黄淮学院下一代数据中心与安全建设项目—
网络安全运营中心建设竞争性谈判公告

（招标编号：HNZB[2024]N0903）

项目所在地区：河南省,驻马店市

一、招标条件

本黄淮学院下一代数据中心与安全建设项目—网络安全运营中心建设已由项目审批/核准/备案机关批准，项目资金来源为自筹资金229万元，招标人为黄淮学院。本项目已具备招标条件，现招标方式为其它方式。

二、项目概况和招标范围

规模：详见采购文件。

范围：本招标项目划分为1个标段，本次招标为其中的：

(001)网络安全运营中心建设;

三、投标人资格要求

(001网络安全运营中心建设)的投标人资格能力要求：1、满足《中华人民共和国政府采购法》第二十二条规定；

2、落实政府采购政策需满足的资格要求：无；

3、本项目的特定资格要求：无;

本项目*不允许*联合体投标。

四、招标文件的获取

获取时间：从2024年09月30日 08时00分到2024年10月09日 18时00分

获取方式：1、时间：2024年9月30日～2024年10月9日，上午8：00时～12：00时，下午15：00时～18：00时（节假日除外）。2、方式：获取竞争性谈判文件时须提供下列资料：提供营业执照副本、法定代表人身份证、法定代表人授权委托书（须注明项目名称、编号、联系电话及邮箱，若因电话及邮箱未留存清楚导致信息接收有误的，采购人及采购代理机构不负任何责任）、被授权

人身份证，以上资料均需是加盖公章的清晰扫描件，按顺序排列为PDF版发送至邮箱1150105437@qq.com。3、竞争性谈判文件每套售价：0元。

五、投标文件的递交

递交截止时间：2024年10月15日 09时00分

递交方式：河南招标采购服务有限公司四楼418室（河南省郑州市纬四路13号），纸质文件现场提交。

六、开标时间及地点

开标时间：2024年10月15日 09时00分

开标地点：河南招标采购服务有限公司四楼418室（河南省郑州市纬四路13号）

七、其他

项目概况

黄淮学院下一代数据中心与安全建设项目—

网络安全运营中心建设采购项目的潜在供应商应在河南招标采购服务有限公司获取本项目竞争性谈判文件，并在2024年10月15日9时00分（北京时间）前提交响应文件。

一、项目基本情况

1、采购项目编号：HNZB[2024]N0903

2、采购项目名称：黄淮学院下一代数据中心与安全建设项目—

网络安全运营中心建设

3、采购方式：竞争性谈判

4、预算金额：2290000.00元；最高限价（如有）：2290000.00元

资金来源：单位自筹

序号 包号 包名称 包预算（元） 包最高限价（元）

1 A 网络安全运营中心建设 2290000.00 2290000.00

5、采购需求：详见附件

6、合同履行期限：合同签订之日起至质保期结束

7、本项目是否接受联合体竞标：否

8、是否接受进口产品：否

9、是否为只面向中小企业采购：否

二、申请人的资格要求

1、满足《中华人民共和国政府采购法》第二十二条规定；

2、落实政府采购政策需满足的资格要求：无；

3、本项目的特定资格要求：无；

三、获取竞争性谈判文件

1、时间：2024年9月30日～2024年10月9日，上午8：00时～12：00时，下午15：00时～18：00时（节假日除外）。

2、方式：获取竞争性谈判文件时须提供下列资料：

提供营业执照副本、法定代表人身份证、法定代表人授权委托书（须注明项目名称、编号、联系电话及邮箱，若因电话及邮箱未留存清楚导致信息接收有误的，采购人及采购代理机构不负任何责任）、被授权人身份证，以上资料均需是加盖公章的清晰扫描件，按顺序排列为PDF版发送至邮箱1150105437@qq.com。

3、竞争性谈判文件每套售价：0元。

四、响应文件提交

1、响应文件提交截止时间：2024年10月15日9时00分（北京时间）。

2、响应文件提交地点及方式：河南招标采购服务有限公司四楼418室（河南省郑州市纬四路13号）现场提交。逾期提交的、未提交到指定地点的响应文件，采购人将予以拒收。

五、响应文件开启

1、响应文件的开启时间：同响应文件提交截止时间；

2、响应文件的开启地点：在河南招标采购服务有限公司四楼507房间（河南省郑州市纬四路13号）。

六、发布公告的媒介及公告期限

本次竞争性谈判公告在《中国招标投标公共服务平台》《河南省电子招标投标公共服务平台》网站上发布。公告期限为三个工作日。

七、其他补充事宜

1、执行《政府采购促进中小企业发展管理办法》[财库（2020）46号]；

2、执行《关于进一步加大政府采购支持中小企业力度的通知》财库〔2022〕19

号；

3、执行《财政部、司法部关于政府采购支持监狱企业发展有关问题的通知》（财库[2014]68号）；

4、执行《三部门联合发布关于促进残疾人就业政府采购政策的通知》（财库[2017]141号）；

5、执行关于印发节能产品政府采购品目清单的通知（财库〔2019〕19号）；

6、根据《关于在政府采购活动中查询及使用信用记录有关问题的通知》(财库[2016]125号)、《河南省财政厅关于转发财政部关于在政府采购活动中查询及使用信用记录有关问题的通知的通知》（豫财购〔2016〕15号）的规定，对列入失信被执行人、重大税收违法失信主体、政府采购严重违法失信行为记录名单的供应商（投标人），拒绝参与本项目的谈判；【查询渠道：（www.creditchina.gov.cn）、“信用中国”网站、中国政府采购网（www.ccgp.gov.cn）】；

