附件1

**江苏吕四港集团有限公司网络安全设备采购项目**

**市场询价表**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **序号** | **设备名称** | **设备参数** | **数量** | **单位** | **所报品牌** | **综合单价（元）** | **合价（元）** | **推荐**  **品牌** |
| 1 | 下一代防火墙 | 1、整机吞吐≥2Gbps;最大并发数≥100万;最大新建数≥3.5万/秒;软硬一体产品。1U机架式，CPU≥4核，内存≥8GB，硬盘≥64GBSSD: 千兆电口≥8个(含2组电口Bypass），千兆光口≥4个，接口扩展槽≥2个。  2、系统定义超过20万条资产指纹库，可识别的主机资产类型包括但不限于通用主机、移动电话、防火墙、网络摄像机、温湿度变送器、呼叫中心、云安全等；  3、漏洞扫描支 持产品内置的默认模板以及自定义模板进行漏洞扫描，可扫描出漏洞名称、漏洞级别、漏洞描述、CVE-ID、CNNVD-ID等信息；支持查看资产关联的漏洞信息，并跳转到详情。  4、系统预定义超过11000条主流攻击规则，包含对应IPS规则的级别、防护对象、操作系统、CVE编号等详细信息。  5、威胁情报检测能力：支持检测C&C、勒索软件、僵尸网络、挖矿软件、矿池地址等安全攻击类型。  6、安全模式支持智能模式和普通模式。在普通模式下，安全引擎处理网络报文遇到资源不足时会将报文直接丢弃，会影响网络转发；在智能模式下，安全引擎将尽可能的处理网络报文，但不影响网络转发。  7、支持基于源IP地址、目的IP地址、端口、协议的黑名单配置，支持自定义黑名单生效时间。  8、提供对控制策略、上网认证策略、带宽策略、策略路由、源NAT等策略的策略分析，可分析并展示问题策略数量以及所占百分比、问题策略详情、策略宽松度分布情况，简化运维工作。  9、系统管理员登录认证支持密码和手机APP令牌的双因子认证。  10、支持SMTP、IMAP、POP3、FTP、Telnet、HTTP、MYSQL、SMB、MSSQL、RLOGIN、POSTGRESQL、ORACLE协议的暴力破解侦查和访问控制，并支持用户根据实际场景修改频率阈值；支持指定接口和网段地址进行SYN、UDP、ICMP等协议的泛洪攻击的侦查和防护；支持对HTTP、FTP、SMTP、POP3、IMAP协议中传输的文件进行检测（包括上传和下载方向），用户可以选择开启其中的任何一个或者多个，可以配置每个协议的处理动作（告警/阻断）；支持查杀邮件正文/附件、网页及下载文件中包含的病毒；支持检测ZIP类型的压缩文件，支持自定义压缩文件大小限制以及解压缩层数；支持病毒排除设置，支持基于病毒文件名设置病毒白名单；支持自定义IPS特征，至少支持TCP、UDP、ICMP、HTTP等协议自定义入侵攻击特征；支持设置检测方向，包括双向、客户端方向和服务端方向。  11、具备关于“高性能多核多平台并行分布式安全操作系统”的《计算机软件著作权证书》 | 2 | 台 |  |  |  | 奇安信，锐捷，安恒 |
| 2 | 日志审计 | 1、授权资产数≥20个:标准1U硬件:CPU≥4线程/2.0GHZ 2MB，内存≥8G，硬盘≥2T，电源:单电源，网口≥6个千兆工作管理口. 每秒事务处理数≥200个（条）  2、采用解决方案包上传对产品进行功能扩展，无需代码开发。  3、支持kafka日志接收转发、大数据安全域同步、APT沙箱报告转发等大数据联调功能。Kafka收发支持SSL加密。  4、日志转发与存储支持数字签名与加密，数字签名支持SM3和SHA256，加密模式支持AES和SM4，日志接收支持解密  5、可通过接收协议限制日志接收速率，包括Http接收、syslog接收、SNMPtrap接收、TCP接收、WMI接收、aliyun接收。  