**广东省职业病防治院**网络信息安全防护服务项目

1. **采购项目清单：**

|  |  |  |
| --- | --- | --- |
| **采购内容** | **最高限价** | **服务期** |
| 广东省职业病防治院网络信息安全防护服务项目 | 185000元（含税） | 本项目服务期为3年  （备注：需提供 3 年免费维护，3 年同代软件版本免费升级） |

1. **项目建设内容及要求：**

|  |  |  |  |
| --- | --- | --- | --- |
| 具体说明 | 具体需求 | 数量 | 单位 |
| 广东省职业病防治院网络安全服务需求 | 当前信息安全形势日益严峻，信息安全防护工作面临前所未有的困难和挑战。日志审计能够帮助用户更好监控和保障信息系统运行，及时识别针对信息系统的入侵攻击、内部违规等信息，同时日志审计能够为安全事件的事后分析、调查取证提供必要的信息。网络监控系统提供相关技术手段监控和记录运维人员对网络内的服务器、网络设备、安全设备、数据库等设备的操作行为。同时需具备高易用性，自动化运维、协议解析、强安全性等特点。 | 1 | 项 |
| 日志审计系统服务需求包括：  日志监控、日志采集、日志存储、日志检索、日志分析、日志转发、日志事件告警、日志报表管理  网络监控系统服务需求包括：能够对运维人员维护过程进行全面跟踪、控制、记录、回放；支持细粒度配置运维人员的访问权限，实时阻断违规、越权的访问行为，同时提供维护人员操作的全过程的记录与报告 |  |  |

