**[招标项目需求](#_Toc488762883)**

**一、项目概况**

本项目旨在为学校构建覆盖全网的主动防御体系，通过部署态势感知平台作为安全中枢，实时整合校内网络流量、设备日志及威胁情报数据，实现校园网络威胁可视化分析与预警；配套分布式态势感知探针，对关键网络节点进行细粒度流量采集与异常行为检测；升级下一代出口防火墙，强化应用层攻击防御与上网行为管控；部署自动化漏洞扫描系统，定期对服务器、终端设备进行弱点评估与修复验证；同时引入提供一站式安全托管服务，涵盖7×24小时安全监控、策略优化、应急响应，形成"监测-防护-响应"闭环管理，有效提升校园网络安全防护能力，保障教育信息化系统稳定运行。

**二、货物清单**

**（一）货物总清单**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **序号** | **项目名称** | **数量** | **单位** | **采购预算金额**  **（人民币元）** | **备注** |
| 1 | 安全设备购置项目 | 1 | 批 | 576,102.20 | 拒绝进口 |

**（二）货物明细清单**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **序号** | **产品名称** | **数量** | **单位** | **备注** |
| 1 | 出口防火墙 | 1 | 台 | 拒绝进口 |
| 2 | 漏洞扫描系统 | 1 | 台 | 拒绝进口 |
| 3 | 态势感知平台 | 1 | 台 | 拒绝进口 |
| 4 | 态势感知探针 | 1 | 台 | 拒绝进口 |
| 5 | 一站式安全托管服务 | 1 | 套 | 拒绝进口 |

**说明：**

**1、进口产品，是指通过中国海关报关验放进入中国境内且产自关境外的产品。**

**注明“拒绝进口”的产品不接受进口产品参与投标；注明“接受进口”的产品允许投标人选用进口产品参与投标，但不排斥国内产品参与投标。**

**2、根据《政府采购货物和服务招标投标管理办法》（财政部令第87号）第31条的规定，提供相同品牌产品的不同投标人参加同一合同项下投标的，处理原则如下：**

（1）采用最低评标价法的采购项目，提供相同品牌产品的不同投标人参加同一合同项下投标的，以其中通过资格审查、符合性审查且报价最低的参加评标；报价相同的，由采购人或者采购人委托评标委员会按照招标文件规定的方式确定一个参加评标的投标人，招标文件未规定的采取随机抽取方式确定，其他投标无效。

（2）使用综合评分法的采购项目，提供相同品牌产品且通过资格审查、符合性审查的不同投标人参加同一合同项下投标的，按一家投标人计算，评审后得分最高的同品牌投标人获得中标人推荐资格；评审得分相同的，由采购人或者采购人委托评标委员会按照招标文件规定的方式确定一个投标人获得中标人推荐资格，招标文件未规定的采取随机抽取方式确定，其他同品牌投标人不作为中标候选人。

（3）非单一产品采购项目，采购人应当根据采购项目技术构成、产品价格比重等合理确定核心产品，并在招标文件中载明。多家投标人提供的核心产品品牌相同的，按前两款规定处理。**（本项目的核心产品为：态势感知探针）**

