**附件3：** 医疗防统方系统采购需求

**一、招标项目一览表**

具体内容如下表：

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **标项****序号** | **标项名称或内容** | **数量** | **单位** | **预算****总金额****（万元）** | **交货地点** |
| 4 | 医疗防统方系统（药品，spd） | 2 | 套 | 16 | 仙居县人民医院 |

1. **技术需求**

|  |  |
| --- | --- |
| **指标项** | **详细功能要求** |
| 授权要求 | 提供2套业务系统的数据库防统方授权。 |
| 部署管理 | 防统方系统不需要改变现有应用程序和数据库的设计，无需改变应用程序代码，无需应用做二次开发，编写接口等，对医院现有系统无影响 |
| ★在探针模式下，通过探针将数据库的所有操作传送到防统方设备；探针支持自动推送安装，且支持探针性能的限制，防止对数据库性能产生影响。（提供产品功能截图） |
| 可支持防统方系统集中化管理功能，基于Web的管理方式和SQL管理接口，B/S架构模式。 |
| 审计对象范围 | ★为满足未来信息化国产化转型需要，需要统方支持除当前我院使用的国产数据库Oracle、SQL Server、MySQL、MariaDB、DB2、PostgreSQL，亦需要支持国产化数据库DM、、KingBase、GBase、神通、GaussDB（高斯）等数据库。（提供产品功能截图） |
| 支持从网络流量中自动发现数据库信息，并添加到防统方平台；支持自动扫描IP地址段，发现数据库信息，并可添加到平台。 |
| 事件处理能力 | 内置大数据搜索引擎，支持模糊检索，亿级数据检索速度在秒级别实现。 |
| 统方审计功能 | 实现SQL语句的细粒度审计，并记录详细的用户行为信息，包括该语句执行的时间、机器名、用户名、IP地址、交换机端口、MAC地址、客户端程序名以及SQL语句、执行结果、执行时长、返回行数、结果集等信息，对数据库操作进行审计，可对查询，新增，修改，删除等行为进行监控。 |
| ★支持通过数据库绑定变量方式的防统方审计能力。（提供产品功能截图） |
| 支持按数据库进行白名单、黑名单审计策略配置，按客户端IP、应用程序、数据库用户配置黑白名单，过滤审计流量，可降低探针网络带宽压力，减小审计存储压力。 |
| ★内置丰富的风险引擎特征库，对于SQL注入攻击、数据库漏洞攻击进行精准识别并智能告警。（提供产品功能截图） |
| 实现数据库登录操作的审计，并记录详细的成功登录行为和失败登录行为信息，能够识别暴力破解等非法登录行为。 |
| 支持应用系统三层架构审计，可以精确的识别操作人，可以精确的识别来自于B/S架构的浏览器终端信息；能精确识别到操作人和应用程序账户，可以精确定位到人 |
| ★支持Oralce、MySQL数据库本地审计；支持客户端SSH隧道代理访问数据库审计；支持本地命令行访问数据库审计。（提供产品功能截图） |
| 对于疑似威胁的操作记录，能够基于会话进行追踪溯源，根据人（用户名、账户）进行追溯，在同一界面展现跟其相关的从登录、访问到退出的全过程。 |
| ★SQL语句提供直译和意译的不同翻译引擎，支持英文翻译成中文，统方代号翻译成常规名称，增加易读性，便于纪委等非技术人员理解报警内容（提供产品功能截图）。 |
| 告警策略 | 根据IP地址、机器名、时间、程序名，sql语句等精细组合对统方表操作行为预设警报策略，并能够为特定的审计需求自定义审计警报规则。 |
| 提供多种安全响应措施，包括数据库记录、邮件报警、短信报警、syslog等。通过这些监控和防御措施，对招标方统方信息进行有效的监控、预防和保护。 |
| 模型分析策略：以操作语句为原型，根据获取的审计内容字段、表名称、条件字段、操作频率等条件设定分析策略； |
| 对于首次出现的终端（IP）、人（用户名、账户），进行高级告警。 |
| 安全告警必须支持基于订阅的模式，每个人可以订阅自己的安全告警事件，页面的安全告警事件必须区分开当前30分钟的安全告警事件和过去的安全事件以方便阅读，支持任意组合的规则订阅，实现人员的个性化订阅管理。 |
| 报表管理 | 定期自动生成：日、周、月、年度综合报表；(投标时要求提供软件功能截图) |
| 支持按时间、范围、报表模板自定义生成报表； |
| 支持下载法规性报表，如SOX法案、PCI报表、等级保护报表； |
| 综合报表展现形式具有多样性，如使用表格、柱状图、饼状图、折线图等多种方式进行展现分析； |
| 所有报表都支持下载；文档支持格式：包括WORD\HTML\PDF\EXCEL等； |
| 定期生成的报表可配置邮箱，定时收取最新生成的报表。 |
| 配置管理 | 支持事件FTP服务器自动备份功能，备份记录支持恢复到平台。 |
| 支持查询结果下载，自定义设置下载字段，下载审计查询的结果。 |
| ★提供事件审阅和自动审阅，自动审阅的审计信息后续出现将不需要再行审阅；依赖于审计信息的访问规则的单键生成,依赖于审计信息的订阅规则的单键生成；（提供产品功能截图） |
| ★原厂资质 | 产品具备国家版权局颁发的《计算机软件著作权登记证书》原厂同时拥有ISO系列证书，9001/27001/20000等。具备CMMI3能力成熟度模型集成认证证书具备成熟度三级及以上的ITSS(信息技术服务标准)认证资格。具备企业信用等级AAA证书。为保证产品为自研产品，需要具备政府颁布的地市级专利示范企业证书。为判断原厂商服务能力，需要原厂商为国家网络与信息安全信息通报机制技术支持单位。 |
| 售后服务能力 | ★要求原厂提供售后服务，且原厂团队成员具备良好的数据库技术支持能力以保障本系统的顺利运行，项目团队成员具体要求如下（要求提供相关证书和社保复印件备查）：1、项目经理同时具备PMP和OCM认证，且是数据安全联盟认证专家；2、实施工程师同时具有OCP（10年以上）和CISSP。3、培训讲师具有两种或以上数据库ACE认证证书和OCM认证证书。 |
| 功能验证 | 中标后，招标人有权要求中标方提供产品进行相关功能验证，如存在虚假应标行为，将废除中标资格，并依法追究相关法律责任。 |

