**关于南京医科大学附属口腔医院服务器杀毒系统**

**征集潜在供应商的调研公告**

南京医科大学附属口腔医院拟对以下项目进行摸底、调研，公开征集潜在供应商。欢迎符合要求的供应商前来报名。

**项目名称：服务器杀毒系统**

**数量：1套**

**项目基本情况介绍：**

南京医科大学附属口腔医院拟采购服务器杀毒系统一套，为数据中心虚拟化平台提供安全防护。

**资质要求：**

供应商应具有独立法人资格，营业执照。提供有效的证书复印件加盖公章。

**请仔细阅读本项目技术参数要求，并提供以下书面材料一式四份。**

1. 本公司满足本项目全部技术参数要求，无疑问。

或

本公司对本项目技术参数有正/负偏离，并附下表表述。

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 指标 | 原技术指标 | 正/负偏离 | 原因 |
| 1 |  |  |  |  |
| 2 |  |  |  |  |

2、本公司对本项目技术参数有疑问，并附下表表述，标明原技术参数，建议修改内容并阐明原因。

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 指标 | 原技术指标 | 建议修改 | 原因 |
| 1 |  |  |  |  |
| 2 |  |  |  |  |

1. 质检报告情况汇总表

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 质检报告名称 | CMA或CANS或国际权威检测机构或其他 | 依据标准 | 质检报告结果（合格/不合格） |
| 1 |  |  |  |  |
| 2 |  |  |  |  |

1. 该项目人员配置

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 姓名 | 所属工种 | 证书 |
| 1 |  |  |  |
| 2 |  |  |  |

1. 与本项目类似的成功案例（合同或中标通知书复印件）
2. 与本项目相关的公司资质证书专利等证明材料。
3. 报价一览表

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **项目名称** | | **南京医科大学附属口腔医院 项目** | | | | |
| **序号** | **货物名称** | | **品牌规格型号** | **数量** | **单价（元）** | **总价（元）** |
| 1 |  | |  |  |  |  |
| 2 |  | |  |  |  |  |
|  |  | |  |  |  |  |
| **合计金额** | | **人民币（大写） 元整**  **（¥ 元整）** | | | | |
| **供货时间** | | **签定合同后（ ）日历天内** | | | | |
| **实施期** | |  | | | | |
| **质保期** | |  | | | | |

