采购需求

前提：本章采购需求中标注“★”号的条款为本次采购项目的实质性要求，供应商应全部满足。标注“▲”号的条款为重要技术条款，非实质性要求。

包 1：PostGre 数据库审计系统

一、★采购标的汇总清单

序号	标的名称	数量	最高限价（万元）	采购标的所属行业
1	PostGre 数据库审计系统	1 套	20.00	软件和信息技术服务业

二、技术参数及要求

（一）项目服务内容

1.医院临床数据中心存储有主要医疗业务数据，有患者基本信息、诊断信息、医嘱、检查申请及结果、检验申请及结果、体检信息、电子病历（清洗后数据）和收费信息。为保证信息安全，保护患者隐私，对该数据中心的所有访问、读写均需有日志、有痕迹。为此采购一套数据库审计系统。临床数据中心采用 PostGreSQL 数据库，数据库审计系统需支持该数据库的所有命令集和标准 SQL 命令集。

（二）技术服务要求

名称	技术参数及要求
硬件规格及性能	1.系统采用高可靠多核硬件平台和安全操作系统，自身内嵌高性能、安全可靠的数据库系统，用户无需另外安装数据库系统；
	2.▲标准 2U 机架式；板载千兆电口*6，（其中一个管理口，五个业务口）；网卡扩展插槽*1；USB：3.0 口*2；串口：1 个；VGA 接口：1 个，内存 32G；硬盘 2*2T；SSD 240G；支持冗余电源；可扩展千兆或万兆光口；采用 SSD、HDD 多级存储架构，系统和业务数据分离，实现高效、安全存储；
	3.▲峰值处理能力不低于 40000 条语句/秒，日志在线存储不低于 64 亿条。
工作部署模式	4.通过端口镜像（SPAN）或者分流器（TAP）模式旁路部署，无需改造网络、无需在服务器上安装插件、对服务器零干扰、不影响性能、无需服务器账号信息、无需重启服务器、不中断业务；
	5.针对虚拟化环境和小型云支持以虚拟交换机的 VEPA 模式部署（vmware、kvm、openstack）；
	6.▲支持在目标数据库安装 agent 解决云环境、虚拟化环境内部流量无法镜像场景下的数据库审计，支持通过 Agent 对流量进行过滤，过滤内容包括端口、IP 地址等内容，可以进行定义，减少网络负载。Agent 运行时 CPU 占用率低于 3%，内存占用小于 100M，程序文件小于 5M；**（提供截图并加盖公章）**

	7.具有成熟的大数据平台对接技术，可以提供 SDN 无插件引流方案与云平台进行对接整合，在鲲鹏云、阿里云、ucloud 云、腾讯云环境中能快速部署审计系统，实现云平台中数据库系统操作行为快速安全审计；支持 Docker 环境快速部署审计系统，实现 Docker 环境下数据库安全审计。
集中管控	8.▲ 支持数据库审计集中管理功能，可快速查看所有审计系统的状态、风险状态等，可统一下发安全管控策略到各子节点；方便管理及防护策略的落实；**（提供截图并加盖公章）**
	9.管理中心和子节点都可存储审计数据，实现大数据环境下磁盘空间的有效利用和扩展，利用率达到 90%；
安全审计类型	10.▲支持传统关系型数据库，如:SQLServer、MySQL、Oracle、Sybase、DB2、Informix、MariaDB 的安全审计；**（提供截图并加盖公章）**
	11.▲支持大数据平台下的大数据库如：Hwi、ES、Impala、Spark、Hbase 、Solr 以及 REST_API 接口审计，JDBC_API 接口调用的安全审计；**（提供截图并加盖公章）**
	12.▲支持国产化数据库，如：DM（达梦）、Kingbase（人大金仓）、虚谷数据库、LibrA、GaussDB、GBase、Oscar（神舟通用）的安全审计；**（提供截图并加盖公章）**
	13.▲支持后关系型数据库 Caché、MongoDB、PostgreSQL 的全面审计**（提供截图并加盖公章）**
	14.▲支持内存数据库 HANA、Redis、工控实时数据库 IP21 等特殊应用场景下的数据库安全审计；**（提供截图并加盖公章）**
	15.▲支持主流业务协议操作的审计，如：Samba 、NFS、Portal、Http、pop3、ssh、SMTP、Telnet、FTP 协议审计；**（提供截图并加盖公章）**
数据库审计能力	16.同时支持 IPv4/IPv6 网络环境流量的审计；
	17.▲全面支持后关系型数据库 Caché的集成工具 Terminal、Portal、Studio、Sqlmanager、MedTrak 工具的审计，其中 Portal 能审计到 Sql 语句、查询 Global 有返回结果，Sqlmanager 支持根据 SQL ID 提取高效审计， Terminal 能审计到 SQL 语句和返回结果,并支持本地审计，基于 C/S 的 MedTrak 工具能审计到操作报表的具体返回结果；**（提供截图并加盖公章）**
	18.▲支持 Hadoop 架构下的数据仓库 Hive 的审计，如：能审计到 Hive_HSQL 创建数据库、建表、删除表、修改表结构、创建 / 删除视图、向数据表内加载文件、将查询结果插入到 Hive 表中、基本的查询等操作；**（提供截图并加盖公章）**
	19.▲支持 Hadoop 架构下的大数据库 Hbase 审计，如：能审计到 JDBC、Java API 等接口的调用操作；**（提供截图并加盖公章）**
	20.▲支持全文检索数据库 solr 的审计，如：能审计到 solr 的查询、插入等行为的操作信息；**（提供截图并加盖公章）**

