**第一项 采购需求**

**采购包一：终端防护中心项目**

### 一、设备清单

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 名称 | 规格 | 数量 |
| 1 | 服务器安全防护软件 | 配置200点服务器端使用授权(支持windows和linux)、质保期内免费升级 | 1套 |
| 2 | 终端安全防护软件 | 配置1000点终端PC使用授权(支持windows和linux)、质保期内免费升级 | 1套 |
| 3 | 终端安全管理平台 | B/S架构管理平台，质保期内免费升级 | 1套 |

### 二、项目要求

终端检测响应平台 EDR，围绕终端资产安全生命周期，通过预防、防御、检测、响应赋予终端更为细致的隔离策略、更为精准的查杀能力、更为持续的检测能力、更为快速的处置能力。在应对高级威胁的同时，通过网“端” 云协同联动、威胁情报共享、多层级响应机制，帮助用户快速处置终端安全问题，构建轻量级、智能化、响应快的下一代终端安全系统。

1、预防能力：为用户提供对终端资产盘点、安全基线核查、智能微隔离、东西向流量可视等预防能力。

2、防御能力：为用户提供对勒索软件、爆破入侵、后门上传、活跃僵尸程序等的实时防御能力。

3、检测能力：为用户提供对恶意文件、入侵攻击、web后门、热点事件的检测能力。响应能力 ：支持全网威胁定。

**三、主要技术参数**

### 1、服务器安全防护软件

|  |  |  |
| --- | --- | --- |
| **序号** | **功能项** | **功能要求说明** |
| 1 | 产品规格 | ★需提供：≥200个点服务器使用授权(支持windows和linux) |
| 2 | 管理可视化 | ▲采用B/S架构的管理控制中心，具备终端安全可视，终端统一管理，统一威胁处置，统一漏洞修复，威胁响应处置，日志记录与查询等功能。控制中心根据客户端点数的增加支持横向扩展； |
| 3 | 多维度  威胁展示 | 支持全网风险展示，包括但不限于未处理的勒索病毒数量、高级威胁、暴力破解、僵尸网络、WebShell后门、高危漏洞及其各自影响的终端数量 |
|  | 提供勒索病毒整体防护体系入口，直观展示最近七天勒索病毒防护效果，包括已处置的勒索病毒数量、已阻止的勒索病毒行为次数、已阻止的未知进程操作次数、已阻止的暴力破解攻击次数 |
| 4 | Webshell  事件处理 | 支持展示终端检测到的WebShell事件及事件详情，包括：恶意文件名称，威胁等级，受感染的文件，发现时间，检测引擎，文件类型，文件名，文件Hash值，文件大小，文件创建时间；可配置WebShell实时扫描，一旦发现WebShell文件，可自动隔离或仅上报不隔离 |
| 5 | Windows  服务器加固 | 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 |
| 6 | 勒索病毒  专防 | 基于勒索病毒攻击过程，建立多维度立体防护机制，提供事前入侵防御-事中反加密-事后检测响应的完整防护体系，展示勒索病毒处置情况，对勒索病毒及变种实现专门有效防御 |
| 支持监控诱饵文件，诱饵文件可被实时监控，当勒索病毒对该文件进行修改或加密操作时进行拦截 |
| 7 | 暴力破解  检测 | 统计单个攻击源及分布式攻击源的暴力破解检测，支持按照RDP、SMB和SSH类型进行封堵并自定义爆破阈值，可对封停时间进行自设置 |
| 8 | 主动防御 | 支持对进程防护、注册表防护、驱动防护、U盘安全防护、邮件防护、下载防护、IM防护、局域网文件防护、网页安全防护、勒索软件防护 |
| 9 | 威胁处置 | 构建全网文件信誉库，当一台终端发现某一病毒文件，全网可进行感知并进行针对性查杀，支持处置病毒时选择是否在其它终端上同步处置 |
| 具备强力专杀云端下发通道，支持在管理端批量下发强力专杀工具到内网各终端快速响应终端威胁。 |
| 10 | 病毒扫描 | 支持基于IP（组）、服务和角色维度进行流量访问控制，实现对应用服务之间的访问隔离，并且支持对配置项的备份以及恢复操作 |
| 支持对压缩包内的病毒扫描，支持多层压缩包的扫描，可自定义配置压缩包的扫描层数，至少大约10层模式下的扫描 |
| 11 | 漏洞防护 | 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Windows补丁批量一键修复（提供产品截图证明并加盖投标供应商公章） |
| 12 | 厂商资质 | 为保障产品自身安全性，所投产品厂商应是国家信息安全漏洞共享平台CNVD用户组成员，提供官网查询截图证明。 |

