合同编号（校内）：HW337250081

郑州大学网络空间安全学院、中原网络安全研究院漏洞挖掘与应用研究分析平台建设项目三期采购项目

甲　　方：郑州大学

乙　　方：北京墨格教育科技有限公司

生效日期：2025.9.4

合同编号：（豫财招标采购-2025-595）

郑州大学政府采购货物合同

甲方（全称）：郑州大学

乙方（全称）：北京墨格教育科技有限公司

根据《中华人民共和国民法典》《中华人民共和国政府采购法》及有关法律规定，遵循平等、自愿、公平和诚实信用的原则，双方同意按照下述条款订立本合同，共同信守。

一、供货范围及分项价格表（详见附件 1、附件 2）

1. 本合同所指货物包括原材料、燃料、设备、产品、硬件、软件、安装材料、备件及专用器具、文件资料等，详见附件 1、附件 2 ，此附件是合同中不可分割的部分。

2. 本合同总价包括但不限于货物价款、包装、运输、装卸、保险费、安装及相关材料费、调试费、软件费、检验费、培训费等各种伴随服务的费用以及税金等。合同总价之外，甲方不再另行支付任何费用。

二、质量及技术规格要求

乙方须按合同要求提供全新货物（包括零部件、附件、备品备件等）货物的质量标准、规格型号、具体配置、数量等应符合招标文件要求，其产品为原厂生产，且应达到乙方投标文件及澄清文件中承诺的技术标准。

乙方应在本合同生效后 7 个工作日内向甲方提供安装计划及质量控制规范；并于 9 月 12 日前进驻安装现场；所有货物运送到甲方指定地点后，双方在 7 日内共同验收并签署验收意见。如甲方无正当理由，不得拒绝接收；在安装调试过程中，甲

方有权采取适当的方式对乙方货物质量标准、规格型号、具体配置、数量以及安装质量和进度等进行检查。甲方如果发现乙方所供货物不符合合同约定，甲方有权单方解除合同，由此产生的一切费用由乙方承担。

三、包装与运输

货物交付使用前发生的所有与货物相关的运输、安装及安全保障事项等均由乙方负责；货物包装应符合抗震、防潮、防冻、防锈以及长途运输等要求，对由于包装不当或防护措施不力而导致的货物损坏、损失、腐蚀等损失均由乙方承担；在货物备交付使用前所发生的所有与货物相关的经济纠纷及法律责任均与甲方无关。

四、质保期与售后服务（详见附件 3）

1. 所有设备免费质保期为 3 年（自验收合格并交付给甲方之日起计算），终身维护、维修。

2. 在质保期内，因产品质量造成的问题，乙方免费提供配件并现场维修，且所提供的任何零配件必须是其原设备厂家生产的或经其认可的。产品存在质量问题，甲方有权要求乙方换货。

3. 乙方须提供一年 2 次全免费（配件+人力）对产品设备的维护保养。

4. 乙方承诺凡设备出现故障，自接到甲方报修电话 1 小时内响应，3 小时内到达现场，24 小时内解决故障问题。保修期外只收取甲方零配件成本费，其他免费。

5. 乙方未在规定时间内提供原配件或认可的替代配件，甲方有权自行购买，费用由乙方承担。

6. 其它：无

五、技术服务

1. 乙方向甲方免费提供标准安装调试及 10 人次国内操作培训。

2. 乙方向甲方提供设备详细技术、维修及使用资料。

3. 软件免费升级和使用。

4. 乙方有责任对甲方相关人员实施免费的现场培训或集中培训措施，保证甲方相关人员能够独立操作、熟练使用、维护和管理有关设备。

六、知识产权

乙方应保证甲方在使用该货物或货物的任何一部分时免受第三方提出的侵犯其知识产权、商业秘密权或其他任何权利的起诉。如因此给甲方造成损失，已方承诺赔付甲方遭受的一切损失。

七、免税

1. 属于进口产品，用于教学和科研目的的，中标价为免税价格。

2. 免税产品应由甲乙双方依据海关的要求签订委托进口代理协议，确认甲乙双方的责任与义务。委托进口代理协议作为本合同的不可分割部分。

3. 免税产品通关时乙方必须进行商检，未商检的，造成的损失由乙方承担。

八、交货时间、地点与方式

1. 乙方于 2025 年 9 月 29 日之前将货物按甲方要求在甲方指定地点交货、安装、调试完毕，并具备使用条件，未经甲方允许每推迟一天，按合同总额的千分之五支付违约金。