**三、技术要求**

**（一）详细技术要求**

**说明：1、带▲号参数为重要参数，其他参数（非▲号参数）为普通参数，如出现负偏离，将按照评分准则做扣分处理；**

**2、评分时，如对一项招标技术要求（以划分框为准）中的内容存在两处（或以上）负偏离的，在评分时只作一项负偏离扣分。**

|  |  |  |
| --- | --- | --- |
| **序号** | **产品名称** | **参数要求** |
| 1 | 出口防火墙 | 1. 性能参数：网络层吞吐量≥20G，应用层吞吐量≥10G，防病毒吞吐量≥1.5G，IPS吞吐量≥1.5G，全威胁吞吐量≥1G，并发连接数≥300万，HTTP新建连接数≥9万 |
| 1. 硬件参数：规格：1U，内存大小≥8G，硬盘容量≥120G SSD，电源：单电源，接口≥8千兆电口，≥2万兆光口SFP+。实配万兆多模光模块2个，光纤跳线2条。 |
| 1. 产品支持路由模式、透明模式、虚拟网线模式、旁路镜像模式等多种部署方式。 |
| 1. 产品支持IPv4/IPv6双栈工作模式，以适应IPv6发展趋势。 |
| 1. ▲产品支持Cookie攻击防护功能，并通过日志记录Cookie被篡改。**（需提供产品功能截图证明及具备CMA/CNAS标识的第三方检测报告）。** |
| 1. ▲产品内置不低于16000种漏洞规则，同时支持在控制台界面通过漏洞ID、漏洞名称、危险等级、漏洞CVE标识、漏洞描述等条件查询漏洞特征信息，支持用户自定义IPS规则。**（需提供产品功能截图证明和具备CMA/CNAS标识的第三方检测报告）** |
| 1. ▲产品支持僵尸主机检测功能，产品内置僵尸网络特征库超过128万种，可识别主机的异常外联行为。**（需提供产品功能截图证明和具备CMA/CNAS标识的第三方检测报告）** |
| 1. 产品支持3种以上的用户认证方式,包含但不限于单点登录、本地账号密码、外部账号密码认证。 |
| 1. 产品支持多维度流量控制功能，支持基于IP地址、用户、应用、时间设置流量控制策略，保证关键业务带宽日常需求。 |
| 1. 产品内置超过4580种WEB应用攻击特征，支持对跨站脚本（XSS）攻击、SQL注入、文件包含攻击、信息泄露攻击、WEBSHELL、网站扫描、网页木马等攻击类型进行防护。 |
| 1. 产品支持服务器漏洞防扫描功能，并对扫描源IP进行日志记录和联动封锁。 |
| 1. ▲产品支持独立的账号安全防护模块，具备事前账号脆弱性、事中账号爆破、事后账号失陷的全生命周期安全防护，在设备界面可以详细展示账号安全相关信息，包括风险业务、风险等级、存在账号入口、存在弱口令、遭受口令爆破、异常登录账号**（需提供产品功能截图和“账号安全”相关计算机软件著作权登记证书扫描件）** |
| 1. 为满足未来链路数量增加的需要，增配一张万兆双光口卡一张。 |
| 2 | 漏洞扫描系统 | 1. 授权：系统漏扫授权IP数≥100，WEB漏扫授权URL数≥20；性能指标：主机漏扫最大并发IP数≥150，WEB漏扫最大并发URL数≥5。 |
| 1. 硬件参数：规格：1U，内存大小≥8G，硬盘容量≥128GB SSD，≥2TB SATA；电源：单电源，接口≥6千兆电口，≥2千兆光口SFP。 |
| 1. 支持全局风险统计功能，通过扇形图、条状图、标签、表格等形式直观展示资产风险分布、漏洞风险等级分布、紧急漏洞、风险资产清单等信息，并可查看详情；支持快速进行漏洞验证，验证漏洞有效性。 |
| 1. 支持全面扫描、资产发现、系统漏洞扫描、弱口令扫描、WEB漏洞扫描、基线配置核查六种任务类型，其中全面扫描支持系统漏洞扫描、WEB漏洞扫描、弱口令扫描同时执行。 |
| 1. 提供检测结果综述分析，按照网络安全等级保护2.0的检测项要求，统计客户业务系统存在的不符合、部分符合、符合、待确认、不适用检测项，直观了解自身业务系统合规情况。 |
| 1. 按“一个中心、三重防护”的架构展示检测结果，每个检测结果呈现具体问题及整改建议，系统支持手动核查确认、整改后重新检测、以及手动导入全局分析和人工核查报告来对测评报告中的结果进行核查确认，其中手动核查确认支持单项核查确认和批量核查确认。 |
| 1. 产品支持对系统漏洞、WEB漏洞、基线配置、弱口令进行扫描和分析，可同时输出包含系统漏洞扫描、WEB漏洞扫描、基线配置核查、弱口令扫描结果的报表。**（需提供产品功能截图证明）** |
| 3 | 态势感知平台 | 1. 性能参数：存储容量：≥21T，在带宽性能1Gbps时存储时长≥1200天/1Gbps。 |
| 1. 硬件参数：规格：2U，内存≥128GB，系统盘≥240GB SATA SSD，数据盘≥32TB，标配盘位数≥12，电源：冗余电源，接口≥4千兆电口。 |
| 1. 支持主机类资产识别，能够识别资产数据来源、IP地址、主机名、MAC地址、基线异常、操作系统、操作系统详请、主机类型、服务与端口、状态、责任人、EDR状态、标签、最近上线时间、所属资产组织、资产名称、应用、IP类型、识别方式、首次发现时间等。 |
