部监控
异常对象



高风险对象
自动告警

受害主机
业务用途

海量数据
自动聚类

一键下发
策略

自动关联
历史告警

自动溯源

情报与知识
关联鉴定

分层检测与关联分析——主动识别威胁

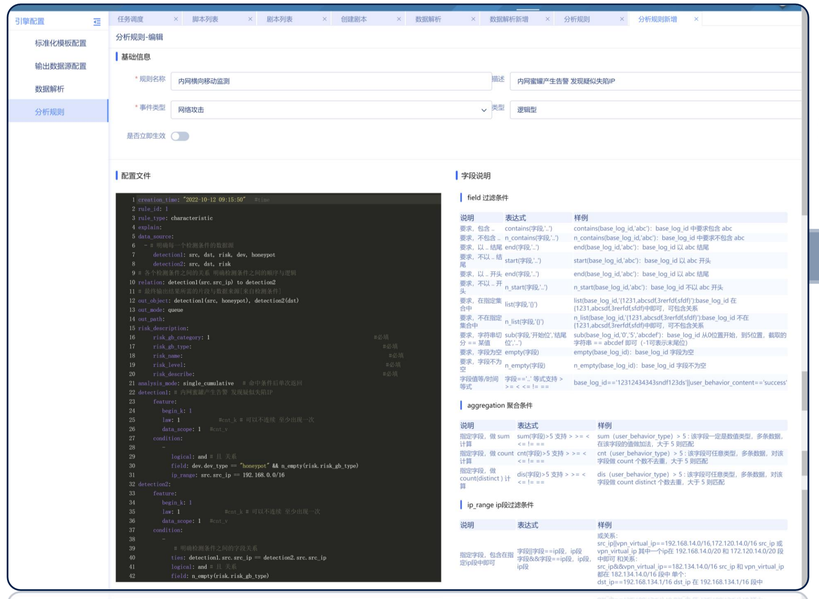
动态对抗威胁

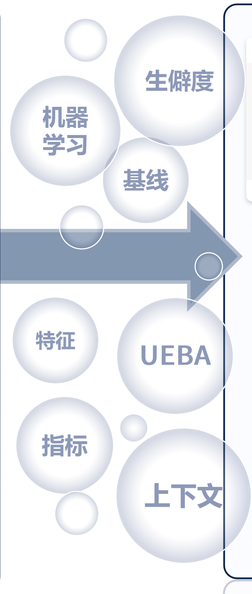
攻击者会根据防御情况动态调整策略，敌暗我明，防守方如果仅采用静态防守策略，在长期对抗运营循环中势必会出现安全能力差距

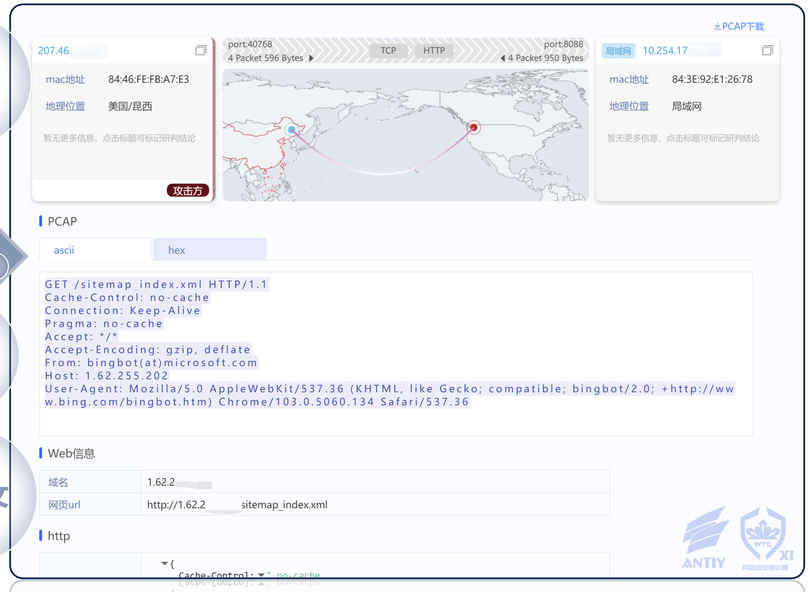
因此必须需要能够根据实际环境、遭受威胁情况、威胁趋势、动态拓展和调整策略的分析能力