2. 乙方负责所供货物包装、运输、安装和调试，并承担所发生的费用；甲方为乙方现场安装提供水、电等便利条件。

3. 安装过程中若发生安全事故由乙方承担。

4. 乙方安装人员应服从甲方的管理，遵守国家法律法规和学校相关制度，否则一切后果均由乙方承担。

5. 货物交付使用前，乙方负责对提供货物进行看管，并承担货物的丢失、损毁等风险。

九、验收方式

1. 初步验收。甲方按合同所列质量标准、规格型号、技术参数以及数量等在现场验收，并填写初步验收单（详见附件 4）。验收时，甲方有权提出采用技术和破坏相结合的方法。

乙方应向甲方移交所供设备完整的使用说明书、合格证及相关资料。乙方在所有设备（工程）安装调试、软件安装完毕后，开展现场培训，使用户能够独立熟练操作使用仪器或设备，尔后由供需双方共同初步验收；甲乙双方如产生异议，由第三方重新进行验收。如果乙方提供的货物与合同不符，甲方有权拒绝验收，由此所产生的一切费用由乙方承担。

2. 正式验收：依据河南省财政厅“《关于加强政府采购合同监督管理工作的通知》【豫财购（2010）24 号】”文件要求，政府采购合同金额 50 万元以上的货物采购项目，由使用单位初验合格后，向国有资产管理处提出验收申请，由采购单位领导牵头，会同财务、审计、资产管理及专家成立验收专家组进行正式验收。学校验收通过后，才能支付合同款项。

十、付款方式及条件

1. 本合同总价款（大写）为：**贰佰壹拾捌万陆仟元整（小写：¥2186000 元）**。

2. 付款方式：货物验收合格后，经审计后，甲方向乙方支付全部货款的 95%；质保期满 30 天内，甲方向乙方支付剩余的全部货款。

十一、履约担保

乙方向甲方以 银行保函 的方式提供合同总额 5% 的履约保证金。货物验收

合格，正式交付使用后予以退还履约保证金。

十二、违约责任

乙方所交的货物产地、品牌、型号、规格、质量以及技术标准、数量等不符合合同要求，甲方有权拒收，由此产生的一切费用由乙方负责；因货物更换而造成逾期交货，则按逾期交货处理，乙方应向甲方每天支付合同标总额日千分之五的违约金。

甲方无正当理由拒收设备，应向乙方偿付拒收设备款额百分之五的违约金。甲方逾期付款，应向乙方支付本合同标的总额的日万分之四的违约金。

十三、其它

1. 组成本合同的文件及解释顺序为：本合同及其附件、双方签字并盖章的补充协议和文件；投标书及其附件；招标文件及补充通知；中标通知书；国家、行业或企业（以最高的为准）标准、规范及有关技术文件；投标书及其附件。

2. 双方在执行合同时产生纠纷，协商解决；协商不成，向甲方所在地人民法院提起诉讼。

3. 本合同共 23 页，一式 8 份，甲方执 6 份（用于合同备案、进口产品免税、验收、报账等事项），乙方执 2 份。

4. 本合同未尽事宜，甲方双方可签订补充协议，与本合同具有同等法律效力。

5. 本合同经双方法定代表人或其授权代理人签字并加盖单位公章后生效。

6. 法律文书接收地址（乙方）：北京市怀柔区雁栖经济开发区雁栖路 33 号。

甲方：郑州大学

地址：郑州市科学大道 100 号

签字代表（或委托代理人）：

电话：0371-63887329

乙方：北京墨格教育科技有限公司

地址：北京市怀柔区雁栖经济开发区雁栖路 33 号

签字代表：刘桂枝

电话：010-80653658

开户银行：中信银行北京三元桥支行

账号：8110 7010 1330 1964 873

合同签署日期：2025 年 9 月 4 日

附件 1：

供货范围及分项价格表

单位：元

序号	设备名称	品牌型号	制造厂（商）	原产地（国）	数量	单位	单价	合价	备注
1	内容安全监测分析系统-流量探针	奇安信/奇安信网神流量管理系统 V5.5（ITM7730）	奇安信网神信息技术（北京）股份有限公司	中国	1	套	379000	379000	免税
2	内容安全监测分析系统	奇安信/奇安信网神上网行为管理与审计系统 V7.0（BAAS-E-SYS）	奇安信网神信息技术（北京）股份有限公司	中国	1	套	389000	389000	免税
3	安全能力中心防火墙系统	奇安信/网神 SecGate3600 防火墙系统 V3.6.6.0（NSG2000-TE45M-PM-QW）	奇安信网神信息技术（北京）股份有限公司	中国	1	台	136000	136000	免税
4	侧加载漏洞检测系统平台	绿盟科技/绿盟侧加载漏洞检测系统（APT-CJZ）	北京神州绿盟科技有限公司	中国	1	套	382000	382000	免税
5	通用操作系统取证采集系统	绿盟科技/绿盟可执行文件解析漏洞研究系统（APT-KZXWJ）	北京神州绿盟科技有限公司	中国	1	套	357000	357000	免税
6	可执行文件解析系统	绿盟科技/绿盟操作系统漏洞利用取证采集系统（APT-LYQZ）	北京神州绿盟科技有限公司	中国	1	套	339000	339000	免税
7	虚拟化平台安全防护系统	天融信/天融信终端威胁防御系统 V1（TopEDR）	北京天融信网络安全技术有限公司	中国	1	套	15000	15000	免税
8	综合运行硬件支撑平台	华为/2288X V5	华为技术有限公司	中国	1	台	98500	98500	免税
9	漏洞安全系统云资源管理平	天融信/天融信超融合管理系统 V3（TopHC-SW-PACK）	北京天融信网络安全技术有限公司	中国	1	套	55500	55500	免税

