附件：

南山区医疗集团总部

安全检测与响应管理平台项目需求

# 项目概述

## 项目名称

南山区医疗集团总部安全检测与响应管理平台

## 项目周期

项目建设周期为60天

## 业务现状和需求分析

### 应用层安全风险

1. 应用系统资产众多，存在大量的资产信息不明，互联网暴露面不清晰等问题；
2. 应用系统存在大量的漏洞未及时修复，暴露在互联网上的业务系统存在文件上传校验不严格以及IIS中间件系统安全漏洞，导致攻击者利用概率极高；
3. 账户安全风险：应用系统存在大量的弱密码、多台服务器使用相同密码、系统管理员使用默认密码等问题存在严重安全隐患；
4. 缺乏有效的应用层安全威胁监测与响应手段，只能等到安全事件发生了才来被动响应溯源，往往损失已经造成了，而有经验的攻击方能够很轻易的抹除攻击痕迹，导致很难溯源；
5. 缺乏应用程序日志审计与备份机制，在网络中又没有流量和行为监测等技术手段，导致攻击者入侵成功后无法及时发现，攻击者退出后如果清除了入口跳板主机上的日志信息后就没有其他途径可以分析攻击者的访问痕迹。

### 网络层安全风险

1. 网络分级分域缺失，需要对互联网提供服务的业务系统服务器直接从内网经过网闸方通提供互联网接入，一旦有一台服务器失陷就导致内部全网被攻陷；
2. 边界应用层监测及防护机制缺失，网络边界现有的传统防火墙无法记录服务器的访问行为和应用层攻击行为，导致攻击行为无法快速发现，攻击成功后难以发现，响应溯源无迹可查；
3. 内部网络全流量监测分析手段缺失，现有安全设备无法记录全流量的主机行为，仅记录明确的攻击行为，对高级威胁攻击的识别和行为记录留存不起作用；

### 终端主机层安全风险

1. 主机上现有部署的杀毒软件仅能实现基于文件特征的检测，无法做到主机文件异常和行为异常的识别，对webshell、命令执行、挖矿、勒索等病毒行为无法做到有效的检测和防御；
2. 主机未及时更新系统补丁，如勒索病毒传播利用的漏洞相关的MS17-010等安全补丁有大量的主机都未修复；
3. 主机存在大量的安全漏洞未修复补丁，对主机漏洞存在的安全隐患缺乏有效的管理手段做到处置闭环；
4. 内部主机存在大量的僵尸网络、勒索、挖矿等失陷事件，缺乏主动发现和处置手段，导致网络内部潜在威胁不断增多。
5. 已有防病毒产品基于病毒特征库方式进行杀毒，在高级威胁持续产生的大环境下，呈现被动、后知后觉等检测特点，无法及时有效防御新型病毒，如WannaCry勒索病毒。另外，本地特征库数量受存储、性能、资源等多方面影响，现有本地特征库文件规模无法满足已知病毒的查杀需求。
6. 如信息系统内某台终端发现病毒，防病毒产品将采取基于文件隔离的方式进行处置，此种方式相对落后，如文件隔离失败情况产生，单点威胁将快速辐射到面，因此传统防毒产品已经无法适应新的病毒传播方式及环境。

### 安全效果运营保障机制缺失

1. 缺乏信息化资产管理机制，对IT资产没有清晰的梳理和持续的变更管理跟踪，导致资产信息脱节严重，安全工作保护的目标都不清楚，僵尸资产、暴露面较多；
2. 信息化资产脆弱性缺乏有效管理，无法做到业务系统脆弱性问题的闭环管理；不管是技术保障还是管理机制都难以匹配脆弱性闭环管理的要求；
3. 安全威胁管理基础几乎为零，威胁监测、分析研判、响应处置等方面技术手段和管理机制保障都很缺乏，仅有基础的网络层访问控制措施。

技术工具是安全运营工作的主要载体和基础。现有各类安全设备和组件各自为战、日志分散、能力不集中，且对内网横向流量与虚拟化平台内部东西向流量缺乏有效检测，无法全面看清全网流量风险。为了自身网络安全防护需要，同时满足合规与主管单位监管要求，亟需搭建一套行之有效的安全运营平台，希望实现以下需求目标：

* 1. 实现全网安全流量与日志的统一汇聚、检测与分析，提供集中安全告警，收敛安全运维入口，提高安全分析与运维效率；
  2. 增强对安全日志的关联分析能力和深度挖掘能力，通过AI、UEBA等新技术的运用，发现新型威胁、潜伏威胁与未知威胁；
  3. 实现安全风险实时可感知，风险多维度可视化监控，可以定期查看整体网络安全态势报告、资产与脆弱性风险报告、运维报告等；

形成自动化联动处置能力，针对高危事件与已失陷主机，能提前预设剧本，联动终端检测与响应系统等安全系统自动化执行策略，缩短MTTR时间。

# 项目初步方案

## 建设目标

1. **安全检测与响应管理平台建设目标**

本次安全运营体系建设以南山区医疗集团总部的网络、重要服务器、核心业务系统等IT资产为保护对象，依据网络安全法、网络安全等级保护要求和相关标准规范，围绕实战化的威胁对抗能力，以效果为核心、以闭环为目的，聚焦检测能力提升，实现精准高效的效果。立足“人员、流程、工具、服务”，构建“3+1+3”体系（即3类用户场景+1类重要配套服务+3项核心能力），实现“让威胁对抗更高效，让运营工作更省心”的目标。建立南山区医疗集团总部网络信息化与组织架构相配套的安全运营中心，实现网络安全从被动向主动、从静态到动态、从单点到整体、从粗放到精准防御的转变，全方位全天候的保障网络信息系统安全可靠，全面监测和阻断已知网络攻击和未知入侵渗透风险，防范来自外部和内部多类型攻击，以安全保发展，以发展促安全，推动南山区医疗集团总部网络安全发展迈向新的高度。

