**采购软件名称**：防统方系统

**软件实现功能：**防统方系统即是防止统方行为发生，根据医疗行业及其应用系统的特点，以操作行为的正常规律和规则为依据，对药品相关计算机系统进行的操作行为产生的痕迹进行监测分析，发现和防范内部人员借助信息技术实施的违规和犯罪。对信息系统运行有影响的各种角色的行为过程进行实时监测，通过监测发现处方统计行为是否合理，从而对该行为进行有效控制，防止非法统计处方行为。

**防统方系统参数要求**

|  |  |
| --- | --- |
| 序号 | 参数要求表 |
| 1 | 系统硬件配置：2U 机架式设备; CPU：>=4核心，8线程; 内存：>=8GB , 磁盘：>=1TB； 监听口：千兆电口\*2。负载能力：每秒至少能处理800Mbps以上网络流量; 支持千兆网络环境及至少1500个客户端并发网络环境监控。 |
| 2 | 系统须实现网络旁路部署，又要支持应用日志采集审计，以便灵活部署。同时，部署时不对现有的网络体系结构（包括：终端、路由器、防火墙、应用层负载均衡设备、应用服务器、数据库等）进行调整，工作时不影响数据库本身的运行与性能。 |
| 3 | 系统具有完善的自身审计功能，包括网络断线、磁盘满、用户登录以及各种操作都有详细记录，对于影响系统正常运行的事件提供实时报警功能。 |
| 4 | 防统方软件需要支持HTTPS的WEB应用访问审计并对统方操作进行报警。 |
| 5 | 能够出具针对纪委、监察室、行风办等相关人员使用的防统方报告，支持每天、每周、每月自动生成统方报告。具有自动将计算机语言翻译成通俗易懂的自然语言的系统机制，便于查看和发现。 |
| 6 | 提供纪监监察部门专用账号，独立于数据库审计的账号，专门实现统方行为的监控、查询、统计等功能，系统需要对药品、耗材相关统方行为进行监控，需要提供统方事件备注审批功能。 |
| 7 | 实时监控医院对于防统方系统的使用情况，对上线情况进行查询，并产生报表，确认系统被使用频率和状态。 |
| 8 | 实现对存储过程进行动态审计（药品、耗材的使用统计相关存储过程），该存储过程中含有定义的异常敏感操作，在该存储过程执行时能够自动报警。 |
| 9 | 实现对统方事件进行汇总统计分析；可以对统方客户端使用的程序、客户端IP、用户名进行排名展示。 |
| 10 | 实现对统方事件进行实时报警；可以对统方事件进行趋势分析并以图形化形式进行展示，并按照重要程度分别统计。 |
| 11 | 系统提供按SQL语句规则匹配次数忽略报警事件的功能。 |
| 12 | 提供防统方事件查询功能，用户可根据时间、地址、数据库类型、用户名、操作类型、数据库名，表名，字段名等多种条件进行组合，进行精确事件查询。 |
| 13 | 系统提供数据备份清理功能，数据备份跨度以天为单位；支持选择时间范围内的数据清理功能。 |
| 14 | 系统可设置审计数据保存期限，至少保存一年的数据并支持实时查询。 |
| 15 | 针对统方行为进行统计分析，能够按照医院科室部门，统计分析每个科室部门统方行为以及对数据库访问的排名情况。 |
| 16 | 支持针对Oracle、SQL Server、MySQL、DB2、Hive、Informix、Sybase、PostgreSQL、KingBase、hbase、cache、GaussDB等主流医疗数据库进行防统方审计，以便满足医院信息化发展需求。（提供截图并厂家盖章证明） |
| 17 | 对于统方行为，一般涉及查询一个月及以上的药品用量信息，统方sql执行时间和对应的执行结果流量具有一定意义,系统需要提供对sql执行时间、执行结果流量进行监控功能，对sql执行时间长短、执行结果流量大小超过设置的进行报警。（提供WEB管理界面截图并厂家盖章证明） |
| 18 | 系统在网络旁路部署的情况下，不得安装插件等其他管理程序，提供统方查询操作阻断功能。提供非应用系统、非数据库发起的select类型的统方查询操作阻断功能，需要提供“阻断策略”管理界面，需要涵盖“阻断配置”功能（可按一天内一个终端最多阻断次数、一天内最多阻断终端个数、阻断持续时间进行阻断配置）、“阻断记录”功能、“阻断白名单”功能（阻断白名单，需要按终端IP、账号、白名单生效时段设置每月生效、每周生效、每天生效等条件）（提供WEB管理界面截图并厂家盖章证明） |
| 19 | 实现对医院多个数据库、应用的防统方功能，可同时针对HIS、EMR、LIS、合理用药、医嘱等业务系统数据库。对HIS系统等，提供内置防统方知识库功能，且具有自动优化防统方策略功能；同时提供自定义规则功能。 |
| 20 | 实时记录用户对数据库的登录、注销、插入、存储、删除等操作过程，并将这些动作还原为SQL执行语句。 |