**三、商务需求**

1. 工期要求：自合同签订之日起60个日历天内完成系统建设并上线运行

2、付款方式：合同签订后10个工作日内支付20%的款项，系统建成并上线运行, 双方签订系统上线报告后支付40%，项目验收并签署验收报告后支付40%的款项。

3、项目实施要求

1）具备科学性、合理性、规范性和可操作性充分的实施方案（包括工期计划，各阶段工作内容，用户使用培训等内容）。

2）开展之前，项目实施人员应制定一套完整科学可行的实施方案，作为系统建设实施的总体计划和步骤。

3）对项目实施管理的进度、质量、变更、风险、文档、团队等各个方面都有成熟的管理体系及对应的管理及制度方案。

4、保修及服务：

1）具备完善的维护服务方案。本项目免费维护期至少3年，维护期以项目终验之日起算。

2）维护期内，向采购单位提供7\*24小时保修和维护服务（电话、远程或现场）。对现场不能完成的工作，1个工作日内给出解决方案，按双方协定时间完成服务。对于必须派人现场解决的问题，保证在收到现场服务通知后，8小时内到达现场。保修和维护服务内容包括但不限于软件的功能增强性维护等应用软件系统扩充升级（其中包括系统维护、新功能开发升级），保证投标人所开发的软件正常运行等。