1. **终端安全管理系统建设目标**

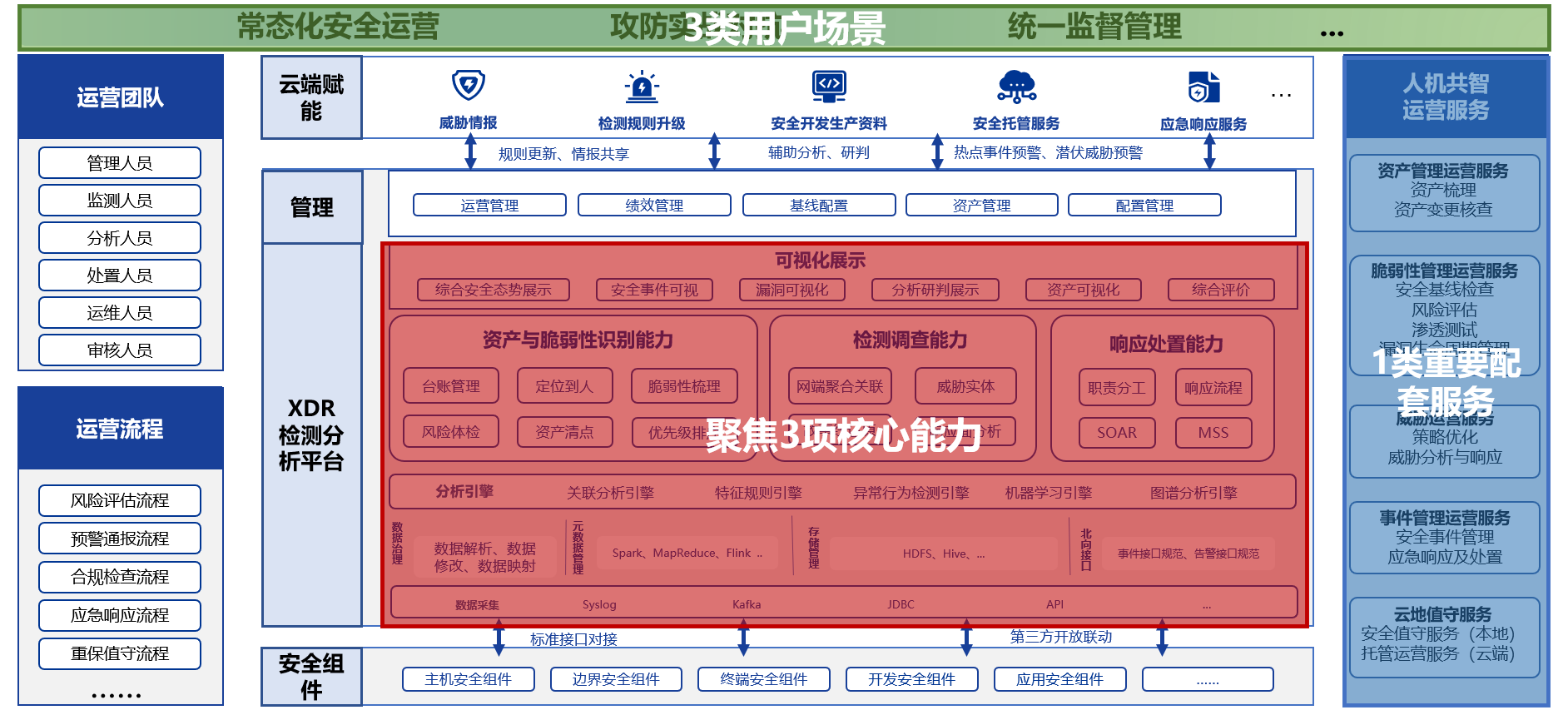
通过终端检测与响应系统的全面部署应用，提供多安全平台联动机制，终端检测与响应系统可与XDR安全检测与响应管理平台进行联动，实现威胁情报的共享与接收效果。终端检测与响应系统在收到其他设备发送的威胁情报时，可第一时间进行隔离处置，有效缩短威胁响应时间，智能化的处置方式，大大减少管理人员维护工作量、提升安全防护水平，并全面形成多平台立体防御壁垒。

## 方案设计

1. **安全检测与响应管理平台方案设计**

通过在核心交换机部署流量采集探针与终端/服务器部署端点采集工具将关键数据聚合上传XDR平台，通过云端专家服务提供威胁狩猎能力。

### 安全运营中心架构模型



图示： 安全运营中心框架

### 安全运营中心核心能力说明

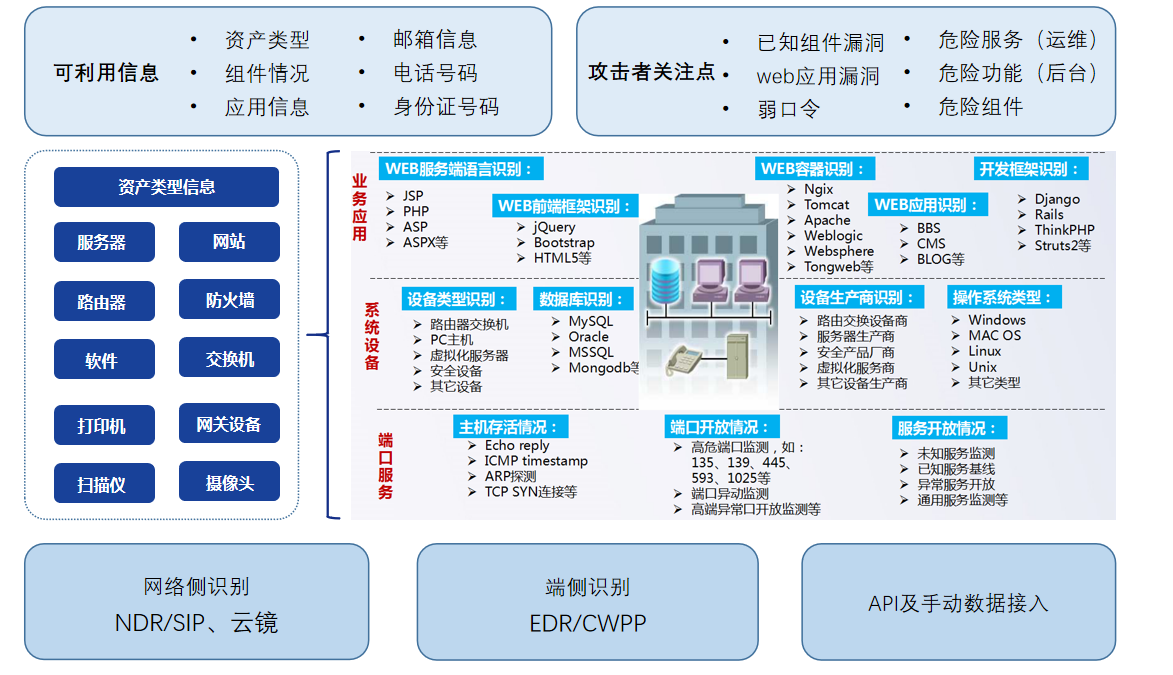


#### 资产管理与攻击面管理

##### **资产管理**

基于安全运营平台（XDR）的资产管理可以解决资产分散、不集中等一系列管理问题。具有识别IT资产、梳理访问关系和建立责任人员组织架构的功能，实现资产的统一管理。其中，可识别的资产类型，包含服务器、终端、网络设备、物联网设备、移动设备和网络安全产品等。

安全运营平台通过网络侧，端点侧和第三方API获取以及手动数据接入来识别资产。通过主动扫描识别、被动流量识别和用户手动三种方式导入资产列表，结合用户页面操作资产信息，对资产进行关联、合并、去重和除错等处理，补充更新资产数据信息。



资产管理

主机资产可以实现识别操作系统、开放的服务与端口、在线离线状态、资产类型。支持业务/服务器资产分类，可定义IP地址、所属资产组、主机名、责任人、责任人邮箱、所属业务、MAC、地理位置、操作系统、服务与端口、最近上线等信息。

