|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **采购项目** | **品名** | **技术参数** | **数量** | **品牌** | **质保** | **预算（万元）** | **报价（万元）** |
| 医疗核心数据库服务器 | 服务器 | 1、4颗20核处理器；  2、1024GB 内存；   1. 配置3\*960GB SSD盘，1\*raid卡； 2. 标配4端口千兆以太网卡和两块10GbE双光口以太网卡（含模块）； 3. 2\*32GB HBA卡（含模块）； 4. 配置冗余电源、风扇模块； | 2台 |  | 5年 | 21.76 |  |
| 光纤交换机 | 32Gb FC交换机-64端口(24端口激活,含24\*32Gb多模SFP,前出风)-双电源(交流)； | 2台 |  | 5年 | 22 |  |
| 存储 | 2U,双控, NVMe,512GB缓存，10\*3.84TB SSD NVMe硬盘，8\*1Gb ETH,8\*32Gb FC口(含多模SFP+)，含快照功能、克隆功能、重删压缩功能、CDP功能、双活、远程复制功能。 | 2台 |  | 5年 | 96.32 |  |
| 医学应用服务器(外网) | 服务器 | 1. 配置 CPU≥2 颗（CPU单颗核数≥24C、主频≥2.3GHz)； 2. 内存≥512GB DDR4 3200MT/s内存； 3. 配置2块480GB SSD； 4. 缓存盘≥1块3.2TB NVME PCI SSD； 5. 数据盘≥3块3.84TB NVME SSD U.2接口），单块盘（缓存盘及数据盘）IOPS≥ 1000k,顺序读写≥6.5G/s； 6. 4个千兆电接口，2块双口10GbE网卡，1块双口25GbE网卡（含4个10GbE多模光模块、2个25GB多模光模块； 7. 提供至少8块盘位U.2接口的硬盘背板）； 8. 国产品牌三年质保 | 3台 |  | 5年 | 30 |  |
| 交换机 | 48个25GE SFP28端口，6个100GE QSFP28端口，双电源，25G多模光模块10个，40G堆叠线1根，三年原厂质保 | 2台 |  | 5年 | 13.52 |  |
| 医学应用服务器(内网) | 服务器 | 1. 配置 CPU≥2 颗（CPU单颗核数≥24C、主频≥2.3GHz)； 2. 内存≥1TB DDR4 3200MT/s内存； 3. 配置2块480GB SSD； 4. 缓存盘≥2块3.2TB NVME PCI SSD； 5. 数据盘≥6块7.68TB NVME SSD U.2接口），单块盘（缓存盘及数据盘）IOPS≥ 1000k，顺序读写≥6.5G/s； 6. 4个千兆电接口，2块双口10GbE网卡，1块双口25GbE网卡（含4个10GbE多模光模块、2个25GB多模光模块； 7. 提供至少8块盘位U.2接口的硬盘背板）； 8. 国产品牌三年质保 | 5台 |  | 5年 | 72.5 |  |
| 交换机 | 48个25GE SFP28端口，6个100GE QSFP28端口，双电源，25G多模光模块10个，40G堆叠线1根，三年原厂质保 | 2台 |  | 5年 | 13.52 |  |
| 医学影像存储 | 存储服务器 | 配置四个分布式存储节点，每节点配置如下：   1. 配置两颗国产化处理器，单颗主频≥2.6GHz，单颗物理核数≥32核； 2. 256GB 内存； 3. 2\*480G SATA SSD硬盘，12\*16TB 7.2K RPM SATA HDD，1\*3.2T NVMe SSD; 4. 4\*1GE电口+4\*10GE光口(含光模块)； 5. 配置冗余电源和风扇并提供配套的电源线； 6. 配置768T文件存储标准版软件授权&3年订阅与保障年费； | 1套 |  | 5年 | 90 |  |
