附件：询价项目技术规格及要求

1. 规格及要求

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **序号** | **名称** | | **技术要求** | **规格型号** | **品牌** | **单位** | **数量** | **价格** |
| 1 | 态势感知 | 态势感知平台 | 1.标准1U机架式设备，冗余电源，专用千兆硬件平台和安全操作系统。  2.网络接口不少于6个千兆电口，1个管理口，2个USB接口，2个接口可扩展插槽，存储容量2TB。  3.包含系统平台框架、资产管理、安全事件管理、基础关联分析、标准脆弱性管理、风险评估、首页、标准的报表模块、标准的响应管理模块、权限管理、知识管理、系统自身管理、内置1个本地事件采集器，还包括工作台管理模块、增强关联分析模块。  4.提供三年硬件质保期，50个管理对象授权。 |  |  | 台 | 1 |  |
| 检测探针 | 1.标准1U机架式设备，单电源。  2.网络接口不少于6个千兆电口，2个千兆光口，1个RJ-个 Console口，2个USB口，1个扩展插槽。  3.网络吞吐量不少于1G，并发连接数不少于300万，新建请求数不少于2万。  4.提供三年硬件质保期，威胁情报升级授权和三年特征库升级授权。 |  |  | 台 | 2 |  |
| 2 | 自动数据采集一体机 | | CPU:10核以上 内存：16G以上 硬盘：2块600G硬盘以上 网卡：2\*GE+2\*10GE |  |  | 台 | 1 |  |
| 采用主动接入方式主动从医院提供的数据源获取医疗卫生机构业务数据，能够支持多种抽取途径，包括数据库、Web服务接口、文件（XML、CSV、Excel等）、技术接口等，支持中联、东软、金仕达等主流厂商业务数据库，包括Oracle、Mysql、SQL Server等，支持异构数据库间的数据集成与协同。 |  |  |
| 提供多种抽取方式，包括定时抽取、实时抽取、全量抽取、增量抽取等，能够满足平台业务系统对数据的各种展示要求。 |  |  |
| 按平台标准完成数据转换功能，提供字典值域映射工具，支持智能匹配及人工调整确认双重映射方法，简化映射复杂性，提升实施效率；支持默认值填充，可自定义默认值内容；支持函数转换，可根据业务需要自定义转换规则，能够实现数据过滤、数据清洗、数据替换、数据计算、数据验证、数据加解密、数据合并、数据拆分、数据裁剪、数据追加、数据丰富等功能。 |  |  |
| 支持字典值域自学习功能，能够支持新增值域的自动识别。 |  |  |
| 支持标准导入功能，导入文本类型包括Excel、XML；支持以SQL方式由数据库导入数据标准。 |  |  |
| 提供标准更新功能，可灵活替换转换标准与校验标准，有效同步平台的标准变更；支持整体/单条标准删除与更新。 |  |  |
| 提供数据检验功能，提供字段级合理性校验及业务级合法性校验，对校验失败的数据，需支持生成校验报告，同时上报给中心平台，反馈给业务机构。 |  |  |
| 与平台无缝对接，支持JMS/MQ、WebService、FTP等多种方式；提供多种上传策略配置； |  |  |
| 提供灵活的上传时间间隔配置界面，能够实现医院业务数据快速上报至平台。 |  |  |
| 3 | web防火墙 | | 标准机架设备，配备≥8个千兆电口（至少包含1对bypass）；配备独立的1个CON口，2个USB3.0口,1个千兆管理电口；配备≥480G SSD硬盘；  HTTP应用吞吐≥2.2Gbps，HTTP并发数≥20万；防护站点数量≥8个；  提供三年WAF规则库授权和升级服务。 |  |  | 台 | 1 |  |
| 4 | 漏洞扫描 | | 标准1U，交流单电源，1\*RJ45串口，1\*GE管理口，6个10M/100M/1000M自适应以太网电口扫描口，提供512个IP授权。最大并发扫描60个主机，最大扫描速度1000 ip/h，最大并发任务数为10。 |  |  | 台 | 1 |  |
| 5 | 安全服务 | | 提供网络安全应急响应服务，在发生安全事件时提供现场/远程技术支持，面向已发生安全事件的事中、事后的取证、分析及提供处置、解决方案、建议等工作；配合院方应急演练 |  |  | 项 | 1 |  |
| 每月进行安全漏洞扫描，扫描范围包括所有服务器、安全设备、专用设备等，后续进行漏洞修复；一年提供不少于6次上门巡检，出具安全健康报告 |  |  |
| 运维服务期间，如上级部门、公安部门、信息化主管部门等单位对医院资产进行安全扫描，根据安全评估结果，协助修复安全漏洞、加固系统平台 |  |  |
| 针对范围内主机提供基线安全加固服务，遵循基线安全加固技术标准对授权的设备进行基线安全加固。使服务器具有基本的安全防护能力，能抵御对操作系统的直接攻击，能在发生攻击时限制影响范围 |  |  |
| 提供日常培训、安全问题咨询、网络安全规划、等级保护咨询服务 |  |  |
| 针对新信息系统进行上线和重要调整前开展安全评估服务。通过人员访谈、漏洞扫描等方式对新上线业务系统进行安全评估，确认是否存在操作系统、数据库、应用弱密码、安全漏洞等 |  |  |
| 对应用系统进行非破坏性质的模拟入侵者攻击的测试，检测外部和内部威胁源和路径，以便掌握系统的安全状况，寻找系统存在的漏洞和风险 |  |  |
| 1年驻场服务，按甲方工作时间上班，每天对安全设备健康巡检以及总结汇报；提供重要时刻专人值守 |  |  |
| 6 | 网闸 | | 1.标准1U机架式设备，单电源；  2.软件系统：设备管理配置功能和定制访问功能；  3.内网接口标配4个千兆电口，1个千兆管理接口，1个千兆 HA接口（双机热备口）；外网接口标配4个千兆电口，1个千兆管理接口，1个千兆 HA接口（双机热备口）  4.开通全功能模块，强制访问控制、文件交换、文件快递、数据库同步、数据库传输、邮件传输、安全浏览、工业控制传输、工业数采、视频传输、入侵检测、抗Ddos攻击等功能。  5.提供三年硬件质保和三年全功能模块升级授权。 |  |  | 项 | 1 |  |