信息安全设备技术参数

为进一步加强信息安全管理，提高我院信息安全保障能力，结合信息系统进行信息安全等级保护测评要求，需要采购一批信息安全设备项目，该项目包含：综合日志审计平台、主机安全及管理系统、态势感知平台、数据库审计与风险控制系统、网闸、IT智能监控软件、防火墙和准入系统。

一、采购内容：

| **序号** | **产品名称** | **型号（模块）** | **质保期** | **数量** | **单位** |
| --- | --- | --- | --- | --- | --- |
| 1 | 数据库审计与风险控制系统软件（防统方）（含三层审计） | 防统方 | 3年 | 1 | 台 |
| 2 | 主机安全及管理系统软件 | 管理中心软件 | 3年 | 1 | 套 |
| 终端安全管理软件-PC  | 3年 | 2100 | 套 |
| 终端安全管理软件-SERVER | 3年 | 350 | 套 |
| 3 | 综合日志审计平台 |  | 3年 | 1 | 台 |
| 4 | 准入系统 | 准入子节点 | 3年 | 2 | 套 |
| 准入管理平台 | 3年 | 1 | 套 |
| 5 | 外网出口防火墙（含VPN） |  | 3年 | 1 | 台 |
| 6 | 专网出口防火墙 |  | 3年 | 1 | 台 |
| 7 | 态势感知平台 | 安全管理平台 | 3年 | 1 | 台 |
| 综合威胁探针系统（2G） | 3年 | 1 | 台 |
| 综合威胁探针系统（1G） | 3年 | 1 | 台 |
| 8 | 网闸 |  | 3年 | 2 | 台 |
| 9 | IT智能监控软件 | 　 | 1年 | 1 | 套 |