6、支持通过界面自定义字段方式实现与第三方平台的数据共享，快速满足第三方平台个性化分析和对接需求。  7、可以基于日志等级进行过滤；可以通过自定义配置过滤掉用户不关心的日志；支持对收集到的重复日志进行自动聚合归并，减少日志量；支持可由用户定义和修改的日志聚合归并逻辑规则；支持将收集到的日志转发，当原始日志设备无法设置多个日志服务器时，可以通过本系统的日志转发功能将日志转发到其他日志存储设备；  8、支持关联规则性能以界面列表形式显示，可了解触发次数、最近一周监控状态等信息  9、产品获得公安部计算机信息系统安全产品销售许可证以及公安部信息安全产品检测中心出具产品检验报告。所提供的产品检验报告须符合《信息安全技术 日志分析产品安全技术要求 GA/T 911-2010》(第三级) | 1 | 台 |  |  |  | 奇安信，锐捷，安恒 |
| 3 | 漏洞扫描 | 1、CPU≥2核4线程，内存≥16GB.硬盘≥2T:电源规格:单电源，额定功率≥250W;管理口1个\*R]45 串口、千兆电口≥6个，USB口≥2个, 并发主机数、并发任务数并发主机数≥80, 并发任务数≥10个. 标准机架式1U设备  2、首页直观展示资产及资产弱点统计信息，包括资产总量分布、弱点总量分布、资产风险分布、风险主机TOP5、风险网站TOP5、主机资产风险/服务分布、弱点发现趋势等模块。  3、漏洞知识库支持自定义编辑，可编辑漏洞描述、修复建议、漏洞等级等内容，在扫描结果和导出报告中应展示编辑后的内容；支持用户自定义系统名称、版权信息和系统的Logo信息，而无需进行定制化。  4、厂商漏洞特征库大于230000条；提供详细的漏洞描述和对应的解决方案描述；漏洞知识库与CVE、CNNVD、Bugtraq、CNCVE、CNVD等国际、国内漏洞库标准兼容；具备弱口令扫描功能，支持弱口令扫描协议数量≥22种，包括FTP、SMB、RDP、SSH、TELNET、SMTP、IMAP、POP3、Oracle、MySQL、MSSQL、DB2、REDIS、MongoDB、Sybase、Rlogin、RTSP、SIP、Onvif、Weblogic、Tomcat、SNMP等协议进行弱口令扫描，允许用户自定义用户、密码字典；扫描结果在产品界面中支持查看目标应用返回的软件版本，可以方便与漏洞描述对比进行漏洞验证。  5、在资产管理页面可直接对单个资产或批量资产下发扫描任务；在做系统扫描任务时发现的新资产能够自动录入至资产管理页面；支持授权管理，对已知用户名和密码的资产可预先进行配置存放至授权管理模块，下发扫描任务时能对该部分资产的授权信息进行同步。  6、提供三权分立的账户体系，支持上下级部门管理，非上下级的不同部门任务、资产隔离；支持对用户有效期进行详细设置，可以设置不限制，也可以设置每天的哪个时段、每周的周几至周几、每月几号至几号才能正常使用；支持针对账户设置允许扫描资产范围。  7、产品支持在线升级和离线升级，至少每周进行一次漏洞特征库定期升级；支持升级服务器地址配置，支持自动更新，在设置的周期时间内自动更新。 | 1 | 台 |  |  |  | 奇安信，锐捷，安恒 |