| 专用交换机 | 48\*10GE SFP+,6\*100GE QSFP28,双交流电源，12\*10G多模光模块；1\*40GE高速电缆； | 2台 |  | 5年 | 10.22 |  |
| 医疗数据上网行为管理 | 医疗数据上网行为管理 | 1、国产化芯片和操作系统，高度≥2U,包括1个串口、2个USB接口，千兆电口≥6个、千兆光口≥4个，含两对bypass电口、双电源,扩展槽位≥3个,带宽性能≥800M; 网络吞吐量≥10G; 最大并发连接数≥100W; 推荐用户数≥8000人; 内存≥32G； 日志存储硬盘≥4T；  2、含3年系统版本升级、URL库及应用特征库升级许可  3、支持路由模式，旁路模式、网桥模式、混合模式部署；切换部署模式无需重启，不影响设备正常使用。  4、支持即插即用功能。不管电脑的IP如何配置，开启即插即用功能后，只要插上网线，即可上网。  5、用户拥有多个网络区域访问权限时，可以实现用户在任意时刻只能访问一个网络，切换网络需要用户点击切换按钮，无需管理员干预，在不影响多网络使用的同时，实现网络逻辑隔离，加强网络访问安全。  6、可支持自定义≥7个网络区域。可支持根据域名划分网络区域。  7、支持通过资产扫描，对网络中的所有资产进行识别和分类。设备类型包括计算机、移动终端、网络设备、安全设备、办公设备、视频设备、物联网设备、存储设备等。  8、设备内存、cpu、会话、接口速率支持告警设置；支持时间告警，支持黑名单告警；支持违规网站、违规搜索、违规帖子、违规上传、违规邮件、还有潜在威胁的告警行为；告警策略要支持syslog、短信、邮件、日志记录，以及任意的方式组合。  9、支持url白名单，添加到白名单的url不受策略控制和审计。  10、支持ip、用户/用户组白名单，添加到白名单的IP不受策略控制和审计。白名单策略可实现基于时间段的控制。支持设置完全放通（不审计，不控制），或者审计但是不统计和控制流量。  11、支持防网络共享行为，针对私接路由器和非法无线热点行为进行识别和管控；检测方式包括但不限于UA识别、共享账号识别、虚拟身份识别、路由器识别、应用特征检测等。  12、支持阻拦终端用户的广告弹窗，至少支持WinRAR、快压、360安全卫士、360画报、金山毒霸、热点资讯、今日热点等广告弹窗。  13、为了日志安全性，设备必须支持独立硬盘存放审计日志，不能与审计系统共用硬盘。  14、支持所有访问的会话日志记录，包括：源IP、目的IP、协议类型、七层应用名称、源端口、目的端口、是否进行NAT转换(可显示转换后的IP和端口)、会话产生的时间和会话持续时间。  15、从整体网络的宏观角度展现网络使用概况、上网目的地分布、热门应用流量分布、网站类型分析、终端类型分析、在线人群趋势、违规行为统计等多维度全方位展现网络的使用综合态势，给网络管理提供依据。  16、支持检测网络中的失陷主机，并依据风险程度，区分出高风险主机和潜在风险主机。 | 1套 |  | 5年 | 8 |  |
| 医疗数据日志审计 | 医疗数据日志审计 | 1、国产化芯片和操作系统，高度≥2U，系统盘容量≥256G Msata，数据盘容量≥4T机械硬盘，千兆电口≥6个、千兆光口≥4个，万兆光口≥2个，冗余电源，扩展槽位≥2个，日志采集处理均值≥3000EPS。日志源授权≥50。  2、数据存储能力：压缩加密存储，压缩比不低10:1；日志存储不低于10000条/M ；支持百亿级数据交互式多条件查询，百亿级数据查询响应时间小于10s；  3、支持独立展示每个被采集源最近24小时的日志数量趋势，便于掌握设备的安全事件情况，支持独立展示每个设备日志的最新采集时间，便于了解设备日志的采集状态。  4、支持在日志查询结果上针对源IP、目的IP、操作、源端口、目的端口等字段一键快速统计，以饼图方式展示，对于源IP和目的IP（公网地址）还支持以中国地图、世界地图方式展示，在统计图上能够进行点击下钻查询对应条件的日志结果；支持基于时间轴展示日志数据分布，能够通过时间轴进行查询分析。  5支持展示日志查询情况，包括查询条件命中数、日志总量、查询耗时等信息。  