八、监督部门

本招标项目的监督部门为/。

九、联系方式

招 标 人：黄淮学院

地　　址：河南省驻马店市开源大道76号

联 系 人：尹老师

电　　话：0396-2853541

电子邮件：/

招标代理机构：河南招标采购服务有限公司

地　　址：郑州市金水区纬四路13号

联 系 人：王西西

电　　话：13271738993

电子邮件：/

招标人或其招标代理机构主要负责人（项目负责人）：_____（签名）

招标人或其招标代理机构：_____（盖章）

采购需求

黄淮学院下一代数据中心与安全建设项目—

网络安全运营中心建设采购项目清单

序号	名称	数量	单位	备注
1	网络安全运营中心	1	项	
2	上网行为管理	1	套	
3	WEB应用防火墙	1	套	
4	日志审计	1	套	
5	应用安全防护平台	1	套	
6	网络安全运营工作站	8	套	
7	触控一体机	1	套	
8	智能门锁	1	套	
9	办公桌椅	2	套	
10	网络安全运营指挥中心环境建设	1	项	

一、技术参数

序号	名称	技术参数要求	数量	单位
1	网络安全运营中心	**一、安全运营服务** 1、提供不低于1名驻场安全工程师，驻场服务期限不低于6年；驻场人员需按国家法定工作日和学校作息时间在学校安全运营中心工作，节假日根据学校实际工作安排，持续现场保障；重大活动期间，提供7x24小时现场保障；驻场服务期间，按照学校要求提供工作日志和每日运营报告；驻场期间学校对驻场人员考核不达标或驻场人员能力无法担任安全运营工作的，学校有权要求供应商更换驻场人员，供应商应即时响应。 2、提供不低于350个数据中心资产（IP）7x24小时安全托管服务。 3、提供中国信息安全测评中心-cisp或教育部教育管理信息中心-ECSP认证证书培训，提供不少于3人次的培训服务，保证参加培训老师获得认证证书。 4、提供3次网络安全周宣传所需展板、展架及其他所需材料，根据学校实际需求，按需提供，所产生的费用由中标人承担。 5、提供不低于5名后端实名网络安全专家，所有网络安全专家以实名方式在运营支撑系统内完成各项服务动作，服务过程与成果记录对应至具体网络安全专家。 6、系统内配置服务质量管理的各项质量指标要求，指标项应不少于 60项，以指标项对项目整体、各网络安全专家进行评价，并在系统中提供专用的运营质量可视化管理功能。基于现场部署的安全运营支撑系统、流量安全监测引	1	项

		擎，以用户数据不离场的方式开展不低于3年期的持续性威胁检测和响应服务。 7、为保证项目网络安全运营部分顺利交付及运营，投入的网络安全专家必须为厂商技术专家，提供证明材料及网络安全专家在安全领域资格认定证书辅证并加盖投标人公章。 8、运营团队应分级、分角色且线上化、工作量化管理，角色包括：一线分析师、二线分析师、三线分析师、交付经理等，工作量化包括：提报事件数量、测试成果数量、处置告警数量、待确认告警、待处理事件任务、待确认资产、待认领任务等。 **1）资产管理服务** 1、提供资产梳理服务。分析师通过用户自主上报、原有台账核对、安全工具扫描等方式对用户内网资产进行全面探测、识别和梳理，协助用户建立资产管理台账，并将资产信息录入部署在用户现场的安全运营支撑系统，作为后续安全运营工作开展的基础。 2、业务系统对象的梳理应至少包含资产对象类型、资产对象名称、资产组、更新时间、等保级别、责任主体、责任人、域名、互联网IP与服务端口对应关系、局域网IP与服务端口对应关系、关联基础资源对象等内容。 3、基础资源对象的梳理应至少包含资产对象类型、资产对象名称、资产组、主机名称、更新时间、等保级别、责任主体、责任人、局域网IP与端口服务组对应关系、基础资源软件、关联业务系统对象等内容。 4、具备资产、事件、漏洞的关联检索能力，可将资产的未整改漏洞、安全事件及各类扫描引擎结果进行关联，精细化管理资产对象的安全属性及相关安全状态。 5、提供整合校内安全组件的能力，不限于WAF、IDS/IPS、日志审计等，实时监测CPU性能、内存性能、存储		

		资源用量，可视化展示本周事件提报数、事件完成审核数、事件待审核数量、本周发出复测安排数量、本周完成复测数量、待执行复测数量。 **2）漏洞管理服务** 1、业务系统漏洞监测与测试成果可进行全生命周期管理，可结构化管理的漏洞数据信息包含但不限于漏洞名称、类型、相关单位、漏洞地址、复现步骤、提报人、业务系统名称、加固建议，发现时间等，分析师利用以上数据提供对漏洞闭环处置工作全流程、全阶段的支撑服务。 2、基础资源漏洞扫描成果可进行全生命周期管理，可结构化管理的漏洞数据信息包含但不限于漏洞名称、漏洞级别、漏洞详细描述、修复建议、CVE编号、CNCVE编号、CNNVD编号、扫描时间、受影响资产系统名称、IP、处置状态等，分析师利用以上数据提供对漏洞闭环处置工作全流程、全阶段的支撑服务。 3、提供每年不低于12次针对学校内网主机漏洞扫描服务，安全分析师基于漏洞扫描引擎，对用户指定的内网主机开展漏洞扫描和弱口令验证，发现可利用的安全漏洞。 4、提供每年不低于12次针对校内业务系统的专项安全测试服务，安全分析师基于测试矩阵，对应用系统开展周期性专项安全测试，专项安全测试内容包括主流热点漏洞（如：SQL注入、弱口令、XSS等）和框架类漏洞（如：spring漏洞、struts2漏洞、ThinkPHP漏洞、java反序列化漏洞等）。 5、专属的有效性验证团队在有效性验证矩阵指导下，通过在不同区域发起针对验证标靶的各类攻击动作，检验网络安全防御体系是否完整、检验运营规则的有效性以及安全设备检测能力的有效性。有效性验证成果报告通过邮件、短信、微信服务号及电话方式与管理员进行沟通处置，并支撑复验过程；在安全数据不		