| 1. 支持整体展示服务器脆弱性风险分析、热点漏洞情况、脆弱性风险详情（漏洞风险、配置风险、弱密码、web明文传输、可用性风险），支持第三方漏扫报告导入和解析，可按资产组分类上传，支持上传文件。 |
| 1. ▲支持威胁定性引擎以分析告警的上下文关联、时序关系、历史告警发生的频率规律性，结合威胁情报与安全专家经验对当前的安全告警进行目的性确认，从而确认安全告警的优先级顺序，支持基于人工渗透、程序自动化、业务相关风险、其它4个维度对告警进行分类，帮助安全人员快速定位高危告警并及时处置。**（需提供产品功能截图，且所投产品必须提供第三方权威机构相关的产品检测报告（具备CMA/CNAS标识），为确保功能真实有效，采购人有权利要求供应商中标后提供样机以备功能查验）** |
| 1. ▲平台支持挖矿专项检测页面，基于规则的本地挖矿检测和基于主动探测技术的云端挖矿检测。支持挖矿实时检测播报本地和云端的挖矿检测分析结果，支持展示挖矿主机数量，支持以列表的形式展示挖矿事件，包括最近发生时间、威胁描述、威胁定性、挖矿阶段、威胁等级、受害者IP、攻击次数、威胁情报等信息；**（需提供产品功能截图，且所投产品必须提供第三方权威机构相关的产品检测报告（具备CMA/CNAS标识），为确保功能真实有效，采购人有权利要求供应商中标后提供样机以备功能查验）** |
| 1. 支持可视化的形式展示威胁的影响面，通过大数据分析和关联检索技术，可清晰直观看清失陷主机对其他主机的影响，评估受损情况，方便客户快速处置。支持通过首页搜索框输入IP/域名/URL/端口/通信对进行搜索，支持基于列表模式展示横向攻击、违规访问、风险访问、可疑行为、正常访问等详细信息，建立全方位的持续性的检测能力。支持入口点溯源功能，分析出首次失陷、疑似入口点、首次遭受攻击等信息，帮助管理人员快速找到攻击入口点。 |
| 1. ▲支持PPT格式导出摘要报告，报告内容包括：网络安全整体解读、网络安全风险详情、告警及事件响应盘点，用户可直接通过导出的PPT报告进行工作汇报，高效体现工作价值。**（需提供产品功能截图证明，为确保功能真实有效，采购人有权利要求供应商中标后提供样机以备功能查验）** |
| 1. 文件威胁分析支持平台内置的恶意脚本分析引擎、webshellkiller智能引擎、save智能分析引擎以及云端分析引擎组合进行综合研判，协议类型有HTTP、FTP、SMB、SMTP、POP3、IMAP多种类型，支持展示查杀数据统计、受害资产攻击数TOP5，支持以列表的形式展示文件威胁信息，包括最近发生时间、威胁描述、威胁定性、威胁类型、攻击阶段、受害者IP、攻击次数等信息。 |
| 1. ▲为确保产品具备基础安全防护能力，要求所投产品符合GB 42250-2022《信息安全技术 网络安全专用产品安全技术要求》、GB/T 42453-2023《信息安全技术 网络安全态势感知通用技术要求》技术规范，**具备网络安全专用产品安全检测认证证书或检测报告，提供有效期内的相关证明文件。** |
| 4 | 态势感知探针 | 1. 性能参数：网络层吞吐量≥1.5Gbps，应用层吞吐量≥500Mbps。 |
| 1. 硬件参数：规格：1U，内存大小≥8G，硬盘容量≥256GB SSD，电源：单电源，接口≥6千兆电口，≥2千兆光口SFP |
| 1. 支持传输安全检测日志，包括网站攻击检测日志、漏洞利用攻击检测日志、僵尸网络检测日志、业务弱点发现日志。 |
| 1. 支持流量抓包分析，基于五元组灵活抓取数据包，可定义配置源IP、源端口、目的IP和目的端口、传输层协议选择添加抓包任务，并支持带标签抓取vlan、mpls等协议数据包，帮助安全工程师高效分析威胁。 |
| 1. 支持命令注入检测、PHP代码检测、XSS攻击检测、Webshell上传检测、SQL注入检测、XXE攻击检测、JAVA代码检测、SQL非注入型检测、MYSQL解析增强、php反序列化检测等自定义配置启用，针对命令注入检测、SQL注入检测等类型支持自定义高检出、低误报模式。 |
| 1. 支持敏感信息检测功能，内置身份证、MD5、手机号码、银行卡号、邮箱等敏感信息，可自定义敏感信息检测策略选择组合的敏感信息，可基于IP统计和连接统计2种方式进行命中次数统计。 |
| 1. 支持HTTP未知站点下载可执行文件、浏览最近30天注册域名、浏览恶意动态域名、访问随机算法生成域名、暴力破解攻击、反弹连接、IRC通信等僵尸网络行为检测。 |
| 1. 支持智能语义引擎检测，可针对http隧道、java反序列化保护等类型进行自定义设置。 |
| 1. 支持检测出网络中的网络拓扑设备进行绘制，更多直观可视化查看网络整体情况。 |
| 1. 支持5种场景的日志传输模式,包含标准模式、精简模式、高级模式、局域网模式、自定义模式，适应不同应用场景需求。 |
| 1. 内置URL库、IPS漏洞特征识别库、应用识别库、WEB应用防护识别库、僵尸网络识别库、实时漏洞分析识别库、白名单库。 |
| 1. 提供三权分立的用户管理能力：系统管理员、审计管理员、安全管理员、普通管理员四个角色相互独立；同时支持IP绑定的登录安全设置。普通管理员角色的权限可自定义模块页面的编辑和查看权限。 |