### 2、终端安全防护软件

|  |  |  |
| --- | --- | --- |
| **序号** | **功能项** | **功能要求说明** |
| 1 | 产品规格 | ★需提供：≥1000点终端PC使用授权(PC支持linux，windows，macos等系统) |
| 2 | 一体化管控 | 单一管理控制中心可统一管理分别部署在Windows PC、Windows服务器、Linux服务器以及国产化服务器的客户端软件 |
| 3 | 管理可视化 | ▲采用B/S架构的管理控制中心，具备终端安全可视，终端统一管理，统一威胁处置，统一漏洞修复，威胁响应处置，日志记录与查询等功能。控制中心根据客户端点数的增加支持横向扩展； |
| 4 | 威胁检测 | 通过智能识别终端环境情况（低配硬件、老旧设备、虚拟化等）和当前终端资源占用，在闲时实时监控和病毒扫描场景，都可智能调整EDR的资源占用（CPU、IO等），为业务让出资源，不卡业务，对业务零摩擦 |
| 5 | 自动分组 | 支持终端自动分组管理，新接入的终端可以根据网段自动分配到对应的分组 |
| 6 | 文件实时监控 | 可实时监控文件的状态，在文件读、写、执行或者进入主机时主动进行扫描，支持根据用户性能偏好设置高、中、低3种防护级别 |
| 7 | 勒索病毒  专防 | 基于勒索病毒攻击过程，建立多维度立体防护机制，提供事前入侵防御-事中反加密-事后检测响应的完整防护体系，展示勒索病毒处置情况，对勒索病毒及变种实现专门有效防御 |
| 支持监控诱饵文件，诱饵文件可被实时监控，当勒索病毒对该文件进行修改或加密操作时进行拦截 |
| 支持用户直接对勒索病毒的家族名、病毒名、加密文件后缀名执行链接查询，可通过直接上传加密文件的方式确定勒索病毒类型，如果能解密可以提供必要的解密工具 |
| 8 | 暴力破解  检测 | 统计单个攻击源及分布式攻击源的暴力破解检测，支持按照RDP、SMB和SSH类型进行封堵并自定义爆破阈值，可对封停时间进行自设置 |
| 9 | 病毒扫描 | 支持对压缩包内的病毒扫描，支持多层压缩包的扫描，可自定义配置压缩包的扫描层数，至少大约10层模式下的扫描。 |
| 10 | 威胁处置 | 构建全网文件信誉库，当一台终端发现某一病毒文件，全网可进行感知并进行针对性查杀，支持处置病毒时选择是否在其它终端上同步处置 |
| 11 | 主动防御 | 支持对进程防护、注册表防护、驱动防护、U盘安全防护、邮件防护、下载防护、IM防护、局域网文件防护、网页安全防护、勒索软件防护 |
| 12 | 桌管 | 支持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 |
| 支持一键拦截已安装软件的恶意广告弹窗，可在客户端查看拦截记录，包括拦截内容、拦截次数等。 |
| ▲支持自定义拦截终端软件弹窗，可在终端设置自动拦截骚扰弹窗开关。（需提供产品截图证明并加盖投标供应商公章） |
|  | 支持扫描和拦截捆绑、静默、强行安装等不良传播行为，一键清理问题软件，可在客户端查看拦截安装日志。 |
| 支持终端自定义选择拦截问题软件安装或者常规软件安装 |
| 13 | Windows  智御 | 支持基于应用、端口和账号的清点，可辅助客户进行已停更Windows系统的风险识别。 |
| 14 | 漏洞防护 | 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Windows补丁批量一键修复 |
| 15 | 产品资质 | 厂商是中国反网络病毒联盟ANVA成员单位、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，需提供相关证书和官方截图证明（投标时提供相关证明材料复印件并加盖投标供应商公章）。 |