二、配置要求：

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **序号** | **产品名称** | **型号（模块）** | **具体配置** | **数量** | **单位** |
| 1 | 数据库审计与风险控制系统软件（防统方）（含三层审计） | 防统方 | 总网络吞吐量：4000Mbps双向审计最大数据库流量：400Mbps峰值事务处理能力TPS：40000条/秒日志数量存储：20亿条支持三层审计功能功能描述：全功能开放数据库实例授权许可数量：25个硬件是否可扩容：是硬件类型：工控机硬件尺寸：标准2UCPU规格：4核内存容量：8GB\*4硬盘容量：4TB\*4（Raid 1）硬盘接口：企业级SATA网口：1管理口+1HA口+8审计口（4个千兆电+4个千兆光）网口类型：1000M电口\*6，1000M光口\*4（多模，标配2个SFP模块、3米LC-LC跳线2根）电源配置；双电源空余拓展板卡位：3个  | 1 | 套 |
| 2 | 主机安全及管理系统软件 | 管理中心软件 | 包含终端管理中心软件一套实现对终端的统一管理和策略下发 | 1 | 套 |
| 终端安全管理软件-PC  | 适用于Windows PC防护支持Windows XP、Windows 7、Windows 8、Windows 10等操作系统 | 2100 | 套 |
| 终端安全管理软件-SERVER | 适用于各类型服务器防护支持Windows server 2003、Windows server 2008、Windows server 2012、Windows server 2016、Centos 5.0 +、Redhat 5.0 + 、Suse11 +、 Ubuntu 14 +等操作系统 | 350 | 套 |
| 3 | 综合日志审计平台 |  | 硬件外形：软硬一体化2U标准机架式设备； 网口：8个工作管理口（千兆电口）内存：64GB磁盘：4T\*4 raid5（支持raid1、raid5）日志处理能力EPS：10000/秒 （峰值：14000/秒）双电源500个日志源 | 1 | 套 |
| 4 |  准入系统 | 准入子节点 | 1）硬件规格：硬件服务器品牌工控机、规格2U、CPU4核4线程、内存16G、硬盘2T、6千兆电口。2）最大支持5000台无代理软件设备安全管理（支持瘦终端、IoT设备、ICS设备）；3）支持策略路由、旁路干扰、Cisco EOU等多种准入控制方式，自带RAIUS服务；4）支持系统内置帐号认证、AD/LDAP帐号认证、邮件帐号认证等多种身份认证方式；5）支持入网安全状态检查、网络访问权限控制、仿冒发现控制、违规外联发现控制、访客外协准入管理等；6）提供三年维保服务 | 2 | 套 |
| 准入管理平台 | 1)终端准入有代理版本硬件中心；2)支持入网安全状态检查、网络访问权限控制、仿冒发现控制、违规外联发现控制、访客外协准入管理等；3）支持802.1x、策略路由、旁路干扰、Cisco EOU等多种准入控制方式，自带RAIUS服务；4)支持系统内置帐号认证、AD/LDAP帐号认证、邮件帐号认证等多种身份认证方式；5）硬件规格：硬件服务器品牌工控机、规格2U、CPU6核12线程、8G\*4内存、硬盘2T、6个千兆电口6）提供三年维保服务 | 1 | 套 |
| 5 | 外网出口防火墙（含VPN） |  | 2U，含交流冗余电源模块，2\*USB接口，1\*RJ45串口，2\*RJ45管理口，8个接口扩展槽位，4个千兆SFP插槽，12个10/100/1000M电口，含SSL VPN、传统防火墙、流量管理、应用管理、IPSec VPN、资产识别功能、一体化防护；由工程师提供上门产品安装、调试，三年原厂服务，包含产品系统升级授权、产品保修服务、远程支持服务。 | 1 | 套 |
| 6 | 专网出口防火墙 |  | 2U，含交流冗余电源模块，2\*USB接口，1\*RJ45串口，2\*RJ45管理口，8个接口扩展槽位，4个千兆SFP插槽，12个10/100/1000M电口，含传统防火墙、流量管理、应用管理、IPSec VPN、资产识别功能、一体化防护；由工程师提供上门产品安装、调试，三年原厂服务，包含产品系统升级授权、产品保修服务、远程支持服务。 | 1 | 套 |
| 7 | 态势感知平台 | 安全管理平台 |  | 2U，2\*CPU（10核），128G内存，256G SSD系统盘，4\*8TB SATA硬盘，2个千兆电口，4个接口扩展槽位，含交流冗余电源模块；绿盟安全管理平台具备日志威胁管理、全流量威胁管理、脆弱性管理、网站安全检测、一键响应、态势感知等功能，提供场景模型升级服务，威胁情报服务。由工程师提供上门产品安装、调试，三年原厂服务，包含产品系统升级授权、产品保修服务、远程支持服务。 | 1 | 套 |
| 综合威胁探针系统（2G） |  | 2U,交流冗余\8G CF卡\6T硬盘\Intel C236\CPU\*1 Intel I7-7700 3.6GHz\16G(DDR4 2133U 8G\*2)\USB口\*2\RJ45串口\*1\千兆电口\*2 Intel I210\3.5寸热插拔硬盘位\*1\四个网络扩展槽，2个万兆SFPP插槽，4个10/100/1000M电口。支持2G吞吐（网络层），包含流量采集、元数据提取、存储等功能。由工程师提供上门产品安装、调试，三年原厂服务，包含产品系统升级授权、产品保修服务、远程支持服务。 | 1 | 套 |
| 综合威胁探针系统（1G） |  | 51B1B平台\1U\交流冗余\intel C3000\64 SSD\1T硬盘\CPU \*1 Atom C3758 2.20GHz 8C\16G (DDR4 2666 8G\*2)\USB2.0\*2\RJ45串口\*1\管理网口\*1(I211)\千兆光口\*4(I350A),千兆电口\*6(1543\*1,I350A\*1,三组bypass)\1个网络扩展\1G吞吐（应用层），包含流量采集、元数据提取、存储、恶意文件检测、入侵行为检测、WEB应用检测等功能。由工程师提供上门产品安装、调试，三年原厂服务，包含产品系统升级授权、产品保修服务、远程支持服务。 | 1 | 套 |
| 8 | 网闸 |  | SIESNX3-5000A采用双主机架构，内外网各6个千兆电口，内外各2个扩展插槽，2个RJ45串口和4个USB3.0口，2U机箱，冗余电源，9Gbps吞吐量，含全部功能模块，4个万兆光口接口扩展卡，4个千兆光口接口扩展卡，8个千兆光口接口扩展卡。由工程师提供上门产品安装、调试，三年原厂服务，包含产品系统升级授权、产品保修服务、远程支持服务。 | 2 | 套 |