	台								
10	漏洞验证资源库	墨格教育/墨格定制	北京墨格教育科技有限公司	中国	1	项	35000	35000	免税
合计：小写：￥2186000 元　　大写：人民币贰佰壹拾捌万陆仟元整									

附件 2：

设备技术规格参数、功能描述及配置清单表

序号	设备名称	具体技术规格参数、功能描述及配置清单描述	单位	数量
1	**内容安全监测分析系统-流量探针**	**硬件规格** 1、满足 100G 带宽网络环境，2U 机架式设备，最大并发连接数 2000 万，最大新建连接数 30 万/秒，配置 16 个万兆光口，5 个扩展槽，内置 8T 硬盘，交流冗余电源，含网页过滤、用户认证、应用控制、内容审计、带宽管理、**行为监控分析等功能。** 2、设备必须提供物理硬件 bypass 按钮，便于设备巡检、设备故障时管理员无需重启、关机、断电即可恢复网络通畅。 **部署模式** 3、支持旁路、网桥（多路网桥），网关（路由转发和 NAT）等多种部署模式，能与学校原有设备系统实现无缝联动，提供原厂的联动承诺函并附与标书中。 4、支持模式选择，可设置为 Portal 模式，实现 Portal 服务器功能； **5、系统监控：**支持集中呈现上网行为风险等级和状态，包括行为风险等级包括安全等级、效率等级、合规等级和管控等级、管控效果、运行状态、安全状态、泄密风险状态、合规状态和应用使用状态。支持自动识别网络中终端的 IP 地址、MAC 地址、终端类型、操作系统、终端厂商和网卡厂商等信息；支持移动终端型号识别，至少识别 10 种移动终端型号； **6、用户管理：**支持 web 本地认证、微信认证、短信认证、二维码认证等，并支持多种认证方式组合的混合认证。支持对 802.1X、华为 controller、NAC、Kerberos、AD、POP3、Radius、syslog、数据库识别、PPPOE、华三 iMC、城市热点、深澜计费等系统的单点登录。内置应用协议库，包含的应用数量 12000 种，应用规则总数 73000 种。 **流量管理**	1	套

		7、支持多级虚拟通道，可以将物理带宽分成 7 级虚拟通道，合理分配物理带宽资源。 8、支持每用户带宽限制，可以指定每个人的最大上传、下载带宽，支持基于连接数进行流量管理，可以每个人的并发/新建连接数量进行控制。 **网页管理与审计** 9、支持当用户的网页访问被网页浏览策略封堵时，用户如果发现分类错误能够在页面中向管理员进行反馈；管理员可查看用户反馈的分类错误，并可以选择向服务器反馈； 10、设备内置 2.8 亿条 URL 数据，在系统有 URL 库更新情况详细说明，支持根据 URL 库及 URL 关键字进行网址访问管理，一条策略实现阻断、记录、告警，方便维护，； 11、支持对网站的发帖正文关键字进行管理，一条策略可同时实现控制、记录、告警、便于维护管理。支持不同网页被阻塞后会跳转不同的阻塞页面；支持用户完全自定义。 **邮件审计** 12、支持 POP3、IMAP 邮件接收进行审计，支持实现 Webmail 以及 SSL 加密的 Webmail 基于发件人、收件人、主题、内容、附件名、附件大小，附件内容关键字维度的记录、阻塞、告警。 **文件审计** 13、可以对网页的文件，根据传输方向、文件名、文件扩展名、文件大小、网站域名进行控制管理，违规文件下载阻塞同时可以告警， **Https 审计** 14、通过 HTTPS 审计功能，可以针对网站分类、证书颁发者、证书所有者、证书有效期等进行审计，加以控制。 **DNS 审计** 15、通过 DNS 审计策略对 DNS 通信内容进行审计和控制。 **SSL 解密** 16、支持 SSL 解密，支持基于用户、位置及工具条件，针对不同用户配置不同策略实现解密；		
2	内容安全监测	**部署方式** 1、支持以软件形式部署，支持与此次内容安全监测分析系统-流量探针配套使用，产品架构采用标准的大数据分析平台，集成 ElasticSearch，Kafka,Spark 等大数据高性能处理组件。	1	套