		离场的情况下，有效性验证的服务成果数据在安全服务设备中流转。 6、提供热点漏洞持续监测服务，一旦发现最新披露的热点漏洞，分析师将立即开展热点漏洞测试，并将最新披露的热点漏洞纳入到周期性专项安全测试范围。 **3）安全事件管理服务** 1、分析过程记录。系统的记录字段应包含但不限于事件标题、事件级别、事件描述、标签、部门、推断发生时间、受影响资产、相关漏洞、可疑对象等，系统应可将威胁事件从检测、分析至处置的全过程保存为卷宗模式存储，确保安全动作可基于记录复盘。 2、运营服务团队应通过聚合、清洗多源情报，提供可直接使用的有效情报进行威胁分析。应能够基于现场网络安全运营支撑平台对事件进行情报碰撞，提高事件检出率，并通过运营脚本驱动在事件分析过程中进行校验。 3、运营服务团队应能够基于运营支撑系统构建运营脚本驱动安全运营人员依照分析流程开展安全运营工作，并具备对每个流程环节进行质量监控的能力。运营脚本要求能够根据不同的威胁事件类型进行针对性设计，细化威胁事件检测的确认过程及分析要点，将检测确认步骤拆分成固定任务，使安全运营人员能够依照运营脚本定义的威胁事件检测任务有序、有效完成威胁事件的检测及确认工作。 4、在运营支撑系统内所维护的运营脚本中，具备对各种类型事件进行调查分析的标准化操作要求，并驱动分析师对每个调查环节进行质量监控。运营服务团队应具备使用 ATT&CK 方法编制安全运营脚本的能力，系统默认内置运营脚本不得少于100个，每个事件脚本中必须包含事件确诊、升级分析、危害扩线与溯源分析、闭环处置等各个阶段的运营动作规范。		

		5、运营脚本应包括紧急、高、中、低等级别分类，支持根据业务场景创建、导入、导出、初始化脚本，创建脚本时提供脚本模板并可关联上下级模板。（提供产品功能界面截图证明，并加盖供应商公章） **4）互联网暴露面管理服务** 1、使用分布式的资产监测引擎对学校互联网出口进行7×24小时监测，对于在互联网侧暴露的资产进行持续探测，当互联网资产发生变化时（如：IP新增、端口开放或关闭、指纹信息变更、服务协议变化等），运营支撑系统会对变化内容进行变更标记，调度客户现场分析师对该资产进行分析，确认资产变化为高危端口/服务后实时进行预警通告，同时调度支撑系统与分析师依据标准测试矩阵对变更资产实时进行专项安全测试，监测结果通过服务接口推送至综合安全运营项目现场部署的运营支撑系统服务工具中，与内部网络资产信息共同构建完整的网络安全资产台账，测试成果纳入漏洞全生命周期台账统一管理，依据相应的运营脚本驱动风险处置。 2、互联网暴露面管理还应包括对敏感信息泄露的管理，如监测任务名称、监测关键词数量、关键词站点数量、网盘敏感信息数量、GitHub敏感信息数量、互联网暴露邮箱数量等。（提供产品功能界面截图证明，并加盖供应商公章） **5）运营质量指标** 1、提供3年期威胁监测、事件分析处置服务，7*24小时安全监控服务。安全分析师实时处理告警信息，确诊安全事件，理清事件影响范围，所有分析出的安全事件在安全运营支撑系统中建立完整分析档案进行管理。 2、运营质量指标至少包括服务项目事件平均定性时长(MTTA)、服务项目事件平均检出时长(MTTD)、任务执行及时率、告警判断的准确率、事件提报准确率、事		

		件处置率等指标，所有指标必须在运营感知平台中以可视化形态进行展示。（提供产品功能界面截图证明，并加盖供应商公章） **6）运营有效性验证** 通过在不同区域发起针对验证标靶的各类攻击动作，检验网络安全防御体系是否完整、检验运营规则的有效性以及安全设备检测能力的有效性。有效性验证成果报告通过邮件、短信、微信服务号及电话方式与管理员进行沟通处置，并支撑复验过程；在安全数据不离场的情况下，有效性验证的服务成果数据在服务设备中流转。 **7）服务交付标准** 《标准化安全运营运营实施方案与计划书》 《标准化安全运营资产梳理矩阵》 《标准化安全运营攻击事件告警》 《标准化安全运营安全预警》 《标准化安全运营验证记录》 《标准化安全运营周报》 《标准化安全运营月报》 《标准化安全运营季报》 《标准化安全运营年报》 《标准化安全运营总结报告》 **二、安全运营管理平台** 支持软硬一体化形态和纯软件形态部署模式，支持集群部署，可扩展到多台设备集群。 1、数据采集与存储 支持接入并管理日志采集器、流量采集器；支持Syslog、SNMP Trap、Netflow、JDBC、WMI、FTP、SFTP、agent等方式采集网络设备、安全设备、服务器等日志，并进行解析、范式化、预处理。 提供智能分诊能力，达到告警的降噪目的。智能分诊		

		模型支持分诊规则、加白分诊规则两种规则的创建，分诊规则支持配置过滤条件和配置过滤条件组，过滤内容包括：告警名称、首次告警时间、源IP、目的IP、源端口、目的端口、通信方向、攻击者等信息 ；智能分诊支持生效时间配置，包括：永久生效和自定义时间。（提供产品功能界面截图证明，并加盖供应商公章） 2、威胁情报 支持本地威胁情报的检索，检索类型支持域名、IP地址、文件MD5值；威胁情报内容支持IOC、攻击链阶段、置信度、类型描述、威胁家族、攻击事件/团伙、影响平台、情报状态、威胁描述等。 支持云端威胁情报查询，查询包含：IP主机信息、IP位置、域名流行度、情报IOC、相关样本、可视化分析、域名解析记录、域名注册信息、关联域名、数字证书等信息。 为提高学校APT攻击发现能力，需要产品制造商提供至少10份以上公开发布的APT报告作为证明。 3、资产管理 支持管理主机资产和网站资产，主机资产包括不限于主机设备、网络设备、安全设备、应用系统等类型；支持管理网站资产。 支持DHCP场景下的资产管理，支持对DHCP网段范围、DHCP租期、资产唯一标识等属性进行配置。支持查看DHCP场景下资产IP的变更记录（提供产品功能界面截图证明，并加盖供应商公章） 4、威胁预警 支持对重大网络安全事件（如log4.j 漏洞）进行威胁预警，针对重大网络安全事件生成威胁预警包，通过系统自动升级的方式分发给平台用户。也支持通过导入威胁预警包并启动威胁预警任务，完成网络安全事件的影响面评估和分析。（提供产品		