**四、相关要求：**

1、所供产品必须符合国家标准，设备和配件为全新原装，功能符合使用要求，保证为正规渠道供货的正宗原厂产品。须提供良好的售后服务，终身提供技术支持。

2、供货方式、时间及地点要求：

合同签订后30天内设备运抵江苏医药职业学院校内指定地点，并完成安装及调试。

3、质保期及服务要求：

（1）培训及售后服务：现场完成安装、调试之后，由中标方工程师提供免费操作培训。培训内容主要包括设备原理、基本操作要领、设备简易故障排除和维护保养知识等。

（2）须提供售后服务团队人员名单清单和联系方式。

（3）质保期：提供至少1年的免费质保期，自验收合格之日起计算。质保期内成交供应商需提供7×24小时热线服务、须定期上门进行例行检查，并做好记录，以保证系统正常运行。若出现重大质量问题，由成交供应商进行免费重新部署安装调试。对于采购方的服务通知，成交供应商必须在接到通知后1小时内予以响应，若有必要，成交供应商工程师必须2小时内到达现场，常见问题 4小时内处理完毕。若大问题在24小时内未能有效解决，成交供应商须免费提供同档次的系统给予采购方临时使用。

质保期外，服务响应时间与质保期内一致，同时系统升级给予以合理优惠价格供应。

4、验收方法及验收标准：

货物发运前，必须对系统的质量、规格、性能等方面的技术数据进行综合检验，需随系统提供检验合格证书和原产地证明书。 现场安装、调试结束后，中标方和采购方相关人员按验收标准进行验收。验收标准为采购文件、投标文件、合同中的相关技术及服务条款内容。

**采购包二：防毒墙系统项目**

### 一、设备清单

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 设备名称 | 基本规格参数 | 数量 |
| 1 | 防毒墙 | ≥2U标准机架式设备，配置≥6 个千兆电口、≥4个万兆光口(含光模块);网络层吞吐率≥10Gbps；防病毒吞吐率≥ 1Gbps;国产CPU,CPU主频≥3.0GHz，8 核,≥32GB内存,≥2TB硬盘,≥双电源,国产操作系统，配置安全集中管控平台对设备进行管理；包含安装部署相关模块和跳纤等配件。中标后提供三年服务承诺函及三年特征码升级授权。（投标时提供承诺，格式自拟） | 1套 |
| 2 | 三层  交换机 | 结构：标准机架式；万兆SFP+光口≥12个（含模块等）、千兆电口≥12个、≥1个Console口，≥1个Manage口；交换性能≥1.28Tbps/12.8Tbps；包转发率≥480Mpps（若存在双参数，则以较小参数为准）；双交流冗余电源； | 1台 |

### 二、项目要求

近年来，挖矿、勒索等病毒事件频发，传统网络边界安全设备往往无能为力。网络边界安全传统设备防火墙，它主要工作在网络层、传输层（4层）之下，通过对协议、地址和服务端口的识别和控制达到防范入侵的目的，可以有效的防范基于业务端口的攻击。