	分析系统	**2、数据采集方式：**支持上网行为数据实时上传，包括日志和审计附件。支持一卡通日志，VPN 日志，业务系统数据、天擎终端数据的接入。支持标准 syslog 日志，数据库日志，文本格式日志，SNMP 日志等日志格式。支持 Oracle、MySql、SqlServer，PostgreSql 数据库的数据采集，支持增量和全量读取； **学生网贷分析** ★3、可以尽早发现关注网贷的学生，和学生访问网贷资源，可以根据学生访问网贷的网址、查询的敏感词、网址标题等分析学生访问行为，并找出风险人员在最近半年时间里都访问了哪些风险资源以及访问次数，做到溯源取证。 4、网贷资源网站可以支持 1900 多种，并且支持手动添加，可有效保障资源更新的及时性。 **图书馆资源分析** 5、支持分析互联网图书资源的使用情况，可以评估各个资源访问情况和下载情况。支持恶意下载分析，找到在一定时间内某用户大量下载资源的可疑行为。 6、支持对已购资源的分析学习，分析购买资源使用率情况。 7、图书资源列表包括 45 个常用国内国外网站，并支持手动添加，可有效保障资源更新的及时性。 **异常兴趣分析** 8、支持校园环境中常见的暴力、色情两个维度进行分析和展示。支持展示一段时间内，访问网站的热度排名，以及风险用户、异常兴趣事件数的走势变化。 **沉迷网络** 9、支持分别从网络游戏和网络视频两个维度，展示学生的上网时长情况。支持展示一段时间内，访问游戏资源和视频资源，以及风险用户、访问数量的变化走势。 **一卡通分析（贫困生分析）** 10、支持通过获取在校学生一卡通数据，对在校生消费行为进行分析，及时发现贫困学生和消费异常现象。 11、支持从学生、班级、POS 机多种维度，展示一段时间内总金额、日均消费金额、平均消费金额、人均消费金额、刷卡次数等详细信息。 12、可及时发现异常消费行为，如：对一次消费过大或超出该用户平均消费额过大的行为，对长期没有任何消费的用户。		

		高校上网态势分析大屏 13、综合分析指数综合评估，权衡包括网贷，游戏沉迷，视频沉迷，一卡通消费和图书馆下载异常等各类异常事件的发生频率和次数，直观展示校园网内发生的学生行为风险 。		
3	安全能力中心防火墙系统	**硬件规格** 1、1U 机箱，冗余电源；网络层吞吐量 8G，并发连接 200 万，每秒新建连接数 10 万；配置 8 个千兆电口，2 个千兆光口，2 个万兆光口，2 个扩展插槽，1 个 Console 口，2 个 USB 接口，无液晶屏，包含访问控制、地址转换、静态路由、动态路由、策略路由、流量控制、VPN 等基础功能； **网络协议** 2、支持 MPLS 流量透传；支持针对 MPLS 流量的安全审查，包括漏洞防护、反病毒、间谍软件防护、内容过滤、URL 过滤、基于终端状态访问控制等安全防护功能； 3、支持 MTU9000byte 的巨型帧 Jumbo Frame 4、支持在源地址转换过程中，对 SNAT（源地址转换）使用的地址池利用率进行监控，并在地址池利用率超过阈值时，通过 SNMP Trap、邮件等方式告警。 5、支持共享上网检测功能，支持共享接入检测和共享接入管控功能，可以通过设置管控地址和例外地址优化管控功能，同时支持阻断或告警动作 **入侵防御** 6、支持木马后门、勒索软件通信防护、异常流量检测、间谍软件功能防护、高危行为动态黑 IP、Flood 攻击防护等功能，已经提供针对软件功能的有效检测报告并附与标书中。 7、能够抵御 ICMPFlood、UDPFlood、SYNFlood、TearDrop、Land 和 Ping of Death 等基本的拒绝服务攻击,渗透成功的包数量小于 5%，正常连接建立大于 90% 8、支持漏洞防护，包含永恒之蓝、震网三代、暗云 3、Struts、Struts2、Xshell 后门代码及等； **SSL 解密** 9、支持 IPv4 和 IPv6 流量的 HTTPS、POP3S、SMTPS、IMAPS 协议进行解密，支持镜像端口偏移，可对解密后的明文流量做镜像时修改端口，以区分原始密文流量和解密后明文流量。 **蜜罐策略** 10、支持威胁引流功能，威胁引流可以通过开关设置是否开启，通过添加蜜罐地址实现引流，同时支持	1	台