**备注： 需提供 3 年免费维护，3 年同代软件版本免费升级。**

1. **项目具体技术(参数)要求：**

3.1日志审计系统服务要求：

|  |  |
| --- | --- |
| ★基本要求 | 提供可存储日志审计服务量≥180天，提供≥80个审计对象服务；  提供三年软件维护升级服务和三年原厂标准维保服务。 |
| 日志采集 | 支持SNMP Trap、Syslog、ODBC\JDBC、文件\文件夹、WMI、FTP、SFTP、SMB、NetBIOS、OPSEC等多种方式完成日志收集功能； |
| ▲支持对主流安全设备、网络设备、服务器、终端、数据库、中间件、大数据组件、应用系统等设备系统进行日志采集，包括交换机和路由器、虚拟化、云平台、安全网关设备、运维安全设备、安全审计设备、隔离交换设备、终端安全系统、Windows/Linux操作系统、分布式存储、列式存储、超融合存储服务器、Apache、Hadoop等设备组件系统，提供具有中国信息安全测评中心、公安部信息安全产品检测中心、国家版权局、国家知识产权局之中任意一家机构出具关于“服务器发现方法、系统及网络安全审计”的相关证书、检测报告等证明功能有效性及加盖原厂公章 |
| ★支持对国内主流国产化数据库进行日志数据采集，包括武汉达梦、人大金仓、南大通用、神州通用等；支持动态表名模式进行数据库采集，能按照时间或者数字的规则动态每天递增采集日志表；（提供产品功能截图） |
| 支持自定义过滤条件进行自动化日志过滤，排除繁杂无用的日志，支持一键清除过滤条件； |
| ▲支持网络流量（安全设备异常攻击流量）协议的自解析，采集器可以进行日志源个数统计并综合展示，包括最近1小时／24小时／7天／30天的采集趋势、日志范式化成功率和失败率、接收事件条数和范式化条数、日志源接入百分比、事件接收类型TOP10等、接收事件速率趋势，需提供产品相关功能截图，并提供具有中国信息安全测评中心、公安部信息安全产品检测中心、国家版权局、国家知识产权局之中任意一家机构出具关于“网络攻击事件定量分级算法的实现能力”的相关证书、检测报告等证明功能有效性及加盖原厂公章 |
| 支持按列表显示日志源地址，设备类型，接入时间，最后活跃时间、日志源告警配置状态和采集趋势等信息； |
| 日志范式化 | ▲支持全智能范式化解析模式，通过配置原始日志标识库，系统自动识别原始日志，并匹配映射系统通用标准字段，支持解析字段的编辑和调整，确保日志解析的高精准度；（提供产品功能截图） |
| ★支持在线编辑解析文件，支持基于标准化后的字段自动生成解析文件，同时支持必配事件字段查看和常用事件字段属性在线调整编辑解析规则；实现范式化文件最优化；（提供产品功能截图） |
| 日志查询 | ★支持自定义事件搜索条件，并作为检索策略保存，以树形结构进行组织，形成一个搜索分析策略树；（提供产品功能截图） |
| 支持实时检索功能，支持输入关键字进行全文搜索，从海量事件原始信息中获取与关键字匹配或部分匹配的所有事件； |
| ▲支持二次检索和嵌套检索，收敛事件范围，点击事件任意属性字段支持正序和倒序展示，并可对统计内容进行点击下钻；（提供产品功能截图） |
| 日志存储转发 | 支持日志加密压缩传输，支持加密压缩方式转发，加密方式支持SM4国密算法，支持定时转发； |
| 支持系统在数据存储时进行阈值设置，包括存储时间不能少于180天、使用容量告警、剩余容量告警、删除方式等设置； |
| 日志统计分析 | ▲支持对选中的事件日志提供在线/离线地图定位、支持源IP与目的IP分布走向的视网膜图展示、支持事件拓扑分析用于描述整个事件的访问关系及过程；（提供产品功能截图） |
| 支持对各统计策略进行基础信息编辑，自定义配置展示列信息； |
| 安全场景分析 | 支持基于规则的关联分析引擎，能够提供逻辑关联、统计关联的关联分析能力；关联规则支持规则嵌套和引用，通过多规则联合，可精确识别复杂安全事件和场景； |
| 支持安全监测场景，至少包含漏洞利用攻击、SQL注入攻击、XSS攻击、越权尝试、后门攻击、暴力登录、账户异常、病毒感染、漏洞端口扫描、僵尸主机等，同时场景支持自定义扩展； |
| ▲支持图形化方式的规则编辑器；规则支持新增、删除、移动、复制、导入、导出、启动、禁用等动作；同时纳入时序关联，支持设定一段时间内事件发生次数的阈值进行场景监控；支持指定重复事件的属性特征进行事件合并；（提供产品功能截图） |
| 支持基于规则进行告警和事件从定义，支持基于规则触发告警进一步进行观察分析； |
| 资产管理 | 支持对资产Web访问和工具访问，访问工具支持ping、telnet和远程访问等； |
| 支持拓扑维护工具，工具至少包含快速添加、连线、框选模式、移动模式、鹰眼、布局等功能； |
| 首页视图 | ★支持大屏展示，包括：支持资产总数、已接入日志资产数/未接日志资产数统计、最新24小时活跃日志源TOP10、最新24小时事件设备类型TOP10展示并支持下钻；（提供产品功能截图） |
| 支持自身资源监控展示，包括CPU、内存和硬盘利用率、日志存储占用空间、已存储天数、剩余存储天数展示； |
| 工作视图 | 支持审计视图自定义展示，系统内置视图模版，可按不同数据指标进行布局设计； |
| ★支持视图中的每个显示区域放大、缩小、拖动等操作；（提供产品功能截图） |
| 产品资质 | ★所投产品需具备中国网络安全审查技术与认证中心颁发的《网络关键设备和网络安全专用产品认证证书》，提供证书复印件及加盖原厂公章。 |