	21.▲支持对实时数据库 IP21 的审计，可审计到 WEB 操作指令及 API 调用的指令，并且可审计到返回的位号；**（提供截图并加盖公章）**
	22.支持数据库嵌套语句、函数(sum 求和函数等）、返回结果、脚本等审计；
	23.支持 SQL 绑定变量的审计，应能审计到变量名及变量值；
	24.▲支持数据库 SSL 加密流量的审计，包括 SSL1.0、SSL1.1、SSL1.2 等；**（提供截图并加盖公章）**
	25.支持 SSH 加密审计、 sqlplus 本地审计、mysql 工具本地审计，有效实现本地运维操作的全面审计
	26.▲支持对操作时间、操作语句、执行结果、返回结果集、影响行数（返回行数）、执行时长、数据库用户名、实例名、源/目的 IP、源/目的端口、源/目的 MAC、客户端主机名、客户端端口、客户端操作系统用户名、操作类型，操作内容，表、字段，操作回应、会话 ID、返回内容等 27 个条件以上进行审计；**（提供截图并加盖公章）**
	27.支持数据库操作类、表、视图、索引、存储过程等各种对象的所有 SQL 操作审计；
	28.在无需重启被审计数据库的情况下，支持对 SQLServer 加密协议的审计，可正常审计到数据库账号、操作系统用户名、操作系统主机名等身份信息；
	29.▲支持超长操作语句审计，针对传统型数据库支持 20 万字节连续审计，审计过程中不截断 ；**（提供截图并加盖公章）**
	30.支持根据数据库 SQL 语句请求以及请求执行状态、执行时长、返回行数、返回字段、结果集内容等信息的双向审计；
	31.▲支持旁路阻断功能，支持根据访问 IP、账号、客户端工具名、时间、客户端 MAC、主机名、操作回复信息等指定规则进行阻断；不改变被审计对象的网络结构、不在数据库操作系统中安装插件，审计系统设备异常不影响网络； 阻断模式具备“严格模式”与“宽松模式”；宽松模式可对单一会话危险操作阻断，危险操作特征外的其他操作不影响；严格模式可对同类型危险操作持续阻断，源 IP 操作的所有请求直接阻断；**（提供截图并加盖公章）**
	32.支持对数据库执行超过 6 小时的操作行为持续不断的进行审计；
应用审计能力	33.▲支持 B/S、C/S 应用系统三层架构 http 应用审计，可提取包括应用系统的人员工号（账号）在内的“六元组”身份信息，精确定位到具体的操作自然人信息，并可获取 XML 返回结果；**（提供截图并加盖公章）**
	34.▲支持带 COM、COM+、DCOM 组件的三层架构应用审计，可提取包括应用层工号（账号）之内的“六元组”身份信息，精确定位到具体的操作自然人信息；**（提供截图并加盖公章）**
	35.▲支持通过部署 agent 实现 java web 环境 100%准确关联，支持框架：tomcat、weblogic、jboss；支持 B/S 业务系统三层关联审计；支持 B/S 三层架构下的应用账户、终端信息关联审计；**（提供截图并加盖公章）**