| 5 | 一站式安全托管服务 | 1. ▲暴露面梳理：投标方应使用安全工具对招标方服务资产开展互联网暴露面探测，以梳理资产面向互联网的开放情况，快速发现违规暴露在互联网中的资产及存在的风险并进行处置，实现对暴露面资产可管可控，降低暴露面资产的风险。   投标方应具备互联网暴露面梳理的服务工具，该工具应当支持全资产和精确资产两种模式暴露资产收集模式，收集到的暴露面信息至少包括域名、域名标题、IP地址、开放端口、资产指纹、网站截图、移动端暴露面，并且能采集对应暴露资产的访问截图向招标方举证，及对应暴露资产存在的漏洞**（提供服务工具具备以上暴露面梳理能力的证明截图）** |
| 1. ▲7\*24小时威胁鉴定：投标方应当具备云端检测和分析平台，通过采集招标方安全设备和工具的安全告警和安全日志，结合大数据分析、人工智能等技术手段，为招标方提供7\*24小时持续不间断的安全威胁分析鉴定，同时在用户界面进行展示；   分析研判包括但不限于对脆弱性、异常流量、攻击日志、病毒日志等数据进行采集和实时分析研判，支持将同一资产的多个告警进行聚合分析发现各类安全事件并生成工单，并在告警详情中展示告警的基本信息，涉及的业务信息、攻击趋势、威胁详情、攻击原理、处置建议等内容，并支持根据客户情况提供备注**（提供云端服务平台告警审核功能界面截图，举证一个告警聚合分析的例子和一个告警详情展示具备上述能力）** |
| 1. ▲受影响资产排查与加固：安全专家应当结合威胁情报主动排查是否对服务资产造成影响并通知用户，及时协助进行安全加固。**（提供一个威胁情报的安全通报工单，工单内容包含威胁情报的基本信息和推送信息以及跟进记录，要求明确说明关联资产信息的排查情况）** |
| 1. 为了提升防护效果，提供不少于30点终端安全防护软件授权（服务器版），不少于300点终端安全防护软件授权（PC版） |
| 1. 重要时期（HW、重大活动）值守：安全专家在值守前主动进行风险排查（外网高风险端口、安全策略、漏洞、弱密码等）、提供风险排查报告；在值守期间调高威胁监测对抗灵敏度，4H一次战报和值守日报；值守结束后提供值守总结（融合到最近季度报告中一起汇报）。 |
| 1. ▲服务质量监控：投标方需为招标方提供的服务成果展示门户（或用户Portal）应具备服务质量可视化展示，投标方能通过可视化的数据，清晰的了解安全专家的服务水平，至少包括脆弱性闭环率、脆弱性平均响应时长、脆弱性平均闭环时长、威胁闭环率、威胁平均响应时长、威胁平均闭环时长、事件闭环率、事件平均闭环时长，以验证投标方所承诺的服务指标（或称为服务SLA）。**（提供服务成果展示门户中服务质量监控相关的截图证明；）** |
| 1. ▲服务交付物管理：投标方需为招标方提供的服务成果展示门户（或用户Portal），可以直观的管理服务过程中生产的服务报告和交付物，包括但不限于《项目启动会PPT》、《首次安全风险分析报告》、《威胁情报》、《安全运营周报》、《安全运营月报》、《安全运营季报》、《年度总结汇报》等。**（提供服务成果展示门户中支持管理上述交付物的相关截图证明；）** |
| 1. ▲投标方云端服务平台应当做好严格的安全防护，并严格按照《信息安全技术—网络安全等级保护基本要求》完成等级保护测评工作，服务平台至少通过等级保护三级测评；**（投标方应当提供云端服务平台等级保护三级测评通过证明，提供报告首页、基本信息表、等级测评结论首页，以上内容中必须明确指出该平台用于为用户提供7\*24小时的安全托管服务；（敏感内容投标方可脱敏展示））** |
| 1. 投标方托管服务平台应具备AI服务工具，支持集成在服务微信群、服务工作台，该工具能力项应支持告警数据包研判、情报查询分析、Payload解码、事件研判定性、自动调用安全设备遏制（IP、域名封堵）、事件调查溯源、运营数据统计（支持在线统计、分析并下载数据）等。 |
| 1. ▲服务过程透明化可视化：投标方需为招标方提供移动端服务过程展示门户（移动端Portal），通过清晰可视化的风险消减图和漏洞消减图，让招标方清晰了解云端安全托管服务的风险消减机制，直观实时了解当前风险闭环情况。**（提供移动端服务过程展示门户中支持展示风险消减图和漏洞消减图的截图证明。）** |
| 1. ▲投标方需为招标方提供移动端服务过程展示门户（移动端Portal），支持实时直观地查阅服务的每日运营动态。运营动态需包括【事件通告】【威胁通告】【威胁情报】【服务报告】【夜间值守快报】等，并支持自定义进行筛选和管理。**（提供移动端服务过程展示门户中支持查阅每日运营动态的截图证明。）** |
| 1. ▲投标方需为招标方提供移动端服务成果展示门户（移动端Portal），支持直观地管理服务过程中安全运营结果，以“资产、威胁、事件三大抓手”为维度，呈现服务后业务实时的安全情况和运营结果。**（提供移动端服务过程展示门户中支持业务侧实时的安全情况和运营成果的截图证明）** |
| 1. 为了保障服务质量和加强投标方与招标方的沟通，投标方应当承诺为招标方配置一名经验丰富的安全专家作为专属服务经理，并且实时响应投标方咨询的网络安全相关问题； |
| 1. 投标方应当为招标方提供7\*24小时的安全守护，不论是白天、黑夜、节假日投标方都应该能做到7\*24H在线服务，并且在节假日期间应当每日为招标方提供《节假日值守总结》 |