		功能界面截图证明，并加盖供应商公章） 支持根据风险资产数量统计自定义关键点节点条件，比如大面积爆发、有效控制、威胁缓解等。支持事态扩散过程发展趋势图的展示及详细告警列表及告警信息展示。（提供产品功能界面截图证明，并加盖投标人公章） 支持与学校现有使用的互联网资产监测系统进行无缝对接，实时同步学校互联网资产测绘情况及相关威胁情报预警，由此产生的费用由供应商承担。（提供对接承诺函并加盖供应商公章） 5、脆弱性管理 支持导入第三方漏洞扫描报告，至少支持绿盟、启明、奇安信、天融信、Tenable等漏扫报告的解析识别和导入管理。（提供产品功能界面截图证明，并加盖供应商公章） 支持与学校现有WEB智能监控系统进行无缝对接，实时同步学校Web应用的漏洞监测情况，及时全面发现学校Web应用风险，及时进行整改加固。由此产生的费用由供应商承担。（提供对接承诺函并加盖供应商公章） 6、威胁检测 预置关联规则覆盖第三方日志源，包括但不限于防火墙、防毒墙、IPS（IDS）、WAF、服务器、VPN等； 支持自定义关联规则，支持类VISIO的图形化连线拖拽的交互配置方式而非编辑逻辑语法树配置方式；提供1100+条预置规则；支持日志关联规则建模，在指定的时间范围内，能够对来自不同数据源的日志进行关联分析，以发现可信度更高的威胁告警；（提供产品功能界面截图证明，并加盖供应商公章） 预置的关联规则分析场景，包括但不限于：攻击利用、恶意软件、拒绝服务、异常事件、内容安全、信息收集、威胁活动、情报命中等场景的分析；预置关联规则支持展示覆盖ATT&CK矩阵情况，支持通过告警关		

		联到ATT&CK知识库 7、告警分析 支持场景化分析能力，专题展示不同场景下的安全风险。支持异地账号登录、暴力破解、明文密码泄露、弱口令、VPN登录地域分布、VPN账号登录行为、邮件威胁分析、邮件敏感关键词、邮件敏感后缀等专题场景化分析及信息展示。 8、事件调查 支持事件调查管理，支持查看事件详情信息及事件调查处置的时间轴信息；事件详情包括事件概览、受影响资产，ATT&CK战术，攻击技术及攻击者信息列表，关键攻击痕迹，证据库（包含：告警、资产及脆弱性、添加的证据截图及描述信息等）、处置建议。支持在证据库- 告警列表页面进行告警搜索过滤，支持在证据库- 资产列表页面进行资产搜索过滤。（提供产品功能界面截图证明，并加盖供应商公章） 9、工单响应 支持通过工单形式通知告警、漏洞、弱口令及配置核查，通知方式包括邮件、短信、企业微信、专用通讯工具；工单状态包含待下发、待处置、处置中、已处置、已完成、已撤销，支持对工单状态的跟踪；工单支持SLA（服务等级协议），支持对工单SLA要求进行设置，SLA超期支持通知提醒。（提供产品功能界面截图证明，并加盖供应商公章） 提供工单专用及时通讯工具平台（非微信、钉钉、QQ等通用互联网应用）免费使用，方便及时沟通威胁告警信息，避免学校敏感信息泄露，要求平台能支持信息加密。 10、联动处置 支持与学校防火墙、上网行为管理等设备进行协同对接及联动处置，可直接在本平台下发封堵的处置策略		

		， 由此产生的费用由供应商提供。 11、态势大屏展示 支持态势大屏，包括资产风险态势、全网脆弱性态势、外部威胁态势、内网威胁态势、安全运营态势、威胁预警态势等可视化大屏。 支持与学校现有使用的校内舆情监测系统对接，为学校提供智慧校园整体安全态势展示，由此产生的费用由供应商承担。（提供对接承诺函并加盖供应商公章） 12、系统管理 支持双因子认证方式登录系统，认证方式支持短信和邮箱，支持对登录的并发会话数的设置，限制同时登陆系统的用户数量。 支持对接威胁情报平台，实现对可疑IP、域名、URL的情报鉴定。（提供产品功能界面截图证明，并加盖供应商公章） **三、网络出口区安全运营流量采集** 1、硬件配置 3U机箱，双电源，配置2个万兆光口，4个千兆光口，4个千兆电口，1个Console口，5个接口扩展板卡插槽，支持液晶面板实时显示，可通过液晶屏直观查看基本信息。 2、性能指标 支持吞吐量不低于20Gbps，HTTP并发连接数不低于1500万，每秒HTTP新建连接数不低于50万/秒。 3、旁路部署 旁路部署在网络中实时采集网络流量数据、威胁检测，支持通过重置会话的方式阻断TCP威胁会话连接，支持通过流量被动识别资产。 4、流量采集 需支持空载荷过滤，支持对采集的流量的上下行载荷		

