**防统方系统升级和维保采购需求**

目前医院使用的防统方系统软件，根据我院一院两区更换HIS系统的需要，要求保留并优化原基础告警规则上，对新换HIS进行数据库匹配升级，针对HIS系统的所有访问记录，准确定位数据库操作，对敏感数据进行分析，协助纪检监察室防统方工作，有效杜绝统方行为。

防统方系统软件V6.10原功能参数：

|  |  |  |
| --- | --- | --- |
|  | 功能模块 | 技术参数、建设要求 |
| 防统方系统 | 系统架构 | 吞吐量 20Gbps  SQL事务数/秒 200,000  接口 10/100/1000M自适应电口 \*6  光纤监听接口：SPF多模光纤，可扩展至4个  工作环境 5℃到35℃  存储容量 标配2T\*8企业级HDD （含64M缓存），raid阵列  存储周期360天以上  内存 64G  交流电源 220-240V、50-60Hz  功能说明 适用三甲医院规模，  准确的定位数据库操作,满足医院伍年的使用需求，不会遇到性能瓶颈，有效防止统方行为。 |
| 系统支持采用旁路部署方式，不需要更改现有网络结构、服务器相关配置，系统运行不得影响现有网络和业务的正常运行。系统应能独立完成审计数据采集，不依赖于数据库自身审计日志系统，不得在现有服务器上安装可能带来风险的程序。 |
| 采用B/S架构，提供中文WEB管理界面以便于管理。并应可以根据不同的安全级别采用不同的实时告警响应方式，包括记录、消息、鸣音、邮件等，并能支持短信平台。 |
| 系统支持双密码用户，安全性更高。 |
| 所有系统数据都支持加密传输，防止信息外泄。 |
| 针对多套系统可以进行分布式部署集中式管理，定时采集直属医疗单位防统方审计报告，便于卫生与健康委员会纪监部门统一监管直属医疗单位系统使用情况。 |
| 系统的时间可以和关键服务器中的数据库的时间进行同步，确保记录时间的一致性。 |
| 系统将预留一定的接口以作维护，二次开发之用。 |
| 系统性能 | 系统支持软硬一体机，支持千兆以上网络环境及大概至少1500个客户端同时并发的监控，应达到每秒140000个以上的事务处理能力。 |
| 审计数据最少支持壹年，并支持外接存储设备进行备份。数据应进行加密保管，只能通过专门工具进行恢复和查询浏览。 |
| 支持集群,系统支持冗余备份。系统配置文件支持导入、导出。 |
| 数据库支持 | 支持对Oracle、MS-SQL 、DB2、MYSQL、CACHE DB、POSTGRESQL和Sybase 等主流数据库提供自动化评估、审计和保护功能,可审计的数据库或集群数量不少于6个，并且支持单家医疗机构多种类型数据库并存的信息系统。 |
| 用户权限 | 通过定义用户角色，灵活制定每个用户所拥有的权限，权限颗粒度能控制到界面视图和按钮操作。 |
| 管理、审计用户权限分开，相应权限的用户只能查看、管理相应的系统功能，责任明确。 |
| 事件管理 | 系统从业务流程角度入手，结合核心数据特征，提供了高度集成的“事前+事中+事后”数据防护手段。 |
| 系统确保最小报警监控时间间隔为5秒，保证统方事件的及时告警。 |
| 主动/被动方式监控关键服务器的开放端口，提供扫描现有应用系统的漏洞。 |
| 根据客户端应用程序名单，实时阻断非法客户端程序或伪装正常客户端程序对关键服务器的访问。 |
| 阻断可疑会话功能，甄别数据访问，阻止非正常数据会话。能根据预定规则阻断SQL语句的“数据库墙”功能，如根据系统设置的客户端IP/MAC黑名单，以及数据内容中的敏感信息，实时阻断黑名单中的客户端对关键服务器的访问。 |
| 多种部署方式（串接/并接）下都可以阻断客户端进行疑似的统方行为。 |
| 能实现与桌面管理系统软件进行防统方事前阻断、截屏、锁屏。 |