6、支持根据设备重要程度设置独立设置每个被采集源的日志、报表数据存储时间为1个月、3个月、6个月和永久保存等参数。  7、支持基于时间轴展示告警数据分布，能够通过时间轴进行查询分析。  8、支持对重点日志源的关注设置，并可通过关注列表快速查看重点日志源的状态、当日日志量、采集日志总量、最近接收时间、业务组等基础信息。  9、系统内置上百种报表模版，支持自动实现智能报表创建，每添加一个日志源，系统自动分析日志源类型进行相应报表创建，无需人工干预，报表和资产一一对应。  10、系统具有防恶意暴力破解账号与口令功能，口令错误次数可设置，超过错误次数锁定，锁定时间可设置。支持将常用IP地址或IP地址网段标记为自定义名称，在日志查询界面可以在IP列中对应悬浮显示自定义名称。 | 1套 |  | 5年 | 8 |  |
| 医疗数据态势感知 | 医疗数据态势感知 | 1、平台：国产化芯片和操作系统，内存≥128GB DDR4 3200，系统盘≥240GB SATA SSD，数据盘≥32TB，电源：冗余电源，千兆电口≥4个,万兆光口≥2个。  2、支持态势大屏展示，包括全网态势、资产态势、漏洞态势、攻击态势、全域态势，支持大屏展示时间设置，支持态势大屏中相关信息下钻跳转到对应的详细页面；  3、支持查看漏洞概况、漏洞影响安全域数量、漏洞影响资产数量、漏洞影响业务系统数量、漏洞安全域漏洞排行、影响业务系统漏洞排行、影响资产漏洞排行、漏洞类型分布、漏洞级别对比、漏洞发现趋势等漏洞信息展示。  4、支持安全指数、全网资产概述、漏洞概况、防护设备日志监测概况、告警趋势、攻击趋势、告警统计、最新告警、威胁类型排行等内容的相关展示  5、支持以全球地图实时展示网络攻击态势，支持以不同颜色攻击线展示攻击过程，支持攻击源和攻击目的国家名称展示，支持攻击目的进行光晕显示  6、支持基于场景的安全策略响应编排，支持预案及案例两种场景类型，支持以列表形式展示预案信息，包括预案名称、预案类型、响应动作、关联案例数、来源、创建时间、描述；  7、支持对预案总数、被引用预案总数、未被引用预案总数进行统计；  8、支持对案例进行新增、删除、启用、停用等操作，并支持案例批量处理；  9、支持从告警维度查看案例对告警的响应处置详情，支持集中管控执行联动处置动作后下发给安全设备的策略管理。  10、支持工单管理，支持指派相关责任人进行处理，支持对工单进行分组管理，分组类型包括我的工单、待处置工单、已处置工单、历史工单；支持在我的工单分组中进行工单分派、取消、查看详情、查看流程图等操作，支持新建工单，包括工单名称、级别、派单人、业务流程、描述等信息，支持工单统计报表导出。  11、针对被保护网络中的安全事件进行线索追溯，对攻击对手、攻击方式、攻击路径、攻击源、攻击目标、攻击事件等进行拓展分析，通过数据融合、数据关联重新刻画安全事件。支持对追溯相关的安全事件的原始日志信息进行展示，支持对关联的安全事件进行列表展示。支持对追溯相关的安全事件的原始日志信息进行展示，支持对关联的安全事件进行列表展示，支持对源、目的地址攻击关系进行分析展示  12、支持资产外联分析，分析维度包括资产外联热力地图、外联资产排名TOP10、访问目的排名TOP10、外联趋势、外联事件列表，支持外联热力地图分析，支持源区域及目的区域按颜色区分展示，支持展示源目的区域间外联连接关系，支持外联热力地图区域缩放，支持对事件列表中的事件进行详情查看、关联日志检索、加入白名单及加入关注名单操作，支持按照目的地域、日志级别、应用协议、时间、日志类型、源地址、目的地址、目的端口进行过滤查询，支持重要资产快速外联分析统计，支持启用关注名单及访问时间段过滤设置。  