| 21 | 能够针对TNS、TDS等协议进行解析还原，包括数据访问的各项要素，如执行的SQL命令、请求内容、执行时长；以及客户端及主机端IP、MAC地址等内容。 |
| 22 | 系统能够对用户数据库的存储过程进行每日扫描，监控存储过程内容中的涉及统方的可疑内容，并进行提醒。 |
| 23 | 系统支持对B/S三层业务系统的审计，能同时实现网页URL审计与数据库SQL操作语句的审计。 |
| 24 | 系统能审计到具体的SQL统方语句、URL统方语句的执行时间，根据SQL语句的响应时间，为使用者提供统方行为判断的有效技术分析能力。 |
| 25 | 系统以图形方式展示系统流量、存储、CPU、内存等使用情况。自动监控系统自身运行状况，系统运行出现故障时，向管理员报警。系统支持SNMP协议、Syslog，能为第三方管理软件提供接口。 |
| 26 | 系统支持数据自动和手动备份操作，备份策略可按天、周、月进行选择，自动备份支持远程设备。 |
| 27 | 系统用户中包含管理员、审计员、安全员、纪检等多种角色，分别进行系统管理，授权及操作日志管理、使用记录管理。 |
| 28 | 审计数据支持10种以上查询方式，支持对查询数据以Excel格式导出，并出具报表。 |
| 29 | 系统支持每周、每月自动生成报表，对报警事件进行汇总分析，并给出分析结果。 |
| 30 | 系统提供“统方行为记录与阻断”能力，支持根据统方规则记录统方事件，根据统方的特征，通过关键字审计到统方的操作行为，触发阻断功能，阻断终端继续操作数据库进行统方行为。（提供截图证明或公安部相关质量检测中心出具的检验报告功能相关合格证明材料） |
| 31 | 系统支持对统方事件进行手机短信、邮件等报警，支持短信平台、第三方API等告警对接方式。告警内容需要包含规则修改情况、系统运行情况、统方事件汇总或详情。 |
| 32 | 考虑对防统方相关事件数据保存时间超过1年及以上，系统需要支持查询优化策略功能，需要提供“优化查询配置”界面，可根据总数据大小、最大查询等待时间、磁盘IO速率等进行查询优化。（提供系统WEB界面截图并厂家盖章证明） |
| 33 | 鉴于防统方系统的使用敏感性，用户环境若要求令牌登录认证，防统方系统需要提供相应管理功能界面，至少具有导入令牌信息、解冻结等功能。 |
| 34 | 防统方系统需要提供“药品代码判断”策略界面，支持定时对新生成的报警进行分析，判断是否涉及到药品编号，如果有药品编号，但这个编号没有在系统中备案，报警信息需要被事件降级。（提供WEB管理界面截图并厂家盖章证明） |
| 35 | 防统方系统需要提供“报警事件汇总”的功能，需要按今日、最近一天、最近7天、最近30天进行不同级别的事件汇总，需要展示最近一个月报警记录，包含源IP地址、操作用户、数据库登录名、所属部门、报警数量等信息，并提供详细查询功能。 |
| 36 | 防统方系统需要提供“按规则汇总”的事件查询功能，需要根据时间范围、规则和源IP地址进行查询展示包含源IP地址、匹配次数等信息，并提供详细查询功能。 |
| 37 | 需要提供报警统计分析界面，需要提供事件统计、最近30天报警趋势、操作类型统计、最近30天事件趋势等可视化图形，并提供最新报警和最新事件展示功能。 |
| 38 | 需要提供查看统方事件相关的SQL操作分布的功能，需要根据源IP地址、时间范围、数据库等进行条件查询，提供SQL分布散点图并进行客户端IP、SQL内容、执行时间（耗时）等内容的详细展示。 |
| 39 | 为了方便用户查询所需要的信息，需要提供对数据库操作的默认查询功能，条件包括操作内容、对象、登录名、源IP地址、客户端MAC、客户端主机名、应用程序名、操作用户，全文检索等；需要提供复杂的自定义查询功能，用户需要使用"或"条件、"与"条件、LIKE、"LIKE%"、"IN"或者"NOTIN"等多条件设置查询。（提供WEB界面截图并厂家盖章证明） |
| 40 | 系统需要提供规则导入导出功能，需要提供丰富的规则管理功能和忽略规则管理功能，对规则可进行批量生效、批量失效的设置，同时为规则管理提供一键“删除零匹配”的功能。（提供截图并厂家盖章证明） |
| 41 | 为了方便系统在内网环境中的运维，系统需要提供内网环境的常用下载，包括下载系统日志信息（精简日志、完整日志、客户端IP信息下载），常用工具下载（SecureCRT、winscp、putty），其他相关工具（hypertrm、UltraEdit、epsnap）等。 |
| 42 | 系统需要支持必要的网络管理功能界面，提供对用户现场的交换机设备的信息查看的功能。（提供WEB界面截图并厂家盖章证明） |