3.2. 网络监控系统服务需求：

|  |  |
| --- | --- |
| **指标项** | **指标要求** |
| ★基本要求 | 提供≥200个授权资源服务数，服务后期可支持广东省职业防治病院业务扩容为无限资源数；  提供三年软件维护升级服务和三年原厂标准维保服务。 |
| 在开启监控审计安全策略情况下，字符审计会话数≥600，图形审计会话数≥200； |
| 部署特性 | 支持在IPV4,IPV6，IPV4与IPV6网络环境下部署 |
| 支持物理旁路，逻辑串联模式，无需镜像、无需改造现有网络结构 |
| 支持单机部署、双机热备（HA)部署 |
| 支持NAT地址映射部署，通过映射后的IP地址访问堡垒机进行管理和运维操作，支持从多个映射地址访问，适用于内外网隔离的复杂网络环境 |
| 资源管理特性 | 支持资源管理功能，包括添加、删除、启用、禁用、移动、修改功能 |
| 支持限制RDP访问使用剪贴板上、下行控制、磁盘映射功能 |
| 支持限定配置中可指定用户通过指定的应用发布服务器对资源进行访问 |
| 支持资源自动发现和添加，便于快速添加资源 |
| 账号特性 | 支持资源制定不同改密分组，执行周期性、手动改密操作 |
| ★支持数据库协议自动改密，改密类型支持：Oracle、PostgreSQL、MySql、DB2、Informix 、SYBASE，Mssql(2005,2008,2012)；（提供产品功能截图） |
| 支持自动改密密码策略支持随机生成不同密码 、随机生成相同密码 、手工指定相同密码，随机密码支持自定义密码强度 |
| 支持通过改密记录进行密码找回，在当前密码丢失的情况下，可找回历史密码，资源再次回到可正常登录的状态。 |
| ▲支持WEB界面上传改密脚本，通过自定义脚本模式实现新增改密类型，满足多种改密需求（提供产品功能截图） |
| ▲支持僵尸、幽灵、孤儿帐号稽核功能，并可以导出异常账号稽核情况报告，方便管理员统计异常账号情况。（提供产品功能截图） |
| 运维审计特性 | 支持实现数据库命令级审计，支持的数据库类型包括：Oracle（支持ORACLE RAC）、SQL Server、IBM DB2、Sybase、IBM Informix Dynamic Server、MySQL、PostgreSQL、Teradata，不需采用数据镜像方式实现，以免增加部署的复杂性和网络负担； |
| ▲支持Oracle、Postgresql、Sybase、MySQL、SQL server数据库下行返回行数记录，发现高危风险操作可及时进行告警、拦截以及阻断，需提供产品相关功能截图，并提供具有中国信息安全测评中心、公安部信息安全产品检测中心、国家版权局、国家知识产权局之中任意一家机构出具的关于“数据库命令行过滤、阻断审计”的相关证书、检测报告等证明功能有效性及加盖原厂公章 |
| ▲支持在Oracle数据库运维，运维人员对变量进行绑定，执行SQL后，堡垒机系统可审计对应SQL中唯一标识符的具体值，协助审计员分析安全事件；（提供产品功能截图） |
| 支持SSH协议服务端启用强加密算法hmac-sha2-256,hmac-sha2-512，提升SSH协议安全性 |
| 支持通过应用发布实现字符协议和文件传输协议的命令级审计和图形审计的双重审计效果，命令级审计便于重现真实的完整操作命令，图形审计便于直观的查看到真实的操作行为，并支持通过搜索操作语句或执行结果中关键字定位审计回放 |
| 支持RDP、VNC图形操作行为的审计，图形回放形式还原真实操作过程 |
| 支持RDP、VNC图形操作过程中键盘输入操作记录和鼠标点击行为记录，并支持开启或关闭键盘输入审计功能 |
| 支持RDP窗口标题审计，并支持通过窗口标题内容检索定位回放 |
| 支持RDP剪切板上、下行控制 |
| 支持实时监控当前连接发生的所有会话信息，发现高危操作可实时切断会话 |
| 支持自定义审计查询条件，包括：时间范围、用户与用户IP、资源IP、资源服务、命令关键字条件 |