		添加例外域名，做到精细化引流管控。 **11、运维管理：**支持资产管理，能够通过设置资产监控、VPN、源安全域来控制资产识别范围，支持 scanner 或 onvif 类型的扫描方式和网段，实现自动或手动资产扫描；支持设置 IP 地址、MAC 地址、资产类型、生效市场、厂商、位置等信息来制定黑/白名单，方便日常资产管理。配置管理功能支持导出最后保存配置、当前配置、历时配置，可将配置文件导出至本地、FTP 服务器、TFTP 服务器，并可配置密文导出，支持导入本地、FTP 服务器、TFTP 服务器的配置文件，并支持三份历史配置文件存储和切换。 **云端协同** 12、支持与云端联动，实现病毒云查杀、URL 云识别、应用云识别、云沙箱、威胁情报云检测等功能；		
4	**侧加载漏洞检测系统平台**	**1、基础能力：**主要用于检测计算机中已安装操作系统的可执行文件是否存在动态链接库（DLL）侧加载漏洞。通过分析程序的 DLL 加载路径策略及权限配置，精准定位可能被恶意利用的风险点。系统交互方法支持采用命令行方式进行操作，最终输出标准化格式的测试验证结果。适用于安全团队快速筛查权限逃逸漏洞、渗透测试人员验证攻击链有效性等场景，帮助用户主动防御由 DLL 加载策略缺陷导致的安全威胁。 **2、PE 文件权限配置解析能力：**能够解析 PE 文件的 manifest 属性，识别 requestedExecutionLevel 和 autoElevate 配置。 支持输出解析结果，明确文件是否需要管理员权限执行或是否允许自动提升权限。 **DLL 加载路径优先级审计：** 3、工具能够扫描并分析可执行文件的 DLL 加载路径，识别潜在的不安全路径。 4、支持对常见路径（如 KnownDLLs、当前目录和系统路径）进行检测，判断是否存在路径劫持风险。 **可信目录劫持模拟引擎：** 5、支持自动化创建测试目录结构，并模拟路径劫持攻击的成功与失败情景。 **DLL 劫持行为动态验证：** 6、工具支持自动生成测试用 DLL 文件，并验证是否能够成功劫持目标可执行文件的 DLL 加载。 7、能够通过模拟执行行为，验证文件加载路径是否存在被恶意替换的漏洞。 **8、攻击结果标准化日志：**所有测试和攻击验证的结果应以标准化格式输出，确保易于理解和处理。日志内容应包括测试目标文件、DLL 路径、执行权限级别和攻击结果等关键信息。	1	套

		9、自动化环境清理机制：能够实现在测试结束后自动清理所有创建的临时文件和目录。支持清理过程中保证系统文件的安全性，避免对原系统环境造成任何影响。		
5	**通用操作系统取证采集系统**	**1、基础能力：**能够系统性地收集系统关键信息，涵盖操作系统版本、硬件配置、系统资源占用等基础内容，有效帮助用户快速掌握目标系统的整体运行状况。在安全事件发生时，所收集的数据（如漏洞利用日志、异常文件、事件日志等）可作为重要的取证资料，帮助用户深入调查事件经过、评估影响范围，并据此采取有效的应对措施。能够对主流 Web 日志进行深度检测，精准识别潜在漏洞。重点检查系统 Web 服务上传目录，查找疑似 Webshell 文件。系统交互方法支持采用命令行方式进行操作，助力用户及时发现并修复漏洞，显著提升系统整体安全防护能力。 **系统信息采集能力：** 2、操作系统指纹采集：自动化采集操作系统版本号、Build 号及补丁状态，确保覆盖主要操作系统类型。 3、硬件配置采集：自动化采集硬件配置，包括 CPU、内存、磁盘等信息，确保硬件状态信息完整。 4、系统资源使用信息：支持采集系统资源使用情况，包括 CPU、内存使用情况、网络连接状态等。 **系统日志采集能力：** Windows 事件日志采集：自动化收集 Windows 事件日志（安全、系统、应用日志）及主流杀毒软件日志（如 360、火绒），支持日志格式标准化处理。 **5、浏览器信息采集能力：** 6、浏览器信息采集：收集浏览器的下载文件、历史访问记录等信息，支持主流浏览器（如 Chrome、Firefox、Edge 等）。 **7、攻击行为分析能力：**Web 日志检测支持对 IIS、Apache、Nginx 等 Web 日志进行解析和异常行为检测。Webshell 检测可以扫描 Web 服务上传目录，自动检测并标记异常文件。 **漏洞利用识别能力：** 8、漏洞扫描矩阵：支持历史 Nday 漏洞扫描与检测，具备识别未公开漏洞的利用痕迹的能力。 **异常文件取证能力：** 9、异常文件检测：能够识别并标记路径超长文件（大于 260 字符）、文件名称过长、伪装系统文件（如 svchost.exe.txt）等异常文件。 **10、取证数据整合：：**结构化日志生成可以按威胁等级分类输出日志（如高危漏洞、可疑文件、异常行	1	套