		长度设置。（提供加盖供应商公章的功能截图证明材料） 5、流量识别与解析 支持精准识别通讯类、语音类、视频类、更新类、下载类、邮件类、金融类、理财类等多类别的应用识别，应用识别库3000+。 支持ICMP、DHCP、HTTP、TELNET、DNS、SSL等基础协议的解析，支持LDAP、Kerberos、Radius等认证解析。 具有自定义解析流量能力，支持基于正则表达式、TLV格式、固定长度等提取模式对流量解析。（提供产品功能界面截图证明，并加盖供应商公章） 6、文件还原 支持还原多种文件传输协议，包括：邮件（SMTP、POP3、IMAP、webmail）、Web（HTTP）、FTP、SMB、TFTP、QQ等。 7、威胁检测 系统具备间谍软件检测能力，可检测常见的病毒蠕虫、僵尸网络、黑市工具、勒索软件、挖矿木马、隧道、代理、后门程序、远控木马等。 系统提供的攻击特征不应少于10000条有效最新攻击规则，特征库需支持自动及手动升级。 本地集成威胁情报库，支持实现基于威胁情报的失陷主机检测，情报不少于200万。 系统需具备专业的查毒引擎，独立的病毒库，支持通过对HTTP、FTP、SMTP、POP3、IMAP、SMB、TFTP、NFS协议进行恶意文件检测。 系统本地需具备攻击告警的过滤能力，能够针对IP地址或端口对攻击告警进行过滤，支持攻击特征高亮展示，方便分析人员事件分析。 8、数据外发 通信模式支持但不限于KAFKA、ZMQ、SYSLOG等协议，		

		需支持多路外发，并支持外发多地址的负载均衡处理。（提供产品功能界面截图证明，并加盖投标人公章） 传输模式支持加密、压缩、以及认证，认证包括但不限于kerberos认证、LDAP认证。（提供产品功能界面截图证明，并加盖供应商公章） 9、流量及样本取证 支持威胁告警的相关pcap数据留存，支持本地下载及外发，外发通信协议包括但不限于KAFKA、FTP、SFTP等。 10、二次开发接口 系统提供二次开发接口，接口形式为Restful API，提供功能配置、统计等接口。 11、协同联动 支持与学校现有的内网舆情系统进行联动，通过内网舆情系统获取解密后的校园网加密互联网流量进行安全威胁分析，由此产生的费用由供应商承担。 **四、服务器区安全运营流量采集** 1、硬件配置 2U机箱，标准配置6个10/100/1000M自适应千兆电口，1个Console口，2个接口扩展板卡插槽配置2个万兆光口，4个千兆光口。 2、性能指标 吞吐量不低于10Gbps，HTTP并发连接数不低于800万，每秒HTTP新建连接数不低于35万/秒。 3、旁路部署 旁路部署在网络中实时采集网络流量数据、威胁检测，支持通过重置会话的方式阻断TCP威胁会话连接，支持通过流量被动识别资产。 4、流量采集 需支持空载荷过滤，支持对采集的流量的上下行载荷长度设置。		

		流量识别与解析 支持精准识别通讯类、语音类、视频类、更新类、下载类、邮件类、金融类、理财类等多类别的应用识别，应用识别库3000+。 支持ICMP、DHCP、HTTP、TELNET、DNS、SSL等基础协议的解析，支持LDAP、Kerberos、Radius等认证解析。 具有自定义解析流量能力，支持基于正则表达式、TLV格式、固定长度等提取模式对流量解析。 5、文件还原 支持还原多种文件传输协议，包括：邮件（SMTP、POP3、IMAP、webmail）、Web（HTTP）、FTP、SMB、TFTP、QQ等。 6、威胁检测 系统具备间谍软件检测能力，可检测常见的病毒蠕虫、僵尸网络、黑市工具、勒索软件、挖矿木马、隧道、代理、后门程序、远控木马等。 系统提供的攻击特征不应少于10000条有效最新攻击规则，特征库需支持自动及手动升级。 本地集成威胁情报库，支持实现基于威胁情报的失陷主机检测，情报不少于200万。 系统需具备专业的查毒引擎，独立的病毒库，支持通过对HTTP、FTP、SMTP、POP3、IMAP、SMB、TFTP、NFS协议进行恶意文件检测。 系统本地需具备攻击告警的过滤能力，能够针对IP地址或端口对攻击告警进行过滤，支持攻击特征高亮展示，方便分析人员事件分析。 7、数据外发 通信模式支持但不限于KAFKA、ZMQ、SYSLOG等协议，需支持多路外发，并支持外发多地址的负载均衡处理。 传输模式支持加密、压缩、以及认证，认证包括但不		

		限于kerberos认证、LDAP认证。 流量及样本取证 支持威胁告警的相关pcap数据留存，支持本地下载及外发，外发通信协议包括但不限于KAFKA、FTP、SFTP等。 8、二次开发接口 系统提供二次开发接口，接口形式为Restful API，提供功能配置、统计等接口。		
2	上网行为管理	1、≥2U机架式结构；≥2TB硬盘；≥96G内存；≥1个串口、≥2个USB接口、≥2个万兆SFP+插槽、≥2个千兆电口、≥2个40GE以太网光接口（QSFP+），≥2个40G多模光口QSFP+模块，≥4个可插拔的扩展槽；自带液晶屏，标配双电源。带宽性能≥30G，网络吞吐量≥60G，最大并发连接数≥1800万。包含应用识别功能，含不低于3年的系统版本，URL库及应用特征库升级许可，不低于3年硬件维保。 2、为保障后续学校网络链路的可靠性，支持两台及两台以上设备同时做主机的部署模式。 3、为保障上网行为可管可控，要求设备支持首页分析显示接入用户人数、终端类型；带宽质量分析、实时流量排名；资产类型分布等。 4、为保障师生业务访问精细化管控，支持为用户添加属性，能够根据用户属性配置上网权限策略、流控策略，审计策略等； 5、结合学校自身信息化发展，支持多种认证方式接入校园网络，支持通过钉钉、企业微信等第三方协同办公软件进行授权认证，支持终端用户账号绑定手机号码和微信号，绑定后可以通过手机验证码和微信扫码实现上网快捷登录认证； 6、用户拥有多个网络区域访问权限时，可以实现用户在任意时刻只能访问一个网络，切换网络需要用户点击切换按钮，无需管理员干预，在不影响多网络使用	1	套