| 4 | 杀毒软件 | 1、包含终端管理中心软件一套，200套PC端防护授权，实现对终端的统一管理和策略下发。支持查看资产的安全态势，并进行统一任务下发、策略配置，对资产进行统一管理  2、支持可视化态势大屏展示，包括终端安全管控大屏和安全概况大屏，安全概况展示内容包括防护概况、检测概况、入侵检测概况、防护风险趋势、安全动态；终端管控包括终端状态、分组分类、版本状态、安装量、防护率、在线率等；支持展示当前待处理的高危风险信息，包括弱口令、待处理病毒、待处理漏洞数据，支持一键跳转到对应处理页面；支持控制台动态更新显示全网终端安全状态分布，包括：终端总数、在线终端数、防护中终端数、异常设备数；支持查看当前TOP5风险资产、TOP5威胁IP、TOP5威胁区域，支持实时查看当前安全动态。  3、支持自动收集终端资产：监听端口、运行程序、账号、软件、启动项、Web框架、Web服务、数据库、Web应用、系统安装包、JAR包、计划任务、环境变量等信息，支持从资产的维度和信息的维度去查看数据，并支持数据的导出。支持管理员远程控制终端，处理终端及系统使用问题，并支持设置自动应答与需要终端用户相应两种模式。支持中心可对全网终端下发资产信息登记任务，支持在客户端和管理平台更新资产信息。  4、内置1500种以上检测规则，可覆盖ATT&CK矩阵的10种以上攻击战术及100种以上攻击技术，建立完整而全面的ATT&CK战技术知识库，并支持已中英文两种语言展示；可精准检测并阻断基于ATT&CK的入侵攻击；检测规则包含初始访问、执行、权限维持、权限提升、防御规避、凭据访问、信息发现、横向移动、数据收集、数据渗漏、命令与控制（C2）、影响等类型，并且可根据规则类型设置可信白名单；支持扫描后对高危漏洞进行自动修复。  5、内核级防火墙（业务间流量东西向隔离）功能，包括IP、端口、协议、流向等细粒度权限控制；支持多引擎设置，包括默认引擎、深度扫描引擎；支持从资产视角和病毒视角展示病毒查杀概况，并对病毒进行处理；  提供专门的挖矿风险评估工具；提供专门的针对未知勒索病毒的行为检测防御引擎，基于文件读写、进程、命令、网络、注册表修改等行为对于未知勒索病毒进行发现和阻断。 | 1 | 项 |  |  | 是 | 奇安信，锐捷，安恒 |
| 5 | 数据库审计 | 1、数据库实例数≥4个:1U机架式;CPU≥2核4线程:内存≥8GB，硬盘≥2TB; 内置≥250W交流单电源；2个千兆电口管理口(admin 口 1、HA口1个)，4个千兆业务电口; 整机吞吐1Gbps；双向审计数据库流量140Mbps；峰值SQL事务处理能力20000条/秒；  2、支持MongoDB、HBase、Hive、Redis、Elasticsearch、Cassandra、HDFS、Impala、Graphbase、Greenplum、SparkSQL、SSDB、ArangoDB、Neo4j、OrientDB 等数据库的审计；  3、审计信息能够记录执行时长、影响行数、执行结果描述、返回结果集  4、产品具有内置规则，规则类型有SQL注入、账号安全、数据泄露和违规操作等，并可依据规则进行邮件告警  5、支持安全规则遍历匹配，针对某个操作，将全部安全规则进行匹配，并返回所有匹配的告警结果；支持在审计日志中一键添加过滤规则，支持在告警规则中一键添加信任规则或规则白名单；设置日志检索条件时，检索条件可根据历史信息自动弹出，即输入检索条件时支持智能联想；支持告警分析功能，告警分析支持按照“客户端IP+数据库账号”的组合对SQL模板维度进行排行，支持在页面一键添加到白名单、一键添加到信任规则。  6、支持日志查询时分析筛选能力，根据查询条件自动分析出存在的数据库账号、客户端IP、客户端工具、操作系统用户名、服务端IP、操作类型、数据库名/实例名、表名、主机名、执行状态、执行时长、影响行数等，并支持在以上各个维度中灵活筛选分析； 可依据客户端工具名、数据库用户名、客户端IP、操作系统用户名、客户端主机名、数据库名、操作类型、服务器IP等配置行为模型，并可查看相应告警日志。  7、可监控Agent的转发速率，以及Agent所在数据库服务器的CPU、内存利用率，并可设置CPU、内存利用率的上限阈值，超阈值时Agent将自动停止转发数据  8、内置一键检测功能，可检测设备状态，包括流量、服务状态、设备状态、配置、许可和日志等；支持自动发现、自动添加流量中的数据库信息，并支持自定义自动发现截止时间；支持审计记录中敏感数据的脱敏处理，内置常见敏感数据脱敏规则，并支持脱敏规则自定义；支持旁路阻断；可自定义审计规则；  9、具备中国网络安全审查技术与认证中心颁发的中国国家信息安全产品认证证书 | 1 | 台 |  |  |  | 奇安信，锐捷，安恒 |