		为），确保数据呈现清晰且易于处理。JSON 格式日志输出可以生成机器可读的 JSON 格式日志，便于自动化处理、存储和后续分析。		
6	**可执行文件解析系统**	**1、基础能力：**提供高度灵活且精确的静态数据分析方式，支持对任意二进制文件的原子级字节操作与位级精度解析。 用户可以在手动或自动化模式下进行自由切换，灵活定制分析过程，充分满足不同科研分析需求。系统采用模块化扩展架构：支持插件的灵活集成，从而拓展其功能以适应不同领域的个性化需求。本工具能够读取任意二进制数据，并支持逐字节、逐位的详细分析。用户可以根据需求选择手动或自动分析模式，灵活控制分析过程。还提供了插件支持，允许用户自定义并添加分析插件，以适应特定的解析需求。该工具广泛应用于二进制格式解析、漏洞研究、恶意软件分析等领域，能够帮助研究人员深入了解二进制数据结构，提升分析效率和准确性。 **数据读取能力：** 2、支持读取 ELF、PE 可执行文件、TXT 文本文件、JPEG 图片等不少于 4 种的二进制数据，以二进制格式展示。 3、系统能够识别并加载多种常见文件格式，包括 ELF（可执行和链接格式）、PE（便携式可执行格式）、TXT（文本文件）和 JPEG（图像文件），确保其能够处理不低于四种文件类型的二进制数据。 4、支持以原始二进制格式展示文件内容，使用户能够直接查看每个字节的数据。支持以原始二进制格式展示文件内容，使用户能够直接查看展示数据。系统主界面布局简洁直观，能够显示程序名字、值、长度（bits）、上下文、历史记录、当前位置等关键信息。 5、支持逐字节二进制数据读取和处理： (1)具备逐字节精确分析的能力，能够逐一读取每个字节的数据，提供细粒度的文件解码。 (2)支持逐字节分析，可在更低的层级上解析文件，精确到每个字节，适用于处理复杂二进制格式或进行详细的位操作分析。 **自定义插件：** 6、具备自定义插件扩充分析能力。 7、支持至少三种分析插件，涵盖常见的数据分析需求，增强工具的扩展性和灵活性。 8、提供插件机制，用户可以根据需要自定义插件，对特定的二进制数据类型或分析任务进行定制化扩	1	套

		展，扩展工具的功能边界。 **数据展示：** 9、支持按照分析插件分析结果展示分析数据。在执行完分析插件后，系统能够根据插件返回的分析结果，结构化地展示分析数据，便于用户查看和理解。 10、数据展示时支持动态更新和自定义视图，根据不同的插件结果展现不同的格式，以满足多样化的分析需求。 **文件处理能力：** 11、系统能够处理 100MB 的文件，确保在面对大规模数据文件时，依然能够保持良好的性能和稳定性。 12、支持文件的自定义分块加载，优化内存使用，避免内存溢出或性能下降。 **自动化工作流：** 13、支持自动化调用分析插件执行自动分析任务：提供自动化工作流功能，自动调用默认插件进行分析，无需人工干预。 **语法解析能力：** 14、支持读取使用 markdown 语法的文档，并在工具中展示： (1)工具能够读取和解析使用 markdown 语法编写的文档，并能够在内置的查看器中渲染展示，保留文档的格式和内容。 (2)支持对文档中的说明进行展示，以增强用户的阅读和分析体验。		
7	**虚拟化平台安全防护系统**	1、支持通过 PING、ARP、NMAP 方式扫描，发现尚未纳入管控的终端，支持展示终端的终端在线、离线、安装情况. 2、支持定制安全防护策略：包括病毒防御（病毒查杀、文件实时监控、恶意行为监控、U 盘保护、下载保护、邮件监控、白名单）；系统防御（浏览器保护、软件安装拦截、系统加固）；网络防御（黑客入侵拦截、IP 协议控制、恶意网站拦截、IP 黑名单）；合规管控（文档检测、文档跟踪、USB 存储、设备监控、进程监控、软件监控、服务监控、账号监控、外联监控）；其他设置（心跳配置、管理员配置、升级配置、补丁配置、弹窗配置、通信管理中心）； 3、支持对 webshell 后门进行扫描检测 ， webshell 后门库数量 100000； 4、支持开启勒索诱捕功能，设置诱饵文件并实时监控，当勒索病毒对该文件进行加密操作时进行拦截；	1	**套**