| ▲支持审计查询关键字和结果显示支持多种编码(UTF-8,Big5,EUC-JP,EUC-KR,GB2312,GB18030,ISO-8859-2,KOI8-R,KS\_C\_5601\_1987,Shift\_JIS,Window-874)，由审计管理员自主选择，需提供产品相关功能截图，并提供具有中国信息安全测评中心、公安部信息安全产品检测中心、国家版权局、国家知识产权局之中任意一家机构出具的关于“信息处理方法”的相关证书、检测报告等证明功能有效性及加盖原厂公章 |
| 支持提供用户统计报表和系统运行报表，支持Word，Excel，PDF，HTML方式导出 |
| 支持用户以手机号码或邮箱地址作为用户身份登录 |
| 支持运维用户多次登录失败自动锁定登录帐号或登录IP，到期自动解锁 |
| 支持限制用户同一时间只能从一个IP登录 |
| 支持密码找回：支持用户忘记登录密码时，可通过邮件方式获取验证码，验证通过后重置登录密码 |
| ▲支持调用运维人员终端电脑上的数据库工具，不改变运维人员使用习惯：SQLPlus、PLSQLDev、Toad for Oracle、Db2cmd（DB2）、Quest Central for DB2、Teradata SQL Assistant、SqlDbx Personal、SqlDbx Professional、pgAdmin3、Mysql Command、SSMS、Dbvisualizer、Navicat（提供产品功能截图） |
| ★支持扫描本地运维工具并进行配置保存，简化运维人员使用配置过程（提供产品功能截图） |
| ★支持C/S客户端模式：提供C/S客户端功能，用于运维人员和管理员通过C/S客户端登录进行运维操作和管理操作，整个运维过程不依赖任何Active或Java控件（提供产品功能截图） |
| 支持运维人员在苹果（iMac,iPad,iPhone）和安卓终端以SSH/RDP直连菜单模式登录堡垒机并进行运维操作 |
| 支持运维用户可以设置自动运维操作定时/周期执行，实现网络设备（华为、思科、h3c）配置的自动备份、供用户查看、下载 |
| 支持通过应用发布开启运维屏幕水印，运维本地无法篡改水印内容，震慑不规范的运维行为，提升运维过程数据安全性。 |
| 管理特性 | 支持管理员下发工单，授权运维人员有权限在指定时间内访问指定的资源 |
| 支持运维用户主动申请访问权限的工单，管理员审批通过后即可登录运维 |
| 实时监控系统CPU、内存、磁盘的使用情况，支持CPU、内存、磁盘使用超过阈值邮件告警，支持对系统关机、重启操作进行邮件告警，并可以设置不同事件级别 |
| ▲支持历史审计日志备份文件导入与历史审计日志查询（提供产品功能截图） |
| 支持以Syslog对外发送运维审计日志 |
| 支持配置多个日志接收服务器 |
| 支持通过WEB更新系统许可，升级系统版本、重启系统、关机 |
| ★支持管理员通过WEB界面自定义上传用户手册，保证使用手册及时更新，（提供产品功能截图） |
| 支持页面空闲超时退出，支持启用验证码，支持多次登录锁定帐号 |
| 支持自定义产品名称、产品logo图片，无需定制开发 |
| 支持系统界面可进行Ping、tracetroute等诊断，并可一键导出诊断信息 |
| 产品资质 | ★所投产品需具备中国网络安全审查技术与认证中心颁发的《IT产品信息安全认证证书》；提供证书复印件及加盖原厂公章。 |
| ▲所投产品需具备全球IPv6测试中心颁发的《IPv6 Ready Logo测试认证证书》，提供证书复印件及加盖原厂公章。 |
| 厂商资质 | ★所投产品的厂商需符合（ISO/IEC 27001）管理要求，取得《信息安全管理体系认证证书》，持有中国网络安全审查技术与认证证书中心出具的认证证书，提供证书复印件及加盖原厂公章。 |
| ▲所投产品原厂商需具备先进的信息安全产品、集成及软件系统的售后服务能力，具备《售后服务认证证书》，提供证书复印件及加盖原厂公章。 |