动态拓展规则与模型

面向动态的威胁，得益于对象化基础，在实战过程中逐步形成了可动态拓展的分析引擎，能够实时和离线的对数据进行检测，通过表单或高级模式(YAML)便捷的编写规则。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





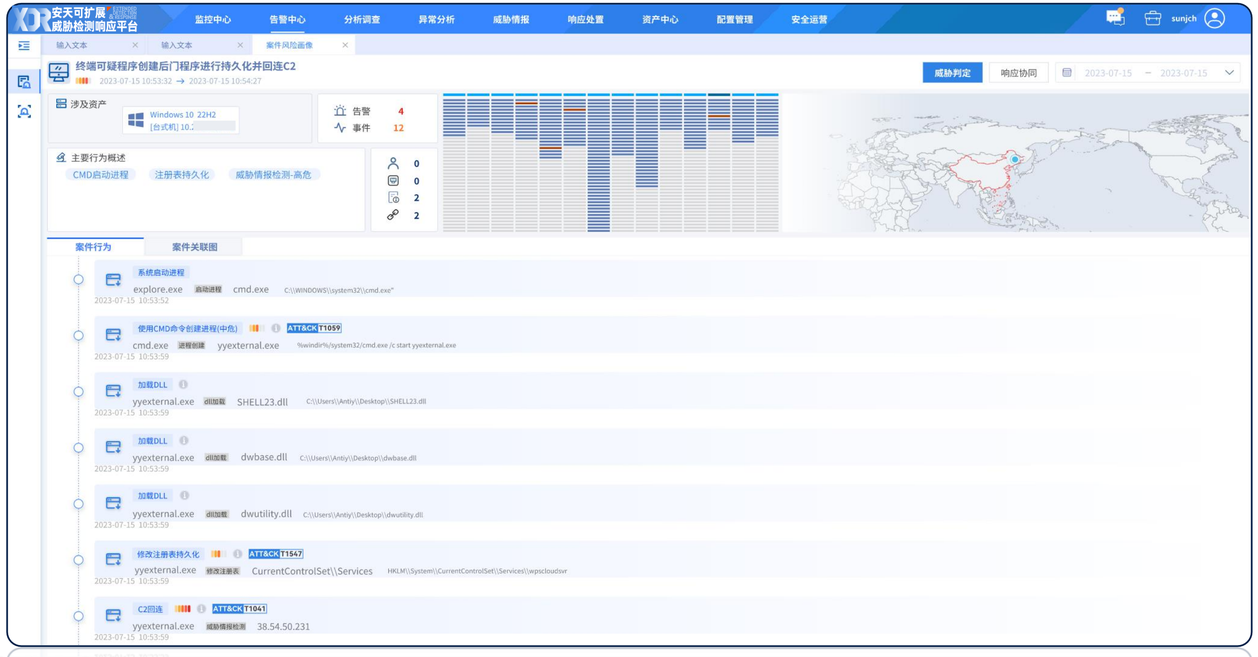


分层检测与关联分析——溯源事件脉络

海莲花样本自动化溯源

基于对象及对象间关系形成自动化溯源能力，在实际环境中能够实现对APT级别事件链路还原