**（二）人员要求**

投标人需为本项目配备1名项目负责人，8名项目团队成员。投标人所安排的项目人员在项目服务期间，未经招标人同意不允许随意变更。

**四、商务要求**

**说明：1、带“★”指标项为实质性条款，如出现负偏离，将被视为未实质性满足招标文件要求作投标无效处理。**

**2、评分时，如对一项招标商务需求（以划分框为准，一个划分框是作为一项招标商务需求）中的内容存在两处（或以上）负偏离的，在评分时只作一项负偏离扣分。**

|  |  |  |
| --- | --- | --- |
| **序号** | **目录** | **招标商务需求** |
| **（一）免费保修期内售后服务要求** | | |
| 1 | 维修响应及故障解决时间 | 在保修期内，一旦发生质量问题，投标人保证在接到通知24小时内赶到现场进行修理或更换。 |
| 2 | 关于免费保修期 | 货物免费保修期 3 年，一站式托管服务免费 1年，时间自最终验收合格并交付使用之日起计算。 |
| 3 | 其他 | 3.1、投标人应按其投标文件中的承诺，提供1次使用操作培训服务。 |
| 3.2、投标人应按其投标文件中的承诺，进行其他售后服务工作。 |
| **（二）其他商务要求** | | |
| **★1** | **关于交货** | **1.1交货地点：采购人指定校区内的安装位置。** |
| **1.2投标人必须承担的设备运输、安装调试、验收检测和提供设备操作说明书、图纸等其他类似的义务。** |
| **1.3签订合同后 20 天（日历日）内交货。** |
| 2 | 关于验收 | 2.1投标人货物经过双方检验认可后，签署验收报告，产品保修期自验收合格之日起算，由投标人提供产品保修文件。 |
| 2.2当满足以下条件时，采购人才向中标人签发货物验收报告：  a、中标人已按照合同规定提供了全部产品及完整的技术资料。  b、货物符合招标文件技术规格书的要求，性能满足要求。  c、货物具备产品合格证。 |
| 3 | 关于违约 | 3.1中标人不能交货的，需偿付不能交货部分货款的 2 %的违约金并按主管部门相关规定处理。 |
| 3.2中标人逾期交货的，按主管部门相关规定处理。 |
| 3.3中标人所交付产品、工程或服务不符合其投标承诺的，或在投标阶段为了中标而盲目虚假承诺、低价恶性竞争，在履约阶段则通过偷工减料、以次充好而获取利润的，将被履约评价工作实施机构评为履约等级“差”并按主管部门相关规定处理。 |
| **★4** | **关于付款** | **货物运送到指定地点安装并调试完毕、验收合格后，凭正式发票按合同全款在15工作日内转帐支付至指定银行账户。** |