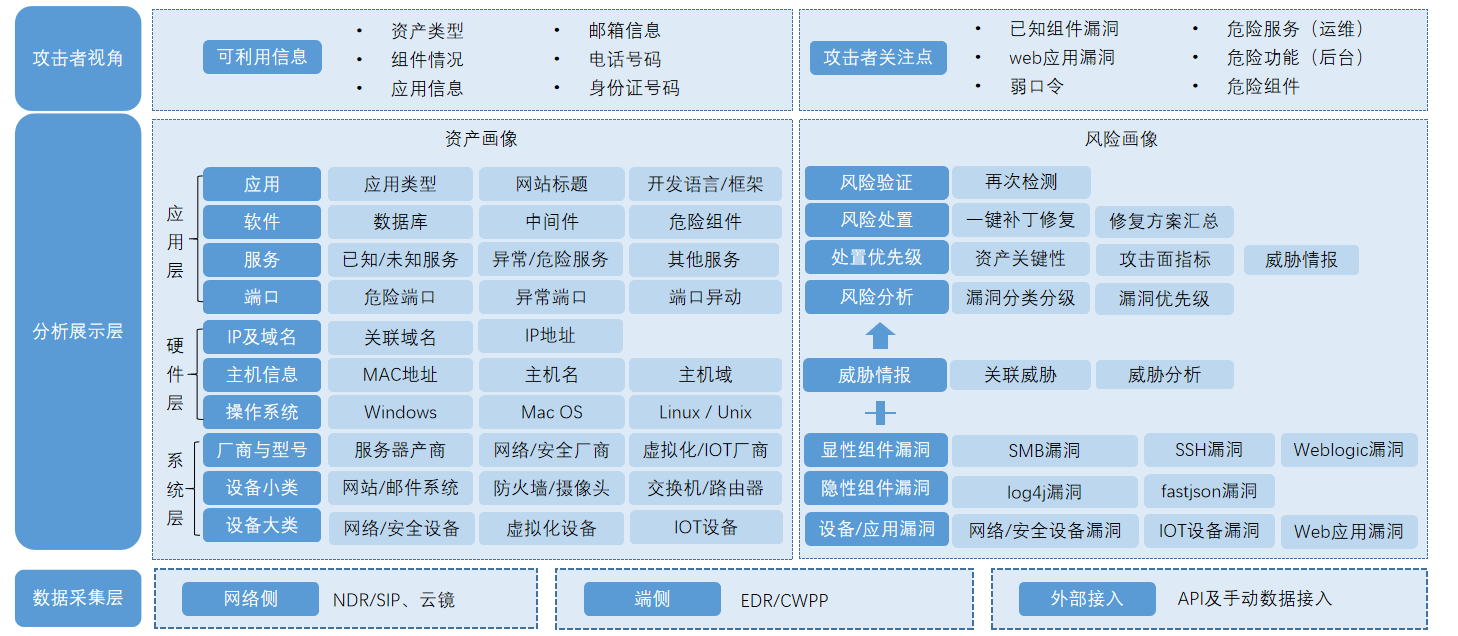
资产详情可以展示资产基础信息包括关联IP、设备信息、地理位置、资产责任人、操作系统、虚拟机信息；开放端口信息、账号信息及登录历史、应用软件信息、硬件信息及数据来源等。

责任人管理支持展示责任人风险资产数及风险标签，可编辑人员部门归属。

##### **攻击面管理**

从攻击者视角看来，能够被攻击者利用以发起攻击，进而对业务造成安全风险的所有攻击点，都是攻击面管理的内容。

传统自下而上的设计受限于采集能力，只能根据采集到的内容被动分析和响应；XDR平台采用自上而下的设计思路，深度洞察攻击面，并根据洞察结果主动提升检测和分析能力，使攻击面管理更主动、更全面、更准确。以攻击视角进行深度资产威胁建模，通过动态运营，收缩暴露面威胁建模，找出攻击关键路径，组件延伸出可能的攻击和利用点，对应出解决方法，进行精准有效加固。

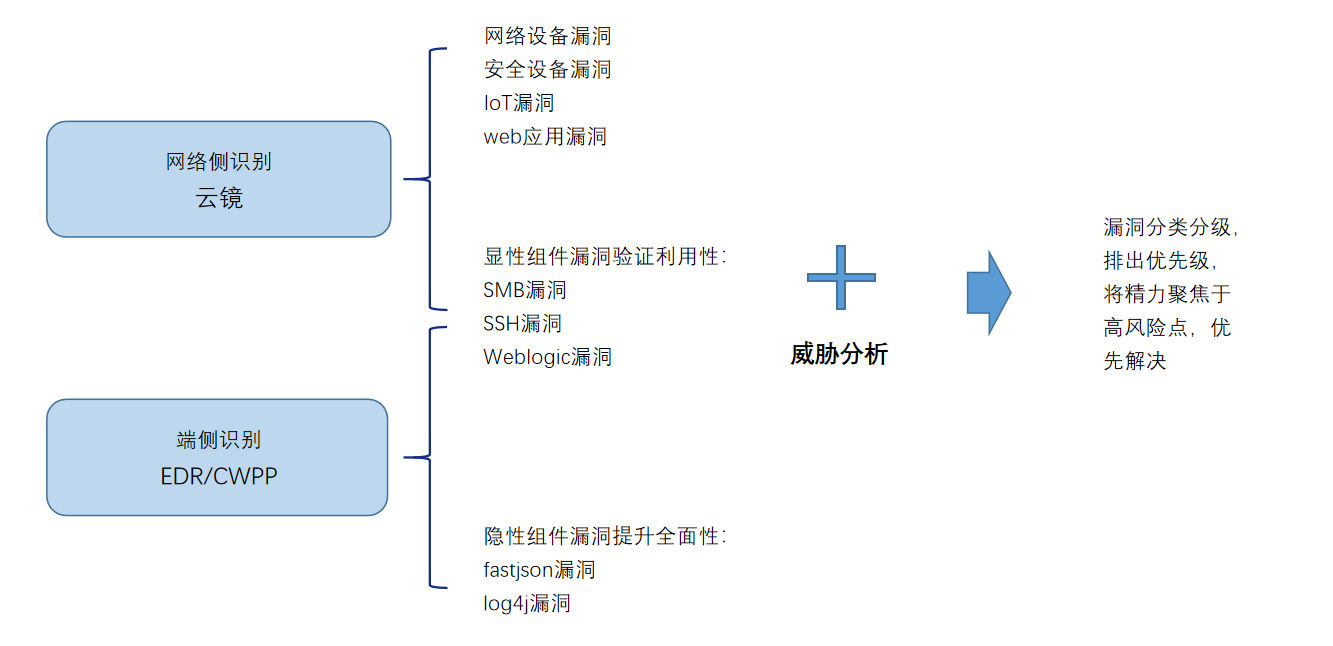


XDR攻击面管理

随着资产数量的增多，系统和应用漏洞频繁爆发，对资产漏洞进行识别与管理是保障业务安全的重要一环。XDR平台结合网络侧以及端点侧识别漏洞检测，能够全面的了解用户设备的真实漏洞情况。

结合漏洞全生命周期机制，对漏洞全生命周期进行管理，包括：漏洞发现、漏洞验证、漏洞处置、漏洞复测，实现漏洞全生命周期状态闭环跟踪，确保重要的漏洞及时处置。具体过程定义如下：

* 漏洞发现：能够主动地对系统、应用层、中间件、数据库等漏洞检测。
* 漏洞验证：能够对紧急漏洞进行排查，主动检测、网络安全设备、主机网络安全管理软件、网络安全漏洞发现算;法等来源的漏洞信息进行自动化的或手工的验证，确定漏洞的有效性。
* 漏洞处置：对发现的漏洞提供处置建议，提供可落地的漏洞修复方案，包括：漏洞修复步骤、补丁下载链接等，漏洞处置方案支持自定义。
* 漏洞复测：当漏洞修复后，对漏洞进行复测，确定漏洞是否已被成功修复。



XDR漏洞管理

脆弱性管理页面展现终端遥测及网络遥测扫描到的资产脆弱性进行展示，可对资风险产类型、风险等级及资产名称、责任人、组名等标签进行筛选，通过图表进行展示。

同时支持对热点事件的展示，以时间轴展示，可展现漏洞名称、风险等级、CVE编号、可检测情况，影响资产、威胁标签、爆发时间及风险评估。对热点事件包含的漏洞，可以展示危害程度、漏洞爆发时间、CVE-ID、CNNVD-ID、威胁标签、漏洞介绍、影响组件、情报来源、漏洞活跃趋势及修复处置建议。

#### 检测调查能力

XDR平台的威胁检测能力体现在终端侧能力、网络侧能力、平台能力三部分：

##### **平台能力**

XDR平台具备聚合分析流量和端点一手数据的能力，同时可通过微剧本半自动化响应事件，实现少量精准的检测效果、自动高效的处置效果，也是构建实战化威胁检测相应体系的核心。通过网侧流量+端侧行为数据以及第三方日志汇聚分析，平台提供的攻击链溯源图能准确还原攻击故事线，对恶意入侵、异常外联、侦查、横向移动、数据外泄等每个阶段发起的所有安全事件和造成的影响进行全面的剖析，形成具有承上启下的安全事件关联集，并围绕被攻击者的攻击链视角进行呈现和告警。同时SaaS能力赋能，将云端的威胁情报、专家能力下发到用户网络和终端，在当前安全“唯快不破”的态势下，云端能力即时更新，快速下发到本地，扭转了以往防落后于攻的不利局面，使得用户能够在安全对抗中抢占先机。云端专家7\*24小时值守，也为南山区医疗集团总部安全运营大大降低了人力成本和门槛，给南山区医疗集团总部带来了省时、省力、省心的用户价值。