审计策略支持	36.内置安全特征库和审计规则库不少于200条，支持对数据库安全进行检查，如SQL注入攻击、跨站脚本攻击、账号提权、导表导库等；
	37.▲支持自定义审计策略，自定义审计策略的条件包括不限于操作类型、关键字、访问工具、客户端IP、客户端MAC、操作系统主机名、操作系统用户名、应用账户名、数据库账号、数据库名、表名、字段名、语句长度、语句执行回应、语句执行时间、返回行数、返回内容、正则表达式、规则生效时间；审计策略条件之间支持等于或不等于、大于等于或小于等逻辑关系；**（提供截图并加盖公章）**
	38.▲系统需内置18种以上审计元素进行数据库操作行为审计，如：数据库操作命令、语句长度、语句执行回应、语句执行时间、返回内容、返回行数、数据库名、数据库账户、服务器端口、客户端操作系统主机名、客户端操作系统用户名、客户端MAC、客户端IP、客户端端口、客户端进程名、会话ID、关键字、时间等；**（提供截图并加盖公章）**
	39.▲支持操作语句系列的组合规则，可根据某一客体的操作行为序列，连续操作了设定的语句序列时进行规则审计告警；**（提供截图并加盖公章）**
	40.支持重复操作的统计审计规则，支持在24小时内检测到重复某项操作达到设定的统计次数进行告警；
	41.支持根据SQL语句执行的回应，如成功或是失败进行规则定义； 支持根据返回行数或阈值设定规则；
态势感知	42.支持对一段时间内的数据机器学习成模，对陌生访问者可监控并联动告警；
敏感数据防护	43.▲系统内置敏感数据类型，可自动发现业务环境中数据库对象中包含敏感数据类型，进行敏感数据级别的定义；支持敏感数据自定义，支持同步敏感数据扫描结果中的敏感数据，支持自定义敏感规则，可根据配置字段包括操作类型、敏感配置（保护对象所属的敏感数据）主体信息（访问工具、访问IP、客户端MAC、操作系统主机名、操作系统用户名）、规则生效时间进行敏感字段的操作行为监控与审计。**（提供截图并加盖公章）**
	44.▲支持根据时间、保护对象、源IP的维度对业务环境中敏感数据进行敏感数据统计、敏感数据访问热度统计及分析、敏感数据访问趋势及分析。**（提供截图并加盖公章）**
大数据下全文检索	45.▲基于大数据全文检索技术，检索效率高达亿条数据秒级响应，快速定位相应的审计内容；**（提供截图并加盖公章）**
报表	46.系统内置分析报表和合规报表，支持源IP、账号、操作类型、客户端进程工具、时间等纬度生成报表；
	47.支持自定义报表，统计条件包括不限于风险级别、保护对象、客户端IP、访问工具、操作类型、数据库账户、数据库名、表名、字段名；支持添加统计模板，通过模板生成自定义报表数据。

