**信息类（设备）项目技术需求表**

项目名称：**江北区中医院等保建设项目采购**

项目编号：**202203dbjs**

交货周期：合同签定之日起15日内

1. **项目需求清单一览表**

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **产品名称** | **数量/单位** | **限价（元）** |
| 1 | 日志审计系统 | 1套 | 156000.00 |
| 2 | 数据库审计系统 | 1套 | 158000.00 |
| 3 | 阿里云安全等保 | 1年 | 120000.00 |
| 4 | 等保服务 | 1年 | 25000.00 |

1. **项目技术需求**
	1. **总体要求**

1.本次项目设备用于江北区中医院网络安全等级保护2.0三级等保项目建设。所有产品应符合等保2.0三级技术要求。

2.投标人需对招标参数逐一应答；需提供证明材料的，请在技术偏离表内说明相应材料对应的准确页码。

3.投标人需完成合同设备的上架、安装调试、线缆连接、业务测试、交付验收、三年保修及售后服务等一系列工作。

4. 投标人除完成招标设备的安装调试外，还需配合完成等保评测过程涉及的整改工作，包含但不仅限于网络设备调试、补丁修复、策略优化、安全加固、制度规范等相关工作。

5．投标人需具备等保安全设备的备品备件，等保评测过程中中标人需配合招标人准备相应备品备件，备品备件包含但不仅限于防火墙、入侵防御、Web应用防火墙、交换机、漏洞扫描设备。

6．优先选择综合技术实力强的供应商；投标人投标时请提供公司资质及项目实施人员资质证书复印件。

* 1. **详细技术参数表**

| **序号** | **名称** | **参数要求** | **数量** |
| --- | --- | --- | --- |
| 1 | 日志审计系统 | ★1、标准2U机架式软硬一体化设备，能独立完成审计日志采集，双电源。含1个千兆电管理口，1个千兆电HA口，≥4个千兆电业务口，≥4个SFP千兆光业务口；内存≥16GB，磁盘≥4T\*4（raid5）。支持磁盘扩展，支持HBA卡扩展，支持扩展万兆光口，扩展插槽≥3个。★2、日志处理能力（每秒日志解析能力EPS）≥12000EPS，日志峰值处理能力（每秒日志解析能力EPS）≥16000EPS，配置资产授权数量≥200个。3、支持Syslog、SNMP Trap、HTTP、ODBC/JDBC、WMI、FTP、SFTP协议日志收集；支持使用代理(Agent)方式提取日志并收集；支持常见的虚拟机环境日志收集，包括Xen、VMWare、Hyper-V等。4、支持目前主流厂商的网络安全设备、交换设备、路由设备、操作系统、应用系统等日志收集。厂家包括但不限于：Cisco(思科)、Juniper、网御、F5、华为、H3C、微软、绿盟、飞塔(Fortinet)、Foundry、天融信、启明星辰、天网、趋势、东软、Nokia、CheckPoint、Hillstone(山石)、安恒信息、珠海伟思、BEA、中国电信、安氏、帕拉迪、戴尔（Dell）、IBM、Citrix(思杰)、Watchguard、中兴、阿帕奇、Windows系统日志、Linux/UNIX syslog、IIS、Apache等。5、支持三维关联分析；通过资产、安全知识库、弱点库三个维度分析事件是否存在威胁，并形成关联事件，需提供公安部、国家保密局或ISCCC其中一家的检测报告关键页证明。6、支持通过在目标主机上安装Agent程序，支持监测目标主机的CPU利用率、内存使用率、磁盘使用率、磁盘使用情况、流量等信息，需提供公安部、国家保密局或ISCCC其中一家的检测报告关键页证明。7、用户支持双因子认证登录，双因子认证令牌支持绑定至具体用户。8、支持按照实际的用户环境进行编辑发布并可以和资产进行绑定。拓扑可以显示资产采集的事件数量被采集资产的状态等信息，需提供公安部、国家保密局或ISCCC其中一家的检测报告关键页证明。9、支持磁盘空间阈值告警，当磁盘使用率达到设定的阈值时可产生并外发告警。10、内置合规性报表1000+种；内置SOX、ISO27001、WEB安全等解决方案包；内置完善的等级保护合规报表。11、产品资质：产品需具备公安部颁发的《计算机信息系统安全专用产品销售许可证（日志审计-三级）》，产品具备《IPv6 Ready Logo认证证书》。（提供以上证书复印件并加盖制造商公章） | 1套 |
| 2 | 数据库审计系统 | 1、★机架式专用设备，带外管理口≥1个，HA口≥1个，千兆电接口≥6个，千兆SFP接口插槽≥4个，接口扩展槽≥2个，RJ45串口≥1个，硬盘≥4T，存储空间≥2T，双电源。被审计数据库服务数≥50个，可扩充。三年原厂质保和服务。2、★审计系统审计事件每秒入库速度≥32000条/秒，日处理事件数≥12000万条3、★支持Oracle、SQL-Server、DB2、Informix、Sybase、MySQL、PostgreSQL、Teradata、Cache数据库审计。4、支持对Oracle数据库状态的自动监控，可监控会话数、连接进程、CPU和内存占用率等信息。5、★支持国产数据库人大金仓、达梦、南大通用、神通数据库的审计。支持MongoDB数据库的审计。6、 支持自动建立数据库操作行为基线。7、 数据库操作行为基线包括数据库账号、操作类型（SQL模板）等行为特征。8、 对超出数据库操作行为基线的操作可自动识别，并及时告警9、★可审计记录FTP、邮件、HTTP、HTTPS、SCP、SFTP等方式传输的文件（包括文本、Word、Excel等格式），并且可对审计到的文件进行查询和下载。10、支持文件内容关键字审计，当网络中传输的文件包含关键字时，可进行告警，对于压缩包中包含关键字的文件可准确定位压缩包中路径。11、★支持用户操作轨迹图展示，轨迹图维度可根据资源账号、源ip、客户端程序名、命令、表名、错误码等按需定义，可根据昨天、最近七天、最近30天以及自定义时间进行轨迹显示，可显示下一节点数量，可在某一维度中进行筛选。12、支持将查询条件保存为固定模板，方便后续查询时使用，支持模板管理，可对已有查询模板进行查询和删除。13、★支持自定义报表模板，包括数据集、图表设计、数据设计等，数据设计可根据不同数据集提供不同的分析维度和指标供用户进行选择。14、产品资质：具有《计算机信息系统安全专用产品销售许可证》；提供证书复印件并加盖投标人公章。 | 1套 |
| 3 | 阿里云安全等保(云服务) | 本项目在阿里云有多台ECS主机，需购买阿里云等保2.0三级基础套餐。包含云防火墙、Web应用防火墙、云安全中心、堡垒机组件。 | 1年 |
| 4 | 等保服务 | 根据等保2.0三级标准，帮助院方建立相应文档，处理相应bug和修正网络结构，配合院方完成等保测评和整改。 | 1年 |

注意事项：带★为必须响应条件，如有缺失，将按无效响应处理。