		的同时，实现网络逻辑隔离，加强网络访问安全。可支持自定义8个网络区域（7个自定义区域+互联网区域）。可支持根据域名划分网络区域。（提供截图证明并提供具备中国认可国际互认检测资质的第三方权威机构功能测试报告证明该功能项） /7、为提升学校管理效率，支持从本地导入，支持以CSV格式文件导入帐户/分组/IP/MAC/描述/密码等信息；用户分组支持父组、子组、组内套组； 8、为保障我校出口网络流量的有效管控，支持在不同线路上，根据不同的应用、目标IP、时间段、日期、用户/用户组、位置、终端类型来保证或者限制流量，可根据百分比或数值设置通道带宽，并支持设置各通道的优先级，并且支持在设置流量策略后，根据整体线路或者某流量通道内的空闲情况，自动启用和停止使用流量控制策略，以提升带宽的高使用率；空闲值可自定义； 9、支持通过指纹识别用户身份，并对用户做控制。（提供截图证明并提供具备中国认可国际互认检测资质的第三方权威机构功能测试报告证明该功能项）； 10、支持网络故障排查，支持PPS异常、丢包异常、ARP异常、内网DOS攻击等异常情况实时监测，显示每日异常事件个数及情况； 11、为提升我校互联网使用的合法性以及可监管能力，支持客户端SSL解密，客户端会自动推送根证书安装，支持记录全部或者指定类别URL、网页标题、网页内容等信息； 12、可对IM聊天软件、邮件客户端、云笔记、网盘、浏览器、远程协助工具、文件传输工具、会议软件等途径的文件外发行为进行管控，管控策略包括禁止外发和允许外发； 13、针对我校校园网络办公师生整体数据安全性，产品应当支持可审计内容审计、ToDesk、向日葵、AnyDe		

		sk远程工具的文件外发行为，可审计WinSCP、Xftp、FileZilla文件传输工具的文件外发行为； 14、支持内置、外置日志中心；支持分级配置管理员日志查看权限，支持以USB-Key方式验证接入日志中心的管理员身份； 15、管理员可自定义新的URL地址和URL分类；能够针对各种URL类型做识别和分类，同时所有URL类型都支持区分“网站浏览”、“文件上传”、“其他上传”、“HTTPS”等细分行为并分别做权限控制； 16、支持url白名单，添加到白名单的url不受策略控制和审计。支持ip、用户/用户组白名单，添加到白名单的ip不受策略控制和审计。白名单策略可实现基于时间段的控制。支持设置完全放通（不审计，不控制），或者审计但是不统计和控制流量。（提供产品界面截图并加盖供应商公章）。		
3	WEB应用防火墙	1、2U,内存≥32G，≥6个千兆电口， ≥4个千兆光口,≥6个万M SFP+插槽（带6个万M多模光模块）冗余电源。应用层吞吐≥20G，网络层吞吐≥35G，并发连接≥410万。不低于3年应用特征库升级许可,不低于3年硬件维保。 2、为支持学校多样化的网络架构以及网络链路可靠性，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，支持链路连通性检查功能。 3、为提升学校网络使用体验，产品支持、协议类型、网络对象等条件进行自动选路的策略路由，支持不少于3种的调度算法，至少包括带宽比例、加权流量、线路优先等。 4、为符合国家要求具备IPV6功能，产品支持多对一、一对多和一对一等多种地址转换方式，支持NAT44、NAT64、NAT66地址转换方式。 5、为提升我校应用管控能力，支持对应用的识别和控	1	套

		制，应用类型包括游戏、购物、图书百科、工作招聘、P2P下载、聊天工具、旅游出行、股票软件等类型应用进行检测与控制。 6、支持应用控制策略生命周期管理，包含安全策略的变更时间、变更类型和策略变更用户，并对变更内容记录日志，方便安全策略管控。 7、为保障防火墙能够有效应对外界新型攻击，产品支持勒索病毒检测与防御功能。 8、支持对ICMP、UDP、DNS、SYN等协议进行DDoS防护的能力。 9、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。 10、支持对请求报文头的X-Forward-For字段检测，并对非法源IP进行日志记录和联动封锁。 11、产品支持用户账号全生命周期保护功能，包括用户账号多余入口检测、用户账号弱口令检测、用户账号暴力破解检测、失陷账号检测，防止因账号被暴力破解导致的非法提权情况发生。 12、支持多种爬虫攻击防护：包括但不限于内置爬虫对象库，自定义爬虫对象，导入或者下载后端服务器robots.txt 等方式提供爬虫攻击防护（提供产品界面截图并加盖供应商公章）。 13、为保障对学校内部服务器的安全管理，产品具备识别与阻断外部扫描器发起的服务器恶意扫描行为，可对扫描器地址进行自定义封堵。 14、对DDoS流量支持检测清洗和强制防御两种模式，检测清洗根据是否到达阈值对流量进行清洗，强制清洗对所有流量直接进行流量清洗判断（提供产品界面截图并加盖投标人公章）。		

4	日志审计	1、网络运行日志留存不低于180天，≥2U机架式设备，≥8*16G内存,系统盘≥240G,数据盘≥4*8T,≥4万兆光口+6千兆电口,≥550W双电源。日志采集处理均值≥30000EPS，默认包含≥1000日志源授权。 2、支持内置多种日志源类型，默认可接入各类硬件设备和应用系统，包含但不限于主机、防火墙、IPS/IDS、WAF、网络设备、安全设备、数据库、应用系统、中间件、存储。设备、虚拟化设备、机房设备等多种设备和系统的日志接入方式。 3、支持业内通用标准数据获取方式，包括Syslog、SFTP、文件、Kafka、HDFS、DB2、Mysql、Oracle、Sqlserver、SNMP、Netflow、WMI等。 4、数据解析规则支持规则嵌套和逻辑组合方式，能够对一组事件进行多层规则解析处理，添加、删除、重命名、合并、拆分与裁剪现有字段，对范式化后字段再解析处理。支持多种数据解析，包含精准匹配、包含再解析、正则匹配后从数据头、尾进行二次解析等处理 。 5、系统具有防恶意暴力破解账号与口令功能，口令错误次数可设置，超过错误次数锁定，锁定时间可设置。 6、支持研判分析过程中在线解码，无需使用其他工具即可实现BASE64\HEX\JSON等常见编码和解码转换功能，提高分析效率。 7、支持报表和报表模板管理，区分不同类别报表，并支持按时间及类型搜索历史报告，并自动清理历史报告信息。 8、支持周期性（每日、每周、每月）自动生报表，并支持通过邮件发送、下载、导出等方式获取，支持导出WORD/HTML等格式。 9、内置SOX、ISO27001等合规报表模板。	1	套