	48.支持 Word、PDF、excel 格式报表导出；
事件查询统计	49.实现对所有违规事件出现频率进行 TOP 的汇总统计分析，并提供对汇总结果的实时查询功能；可以对客户端使用的程序、客户端 IP、用户名进行 TOP 排名展示，并生成报表；
	50.可根据事件的时间范围、客户端 IP、关键字、进程名、数据库账号、规则名、客户端端口号、返回内容等多种条件进行事件回放，回溯事件过程；
审计配置管理	51.▲翻译功能：支持在审计时自动将审计结果翻译成自然语言，支持系统定义和用户自定义翻译，按照业务的行为和分类来进行信息的组织和展现，便于审计人员方便、简单的获得并了解数据库审计的结果；**（提供截图并加盖公章）**
	52.三权分立：提供管理员权限设置和分权管理，安全管理，系统管理、审计管理权限分开，相应权限的用户只能查看、管理相应的功能，责任明确
	53.▲系统支持对所有数据库审计系统管理人员的操作行为进行审计记录，如登审计系统系统管理人员的登录登出、规则修改、规则启用等，并由审计人员进行查询和审计，具有自身审计功能；**（提供截图并加盖公章）**
	54.提供系统 CPU、内存、磁盘存储容量不足等情况时的自动报警提醒能力；
	55.系统支持管理界面告警、Syslog 和 SNMP trap 告警、邮件和短信告警；
	56.提供审计策略和配置的导入导出，方便运维人员进行数据库审计系统的简单运维；
审计数据管理	57.提供审计数据管理功能，能够实现对审计数据的自动备份、手动备份，支持增量、全量备份方式；
	58.▲有多级缓存机制，能够在突发流量超出性能设计指标的 30%以内流量时，系统能够保证在 2 个小时内不漏审。**（提供截图并加盖公章）**
	59.支持根据系统语句（SQL 语句）和白名单（条件为 IP/MAC/数据库账户/审计对象/操作语句）定义规则进行应用层过滤，将客户关注的信息进行保留，避免无用信息的堆砌造成磁盘空间的浪费和性能的耗损；
	60.备份数据可自动存储在指定的 FTP 服务器上；
	61.▲审计结果隐秘设置，通过*号脱敏技术对审计结果中的重要信息进行隐秘处理，防止二次泄密；**（提供截图并加盖公章）**
攻击检测能力	62.▲支持对 SQL 注入、跨站脚本攻击、信息泄露、数据库 CVE 高危漏洞、攻击溢出等攻击行为的识别与告警；**（提供截图并加盖公章）**
	63.系统应具备防范非法 IP 地址、防范暴力破解登录用户密码（能够对连续失败登陆进行自动锁定，锁定时间可设置）等安全功能；
	64.支持配置信息、系统日志一键导出导入功能；支持根据保留天数和占用百分比自动清理，防止因磁盘空间满导致审计系统不可用；
	65.支持管理员多因子认证登陆：静态口令认证，短信验证，支持密码的复杂性管理，

	比如大小写、数字、特殊字符、长度等，支持锁屏功能；
	66.支持审计数据管理功能，能够实现对审计数据的自动备份、手动备份，支持增量、全量备份方式，备份数据可自动存储在指定的 FTP 服务器上；
第三方接口功能	67.支持 Syslog 和 SNMP TRAP 方式向外发送审计日志到第三方日志管理平台统一管理，可外置短信猫，支持 GSM 卡，支持与第三方邮件和短信系统对接，提供接口可实现与网络设备的联动；
	68.支持与现有数据库防火墙关联审计违规操作行为；
	69.支持与现有堡垒机联动关联审计运维数据库的操作行为审计；
	70.提供客户需求的系统二次开发的定制服务；
	71.支持与 FTP 服务器对接（备份与还原）；
	72.FTP 存储进行加密处理，只有通过专门的工具进行恢复和查询浏览；

★商务要求（各包通用）

（一）项目最高限价：20 万元

（二）项目交付（实施）时间（期限）：合同签订后 60 日内

（三）项目交付（实施）地点（范围）：成都医学院第一附属医院指定地点

（四）付款条件（进度和方式）：

（1）合同签订后支付 50%的预付款；

（2）中标人完成相应系统开发及设备安装、调试完成，经采购人验收合格后，支付合同金额的 50%；

（五）项目售后服务要求

(1)产品售后服务按产品的出厂标准执行，验收合格后 1 年免费售后服务，供应商承诺的售后服务优于出厂标准的，将作为相同分数优先成交的重要依据；

(2)在接到故障报告后，供应商应满足7×24×365售后服务以及20分钟内电话响应，远程解决不了的问题，8小时内工程师到达现场；一般性故障应在24小时之内排除，重大故障应在48小时之内排除。