##### **威胁检测引擎**

##### 基于特征规则的检测算法

由安全专家对入侵/攻击进行精准的特征提取和描述，形成规则。算法依据规则，来识别网络流量和主机中的攻击。该算法识别精准，误报少，可以广泛覆盖已知威胁。包括：账号安全检测、邮件安全检测、web攻击检测、漏洞攻击检测、C&C检测、隐蔽隧道、恶意文件/软件检测等。

##### 基于无监督学习的检测算法实现

基于无监督学习的检测算法：使用机器学习、深度学习对主机数据、用户行为数据、和网络流量数据进行建模，建立正常行为基线，然后比对实时数据来检测异常行为。用于发现内部违规和高级别攻击。包括：异常行为检测和未知攻击路径检测。关联分析实现。

##### 告警优化算法

告警优化功能的目的在于消除告警疲劳，防止真正的安全威胁淹没在海量的告警当中。原始安全告警与优化后的安全事件的比例为N：1。算法将各个安全设备、安全产品、安全系统、各厂商的安全算法模型上报的海量安全告警通过大数据关联分析将聚合、归并、关联、统一，并进行归并去重优化、白名单优化、攻击场景优化。可以大幅降低重复的、无效的、低危的告警数量，突出真正高危攻击，便于真正的风险能够及时处置闭环。从而消除告警疲劳，大幅降低事件处置工作量，提高其处置效率，从而提高安全威胁决策指挥能力。

##### **关联分析能力**

XDR平台使用Flink CEP（Complex Event Processing复杂事件处理引擎）技术作为底层数据处理的核心，通过结合多种关联规则模板来实现复杂的CEP语义。将终端侧和网络侧收集的数据，与云端威胁情报、资产、时间等因子做复杂关联，最终生成平台侧的关联事件。

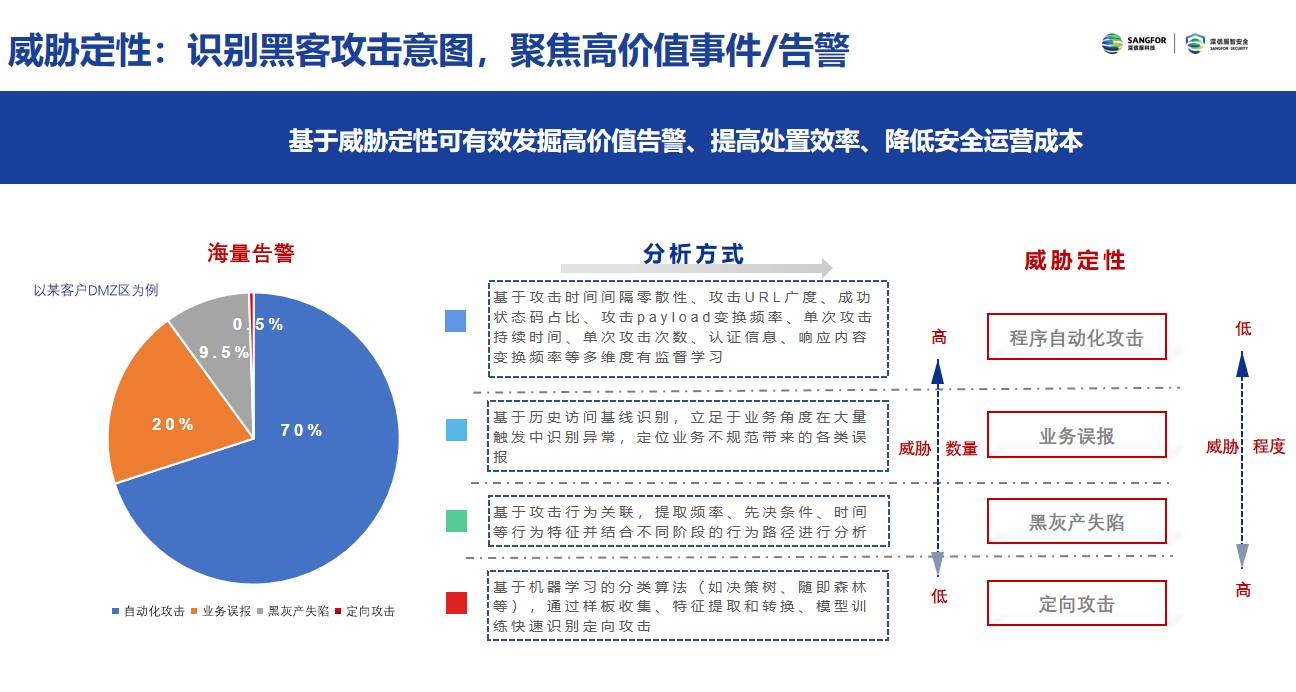
对与组件强加强的告警信息，平台提供可视化和高可见性，结合精准详尽的处置响应建议，帮助安全运营人员提高效率，显著降低了MTTD（Mean Time To Detect，平均检测时间）/MTTR（Mean Time To Response，平均响应时间）。

对于组件弱加强的告警信息，平台通过多因子关联提升检测精度，有效降低告警误报量，针对原本单一网络侧或终端侧无法精准检测的攻击，如Webshell上传成功、RDP爆破成功等，基于E+N关联分析实现网络和终端数据相互印证，互为补充，大幅提升了检测精度。

对于组件弱加弱的告警信息，平台对于二者进行整合，提升了威胁检测的覆盖广度，无论是低危的自动化脚本攻击，还是高危的高级持续威胁，在XDR平台下都将无处遁形。

##### **威胁定性**

威胁定性：通过上下文、资产和脆弱性数据、威胁情报等数据进行大数据关联分析，对安全设备上报的海量告警数据进行威胁定性，确定威胁等级（区分事件和威胁）和主机失陷等级。并能够挖掘出攻击成功事件，包括暴力破解成功识别、Web攻击成功识别、漏洞攻击成功识别等。以上安全事件，和威胁检测算法的C&C（DGA、隐蔽隧道通信），以及木马后门、勒索、挖矿、webshell等构建全面的安全事件/攻击成功识别。





如下表所示，各场景下的攻击成功识别，所用的数据源，以及算法模型简介。

|  |  |  |  |
| --- | --- | --- | --- |
| 场景 | 威胁子类型 | 数据源 | 安全分析方法 |
| 账号爆破成功 | 暴力破解成功:SSH/SMB/FTP/RDP等常见服务。 | 主机/应用登录日志、流量日志 | 关联分析：  登录日志+攻击源IP关联；  登录日志+威胁情报关联； |
| 数据库暴力破解成功：Mysql、Oracle、MSsql | 数据库日志、流量日志、 |
| Web后台账号爆破成功 | web日志、流量日志、 |
| Web攻击成功 | web组件漏洞攻击成功 | 告警日志、流量日志、web日志、数据库日志等 | 上下文关联分析 多维数据关联分析 |
| Sql注入成功 |
| 命令注入成功 |
| 代码注入成功 |
| Webshell上传成功 |
| 漏洞攻击成功 | system漏洞攻击 | 告警日志（漏洞攻击，C&C、病毒文件）、系统应用日志等 | 关联分析：  漏洞攻击成功后，会出现C&C、恶意文件下载等。 |
| SMB漏洞攻击 |
| 数据库漏洞 |
| 其他常见应用漏洞 |
| 其他攻击成功 | 其他类型攻击成功 | 安全设备告警日志 | 告警日志间关联分析 |

