防统方

|  |  |  |
| --- | --- | --- |
| **技术参数要求** | | |
| 序号 | 指标名称 | 技术参数 |
| **1** | **系统要求** | 1）要求为一个采集、管理、存储一体化软硬件专用设备，无需用户另行提供额外服务器、操作系统、数据库、防火墙、日志系统等；  ★2）内置≥4TB磁盘存储空间，至少可保存3年以上数据并支持实时查询，吞吐量≥2Gbps，业务端口≥4千兆电口和≥4个千兆光口，支持外部网络储存功能，峰值处理能力不低于25000条语句/秒  ★3）设备支持LCD，通过LCD显示设备自身信息。，通过操作按键可以配置设备基本信息（如IP地址、网关等）。  4）支持设备集群化部署，可通过集群中单独某一台设备查看集群中其他设备的审计与告警信息  ★5）设备具备旁路部署模式，设备部署不影响原有网络结构。产品本身故障不影响被审计系统的正常运行，不得在现有服务器上安装可能带来风险的程序。。  6）管理方式：B/S |
| **2** | **功能要求** | ★1）全面支持Oracle、sqlserver、DB2、MySQL、后关系型数据库Cache等数据库审计分析。具备数据库操作记录分析、审计等功能。支持对服务器端、客户端信息的审计，包括IP地址、端口、MAC地址。审计信息包括但不限于：语句执行的时间、主机名、操作系统用户名、客户端IP、MAC地址以及SQL语句等信息，对数据库操作进行审计，可对增删改查等行为进行追溯。（须提供真实操作视频证明以及截图并加盖原厂公章）。  2）系统界面可显示所支持的Cache和iMedical版本信息（要求支持此两系统高于医院使用版本）（须提供真实操作视频证明以及截图并加盖原厂公章）。  ★3）考虑到整体系统的兼容性，保障院方信息系统稳定运行，须提供所投防统方系统与院方使用相同厂家即东华医为科技有限公司的HIS系统相互兼容认证证明  ★4）所投防统方系统如遇到与院方现有业务系统或数据库（当前使用版本和未来更新的版本）兼容对接问题，涉及接口服务费用由防统方系统产品厂商承担。（需要防统方系统产品厂商提供承诺书，加盖公章）  5）要求所投防统方系统支持Cache和iMedical当前最新版本（IRISHealth2021和iMedical8.5.2）的审计（提供系统录屏视频证明），并提供当Cache和iMedical升级后防统方系统不晚于一周的同步升级支持服务承诺。（投标人须提供原厂商承诺书，并加盖公章） |
| ★6）能够支持针对纪委、监察室、行风办等相关人员使用的防统方页面，用户使用该功能能够对告警行为进行集中化处理与显示（须提供真实操作视频证明以及截图并加盖原厂公章）。 |
| 3）支持对东华HIS系统、Cache SuperServer端口、Telnet、Cache PORTAL、FTP等信息的采集和审计。 |
| 4）支持对客户端信息的审计，包括IP地址、MAC地址、端口、发生时间、客户端程序；支持对服务器端信息的审计，包括IP地址、端口、发生时间、MAC地址 |
| 5）支持在界面还原对统方行为操作的详细内容 |
| 6）支持对自定义用户、审计时间的审计，支持多种不同的数据库进行同时审计 |
| 7）支持接口总带宽分析，根据带宽数值大小排名；支持服务器活跃度分析，如显示总连接数、最大连接数、最小连接数等；支持服务器带宽分析和流量分析 |
| 8）实现统方操作过程上下文关联，针对统方行为记录所有操作过程，并能实现回放功能，针对统方行为进行统计分析，能够按照医院科室部门进行统计分析每个科室部门统方行为及对数据库访问的情况； |
| 9）实现统方行为的监控、查询、统计、分析等功能，系统在不适用数据库账号查询的情况下，能够对统方行为的结果进行自动还原，审计内容至少包含前50条数据库操作结果。确保统方行为事后对统方结果相关内容的追查和确认。 |
| 10）支持对关键词的审计并告警、支持关键词信息导入 |
| 11）支持系统内置规则库，包括SQL，Cache, Oracle ,telnet， his web ,medtrak等告警规则，支持对告警行为进行二次人工研判。支持对数据库告警查询、显示告警级别和处理状态。支持自定义通用告警规则，包括对请求和响应数据的关键字告警，响应数据的响应时间，返回行数告警，支持告警白名单，支持邮件告警功能，支持短信告警功能。 |
| 12）提供完善、丰富的报表展现，支持pdf、excel、word等报表格式输出，支持报表报告定制功能，支持日报、周报、月报、年报和自定义时间段等形式报告，并能自动发送指定用户信箱；支持对用户操作数据库次数、统方事件、涉及人员排名及所占比重等信息统计；支持根据客户端IP、用户名/工号、操作选择等进行搜索，支持在界面还原对统方行为操作的详细内容，支持对数据库告警查询、显示告警级别和命中词等；实现对所有统方事件出现频率进行统计分析； |
| 13）支持WEB、SSH、Console进行管理配置，支持管理员权限划分，可自定义管理员角色，支持系统日志，支持授权管理，支持系统数据备份，支持系统数据定期清理 |
| 14.设备支持SNMP协议，能够为第三方管理软件提供接口 |
| **3** | **服务要求** | ★1）当突发网络安全事件时，1小时内到达现场，协助对遇到的突发性安全事件进行紧急分析和应急处理，内容包括突发事件信息收集、事件分析、分析报告提交、问题解决建议等。  ★2）提供季度巡检服务，周期性地、有针对性地对软件产品服务端及硬件产品的健康巡检，软硬件设备及其运行状态、策略检查、核心功能状态等健康评估，并出具巡检报告。  3）统计分析出审计中体现出的安全问题的变化趋势，对新出现的网络安全问题进行分析，并给出相应的报告及建议。  4）提供原厂技术培训服务，提供安全咨询规划服务，包括但不限于产品使用、功能咨询、问题交流、对接规划等各种服务。  5）厂家能够提供快速本地化现场技术支持（1小时内到达用户现场），提供7\*24小时技术服务支持。12小时到达现场排除故障，在规定时间内仍无法排除故障的投标人必须提供备机。  ★6）符合等级保护2.0测评三级要求。  ★7）考虑到整体系统的兼容性，保障院方信息系统稳定运行，所投产品及中标方需完成与院方现有信息系统HIS及数据库系统无缝对接。采购人不再另行支付系统改造或对接费用。（投标人须提供承诺书，并加盖公章）  8）所提供的产品要采用国家或行业规定的标准进行包装，应含有详细清单、合格证、检测报告、使用说明书及维修手册等相关资料。质保期内出现任何有中标单位设计或设备缺陷引起的故障，免费提供保修、包换、包退服务，所产生的费用由中标单位承担；超过质量保修期的维修、保养等服务及零部件更换，只收取成本费用。  提供设备原厂商基于本次项目的原厂授权正本 |
| **4** | **质保** | ≥3年自货物验收合格之日起，对系统提供三年的免费质量保修期，对系统软件提供终身免费授权。 |
| **5** | **交货时间** | 合同签订后30个工作日内交货实施。 |