一、日志综合审计系统

|  |  |  |
| --- | --- | --- |
| **指标名称** | **指标项** | **详细描述** |
| 系统架构 | 产品结构 | 要求为一个完整的软硬件一体化产品,1U机架式设备；无需用户另行提供服务器、操作系统、数据库、防火墙软件、及用户手动升级系统补丁； |
| 产品架构 | 采用标准机架式硬件 |
| 操作系统 | 深度定制优化的Linux系统； |
| 管理方式 | B/S方式，采用HTTPS方式远程安全管理，无需安装管理客户端； |
| 设备部署 | 提供旁路接入模式，设备部署不影响原有网络结构； |
| 数据存储 | 所供系统设备必须自带本地存储功能；  采用先进的高性能日志及行为审计系统；  采用基于海量日志专用存储的文件系统；  硬盘≥4TB；日志存储量至少十亿条；（指标以原厂公开资料为准）；  RAID架构以保证数据可靠性,（指标以原厂公开资料为准）；  支持后期扩展外部网络存储(IP SAN、NAS、DAS、磁盘阵列等)；  支持云备份存储及公有云存储容量扩展，支持云数据脱机阅读。 |
| 网络接口 | 探测器至少提供千兆RJ45\*4，可以支持3路监听； |
| 处理性能 | 日志采集能力：≥5000条/秒，日志源数量不限制。 |
| 功能要求 | 数据采集 | 支持通过页面直接将日志文件导入或以syslog方式接收日志信息，支持日志类型：UNIX、WINDOWS事件[2000、2003、2008、XP、VISTA、Win7及以上版本]、网络及安全设备[Cisco、Array、Juniper、H3C、神州数码、绿盟、天融信、安氏领信、深信服、网神]、AS400日志、数据库访问[Mysql]、WEB访问[Apache、IIS、Tomcat、Nginx、Weblogic、Resin、Websphere]、文件访问[VSftpd、Pureftpd、NCftpd、IISftpd、Proftpd、Glftpd、Serv-u]、数据库服务[Oracle、Mssql、Mysql、DB2、Informix、Sybase]、WEB服务[Apache、Tomcat、Nginx、Weblogic、Resin、Websphere]、FTP服务[VSftpd、NCftpd、Proftpd、Glftpd、Serv-u]；  支持SNMP日志采集，支持日志类型：网络及安全设备[Cisco、Array、Juniper、H3C、神州数码、绿盟、天融信、安氏领信、深信服、网神]  支持Opsec Lea日志采集；  支持镜像数据采集，支持类型：数据库模块[Oracle、Mssql、Mysql、DB2、Informix、Sybase]、文件传输模块[FTP、SMB、HTTP]、邮件模块[SMTP、POP、HTTP]、即时通讯模块[淘宝旺旺、MSN、QQ]、远程控制模块[Telnet]、网站访问模块[网页浏览、论坛微博]、入侵检测、业务检测、流量监控；  支持文本型日志文件定时采集，可自动将日志文件采集到系统中分析存储；  支持文本型日志原始文件管理，可将系统作为日志服务器使用；  支持FTP行为审计并提供FTP二次登陆系统及实现文件传输和过程监控的方法技术先进性证明；  支持Telnet行为审计并提供一种安全终端仿真协议监控时实现会话复制和跟踪的方法 |
| 基本功能 | 监控功能 | 支持以图表方式（饼图、柱图、曲线图）显示当日日志数据分布情况；  支持自定义配置实时监控的日志类型；  支持对所添加的资产进行实时监控，并能以不同图标显示发生的事件及告警；  支持以图表方式（饼图、柱图、曲线图、清单列表）显示当日安全事件及告警日志数据分布情况；  支持实时监控系统当前运行状态，包括系统CPU、内存、硬盘状态及管理员操作； |
| 报表分析功能 | 系统内置多种类报表模板；  支持动态\静态（日报、周报、月报）两种系统生成方式；  支持报告的邮件转发、生成提醒功能；支持多人邮件接收；  支持自定义审计报告；  支持导出html、Excel、PDF；  支持管理员自定义审计报表模板； |
| 查询分析功能 | 支持多种方式的查询检索，包括：日志检索、事件检索、告警检索、高级检索及文件检索；  支持以日志类型、时间范围及条件字段快速检索过滤；  支持高级检索以多条件组合查询方式，可以将每一个日志字段作为查询条件进行查询；  支持按日志文件的名称、内容进行检索，并提供页面下载原始日志文件；  支持查询模版创建、修改、删除功能；  支持查询结果导出； |
| 策略管理功能 | 支持内置归并策略，对HTTP数据进行自动归并处理；  支持内置关联分析策略，可设定用户在规定时间内连续多次输入错误口令产生告警或事件；  支持数据策略，可设定采集多种WEB访问数据，包括：脚本访问、样式访问、图片访问及地理数据访问；  支持自定义创建实时审计规则：根据日志字段为条件预设置分析策略；  规则条件设定支持逻辑运算符与支持正则表达式；  支持自定义三层业务策略：支持通过该策略配置，识别数据库三层架构中用户信息；  支持以告警页面、短信、邮件、SYSLOG、SNMP等各种方式呈现告警信息； |
| 数据管理功能 | 支持按日志属性、日志类型、时间范围进行数据备份；  支持WEB界面备份及日志恢复导入工作；  支持自动与手动两种备份归档方式；  系统支持以FTP上传方式将归档文件存储到第三方存储系统中；  提供业务监控状态的回溯分析，状态数据粒度不超过1分钟；  提供针对业务的原始数据包的自动关联回溯分析； |
| 系统配置功能 | 支持审计系统用户（组）管理（添加、修改、删除、停用、启用）；  支持资产管理，即所有采集日志源管理维护；  支持密码长度、复杂度，密码猜测自动锁定账号以及系统超时设置安全策略；  支持证书页面生成下载；  支持系统配置备份恢复；  支持时间同步页面配置；  支持页面方式系统升级以及设备关闭、重启；  支持从WEB界面查看网卡IP设置，修改静态路由设置等内容；  支持安全页面（SSL）证书下载； |
| 系统安全 | 系统自身安全 | 系统内置安全防火墙；支持控制访问审计主机范围；  必需提供内部通讯检查机制，传输128加密；  管理接口支持串口或电口的方式管理；  管理界面与其他功能模块分离； |
| 日志数据安全 | 审计日志文件方式存储；  审计日志加密导出审计系统；  支持对所有审计管理员操作审计系统的动作进行审计；  提供专用数据存储系统的著作权证书；  提供高性能日志及行为审计系统证书； |
| 日志权限 | 审计员只限于操作权限设置范围内的日志数据，无权限日志数据透明；  支持日志类型、IP地址权限设置；  支持页面功能模块权限设置； |
| 其他要求 | 审计平台联动能力 | 支持与运维安全管理系统实施联动部署，全面实现数据库业务访问、后台维护操作、网络运行日志及应用系统日志的综合审计； |
| 系统升级二次开发 | 在设备维保期内，厂家提供对系统软件的免费升级服务，保证系统软件为最新版本；  根据用户需求定制开发相关内容，包括关联报表和特定业务日志审计等功能； |
| 系统许可方式 | 永久许可方式，审计源无数量限制； |
| 质保服务 | 提供三年原厂保修及原厂免费现场服务，产品的安装、培训由原厂工程师完成实施，提供备品备件 |

通用要求：报价人应急响应时间：报价人接到采购人应急要求后2小时内到达现场进行服务。