#### 终端侧能力

传统终端侧威胁检测主防以规则为检测手段，通过规则发现攻击威胁，难以覆盖高级威胁，例如无文件攻击、模仿攻击（Mimicry）以及跨重启跨长时间窗口的APT攻击。终端侧高级威胁检测能力通过在端侧采集全面的数据，包括终端、用户、文件、进程、行为等数据。数据在本地做分层，聚合有效数据上传至平台。结合用户真实环境做上下文强关联分析，提升攻击研判精准度。行为检测基于多事件复杂关联规则匹配算法，依靠IOA泛化行为规则提高已知和未知高级威胁攻击检测能力，补充复杂行为关联检测领域空白，构建行为检测防御层级，增强多层次纵深防御检测能力，帮忙用户有效抵御已知和未知高级威胁攻击。

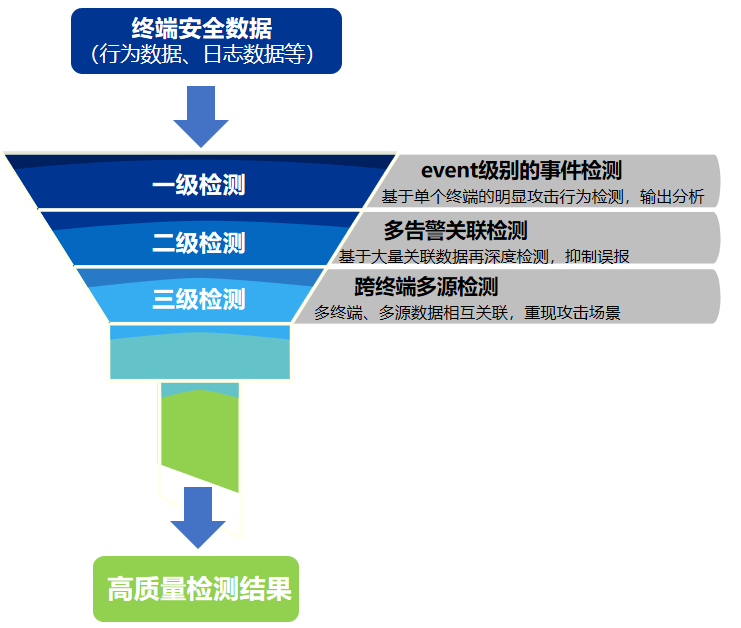
采用三级检测机制，呈漏斗状。

第一级是系统事件（Event）级别的事件检测，基于单个终端的明显攻击行为检测，输出分析；

第二级是多告警关联检测，是基于大量关联数据再深度检测，抑制误报；

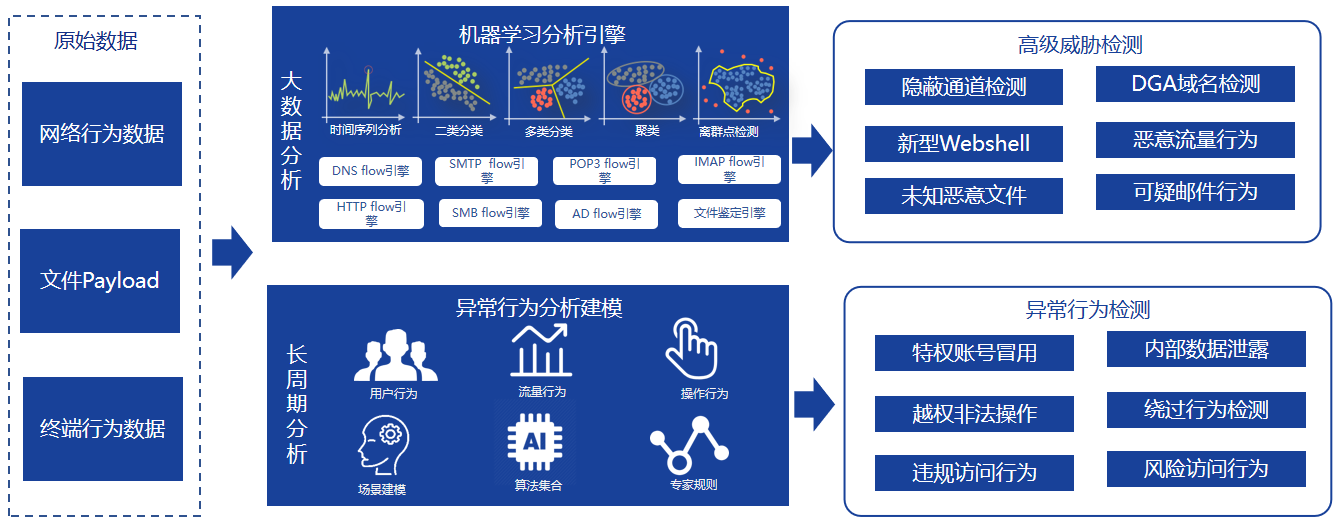
第三级是跨终端多源检测，基于多终端、多源数据相互关联，重现攻击场景。

通过上述三级检测引擎，输出高质量的检测分析结果。



#### 网络侧能力

网络侧基于流量采集和日志采集，通过WAF\IPS\PVS漏洞检测\威胁情报四种规则进行初步分析做数据标记和特征检测，之后再结合EBA和AI中基础的威胁检测模型来进行匹配，快速定位出场景威胁如流行病毒、黑客工具、爆破、扫描、DGA等，针对一些更复杂的不规则的一些组合威胁攻击手段如攻击成功识别、自定义工具、0day漏洞利用、代理转发工具、隐秘隧道等，基于整个会话流量进行检测，包括对流量的请求回显、特征异常关联、异常行为利用、多阶段攻击利用等行为进行完整回溯关联，最终定位出来异常风险。最后是基于优化算法模型，对一些典型的加密流量、0day漏洞利用特征进行优化检测，实现高检出低误报。



#### 响应处置能力

通过安全运营平台（XDR）构建分层响应体系，可协同联动相关组件，具备自动化响应与处置能力，提升威胁应对的效率。通过安全运营提供的事件响应处置能力，制定全面的事件响应（IR）计划，帮助安全团队对网络安全事件做出完整，快速和有效的响应，通过准备、检测、抑制、根除、恢复、跟踪等多个阶段的响应处置工作，降低因安全事件带来的损失。

##### **设备联动能力**

当攻击行为发生时，相关的安全设备能相应地协同响应，作出防御措施，如网络流量检测设备在发现威胁时，能够通知防火墙对非法IP进行阻断，或防火墙在发现非法外联行为时，阻断非法外联行为，同时通知相关终端安装的终端检测与响应系统软件进行杀毒操作。通过这种联动机制实现对信息系统的综合防御能力，而这种防御措施都应该在安全运营的有效部署和协调下准确高效地完成。

安全联动能力的建设应该能够联动安全产品进行安全防护和处置，从数据接入、安全能力融合、协同联动等多方面入手，大大降低了用户进行安全防护的难度，提升了安全系统的可用性。

* 联动防火墙功能。联动防火墙功能主要通过从防火墙同资产数据，安全日志，访问日志，联动封锁日志等信息，在XDR平台上进行安全分析后，自动联动防火墙进行访问控制和联动封锁。
* 联动上网行为管理功能。联动上网行为管理功能主要通过从上网行为管理同步资产信息，在线用户和安全日志等信息，在XDR平台进行安全分析后，自动联动上网行为管理进行账号冻结、准入控制和上网提醒。
* 联动终端检测与响应系统功能。联动终端检测与响应系统功能，主要通过从终端检测与响应系统同步资产信息，安全日志，系统日志、终端行为日志、漏洞日志等信息，在XDR侧进行联动封锁，一键查杀，进程取证。
* 自动联动功能。自动联动功能，主要通过分析不同来源的安全日志，结合资产信息和访问日志进行关联分析。之后根据不同的安全问题，下发不同的安全策略。