(3)供应商应确保货物在配送、安装过程中无安全事故发生，若出现安全事故其责任和损失由供应商自行承担。若因货物安装交付使用后，因供应商安装不当造成的安全事故其责任和损失由供货商负全责。

（4）如遇自然灾害原因和人力不可抗拒的因素，可由采购人和中标供应商双方协调解决。

（5）为了保证采购人：成都医学院第一附属医院在使用的时候确保是最终使用用户、得到原厂售后服务及顺利升级，避免出现非原厂家授权产品交货。中标后签订合同前需提供原厂对成都医学院第一附属医院使用授权及提供原厂成都医学院第一附属医院售后服务承诺函。

（提供承诺函，格式自拟）

（六）项目验收标准

1、按国家有关规定以及招标（采购）文件的质量要求和技术指标、供应商的投标（响应）文件及承诺与合同约定标准进行验收;双方如对质量要求和技术指标的约定标准有相互抵触或异议的事项，由在招标（采购）文件及投标（响应）文件中按质量要求和技术指标比较优胜的原则确定该项的约定标准进行验收；

2、验收时如发现所交付的货物有短装、次品、损坏或其它不符合标准及合同规定之情形者，

应做出详尽的现场记录，或双方签署备忘录，此现场记录或备忘录可用作补充、缺失和更换损坏部件的有效证据，由此产生的时间延误与有关费用由供应商承担，验收期限相应顺延。如质量验收合格，双方签署质量验收单。

（七）项目验收要求

包括但不限于：

1.项目验收人员组成：由采购方使用人员及供应商技术人员共同验收；

2.验收标准：按照招标文件及供应商投标文件响应的技术参数进行验收。

（八）双方违约责任：

一、采购人违约责任

1.采购人无正当理由拒收货物的，采购人应偿付合同总价百分之五的违约金。

2.因采购人原因逾期支付货款的，除应及时付足货款外，应向投标人偿付欠款总额百分之一/天的违约金；逾期付款超过 30 天的，投标人有权终止合同；采购人偿付的违约金不足以弥补投标人损失的，还应按投标人损失尚未弥补的部分，支付赔偿金给投标人。

二、投标人（供应商）违约责任

1.投标人（供应商）交付的货物质量不符合合同规定的，投标人（供应商）应向采购人支付合同总价的百分之五的违约金，并须在合同规定的交货时间内更换合格的货物给采购人，否则，视作投标人不能交付货物而违约。

2.投标人（供应商）不能交付货物或逾期交付货物而违约的，除应及时交足货物外，应向采购人偿付逾期交货部分货款总额的百分之一/天的违约金；逾期交货或未能按时完工超过 30 天，采购人有权终止合同，投标人（供应商）则应按合同总价的百分之五的款额向采购人偿付赔偿金，并须全额退还采购人已经付给投标人（供应商）的货款及其利息。

3.如货物经投标人（供应商）3 次维修仍不能达到合同约定的质量标准，采购人有权退货，并视作投标人（供应商）不能交付货物而须支付违约赔偿金给采购人，采购人还可依法追究投标人（供应商）的违约责任。

4.投标人（供应商）货物经采购人送交具有法定资格条件的质量技术监督机构检测后，如检测结果认定货物质量不符合本合同规定标准的，则视为投标人（供应商）没有按时交货而违约，投标人（供应商）须在 30 天内无条件更换合格的货物，如逾期不能更换合格的货物，采购人有权终止本合同，投标人（供应商）应另付合同总价的百分之五的赔偿金给采购人。

5.投标人（供应商）保证本合同货物的权利无瑕疵，包括货物所有权及知识产权等权利无瑕疵。如任何第三方经法院（或仲裁机构）裁决有权对上述货物主张权利或国家机关依法对货物进行没收查处的，投标人（供应商）除应向采购人返还已收款项外，还应另按合同总价的百分之五向采购人支付违约金并赔偿因此给采购人造成的一切损失；投标人（供应商）偿付的违约金不足以弥补采购人损失的，还应按采购人损失尚未弥补的部分，支付赔偿金给采购人。

（九）其他要求

1、质保期结束后，维保费用不得高于合同金额的8%（**提供承诺函，格式自拟**）