		5、支持系统加固，从系统文件保护、病毒免疫、进程保护、注册表保护、危险动作拦截、执行防护等多个维度对系统进行防护。 6、支持从终端、资产两个维度统计终端软件安装情况，可自定义查询并导出软件资产。 7、支持动态认证，配置动态认证策略可以在用户本地以及远程登录系统时进行口令认证。 8、支持文档检测功能，针对 txt,doc,docx,xls,xlsx,ppt,pptx,rtf,pdf 等格式文档的名称、内容进行包含关键字检查，对含有指定关键字的文档进行禁止发送、禁止拷贝等管控，消息提醒的同时将文档违规信息上报管理平台。 9、支持文档跟踪策略，可按照不同文件、压缩包类型跟踪文档内到外、外到内、外到外、内到内等流转方向，并可跟踪文档包括拷贝、压缩、解压缩、修改、删除、重命名、移动等操作形成详细审计日志。 10、具备网络攻击资源的标注能力，通过获取网络中相关手动标记的攻击集合；根据智能算法进行内容监督的学习训练，通过训练达到预设条件，将达到条件的网络攻击资源进行标注，作为目标攻击模型；从而实现对网络攻击资源进行标注的自动化，提高资源标注能力。 11、系统具备安全攻击信息的获取能力；通过接收终端安全管理中心发送的异常访问信息；根据网络中异常的访问信息，获得发起网络安全攻击行为的异常程序对应的资料；将信息上报至管理中心，转发至安全网关，使得厂家的安服人员根据网络攻击信息直接进行攻击行为的证据获取，提高客户工作效率与安全性。 12、系统可与项目中防火墙实现联动防御，对未安装 EDR 客户端的终端阻断连接，禁止上网，可重定向至 EDR 下载页面指引安装，边界-终端协同联动，智能响应，提高整体安全水平。		
8	**综合运行硬件支撑平台**	1、平台能够与一期二期相关硬件运行支撑平台兼容，实现运行算力集群，通过分布式架构实现资源的统一池化，弹性扩展和部署软件的智能化管理。 2、配置 2 颗处理器，核心数 20 核；主频 2.5GHz, 最大睿频：3.7GHz, 3、配置 512GB 内存，内存类型为 ECC DDR4 2666 RDIMM 内存，最高可用 2666 RDIMM 内存，内存插槽数 24 个插槽,最大容量 1TB；支持 SDDC、双设备数据更正 DDDC、内存镜像、内存冗余位校验 ECC 校验，内存热备技术 4、配置 2*480 SATA 2.5 固态硬盘和 1.6T 固态硬盘和 10 块 4T SATA 机械硬盘，支持热插拔 SAS/SATA/SSD 硬盘	1	台

		5、配置独立 RAID 卡，支持 RAID 0/1/10， 6、最多 11 个 PCIe 扩展槽位：4 个全高全长的 PCIe3.0 x16 标准卡(信号为 x8)，3 个全高半长的 PCIe3.0 x16 标准卡(信号为 x8)，1 个全高半长的 PCIe3.0 x8 标准卡(信号为 x8)，1 个 RAID 卡专用的 PCIe 扩展卡，1 个灵活 LOM 插卡 7、板载网卡：2 个 10GE 接口，灵活插卡：可选配 2*GE 或 4*GE 或 2*10GE 或 1/2 个 56G FDR IB 接口 8、支持 2 个双槽位的全高全长的 GPU 或 FPGA 异构加速卡 9、可管理和维护性：（1）集成系统管理处理器支持：自动服务器重启、风扇监视和控制、电源监控、温度监控、启动/关闭、按序重启、本地固件更新、错误日志，可通过可视化工具提供系统未来状况的可视显示；（2）具有图形管理界面及其他高级管理功能；（3）配置独立的远程管理控制端口，支持远程监控图形界面，可实现与操作系统无关的远程对服务器的完全控制，包括远程的开机、关机、重启、虚拟软驱、虚拟光驱等操作 10、基于 iBMC 芯片，提供全面的故障诊断、自动化运维、硬件安全加固等管理特性；支持 Redfish、SNMP、IPMI2.0 等主流标 准接口，易于被集成；提供基于 HTML5/VNC KVM 的远程管理界面；支持免 CD 部署、Agentless 等特性简化管理复杂度。		
9	**漏洞安全系统云资源管理平台**	1、满足对学校原有服务器计算机虚拟化资源的统筹管理，实现对算力资源整合利用率的的最大化。 2、实现对一期，二期建设的核心系统平台虚拟化扩展部署，部署不影响平台日常教学科研使用，确保平台各项功能指标不受的影响。 3、支持服务器节点退役功能，退役主机的数据自动迁移至其它正常服务器节点 4、可提供 IT 资源的全融合交付模式，在同一管理界面下，可以支持同一品牌超融合、桌面云、云容器的管理，无需多个管理界面进行切换 5、超融合管理平台支持无代理杀毒功能，无需在每台云服务器上单独安装杀毒软件，降低资源开销，同时支持对主流 Windows 和 Linux 操作系统主机进行整体的安全防护，管理平台集成并提供统一的防病毒配置界面以提升便捷性。 6、支持与 UPS 进行联动，且支持关联多个 UPS 电源。当 UPS 电量达到第一阶段电量阈值预警时，可自动关闭优先级别为中和低的云服务器；当 UPS 电量达到第二阶段电量阈值预警时，可自动关闭优先级别	1	套