| 预警管理 | 系统应能对自身的事件（包括登录、系统参数修改、系统异常等）进行审计并预警。 |
| 可根据用户自定义规则实时发出手机短信通知和邮件提醒等多种方式的告警信息，并支持配备相应的告警信息发送设备，可以提供阿里云服务发送短信告警。 |
| 可针对事件执行指定预警操作。 |
| 统方白名单权限的设置，可对授权统方行为的操作人员工号、操作类型、IP地址、客户端工具、操作系统用户名、主机名、MAC地址、SQL语句和操作的时间范围等条件进行设置，只有通过了授权和验证才可以获得统方权限。 |
| 可根据SQL执行的时间长短设定规则，如命令执行时长超过30秒进行告警；可根据返回记录数多少设定规则，如SQL操作返回的记录数或受影响的行数大于等于10000行时进行告警。 |
| 提供数据库登录用户名称异常探测、数据库操作源终端异常探测、数据库操作源程序名称异常探测、数据库操作源终端用户名称异常探测，可设定异常黑白名单，对客户端地址、客户端程序、数据库账号、客户端用户名以及执行结果等异常的行为进行异常告警，支持自主学习能力。 |
| 能够检测网络拷贝等操作,能够检测通过网络KVM发出的指令。 |
| 审计方式 | 系统应能支持对数据库SQL操作语句的详细审计，可以分析出每条语句的操作方式、表名、存储过程名、详细操作内容，执行时长、操作成功/失败，受影响行数，关联表与关联表数等字段信息，可审计并还原SQL操作语句。 |
| 可以监控和审计用户对数据库中的数据库表 、视图、序列、包、存储过程、函数、库、索引、同义词、快照、触发器等的创建、修改和删除等，分析的内容可以精确到SQL操作语句一级。 |
| 支持对超长SQL语句完整解析 |
| 支持对双向数据包的解析、识别及还原，不仅对数据库操作请求进行实时监控，而且还可对数据库系统返回结果进行完整的还原，根据统方行为的特征实时告警。 |
| 支持包括ASCII、Unicode、UTF-8、UTF-16、GB2312、EBCDIC等编码格式，避免因编码格式不同而导致审计报表出现乱码的情况，保证了审计报表的可读性。 |
| 系统应能支持多个网段客户端对数据库操作行为的会话审计，能够对各种访问数据的途径（如客户端软件、PL/SQL、SQL\*Plus、PB、Toad等各种SQL操作工具）进行监控和设计，可以跟踪审计某某时间、某某IP、某某计算机名、某某用户对数据库服务器进行了该类操作，具有可疑对象定位功能，可以精确定位可疑对象的物理位置。 |
| 支持加密方式的数据库连接信息分析（如MS SQL SERVER2005及更高版本等）。 |
| 系统可以监控、记录并且还原客户端连接到服务器的TELNET/FTP等远程登录操作信息，记录内容包括客户端IP地址，客户端MAC地址，服务器地址以及产生记录的时间，并提供多种查询，支持多种文件格式导出。 |
| 分析可疑对象的信息，包括IP、端口、MAC、主机名、程序信息、数据库连接信息。 |
| 支持对接医德医风系统，具有医德医风系统的。 |
| 非关注内容过滤 | 支持指定非关注策略，系统将非关注的内容进行过滤，不进行记录，降低了存储空间和无用信息的堆砌。策略因子包括：数据库操作来源IP地址、数据库登录用户名称、数据库操作源程序名称、数据库操作源终端名称、数据库操作源终端用户名称、SQL操作语句（DDL、DML、DCL）、数据库表组（表、列）等。 |
| 审计内容 | 支持医院信息管理系统多层结构，提供全方位的三层（应用层、中间层、数据库层）的访问审计，三层关联必需支持自动关联，以提升关联准确度和审计人员追踪索源难度，同时需要支持手动关联，可以直接追踪到前端业务的操作人员IP地址、MAC地址和用户. |
| 虚拟化和上云是医院信息化的趋势，对虚机的监控不能成为盲点，系统支持纯软模式对虚机内部相互访问进行监控。 |