		10、支持自定义报表图形化结果展示，包括但不限于柱状图、折线图、区域图、明细表格等。 11、支持FTP/SFTP外发日志进行备份。 12、支持基于时间轴展示告警数据分布，能够通过时间轴进行查询分析；（提供产品界面截图并加盖供应商公章） 13、支持用户功能分权和数据分权管理，功能分权可以将平台的每个功能进行独立指定不可见、只读和读写权限；数据分权能与组织机构进行映射，通过类SQL结构化检索语言定义日志、告警的字段、字段组合进行数据分权范围。 14、支持SNMP v1/v2c/v3协议采集其他设备信息，并可配置采集频率，并支持随时启停操作，通过SNMP协议监控交换机、路由器等设备可用性，监控指标包含CPU使用率、内存使用率、上下行流量。 15、支持根据设备重要程度设置独立设置每个被采集源的日志、报表数据存储时间为1个月、3个月、6个月和永久保存等参数；（提供产品界面截图并加盖供应商公章）。		
5	应用安全防护平台	1、2U冗余电源，≥32G内存，≥128G SSD，≥2T企业硬盘，≥6个千兆电口，≥2个扩展口。 2、系统支持国产统信服务器操作系统，并支持鲲鹏、飞腾、龙芯等类型CPU；支持高可用性：支持主备，保障业务服务不中断； 3、产品指标要求： 产品需同时支持浏览器和客户端使用方式。产品应在无需安装客户端或控件情况下，在后端进行业务发布方式即可访问学校电子图书资源、OA、科研、财务、教务系统等各类B/S业务系统。产品支持客户登录成功，可以通过点击对应访问图标的方式进行一键式访问。	1	套

		产品支持WEB终端。在不安装任何控件下，只需从浏览器就可使用如：RDP、SSH、VNC、Telnet等维护工具； 产品需支持IPV4 /IPV6双栈接入访问，IPV4和IPV6互访。 产品需与门户系统、网上办事大厅等系统做深度融合，保证用户不受时间地点限制，内外网使用体验感完全一致。 产品需提供CAS、OAuth、SAML、LDAP、RADIUS、AD、DB、REST、MySQL、Oracle、SqlServer、短信认证等认证方式。可针对用户支持短信、邮件等多因素认证。（提供产品界面截图并加盖供应商公章）； 产品支持多种社交化认证方式，如微信、企业微信、钉钉扫码等。 支持创建临时账号，管理员可设置账号类型为临时或永久，临时账号可选择使用日期，过期后自动失效（提供产品界面截图并加盖投标人公章）； 支持对于第三方用户进行用户组切换，便于对第三方人员权限进行细粒度的划分，支持开启/关闭反同步功能（提供产品界面截图并加盖供应商公章）； 支持企业微信应用对接、钉钉应用对接； 支持通过SDK包集成方式集成移动端APP。实现用户移动端无感知接入。 支持针对不同用户/用户组分配不同的隧道地址网段，进行隧道地址区分（提供产品界面截图并加盖供应商公章）； 4、安全支持要求 支持针对本地账号开启认证策略，包括：强密码策略，密码容错、超期策略，二次认证策略，登录限制策略，绑定策略等； 支持创建临时账号，管理员可设置账号类型为临时或永久，临时账号可选择使用日期，过期后自动失效； 支持一键断网能力，对网关进行一键下线，禁止提供		

		服务； 支持访问白名单机制，把不在访问策略范围内的资源直接通过原有路径进行访问。（提供产品界面截图并加盖供应商公章）； 支持访问web页面添加水印，水印内容需支持账号、公司、主机名、IP、日期等信息，用户可自定义水印内容（提供产品界面截图并加盖供应商公章）； 支持数据脱敏，对用户访问过程中，可对身份证、手机号、银行卡信息进行脱敏处理；（提供产品界面截图并加盖供应商公章）。 C/S端场景下，支持浏览器缓存、设备系统检测、Android防截屏、杀毒软件检测等功能；（提供产品界面截图并加盖供应商公章）； 产品能够有效阻止外部工具对内部业务系统的扫描探测，并针对所发布的浏览器应用进行URL地址伪装，防止服务器真实IP地址泄露，免遭恶意攻击，保障内部系统安全； 产品支持DES、3DES、SHA、RSA等商用密码以及SM2、SM3、SM4国密算法保障传输安全； 支持通过策略区分内外网访问环境，并根据实际需求灵活配置可以访问的应用和可以访问的用户。（提供产品界面截图并加盖供应商公章）； 5、系统管理要求 产品支持多级管理员管理，超级管理员可以设定多个不同权限的管理员，并且支持管理员只读和读写全选的切换。 支持详细的账户控制策略，包括但不限于：登录时间策略、登录密码复杂度、多因子配置（提供产品界面截图并加盖供应商公章）； 支持单台或多台Syslog服务器日志转发； 6、日志审计要求 产品日志提供详细记录用户登录日志（账号、用户名		