自动还原进程的本地调用链、注册表操作、网络行为及业务影响，并在过程中结合本地与云端威胁情报信誉综合判定

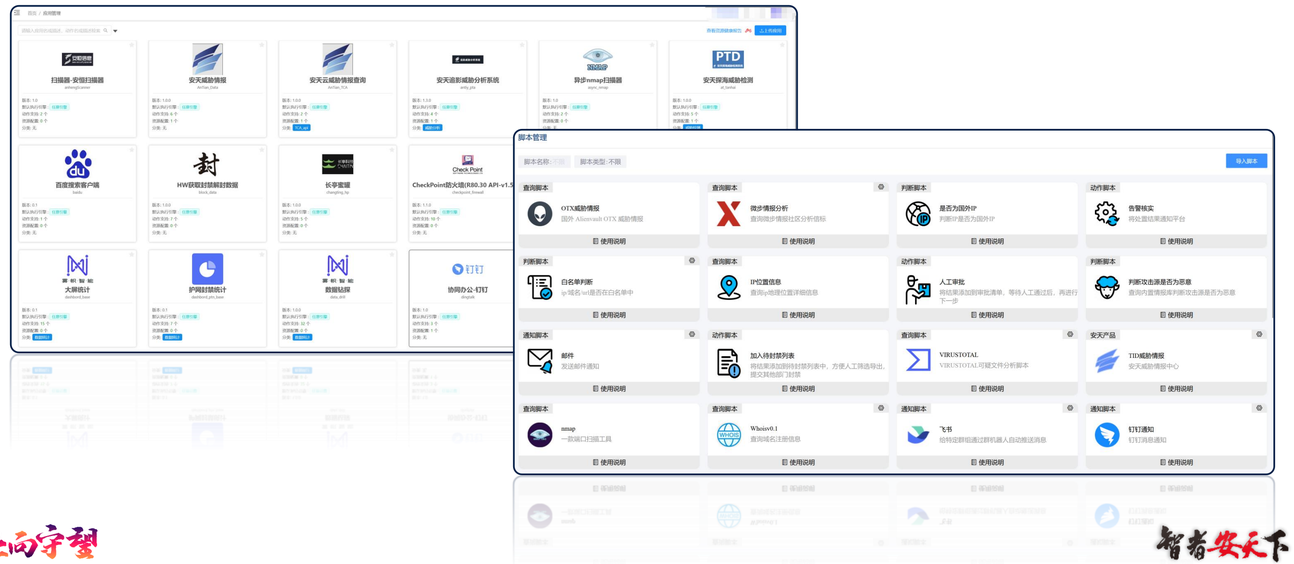


灵活适配第三方设备实现场景化细粒度威胁处置

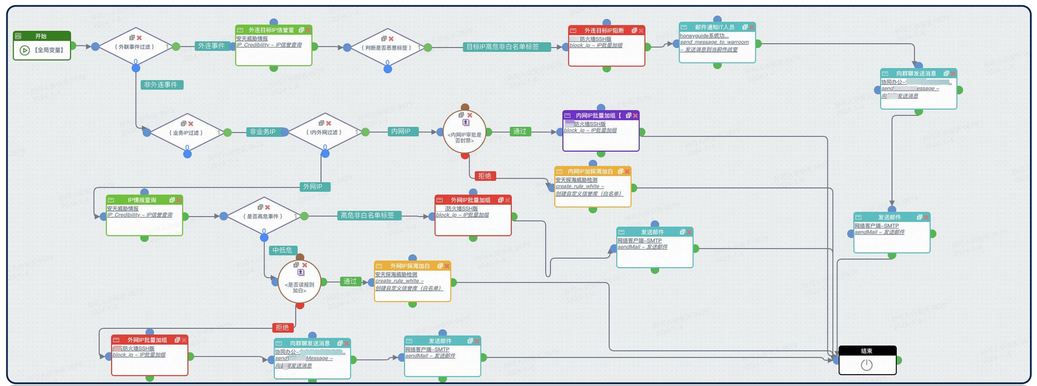
通过安天XDR与雾帜SOAR协同，实现面向不同场景的细粒度处置剧本

100+	300+	150+
开箱即用的 安全事件响应剧本模板	主流安全产品、网络设备 SaaS服务和IT系统能力对接	不同行业客户，不同业务场景 不同运行环境的PoC案例积累