| 支持对指定时间内全院抗菌药物品种、剂型、规格、使用量、使用金额，使用量和使用金额分别排名前N位的抗菌药物品种进行分析，自动生成报表. |
| 除了HIS系统，也可针对高值耗材、SPD、CDR、检验试剂、合理用药、BIS、CIS等医院新的信息化系统进行全方位监控。 |
| 支持应用层追踪，通过HIS统方的可以追踪到所使用的HIS工号。 |
| 支持Terminal、Studio、Protal、T-SQL、web等五种Cache访问方式审计；支持Cache运行功能。 |
| 系统对于图形会话的操作审计可以完整记录普通用户的图形操作。 |
| 对于审计结果的查看，可以对操作录像拖拉定位回放。 |
| 对于支持的图形连接的单点登录功能，无需用户输入用户名密码。 |
| 系统监控 | 既有传统的HIS知识库，也有其它如合理用药、SPD、耗材等等的知识库。更有全新的行为知识库。 |
| 系统内置故障排错系统，判断故障所在，帮助管理人员快速排查问题。 |
| 具备用户行为记录功能，记录用户所有的操作（业务访问、系统维护、策略配置等）。 |
| 可疑对象定位功能，可以精确定位可疑对象的物理位置。 |
| 报表管理 | 报表的生成方式分为手工报表和自动报表两种，支持多种格式(excel、pdf、txt等)导出。 |
| 可以对某统方行为的所有操作以及操作结果关联起来，以报表的形式呈现给使用部门，便于使用部门分析和追溯统方事件。 |
| 能够出具针对纪委、监察室相关人员使用的防统方审计报告（支持每天或多天生成统方审计报告，报告需简单明了，且具有主动将所有的计算机语言翻译成通俗易懂的自然语言的系统机制，支持将整条SQL语句翻译成中文，帮助医院建立基于内部网络的党风廉政、廉洁警示、院内敏感职权使用的防控专网，支持对接廉政风险防控系统。 |
| 用户可以根据需要自定义规则，并能根据设定的条件产生审计报告。能对审计结果进行多条件组合查询，比如按下列条件查询：IP地址、MAC地址、表名、操作方式、计算机名、数据库名、程序名等。并就能支持按关键词进行模糊查询。查询结果应支持多种格式(excel、pdf、txt等)导出。 |
| 应用云计算功能提供数据分析平台，对用户提交的数据进行自主分析，并生成报告和相关建议规则反馈给用户。 |
|  | 知识产权与安全要求 | 系统具有自主知识产权，需提供防统方系统的软件著作权证书。  需提供防统方系统软件产品登记证书和防统方集中管理系统软件产品登记证书。  提供的防统方系统软件需获得公安部计算机信息系统安全产品销售许可证。  产品获得防统方系统医院科技创新奖。 |

升级内容V6.30版本后

|  |  |
| --- | --- |
| **序号** | **功能内容描述** |
| 1 | 鉴于新HIS系统架构和数据结构的变更，需要对防统方系统进行定制开发适配，进行数据优化匹配； |
| 2 | 保留老HIS已经磨合好的敏感数据判定规则，导入开发适配新HIS数据监测； |
| 3 | 对现有短信猫进行版本升级，对新HIS敏感信息进行报警提示; |
| 4 | 对现有设备存储进行优化清理，整理存储数据碎片和冗余数据，划分RAID新空间给新HIS进行数据写入、分析、敏感信息报警 |

防统方系统2025年度的维保内容：

|  |  |
| --- | --- |
| **序 号** | **内容描述** |
| 1 | 对软硬件进行全面检测； |
| 2 | 系统漏洞补丁升级；  。 |
| 3 | 防统方知识库升级； |
| 4 | V6.30大版本优化V6.3X系统小版本更新； |
| 5 | 为院方使用部门进行使用答疑和培训； |
| 6 | （一年四次上门巡检(每季度上门一次)，7\*24小时电话支持）； |