但随着信息化的发展，安全威胁呈现了“多、快、高”的发展趋势。“多”是指安全事件数量多，全球权威的恶意软件监测组织 AV-test.org的统计分析显示, 每年的全球病毒与恶意软件数量持续增长并有加速的趋势。“快”是指安全威胁入侵的蔓延速度快、发现漏洞后攻击出现的时间快，最新的蠕虫病毒可以在几分钟之内就蔓延到全球范围，新的漏洞公布后几个小时就出现针对漏洞的攻击行为或工具，“高”是指安全威胁的层次越来越高，目前的威胁多数已经从网络层发展到应用层。特别是近年来勒索软件、挖矿病毒愈演愈烈，因此针对第7层应用层的防护显得尤为重要。

我校网络防毒墙体系建立的目的，是为了完善我校安全建设体系，构建一个强壮、有效的边界防御体系，保护外链流量的安全，检测并拦截外网进出流量的恶意行为、恶意软件病毒、威胁攻击。同时可以满足国家《网络安全法》和等级保护制度的相关要求。

**三、主要技术参数：**

**1、防毒墙技术指标**

|  |  |  |
| --- | --- | --- |
| **序号** | **指标项** | **指标参数** |
| 1 | ★硬件  规格 | ≥2U标准机架式设备，配置≥6 个千兆电口、≥4个万兆光口(含光模块);网络层吞吐率≥10Gbps；防病毒吞吐率≥ 1Gbps;国产CPU,CPU主频≥3.0GHz，8 核,≥32GB内存,≥2TB硬盘,≥双电源,国产操作系统，配置安全集中管控平台对设备进行管理；包含安装部署相关模块和跳纤等配件。中标后提供三年服务承诺函及三年特征码升级授权。（投标时提供承诺，格式自拟） |
| 2 | ★性能 | 网络层吞吐率≥10Gbps、防病毒吞吐率≥1Gbps |
| 3 | 仪表盘 | ▲能够对威胁进行可视化展示，展示维度至少包括威胁类型统计（至少包含勒索、挖矿、病毒、APT、漏洞利用威胁事件）、近30天威胁事件趋势、攻击源IP TOP5、受影响主机TOP5、勒索&挖矿事件拦截统计、热门威胁事件TOP5、自定义黑名单TOP5等.(提供产品界面截图并加盖投标供应商公章） |
| 4 | 防病毒 | 支持超过不少于100种协议的解析, 包括但不限于：HTTP/SMTP/POP3/FTP/SMB/TFTP/TCP/UDP/NFS/SNMP/ICMP/RTMP/DNS/IRC等 |
| ▲能够支持SMBv1/SMBv2/SMBv3文件共享协议的病毒检测与查杀.(提供产品界面截图并加盖投标供应商公章） |
| 能够防御多种类型的恶意软件 (包括但不限于病毒、木马、蠕虫、后门、间谍软件、灰色软件、Rootkits等) |
| 能够启动更加先进的防病毒引擎，用以查杀不同级别的具有可疑行为的文件 |
| 支持能够提交可疑文件至APT增强定制化沙箱模块做联动分析，且能从沙箱模块同步、文件SHA1、URL、IP及域等情报做进一步处理.(提供产品界面截图并加盖投标供应商公章） |
| 能够支持两个的防病毒引擎同时工作，并能够按需开启 |
| 所投产品的厂商需具备自主研发能力，产品需至少具备自研防病毒、深度包解析和威胁情报引擎。能够精准高效对勒索、挖矿、病毒、APT、漏洞利用威胁事件检测拦截，同时支持0day或者N day漏洞快速响应。 |
| 能够支持快速扫描模式和深度扫描模式切换，确保在不同网络环境下的查杀效率 |
| ▲能够允许定义被扫描文件的大小范围，最大不小于2G。(提供产品界面截图并加盖投标供应商公章） |
| 5 | 挖矿治理 | 产品需要具备在网络边界的挖矿检测和拦截能力，并能够直观展现拦截的挖矿事件 |
| 6 | 威胁情报 | 能够支持威胁情报能力以覆盖更大范围的威胁检测 |
| 支持用户自定义黑/白名单，支持URL黑/白名单设置、支持邮件收发件人黑/白名单设置、支持基于SHA1的文件黑/白名单设置。 |
| 7 | 部署 | 支持桥接、路由、监控模式部署所投产品需部署方式灵活以适应客户丰富的应用场景，支持ICAP部署模式 |
| 8 | 安全性  和可靠性 | 为保证稳定性，所投产品需具备流量扫描优化的高可靠机制： |
| 支持bypass功能 |
| 可对CPU、内存阈值进行设置，当超过该阈值，防毒墙主进程自动清理且不中断业务 |
| 9 | 产品资质 | ▲产品必须是自主开发，国家信创产品，拥有自主知识产权，市场主流的，非OEM产品 |
| ▲产品必须为专业网关防病毒产品，非防火墙/下一代防火墙、UTM、IPS等具有防病毒功能模块的产品，提供公安部“网关防病毒”销售许可证书(提供证书复印件和证书查询截图并加盖投标供应商公章)，并且在计算信息系统安全专用产销售许可服务平台上防病毒类中的网关防病毒类别内可查询；查询网址:https://ispl.mps.gov.cn/ispl/jsp/common/ProductList\_Public.jsp |
| 产品获得国家强制性产品CCC认证证书。(提供证书复印件并加盖投标供应商公章) |