对接第三方设备 提供可供调用且灵活拓展的能力单元

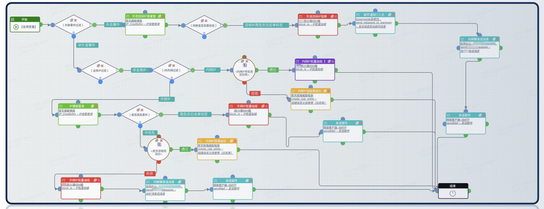


细粒度处置剧本 不同场景精细化策略配置

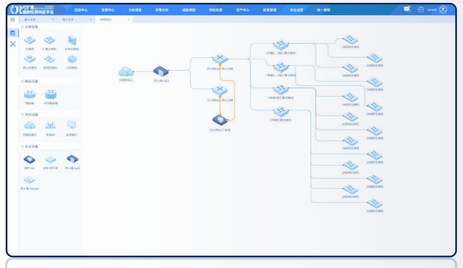


通过编排与自动化协同加速闭环

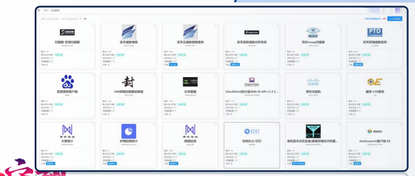
细粒度处置剧本 不同场景精细化策略配置



网络环境可见性 支撑防御策略下发



对接第三方设备 提供可供调用且灵活拓展的能力单元



基于网络环境信息以及细粒度处置剧本的加持，通过自动化驱动，得以在第一时间定位需联动设备，并下发处置策略对于高威胁等级、业务影响等情况，可通过IM/OA协同管理员及责任人，推进整体处置效能