| 6 | 堡垒机 | 1、CPU≥4核4线程，内存≥8GB，硬盘≥2T，单电源（额定功率≥60W），千兆电管理口≥2，千兆业务电口≥4，USB口：USB2.0\*2，串口：RJ45串口\*1；授权资产数≥100个，并发字符连接最大数≥100个，并发图形连接最大数≥20个。  2、支持用户多角色划分功能，如系统管理员、部门管理员、运维员、审计管理员、密码管理员等，对各类角色需要进行细粒度的权限管理。支持自定义用户权限。  3、支持按部门组织架构（至少5个层级的部门）管理用户数据、资产数据、授权数据、审计数据，且数据相互隔离；可按部门层级分别设定各部门不同权限的管理员，如部门内的运维管理员、审计管理员、系统管理员等  4、支持标准化对接CAS、JWT单点登录认证，且支持配置是否自动创建堡垒机中不存在用户  5、支持常用的运维协议：SSH、TELNET、RDP、VNC、FTP、SFTP、rlogin；可通过应用发布的方式进行协议扩展，如数据库Oracle、MSSQL、MySQL、VMware vSphere Client、浏览器等客户端工具  6、单点登录支持调用多种本地客户端工具：字符：xshell、secureCRT、putty，图形：mstsc、realvnc，文件传输：secureEX、flashFXP、filezilla、winscp，数据库：ssms、sqlwb、mysqlworkbench、mysql、dbvisualizer、plsql、sqlplus、toad、db2cmd、quest central，无需应用发布服务器；支持设置共享账户，用于不同主机拥有相同账户名及密码的场景  7、支持对数据库运维会话的上行和下行命令进行审计  8、运维人员可以向管理员申请需要访问的设备，申请时可以选择：设备IP、设备账户、运维有效期、备注事由等，并且运维工单以邮件方式通知管理员；支持B/S架构进行堡垒机运维管理，至少支持使用IE、谷歌、火狐、Microsoft Edge等浏览器打开堡垒机的Web页面直接调用mstsc、VNC、Xshell、SecureCRT、Putty、winscp、flashFXP、FileZilla、SecureFX等本地运维客户端工具。  9、运维客户端自带运维工具，可不依赖 xshell/Securecrt/mstsc等工具进行运维操作  10、内置根据运维人员生成各种维度的分析报表，维度包含运维次数、时长、运维时长、活动时长、会话大小、字符命令数、传输文件数、来源IP访问数、运维时间分布等。可分别从全局及平均值、最大值、最小值、单次运维、单个会话等角度提供；内置丰富的报表统计模板，可点击曲线图进行数据钻取分析，且支持PDF、doc、html格式导出  11、支持运维报表自动定期发送，提供一键导出符合等级保护、SOX法案要求的综合分析报告  12、支持输出堡垒机告警和自身状态信息。支持邮件/syslog方式输出告警日志，可配置日志重要程度；支持通过SNMP方式输出系统信息，兼容SNMPv1、v2c和v3版本  13、支持内置VPN模块，无需与其他VPN设备联动，实现运维入口安全接入 | 1 | 台 |  |  |  | 奇安信，锐捷，安恒 |