9. IT智能监控软件

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **模块名称** | **功能点** | **功能说明** | **数量** | **单位** |
| 云融合框架 | CentOS系统平台 | 支持在CentOS系统X86平台上安装部署，支持易用的一键式安装模式。提供多服务器扩展能力，LCN注册服务，统一文档等系统级服务。提供数据备份还原、补丁安装、问题上报等系统维护功能。保障应用服务的无缝扩展和集成运行。用户管理，权限管理等 | 1 | 项 |
| 采控中台 | 采控中台（2000节点版） | 提供监控对象的建模能力，监控对象的采集规则管理，监控对象指标数据的存储管理。不包含IP示意节点的最大处理能力为2000节点。缺省内置1个本地采集器。含50基础资源节点。 | **1** |
| 基础资源节点授权（25节点包） | 包含网络设备（包含无线AC）、操作系统、数据库、Oracle-rac（clusterware)、中间件、标准应用、虚拟化宿主机的节点授权。支持25个上述任一种节点的数据采集管理。 | 16 |
| 存储节点包授权（5节点包） | 包含存储设备（磁盘阵列，光纤交换机，磁带库）的节点授权。 | 5 |
| 虚拟机节点包授权（50节点包） | 包含各类虚机的（Vsphere，KVM，Xensever，fusionComputer）的节点包授权 | 8 |
| 通知管理 | 多方式通知能力 | 提供http、数据库、短信、邮件4种通知方式，以模板化方式进行配置前端使用相关参数，便于快速实现客户现场的通知通道的部署。 | 1 |
| 统一CMDB | 统一CMDB | 提供模型管理能力，包括监控、视频、物联网以及资产四类模型。支持查看配置项（即CI）及其关系，并允许用户以配置项属性为条件创建资源组。 | 1 |
| 告警管理 | 告警管理 | 提供阈值事件，IP地址事件，syslog，trap事件设置告警规则。允许根据事件触发通知，和智维场景实现告警的快速处置。提供当前告警的统一查看，并允许对于历史告警的多条件查询，快速定位到历史告警。提供按照发生对象、指标、规则进行归类分析，实现故障频发现象的分析总结。提供告警异常调用中台通知服务实现告警的即时通知。 | 1 |
| DIYOPS场景管理 | DIYOPS场景管理 | 用户可以基于自然语言，以图形拖拽的方式，自定义探索并编排个性化的运维场景，自助实现运维线下工作线上化。功能包括场景编排、场景调试、场景执行、场景联动等。 | 1 |
| 监控管理 | 操作系统管理 | 支持对于windows、linux、hp unix、Aix、solaris类型操作系统的管理，实现主机状态的集中查看和单个设备查看结合的管理，支持对于基本信息、运行状态、硬件状态、运行内容的一体化管理，购买本模板赠送系统拓扑视图模块； | 1 |
| 标准服务组件管理 | 提供数据库、中间件、标准应用单实例的管理，实现状态、性能、相关进程的一体化管理，购买本模板赠送系统拓扑视图模块。 | 1 |
| 网络拓扑管理 | 提供对网络设备拓扑关系展现、设备性能、设备状态的实时展现和监控。 | 1 |
| Vsphere虚拟化管理 | 提供对于vSphere虚拟化环境的监控，以虚拟拓扑图为基础，提供宿主机、虚拟机的配置、状态、性能的一体化展现，支持CPU、内存、数据存储的使用、预防、回收方面的分析和建议，为虚拟性能进行使用分析，并提供改进建议。 | 1 |
| 存储管理 | 提供支持存储设备（磁盘阵列、光纤交换机）的设备状态、性能管理，以及各个磁盘、控制器的状态监管； | 1 |
| 自定义指标 | 支持通过（SNMP、SSH、SQL）方式扩展用户专有设备和指标，相关指标可在告警，个性首页，历史记录，业务视图中进行管理使用。 | 1 |
| 智能巡检管理 | 提供日、周、月、季、年多种周期的巡检任务的设定，系统可以根据既定周期进行巡检任务的自动执行；并可生成巡检报告统计； | 1 |
| 报表管理 | 报表管理与数据分析 | 提供各类管理对象1年数据无压缩存储和查询能力，通过简单设置可实现不同管理域的个性化报表，同时可提供日周月季年多个统计周期的报表，为动态数据提供有效的分析方法。 提供基础报表模板，包括：可用率分析模板、性能负载模板、告警统计模板、容量分析模板。 | 1 |
| 安全服务 | 安全服务 | 要求每年四次巡检服务及一次漏扫服务；协助院方参与等保测评相关活动；院方有相关信息安全问题我方15分钟内电话响应并2小时内到达客户现场，帮助协调并配合院方解决信息安全方面的问题。 | 1 | 套 |

三、其他

1.交付时间：

1.1、交付工期：合同签定后2个月内安装调试完成。

1.2、交付地点：医院指定地点。

1.3、实施进度：按照医院进度要求完成安装和调试，如在规定的时间内由于卖方的原因不能完成实施，投标方应承担由此给用户造成的损失。

1.4、实施标准：符合我国国家有关技术规范要求和技术标准。

1.5、实施过程中发生的费用由投标方负责。

2.售后服务：

2.1、投标方应在投标文件中说明在保修期内提供的服务计划，维护范围包括（包括但不限于）软、硬件安装，调试、维修，接口、集成等内容。

2.2、在系统的服务期内，投标方应确保系统的正常使用。在接到用户服务要求后应立即做出回应，并在承诺的服务时间内实施服务。

2.3、投标人有良好的售后服务能力，需提供全年7天24小时服务（电话、远程或现场），并在接到招标人通知后15分钟内电话响应并2小时内到达客户现场。项目验收合格后，每年不低于4次的例行维护及巡检。

3.培训要求：

3.1、中标人负责所供设备、软件的安装、调试及上线，招标单位予以配合。设备、软件的安装、调试所需的工具、仪表及安装材料等应由投标人自行解决。

3.2、培训：根据医院的情况制定相关培训方案，所有的培训费用必须计入投标总价。