在运营过程中，对高置信威胁能够达到**秒级**的处置效率，相对传统人工处置，平均响应时间可以缩短超过**93%**

处置自动化 对象&属性级处置

研判助手 一键分析和处置

04

动态适应

使用XDR/MDR快速开始高效运营

使用安天XDR/MDR开始高效运营

通过安天XDR开始高效运营

传统的安全运营中心的建设和改造成本过高，且难以根据信息化发展持续保障建设的有效性

使用XDR / XDR SaaS可以实现小成本/0成本部署，根据场景和业务分步建设动态拓展

低成本建设 快速启动

SaaS、私有云、本地化等多种方式建设

接入设备即可快速开始运营，降低建设和运维成本

既有安全建设 有效利用

有效利用既有的安全建设成果进行分析和响应，真正做到分步建设，有效统筹

依场景动态拓展 灵活适应

根据实际安全业务的发展和阶段性安全建设规划

灵活扩展分析和响应能力

强化安全运营 提高效率

通过全流程的自动化提高运营闭环的效率，

提高威胁对抗能力

通过MDR开始全天候托管运营

依托XDR平台，通过安全专家7*24小时值守与应急响应，

MDR/MSS的托管模式可以提供全天候全方位的监控和响应服务，提供更加专业的安全运营与威胁对抗能力

XDR + 安管 + MDR 双中心托管运营建设案例

案例背景

高校数据量庞大、各类系统繁多、人员繁杂，面临着VPN入侵、供应链违规、挖矿行为等网络风险。近二十种各类安全设备各自为战，无法形成有场景化的针对性防御

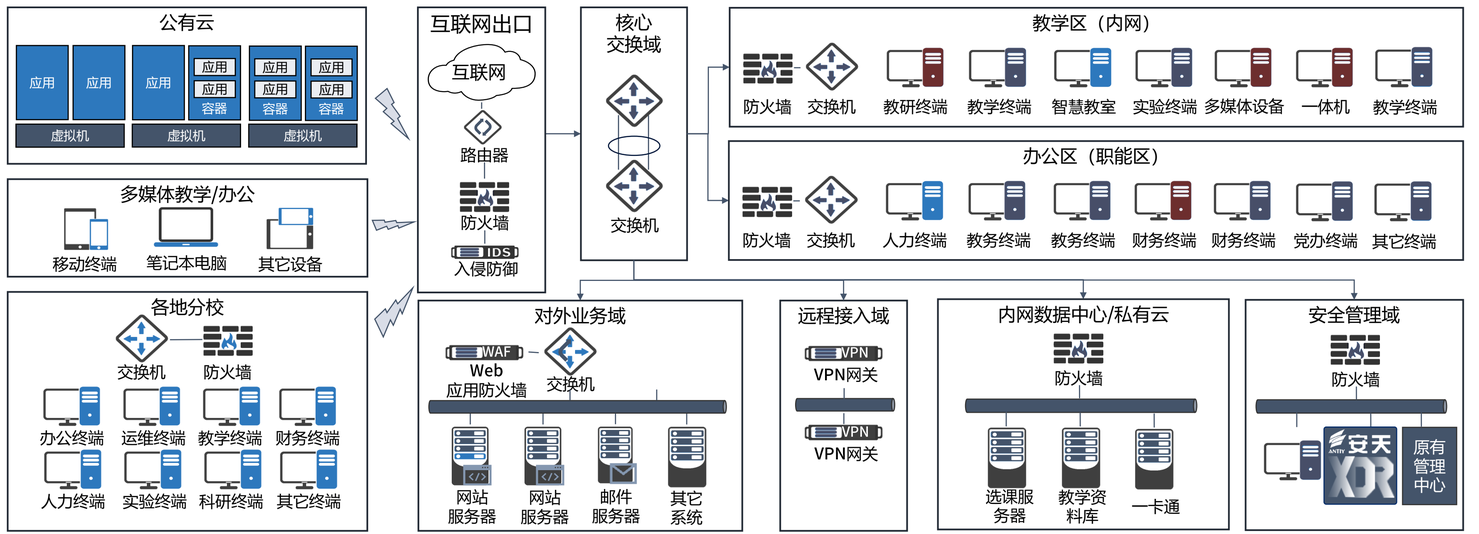
XDR方案

安天XDR，集成探海NDR、智甲EDR、捕风蜜罐、集成**已有安管平台**及第三方设备及系统共20余种。通过**MDR服务开展**7*24H持续值守

- 跨设备关联分析对攻击事件集中告警和监控，还原详细的攻击路径
- 提供VPN、供应链、挖矿、邮件等十几种场景化分析模型

客户价值

- 实现了全网的统一监控分析和处置，结合自动化能力将告警数量降低93.5%，响应效率(MTTR)提高94.1%，运营效果显著提高
- 攻击事件自动化联动身份认证和准入追溯人员身份并发送通知，提高多系统溯源的效率
- 发现账号盗用滥用上百起，发现十余家供应商风险行为，均在产生重大损失前有效遏止



*示意图，非客户实际结构

XDR+安管 双中心协同

运营建设案例——某单位

案例背景

日常安全运营需要统一平台集中监控，需自动化处置能力提高安全运营效率。在重大安全活期间需加强监测与处置能力。同时需要级联上下级单位，数据互通统一监控，实现处置任务与处置结果的上通下达。