##### **SOAR剧本**

依托XDR平台内置的SOAR模块，可进行图形化的安全编排，根据不同的安全事件可自行灵活地编排不同的处置流程，将安全运营相关的技术、流程和人员等各种能力整合在一起工作。可通过剧本的方式编排响应处置流程，可通过SOAR统一构建自动化分析、响应、处置剧本，一旦发现安全问题就立即启动预定义的剧本，快速将安全事件进行闭环，实现了根据不同类型的风险自动化执行不同的处置流程

#### 多样化对接能力

##### **多源数据对接**

安全运营平台需要实现统一管理与统一调度能力，需要实现与第三方日志、第三方应用的对接，需要收集网络流量数据、主机终端数据、安全设备告警数据、情报数据等。

#### 深度威胁狩猎服务

安全专家可针对内/外网或特定业务系统及特定漏洞，基于客户业务定制检测逻辑，尽可能快地发现漏洞或攻击痕迹，发现潜在的安全隐患和已失陷的主机/被钓鱼成功的员工/账密信息泄露等，最大限度地降低攻击者造成的危害，评估造成的损失等内容，最终帮助客户验证风险并推动发现的问题和隐患进行闭环处理。

#### 内置剧本交付服务

结合南山区医疗集团总部的实际需求，完成工单&soar模块的内置流程/剧本的优化交付，具体包括： 1、业务/流程需求调研 2、内置剧本优化配置与试运行。 3、内置剧本使用说明。

#### 移动运营小助手

1. 安全事件推送：XDR平台产生的安全事件（非告警）、云端狩猎挖掘的事件、最新发生的新型威胁影响评估报告等事件，可以推送到服务号，随时掌控安全态势；
2. 移动处置运维：XDR移动运维小程序可以实时展示安全事件的详情信息，并且联动网络/端点设备一键处置威胁；
3. 移动专家直连咨询：遇到不好理解、不易分析、难以处置的安全事件，可以立即联系专家协助处理；
4. **终端安全方案设计**

管理端有软件管理端和硬件管理端，其中软件管理端支持在真实物理环境及虚拟化环 境进行部署。EDR客户端Agent支持安装在Windows PC、Windows Server、Linux、MAC OS和信创终端。为确保EDR各项功能正常使用，需要放行Agent客户端到管理端连通性、以及管理端到云端服务器的连通性。

### 统一管理平台适配全类型资产

适配全类型资产

* 桌面云，传统PC，笔记本，私有云，服务器，私有云，公有云全适配
* 终端系统兼容性广阔
* 与底层虚拟化解耦，适配全部虚拟化底层平台

### 基于多维度的智能检测技术

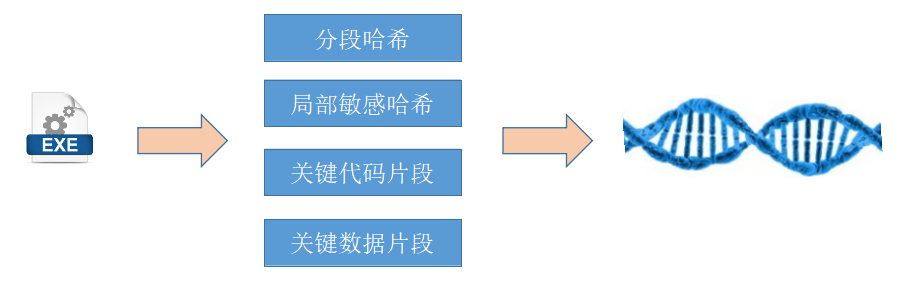
#### 检测引擎

终端上的安全检测是核心的技术，传统的病毒检测技术使用特征匹配，而特征匹配没有泛化能力或泛化能比较弱，当病毒经过简单的变种，就必须新增加特征规则，因此，随着病毒数量越来越大，病毒特征库也就跟着越来越大，同时运行所占资源也就越来越多。而基于AI技术的查杀引擎，利用深度学习的技术，通过对海量样本数据的学习，提炼出来的高维特征，具备有很强的泛化能力，从而可以应对更多的未知威胁。而这些高维特征数量极少，并且不会随着病毒数同步增长，因此，AI技术具有更好检出效果、更低资源消耗的优点。

当然，仅靠一个AI杀毒引擎是不够的，终端检测与响应系统 产品构建了一个多维度、轻量级的漏斗型检测框架，包含基因特征检测引擎、AI 技术的 SAVE 引擎、行为引擎、云查引擎等。通过层层过滤，检测更准确、更高效，资源占用消耗更低。

##### **基因特征检测引擎**

终端检测与响应系统的安全运营团队，根据安全云脑和终端检测与响应系统产品的数据运营，对热点事件的病毒家族进行基因特征的提取，洞见威胁本质，使之能应对检测出病毒家族的新变种。相比一般的静态特征，基因特征提取更丰富特征，家族识别更精准。



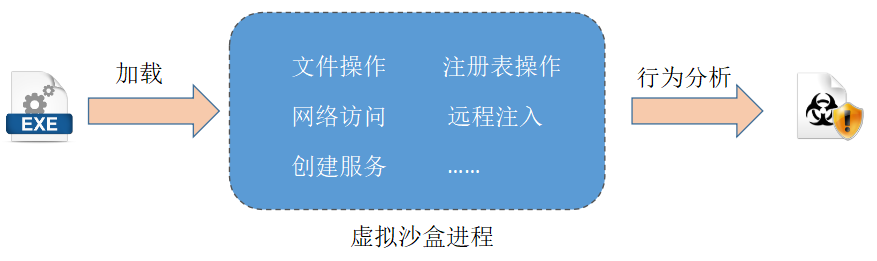
##### **AI技术SAVE引擎**

SAVE（Sangfor AI-based Vanguard Engine）是由创新研究院的博士团队联合 终端检测与响应系统产品的安全专家，以及安全云脑的大数据运营专家，共同打造的人工智能恶意文件检测引擎。该引擎利用深度学习技术对数亿维的原始特征进行分析和综合，结合安全专家的领域知识，最终挑选了数千维最有效的高维特征进行恶意文件的鉴定。

* 基于人工智能技术，拥有强大的泛化能力，能够识别未知病毒或者已知病毒的新变种；
* 对勒索病毒检测效果达到业界领先，包括影响广泛的 WannaCry、BadRabbit等病毒。2018 年 10 月新发现的 GandCrab5.0.3、Rapid、GandCrab5.0.4、KrakenCryptor2.0.7 勒索病毒，使用 9 月已经合入产品并发布的 SAVE1.0.0可以全部检出和查杀。对非勒索病毒也有较好的检出效果；
* 云+边界设备+端联动，依托于安全云脑海量的安全数据，SAVE 能够持续进化，不断更新模型并提升检测能力，从而形成传统引擎、人工智能检测引擎和云端检测引擎的完美结合的整体解决方案。

##### **行为引擎**

传统静态引擎，是基于静态文件的检测方式，对于加密和混淆等代码级恶意对抗，轻易就被绕过。而基于行为的检测技术，实际上是让可执行程序运行起来，“虚拟沙盒”捕获行为链数据，通过对行为链的分析而检测出威胁。因此，不管使用哪种加密或混淆方法，都无法绕过检测。最后，执行的行为被限制在“虚拟沙盒”中，检测完毕即被无痕清除，不会真正影响到系统环境。