| 7 | 服务器 | 1、2颗Intel至强4314可扩展处理器；主频≥2.4GHz且≥16核 ，散热片\*2  2、≥256GB 3200MHz，配合Intel持久内存最大支持≥6TB内存扩展或最大支持32根内存插槽  3、配置≥2块600GB 10K SAS硬盘，阵列卡支持0/1/10/5 RAID级别  4、配置≥2个千兆网卡， 1+1热插≥800W拔冗余电源 | 1 | 台 |  |  |  | 浪潮，曙光，联想 |
| 8 | 气体消防 | 无管网气体消防柜70L瓶体，药剂为无色、无味的气体，其臭氧耗损潜能值（ODP）为零，在ISO认可的洁净气体灭火剂中，其洁净性最好，具有清洁、低毒、电绝缘性能好、灭火效率高 | 1 | 套 |  |  |  | 蓝天，浙安，精胜 |
| 9 | 精密空调 | 1、机房空调总冷量应≥5.5kw，上前送风机组，机组风量≥1800m³/h，含风冷室外机；  2、机房空调采用高效换热“U”型蒸发器盘管，三面回风，并且具备安装灵活特点，可背面或两侧靠墙摆放于地面或墙角；  3、 机房专用空调应具有高效节能性，要求投标产品能效比（EER）≥3.0,显热比≥0.9,；  4、 室内风机应为多级驱动高静压直连式轴流风机，风扇数量≥2个，支持在线热插拔，不接受蜗壳式不接受蜗壳式或其他类型风机形式；  5、机房专用空调机组的风冷型室外冷凝器应采用无极全调速方式，可根据冷凝压力自动调节，以达到节能降噪的目的，并且室内外风机叶片应为全金属材质，不接受由非金属叶片风机的室外机产品。 | 1 | 台 |  |  |  | 山特，艾特网能，维谛 |
| 10 | UPS | 1、10KVA高频塔式UPS，输入功率因数（100％负载） ≥0.99，输出功率因素≥0.8.  2、输出波形为连续的正弦波，在带 100%不均衡负载时，波形失真度 ：线性负载≤2％；非线性负载≤4％。  3、整机效率：满载时双变换模式工作效率： ≥95.5％。  4、UPS 采用先进的逆变技术，高效节能，具有先进的逆变电路及电源系统，采用 UPS 直接将输入交流对外输出,利用母线输出能量对输入电压进行互补输出稳定的交流电压,使得部分交流经过双转换,降低了能量损失﹑提高了转换效率,整流部分不需要全功运转。  5、市电电池切换时间：UPS 在市电和电池两种状态间切换的时间应为 0。  6、瞬变响应恢复时间：从输出电压发生阶跃变化起到恢复到稳压精度范围内时止所需要的时间≤20ms  7、12V100AH蓄电池组，16节。  8、可放置16节12V100AH电池柜，电池柜内需包含电池连接线缆、电池直流开关。 | 1 | 台 |  |  |  | 山特，艾特网能，维谛 |
| 11 | 门禁控制系统 | 嵌入式Linux操作系统，LCD液晶屏，单目摄像头，存储容量300人脸600卡；识别方式刷卡、人脸、密码 | 1 | 套 |  |  |  | 海康，大华，得力 |
| 12 | 机房装修 | 矿棉板天面、门窗封闭、静电地板、强弱电改造、机柜、布线等 | 1 | 项 |  |  |  |  |
| 13 | 等保测评 | 对指定的一个二级系统提供第三方等保测评服务，提交测评报告及整改建议 | 1 | 项 |  |  |  |  |
| 14 | 运维服务 | 服务内容：日常安全支撑、常规安全问题处置、辅助采购方建立检查、管控机制  服务周期或次数：壹年（不少于壹月/壹次）  服务要求：  每月至少提供一次安全巡查，配合采购方完善制度和文档资料。  根据采购方需要，派遣安全团队，对重大活动、迎检活动等进行安全保障，完成各类制度、台账和迎接检查资料。 | 1 | 年 |  |  |  |  |
| **合计** | | **人民币大写： ；￥ 元** | | | | | | |

本报价表须机打并加盖报价单位公章，手填无效。

报价单位（盖公章）：

联 系 人：

联系电话：

日 期：