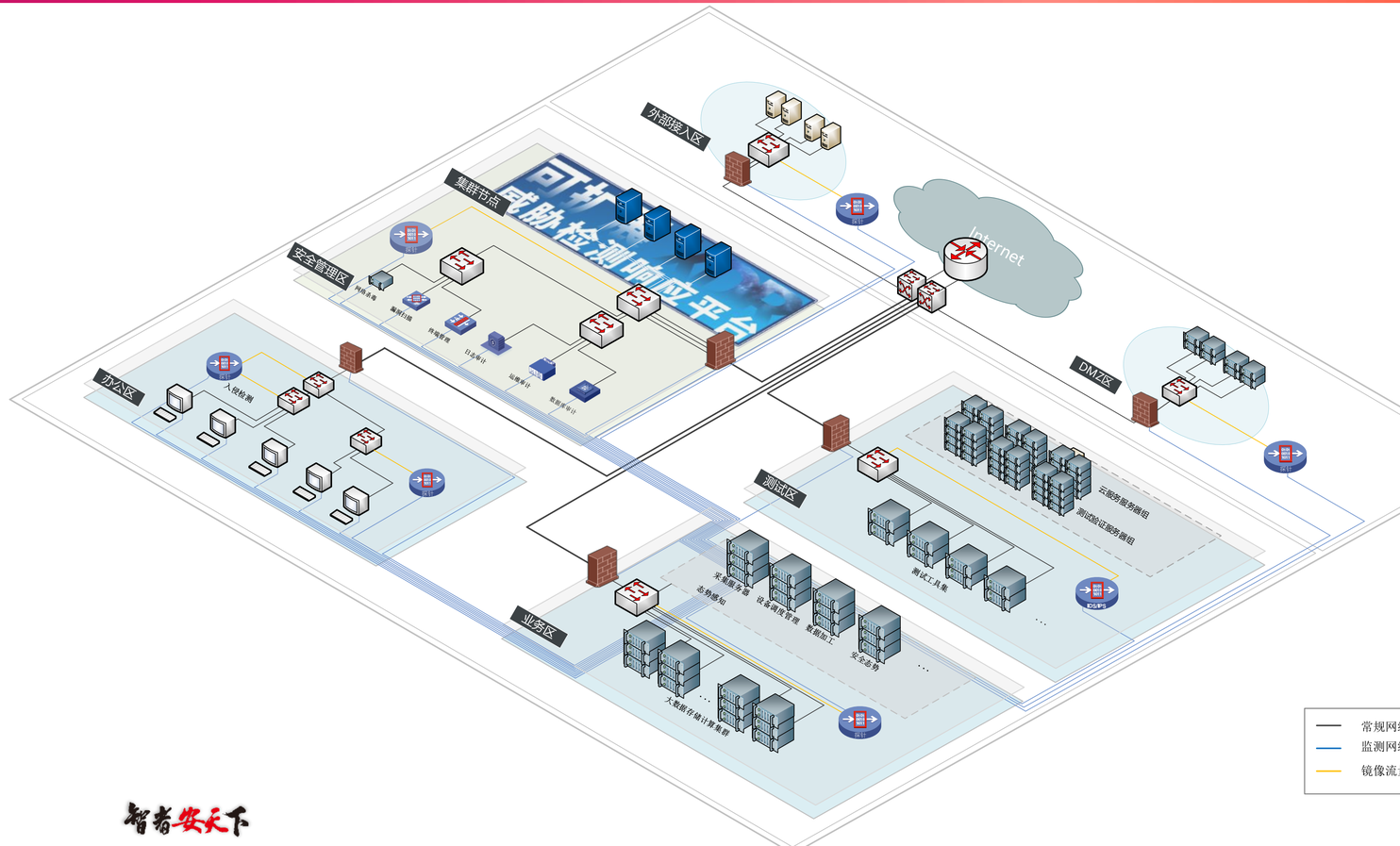
XDR方案

安天XDR，接入探海NDR、智甲EDR、镇关FW、WAF及其他第三方设备，通过MSS持续监控和响应

- 攻击事件集中告警和监控，通报工单联通上下级单位协作安全运营
- 结合安全运营需求创建处置剧本，每日自动化执行处置任务

客户价值

- 通过平台的自动化能力辅助安管人员快速发现并处置安全事件，实现了本部的多隔离网及下属单位的统一安全运营
- 在半年内将日均威胁数量降低了三个数量级，且在多次演习和重保中均获得较好的表现



网络空间威胁对抗与防御技术研讨会
暨 第十一届安天网络安全冬训营

安天XDR/MDR

期待您的使用与反馈

安天冬训营 wtc.antiy.cn

执行体治理赋能与大模型辅助

北向守望