行为引擎在分层漏斗检测系统结构中，与云查引擎处于最低层，仅有少量的文件到达该层进行鉴定，因此，总体资源消耗较少。

##### **云查引擎**

针对最新未知的文件，使用IOC特征（文件hash、dns、url、ip等）的技术，进行云端查询。云端的安全云脑中心，使用大数据分析平台，基于多维威胁情报、云端沙箱技术、多引擎扩展的检测技术等，秒级响应未知文件的检测结果。

#### 终端安全基线核查



图4-4 安全合规审查

终端的安全合规性是重中之重，信息系统中终端一旦不合规将产生不可预知的安全风险，正因如此，无论是国家法律法规，还是组织内部的规章指引，对于主机方面都具有明确的安全要求，本方案将通过全面部署应用终端检测与响应系统，对内部终端进行安全合规审查，依据等级保护的主机安全要求进行设计，对身份鉴别、访问控制、安全审计、入侵防范、恶意代码防范等策略进行合规性审查，满足南山区医疗集团总部建设等级保护系统的主机安全要求。

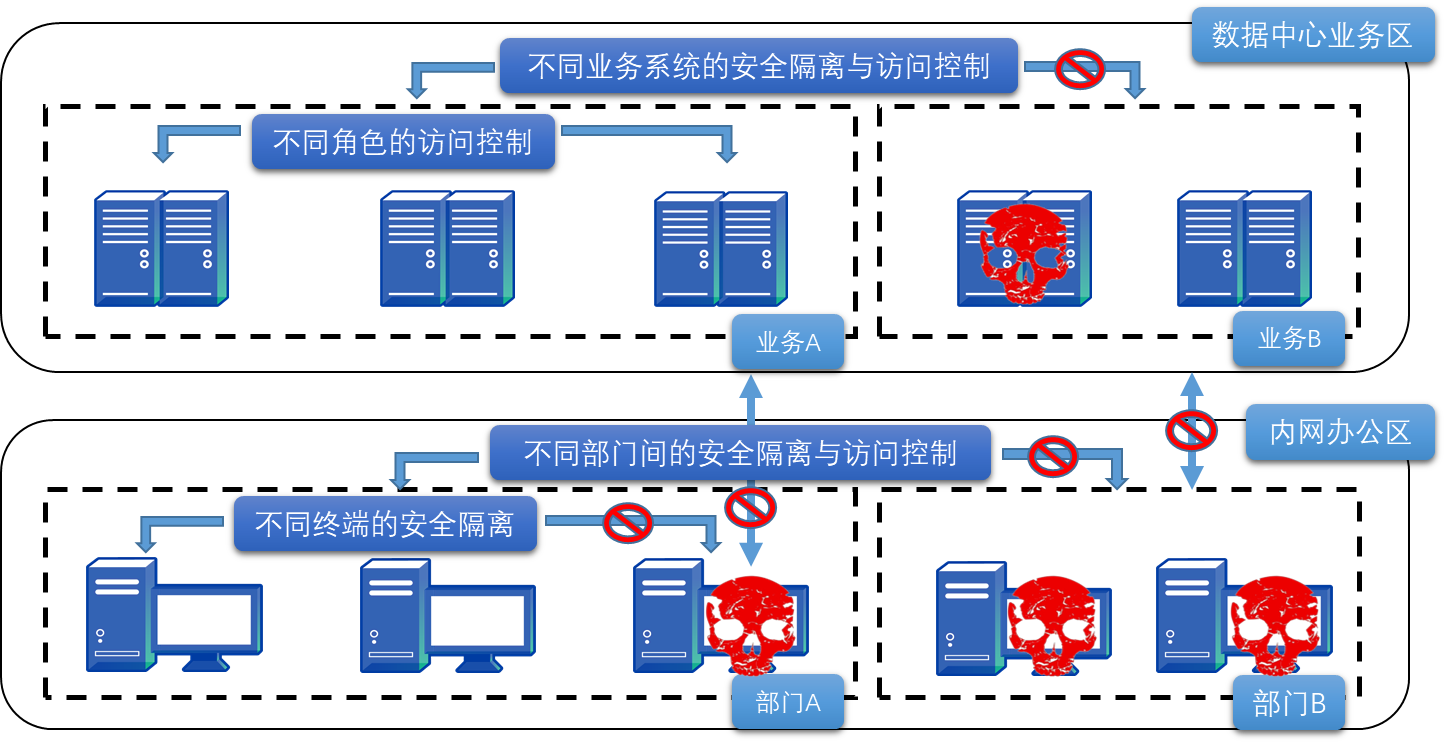
### 应用创新微隔离技术的动态防护体系

#### 创新微隔离技术

终端检测与响应系统微隔离方案提出了一种基于安全域应用角色之间的流量访问控制解决方法，系统可实现基于主机应用角色之间的访问控制，做到可视化的安全访问策略配置，简单高效地对应用服务之间访问进行隔离控制。优先对所有的服务器进行业务安全域的逻辑划域隔离，并对业务区域内的服务器提供的服务进行应用角色划分，对不同应用角色之间服务访问进行控制配置，减少了非法人员对物理、虚拟服务器攻击机会，集中统一管理服务器的访问控制策略。并且基于安装轻量级主机Agent软件的微隔离访问控制，不受虚拟化平台、物理机器和虚拟机器影响。另一方面，微隔离功能的应用，可在发生病毒感染情况下，将威胁放置在可控范围内，从而有效提升安全防护水平。

#### 终端间访问关系控制

在东西向访问关系控制上，优先对所有的服务器进行业务安全域的逻辑划域隔离，并对业务区域内的服务器提供的服务进行应用角色划分，对不同应用角色之间服务访问进行访问控制配置，减少了对物理、虚拟的服务器被攻击的机会，集中统一管理服务器的访问控制策略。并且基于安装轻量级主机 Agent 软件的访问控制，不受虚拟化平台的影响，不受物理机器和虚拟机器的影响。



通过全面部署应用终端检测与响应系统，可全面解决信息系统内部网络互访不可控问题，规范化主机、业务等网内不同对象的网络访问行为。

利用应用角色之间的主机流量访问控制的技术，提供对业务安全域之间、业务安全域内不同应用角色之间、业务安全域内相同应用角色之间的访问控制策略配置，提供简单可视化的安全访问策略配置，提高安全管理效率。

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 业务安全域 | 应用提供者 | 应用服务 | 应用使用者 | 策略动作 |
| 门户网站业务域 | WEB应用角色 | Apache（Http，80） | All | 允许 |
| 门户网站业务域 | DB应用角色 | MySQL（TCP，3306） | WEB应用角色 | 允许 |
| 门户网站业务域 | ALL | ALL | ALL | 拒绝 |
| OA业务域 | DB应用角色 | MySQL（TCP，3306） | 邮件应用角色 | 允许 |
| OA业务域 | ALL | ALL | ALL | 拒绝 |