#### 2、三层交换机技术指标

|  |  |  |
| --- | --- | --- |
| **序号** | **指标项** | **指标参数** |
| 1 | 三层交换机 | 1、★万兆SFP+光口≥12个、千兆电口≥12个、≥1个Console口，≥1个Manage口；  2、▲交换性能≥1.28Tbps/12.8Tbps；包转发率≥480Mpps；（若存在双参数，以较小参数为准）；  3、双交流电源1+1冗余；  4、支持≥32K MAC地址；  5、交换机支持：二层广播、配置静态IP地址、DHCP Option43、DNS域名等方式自动发现控制器平台；  6、三层功能：支持静态路由、OSPF、RIP等动态路由；  7、▲支持M-LAG技术，跨设备链路聚合，要求配对的设备有独立的控制平面，提供功能配置截图或官网截图证明；  8、为保证内网安全性，防止病毒在内网横向传播，要求交换机具有东西向风险流量安全功能；  9、为禁止非法终端(例如私接路由器)接入；需支持终端类型库，能自动识别PC、路由器、监控终端设备等； |

**四、质量和服务要求：**

1、所供产品必须符合国家标准，设备和配件为全新原装，功能符合使用要求，保证为正规渠道供货的正宗原厂产品。须提供良好的售后服务，终身提供技术支持。

2、供货方式、时间及地点要求：

合同签订后30天内设备运抵江苏医药职业学院校内指定地点，并完成安装及调试。

3、质保期及服务要求：

（1）培训及售后服务：现场完成安装、调试之后，由成交方工程师提供免费操作培训。培训内容主要包括设备原理、基本操作要领、设备简易故障排除和维护保养知识等。

（2）须提供售后服务团队人员名单清单和联系方式。

（3）质保期：提供至少3年的免费质保期，自验收合格之日起计算。质保期内中标人需提供7×24小时热线服务、须定期上门进行例行检查，并做好记录，以保证设备正常运行。对于采购方的服务通知，中标方必须在接到通知后1小时内予以响应，若有必要，中标方工程师必须2小时内到达现场，常见问题 4小时内处理完毕。若大问题在48小时内未能有效解决，中标方须免费提供同档次的设备给予采购方临时使用。

质保期外，服务响应时间与质保期内一致，同时备品备件以合理优惠价格供应。

4、验收方法及验收标准：

货物发运前，必须对系统的质量、规格、性能等方面的技术数据进行综合检验，需随系统提供检验合格证书和原产地证明书。 现场安装、调试结束后，中标方和采购方相关人员按验收标准进行验收。验收标准为采购文件、投标文件、合同中的相关技术及服务条款内容。