**注：如有配件及耗材需同时提供报价**

**单位名称（公章）：**

**法定代表人（授权代表）签名：**

**联系电话（手机）：**

**年 月 日**

**七、时 间：**2022年9月6日(星期二)上午9:00

（请各供应商委派技术人员参会）

**地 点：**江苏省口腔医院新综合楼十三楼1301会议室

信息中心： 陈主任 联系方式：69593126

采购中心： 李老师 联系方式：69593106

注： 1. 提供虚假文件一经查实将终止其参与资格。

2. 资料一式四份，加盖单位公章并装订成册，概不退还。

**附件：服务器杀毒系统技术参数要求**

|  |  |  |
| --- | --- | --- |
| **类别** | **指标项** | **技术规格要求** |
|  | 数量 | ★配置≥12颗物理CPU虚拟化集群内350个虚拟机的虚拟化防护合规授权。 |
| 环境要求 | Windows 服务器客户端支持 | Windows Server 2003/Windows Server 2008/Windows Server 2008 R2/Windows Server 2012/Windows Server 2016等。 |
| Linux 服务器客户端支持 | CentOS/Ubuntu/Debian/RHEL/SUSE/Red Flag Asianux Server/Oracle Linux等。 |
| 全网威胁展示 | 多平台联动防御展示 | ★支持同时展示与同品牌的下一代防火墙、安全感知平台、上网行为管理等管理平台的联动状态（需提供产品截图证明）。 |
| 多维度威胁展示 | 支持按“最近7天”、“最近30天”、“最近三个月”不同时间维度展示病毒查杀事件爆发趋势和病毒TOP5排行榜，并展示对应的事件数及虚拟化服务器数等。 |
| 配置管理 | 自动分组 | ★支持自动分组管理，新接入的虚拟化终端等可以根据网段自动分配到对应的分组（需提供产品截图证明）。 |
| 资产管理 | 支持对系统账号信息进行梳理，了解账号权限分布概况以及风险账号分布情况，可按照隐藏账号、弱密码账号、可疑root权限账号、长期未使用账号、夜间登录、多IP登录进行账号分类查看，支持统计最近一年未修改密码的账户。 |
| 支持对系统高危端口执行一键封堵。 |
| ★支持采集服务器资产详情，包含数据库、web站点、web框架、web服务、web应用等信息，更精细化地了解服务器资产现状，大幅提升资产管理效率（需提供产品截图证明）。 |
| 威胁防御 | 威胁检测 | 支持极速、均衡、低耗三种病毒扫描模式，支持虚拟化环境下优化病毒扫描时的资源消耗。 |
| 支持本地查杀缓存，具备二级缓存机制：终端侧使用全盘文件缓存，加速本地二次扫描速度，减少对本地虚拟化环境的资源消耗；管理平台侧使用全网文件缓存，加速云查杀速度，减少通过互联网进行云查杀的带宽消耗。 |
| 具备自研的基于人工智能的检测引擎，支持无特征检测技术，有效应对恶意代码及其变种。 |
| Windows服务器安全加固 | ★支持对服务器重要目录进行权限控制，仅允许配置的可信进程操作该目录并提供配置指引（需提供产品截图证明）。 |
| 提供基于可信鉴定方式的进程防护方式，通过人工智能自学习机制，自动建立信任进程名单，阻断非可信进程的运行并提供配置指引，同时支持通过模板和手动的方式添加信任进程。 |
| 支持windows服务器RDP远程登录保护，可开启RDP远程登录二次认证，以防止黑客对服务器的入侵。 |
| Windows服务器合规检查 | ★一键式操作对指定终端/终端组进行合规性检查，包括身份鉴别、访问控制、安全审计、剩余信息保护、入侵防范、恶意代码防范，对不合规的检查项提供设置建议，并可视化展示终端的基线合规检查结果（需提供产品截图证明）。 |
| Linux服务器合规检查 | ★一键式操作对指定终端/终端组进行合规性检查，包括身份鉴别、访问控制、安全审计、 SSH策略检测、入侵防范、恶意代码防范，对不合规的检查项提供设置建议，并可视化展示终端的基线合规检查结果（需提供产品截图证明）。 |
| 漏洞扫描 | Linux漏洞扫描 | 支持对Linux终端扫描系统漏洞、提供漏洞分析详情和修复建议。 |
| windows漏洞修复及补丁管理 | 支持对Windows终端的漏洞情况进行扫描，并查看漏洞具体情况及KB号，并显示具体修复情况。 |
| ★支持流行Windows高危漏洞的轻补丁免疫防御，支持支持Windows补丁批量一键修复（需提供产品截图证明）。 |
| 微隔离 | 流量可视 | 服务器详情支持展示服务器的资源状态（CPU占有率、内存占有率和磁盘率）、流量分布Top5、该服务器开放的服务。 |
| ★支持图形化显示业务系统、服务器及流量详情（需提供产品截图证明）。 |
| 流量线详情支持展示该流量线对应的控制策略；图形化显示服务器间流量关系，包括访问详情、流量趋势等。 |
| 桌管功能 | 远程桌面控制 | ★支持对Windows服务器远程控制管控终端桌面的功能，便于管理员能够及时对存在故障的终端进行维护（需提供产品截图证明）。 |
| 违规外联 | 支持Windows服务器侧的违规外联动能，有效帮助管理员规范终端上网行为。 |
| 资质 | 厂商资质 | ★所投产品的生产厂商应是国家互联网应急响应中心网络安全应急服务国家级支撑单位，提供有效证书的复印件。 |
| 要求所投产品的生产厂商为国家信息安全漏洞共享平台(CNVD)技术组成员，提供有效证书的复印件。 |
| ★要求所投产品的生产厂商具备中国网络安全审查技术与认证中心的信息安全软件开发服务资质，提供有效证书复印件。 |
| 产品售后服务 | ★要求原厂商在南京设有独立法人直属办事处等服务机构，以便于为客户提供完善、及时的售后服务。 |
| 必须提供7×24小时400电话支持；本地化应急服务紧急攻击事件2小时内响应，最大限度减少损失。 |
| 必须提供产品相关的使用和技术培训。 |