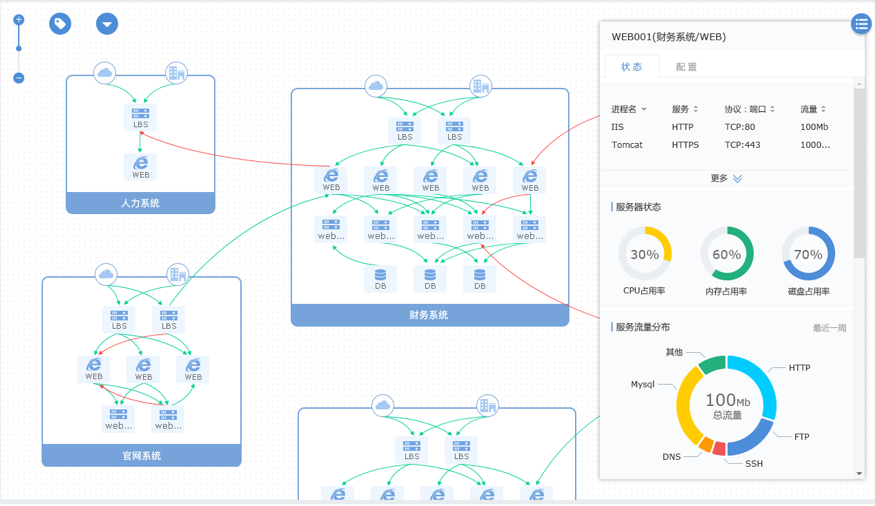
表4-1 微隔离角色访问控制

例如门户网站业务域的WEB应用角色服务器组提供Apache应用服务，策略动作允许门户网站业务域内所有主机的访问，而DB应用角色服务器组提供的MySQL应用服务，策略动作只允许门户网站业务域内的WEB应用角色服务器组的访问。

门户网站业务域内WEB应用角色之间的主机，由于没有访问需求，配置为隔离拒绝策略。

#### 终端访问关系可视化

在访问关系可视化中，采用统一管理的方式对终端的网络访问关系进行图形化展示，可以看到每个业务域内部各个终端的访问关系展示以及访问记录，也可以看到每个业务域之间的访问关系展示以及每个业务域的流量状态、访问趋势、流量排行，同时可以根据每个访问关系会生成访问关系控制策略，让用户决定是否启用该策略，减少了手动新增策略的工作量，提高了安全管理的效率



创新微隔离技术，有效应对高级威胁快速传播，将病毒遏制在指定范围之内，使信息系统环境可控性大大提高。

### 全网资产盘点

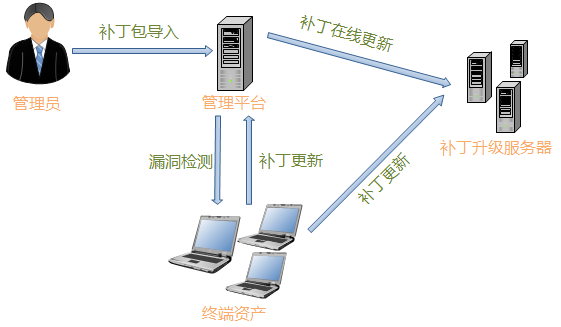


图4-3 全网资产管理

现信息系统中服务器、PC终端、应用等资产随着业务的增加而增加，资产的所有者与资产的关联关系不够清晰，安全责任难以落地。围绕资产的自身安全防护措施难以执行。对此，本方案将通过全面部署应用终端检测与响应系统，实现全网终端资产的全面管理功能，管理对象包含业务服务器主机和用户PC终端。盘点每台终端设备的名称、IP地址、MAC地址、所属组织、责任人、资产编号、资产位置等信息。使每台终端资产信息清晰展示，每个安全事件责任到人，从而将安全管理工作落实到位。

### 漏洞补丁管理

补丁检测极大地简化了管理员甄别终端资产漏洞的流程，终端检测与响应系统产品支持各种类型不同的操作系统以及不同版本的操作系统的补丁规则库的更新，可以做到最新漏洞的实时检测与防御，并提供了漏洞检测与处置的功能，可以指定不同的终端进行全部、高危或者指定漏洞的检测，得到每一台终端的全部漏洞信息，并且可指定漏洞进行修复或者忽略处理。终端根据最新的补丁规则库进行系统补丁检测，匹配来判断当前是否已经进行补丁的安装，同时终端支持多种方式来获取最新的补丁安装包，包括微软补丁服务器、官方补丁服务器、管理平台以及自定义服务器。保证在网络隔离环境下，终端也可以通过管理平台来进行补丁的升级。终端检测与响应系统产品的漏洞检测、补丁更新，大大提高了管理效率，增强了终端资产的安全性。



### 全网威胁定位

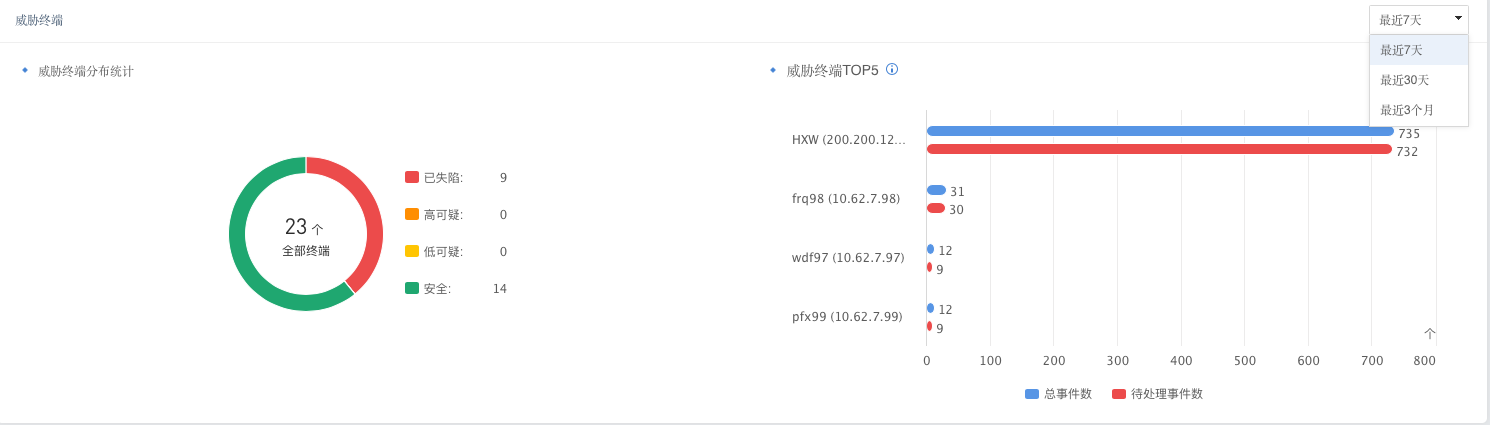
#### 内网威胁定位



终端概况



待处理高危事件



威胁终端



风险事件

#### 全网威胁定位

终端检测与响应系统，可提供全网威胁展示及定位功能，通过安全云脑的全球大数据安全分析，可将热点事件的IOC情报数据推送至终端检测与响应系统。终端检测与响应系统能根据IOC情报数据快速进行全网威胁定位分析，及时发现和响应最新的热点事件，该功能的有效应用，可实现快速定位网内威胁终端、同步处理、快速清除威胁等效果。

## 设备清单

|  |  |
| --- | --- |
| **设备名称** | **描述** |
| 终端检测与响应系统探针版 （XDR-软探针) | 包含1个控制中心+300个客户端（服务器探针版）软件及授权；控制中心含终端资产管理清点、终端基线检测、高级威胁行为检测、攻击可视化展示、威胁狩猎、级联管理、行为日志采集、安全日志采集等功能。 |
| 分布式XDR硬件平台 | 基于分布式架构，包含3节点，日志量/天：4亿，每节点硬件设备规格如下：2U，CPU：2颗Intel® Xeon® Silver 4210R 2.4G（10C），内存：4\*32GB DDR4 3200，系统盘：1\*240GB SATA SSD，缓存盘：无缓存盘，数据盘：选配，标配盘位数：12，电源：白金，冗余电源，接口：4千兆电口+2万兆光口。  含：高级漏洞管理、第三方日志分析、SOAR、云端威胁情报、安全事件深度挖掘XTH、移动运营小助手等模块；内置剧本交付服务；深度威胁狩猎服务(4次/年，共3年)；产品质保3年；软件升级3年 |