13、支持从日志中发现威胁源，支持以列表形式展示威胁源相关信息，展示信息包括（区域）IP、威胁等级、影响资产、威胁类型、威胁数量、首次发现时间、最新发现时间、处置状态等，支持按照日期、IP、区域、威胁等级、威胁类型、关注名单匹配、是否命中情报、处置状态等条件进行过滤查询，支持威胁加入白名单、关注名单、加入威胁情报库、立即封堵等操作，支持与云端情报进行碰撞，支持按照TXT、CSV、EXCEL等格式进行威胁信息导出，支持影响资产、威胁类型、威胁数量等字段下钻，支持鼠标滑过处置状态悬浮显示封堵信息；  14、支持对日志的详情展示，支持日志的详情、溯源、附件、一键封堵、加入白名单、加入关注名单、封堵申请等操作  15、支持资产探测任务管理，支持任务添加、修改、删除、开始扫描、重新扫描等操作，支持任务列表展示，展示信息包括任务名称、扫描范围、类型、状态、更新时间等，扫描范围支持单个IP、IP段、子网范围，支持查看扫描结果，结果信息包括所属任务、设备名称、设备IP、MAC、操作系统、时间、端口服务。  16、支持对EDR的管控，支持EDR策略新建、删除、查看、编辑、下发、下发记录等，支持策略标签管理，策略内容包括名称、标签、设备类型、执行设备、策略分类、配置项类型、状态、源地址、源端口、目的地址、目的端口、终端地址。  17、安全技术体系建设支持查看纵深防御下的便捷防护设备、漏洞扫描设备、威胁检测设备、终端防护设备、安全审计设备数量，支持下钻查看详细每类设备的具体数量和设备作用，以及当前平台已处理该设备的日志数量，支持查看安全域的数量以及名称、攻击数、防护设备数。支持查看资产总数、防护设备总数。支持查看业务系统的数量以及名称、攻击数、防护设备数。  18、支持威胁情报管理，包括恶意IP地址、恶意URL、恶意样本、恶意域名、垃圾邮件等，支持情报进行分类自定义查询，支持自定义威胁情报信息，支持威胁情报的导入；  19、探针（内外网各一个）：国产化芯片和操作系统，威胁检测能力≥2Gbps，内存≥32G，硬盘容量≥4T，千兆电口≥6个、千兆光口≥4个，TCP最大并发连接数≥100W，冗余电源，扩展槽位≥4个。  20、支持固网恶意程序检测智慧引擎、移动恶意程序检测智慧引擎、DGA恶意域名检测智慧引擎、恶意TLS流量检测智慧引擎、SQL注入检测智慧引擎、XSS攻击检测智慧引擎、命令注入检测智慧引擎、HTTP隧道检测智慧引擎、WEBSHELL上传检测智慧引擎进行升级。  21、支持DDoS攻击事件分析，按照时间范围综合分析DDoS攻击类型分布、被攻击IP Top10、被攻击IP排名、被攻击IP流量排名等信息。  22、支持对攻击逃逸报文进行深度智能检测，包括：IP分片、TCP分段、RPC分片分段、SMB分片分段、HTTP-Header折叠、HTTP-Body UTF-7编码、HTTP-Body UTF-16（LE/BE）编码、HTTP-Body UTF-32（LE/BE）编码、HTTP-Body压缩、HTTP-Post数据编码、邮件体编码、URL多重编码、URL斜线分隔符、URI相对目录欺骗、HTTP-Javascript编码、邮件头折叠等类型。  23、支持独立的僵尸主机检测引擎，涵盖11000种以上的僵尸主机规则库。规则库支持按照攻击类型、操作系统、风险等级、ATT&CK、攻击阶段等方式进行分类。支持能够检测包括：僵尸网络、木马控制、蠕虫、挖矿、勒索、移动端木马控制、APT等多类型的僵尸主机行为。  24、支持文件还原捕获，可自定义捕获文件大小，最大支持还原100M大小的文件。捕获文件类型包含恶意文件、疑似恶意文件、无风险文件。  25、支持注入和WEBSHELL攻击检测，包括：SQL语法分析引擎检测、SQL注入智慧引擎检测、XSS攻击智慧引擎检测、命令注入智慧引擎检测、WEBSHELL上传智慧引擎检测、WEBSHELL行为检测。  26、支持取证功能，取证类型包括：PCAP取证、样本取证两种形式，PCAP取证文件支持在线预览。  27、支持恶意加密流量检测，采用恶意TLS流量智慧引擎、异常握手、非法证书和内网流量检测恶意加密流量。  28、具备独立威胁情报库，包括：木马程序、病毒程序、僵尸网络、APT攻击等30余种情报标签，威胁情报库数量超过800万。 | 1套 |  | 5年 | 37 |  |