		、主机IP、访问时间）、应用访问日志（账号、主机IP、访问内容）、管理员日志（管理员、主机IP、时间、管理行为、对象）、系统运行日志、告警日志；可根据用户名、主机IP等信息进行用户行为查询；可提供用户流量排名、用户下载量排名、活跃用户排名、用户访问类型分布、应用流量排名、应用访问量排名、浏览器类型分布等记录。（提供产品界面截图并加盖供应商公章）； 支持用户概览、应用概览、登录审计、异常审计分析日志的图表化PDF报表导出； 产品提供态势感知大屏功能模块，智能化统计安全数据。支持把这些信息统一通过数据接口实时传输给其他态势感知平台或者数据安全监控平台或者大屏幕系统，以便做更全面的用户行为分析和数据安全分析。		
6	网络安全运营工作站	安全运营工作站共计8台，具体参数要求如下： 一、台式机工作站6台 1、CPU：不低于Intel第14代酷睿i7-14700F处理器 2、液晶屏：≥27英寸4K显示器 3、声卡：集成声卡 4、内存：≥32GB DDR5 5600MHz 5、硬盘：≥1T PCIe-NVME SSD 6、显卡：不低于Nvidia RTX4060Ti 7、无线网卡：不低于WIFI6E(802.11AX) 8、标准接口：≥3*USB A接口、2个Type-C接口，HDMI、RJ45接口 9、操作系统：原厂正版Windows 11 操作系统 10、键鼠：同一品牌抗菌键盘及光电抗菌鼠标。 二、便携式工作站2台 1、CPU:≥英特尔酷睿Ultra7-155H 2、内存:≥32GB 3、硬盘:≥1T 固态硬盘 4、显卡:集成显卡	8	台

		5、网卡:集成100/1000M自适应网卡; 6、电池:≥57Wh 7、无线:Wi-Fi 6E及蓝牙 8、声卡:内置麦克风 9、端口:≥2个USB-C，≥2个USB-A，HDMI接口 10、屏幕:14英寸屏，刷新率不低于120Hz，分辨率不低于2880*1800 11、重量：不高于1.11kg 12、厚度：不高于14.96mm 13、键盘:全尺寸防泼溅键盘		
7	触控一体机	1、显示尺寸≥98英寸。 2、内置安卓系统，与Windows系统形成双系统备份，安卓系统不低于9.0版本。 3、触控技术：支持Windows系统中≥10点触控，Android系统中≥10点触控。 4、屏幕分辨率：3840×2160，支持4K显示。 5、屏幕对比度≥1400：1，亮度≥450cd/㎡。 6、要求所投智慧大屏具备物理开机防蓝光功能。 7、前置接口：USB≥3个，Type-C ≥1个。 8、提供节能产品认证证书。 9、提供Windows系统桌面，提供OPS电脑。 10、≥i7 CPU；≥8G DDR4运行内存；≥256G SSD固态硬盘。 11、视频输出接口：HDMI≥1个。 12、支持4k清晰度高清视频流畅解码播放，支持显示信号输出到4K显示器上。 13、要求支持无线投屏功能，通过校园无线网进行电脑、手机投屏。 14、要求与现有大屏云管理系统进行对接，实现与现有大屏统一管理。供应商出具对接承诺函（因对接产生的费用由供应商承担）	1	套
8	智能	1、开锁方式：指纹、密码、刷卡、蓝牙等。	1	套

	门锁	2、外壳材质：ABS+合金。 3、指纹头：半导体指纹头。 4、具备应急供电口。 5、适用门型：玻璃门、有框铝合金门、木门、平移门等。		
9	办公桌椅	1、双人位烤漆工作台桌椅组合（含灯带），尺寸不低于3000*800*760mm。	2	套
10	网络安全运营指挥中心环境建设	提供安全运营指挥中心环境建设，包括加装玻璃隔断、线缆敷设、设备安装调试等。	1	项

二、商务要求

质保期	六年
售后技术服务要求	售后技术含安装、调试、维修、保养、人员培训等，售后服务要达到合同要求。
合同签订时间、交货时间及地点	合同签订时间:成交通知书发出之日起5日内。 交货时间:合同签订之日起30日内。 地点:采购人指定地点。
付款方式	中国工商银行股份有限公司驻马店分行、黄淮学院正式验收合格之日起30个工作日内，成交供应商向黄淮学院提供合同金额5%(质保期按第三章采购需求中的相关要求执行)的银行保函，中国工商银行股份有限公司驻马店分行向成交供应商支付合同金额的100%货款。
备品备件及耗材等要求	供应商需提供必要的备品、备件及耗材以完成系统的安装、调试。
售后服务保障或维修响应时	提供原厂商现场培训服务。在保质期内出现故障时，原厂商提供7×24小时电话响应，故障响应时间30分钟，原厂商工程师1小时到达现场，2

间要求	小时修复。若设备不能在2小时内恢复正常，供应商免费提供备用设备，保证不因为供应商设备问题影响采购人使用。供应商和原厂商分别出具加盖公章的售后服务承诺函。

三、采购人对项目的特殊要求及说明

采购人的特殊要求及说明理由	1、采购人根据本项目技术构成、价格比重等合理确定核心产品是：网络安 2、供应商提供虚假材料，成交后提供货物不满足采购文件技术要求的取消 3、为保证本次采购设备和软件平台可以满足学校需求并稳定运行，要求成 4、不收取履约保证金。 5、不接受联合体投标。 6、所投所有软件平台不接受定制开发，要求为成熟软件，供应商提供所投 7、供应商需出具书面承诺，承诺免费配合第三方进行软硬件集成（包括移 8、所投所有软件平台综合要求： （1）操作系统：运行环境服务器端操作系统不使用centos操作系统。 （2）浏览器兼容：客户端需支持edge、chrome、360、火狐、ie等常用浏 （3）系统部署：系统部署时需集群部署，需支持根据学校业务需求扩展业 （4）安全要求：①涉及用户隐私信息展示时需要进行去标识化处理；②平 针对以上要求提供加盖供应商公章的承诺函。 9、所投所有软件平台对接要求： （1）免费提供系统全量数据接口，数据中间库及数据字典。 （2）免费配合接收学校数据平台推送的与本项目系统相关的必要基础数据 （3）对于不满足学校信息标准的系统数据，需按学校要求进行修改。对于 针对以上要求提供加盖网络安全产品厂商公章的承诺函。 10、保密性要求：要求成交供应商及产品厂商在签订合同前，与学校签订