		为高的云服务器。 7、支持分布式电源管理功能（DPM）,根据集群内主机资源负载情况，在不影响业务的情况下实现自动的服务器开、关机，达到能源效率和资源分配，节省电力和制冷开支 计算虚拟化： 8、云服务器支持 CPU 基准配置，实现同一集群内的异构 CPU 配置，集群中云服务器可以在不同配置 CPU 的服务器上实现在线的迁移，同时支持资源池的 CPU 基准统一配置，提供更高的兼容性。 9、支持云服务器级别副本设置，可以针对不同场景给不同云服务器设置不同数量副本，提升灵活性。最小可以支持 1 副本，最高可以支持 6 个副本，并可以支持动态在线增加和删除副本 10、为提升运维效率，在发生意外故障导致的云服务器停机时，具备将云服务器奔溃前最后一屏报错信息代码进行截图的功能，为后续排错提供依据（ 11、支持通过支持 VNC、Spice 以及 VNC+Spice 模式远程访问云服务器控制台；支持 Spice 方式设置独立访问密码 存储虚拟化： 12、支持提供统一存储服务，包括块存储，文件存储和对象存储，最少只需 3 个节点集群即可同时提供虚拟化、分布式块、对象、文件存储服务。其中对象和文件服务必须在宿主机上提供，和超融合自研同品牌，不能以应用跑在虚拟机上的形式提供，并提供 500T 的存储容量授权。 13、为方便云平台用户文件的共享与访问，提升文件的管理效率，需具备网盘功能，此功能无需额外购买授权即可使用。 超融合分布式存储可以支持文件存储、块存储、对象存储服务，可以向外部系统提供对象存储服务，块存储支持 SCSI 及 iSCSI 接口,可以支持 iSCSI 加密传输； 14、超融合内部的分布式存储支持基于存储卷级别的灵活副本设定，可以针对不同场景对不同的存储卷灵活配置不同级别的副本数，最小支持 2 副本，最高支持 6 个副本，并可以支持动态在线增加和删除副本，不需停机即可操作。 15、支持存储卷的数据块副本图形显示和操作的功能，可以监控数据块的当前状态，可以按需迁移数据块所在的主机和磁盘，可以指定数据块副本的读取优先级。 16、支持存储数据卷安全分级管理，安全级别可设置弱一致、强一致、最终一致。		

		网络虚拟化： 17、支持安全组功能，可用于某一特定云服务器上的网卡（链路实例）的出入流量进行控制，具有默认安全规则以及自定义规则，可基于 IPv4、IPv6、端口号、协议、优先级、TCP flag、ICMP Type 等设置访问规则，支持 1-4 层的安全防护； 18、支持网络微分段 URL 黑白名单功能，实现针对 HTTP 和 HTTPS 进行管理限制，实现安全访问控制。 19、关联黑名单后，不可以访问黑名单内 URL；关联白名单后，只可以访问白名单内 URL。URL 输入格式支持前缀匹配，后缀匹配，关键字匹配和精准匹配。 20、为保障超融合产品的核心功能模块为厂商自主原创，超融合系统核心功能模块应通过中国信息安全测评中心的自主原创产品测评。 21、超融合产品支持 IPv6 网络环境。		
10	**漏洞验证资源库**	1、提供 10 套漏洞科研验证资源。 2、所提供资源需结合学校漏洞科研重点研究方向，提供重点靶标的漏洞验证模块，交付内容包括但不限于：POC、复现文档、演示视频等。 3、通过模拟重点靶标研究对象的运行实际环境，触发靶标漏洞利用的相关研究场景，实现重点靶标的漏洞测试和研究工作。 4、对挖掘靶标漏洞的攻防利用过程进行可视化展示，展现漏洞的危害性，为科研提供支撑。 5、能够对漏洞利用的演示环境进行高效管理，可以迅速组织开展相应漏洞的利用演示过程。从实战角度真实直观体验漏洞安全问题。同时为漏洞挖掘人员进行挖掘的漏洞风险复盘提供有效支撑。	1	**项**

附件 3：

售后服务计划及保障措施

我们郑重声明如下产品质量保证及售后服务承诺：

我公司保证本次项目提供所有产品均为全新、未使用过的正品，具有一定的先进性和可靠性。我公司能严格履行招标文件及合同条款所规定的质量、服务、交货期等各项要求。

我公司依靠现代化的服务体系，改变传统的“有故障才维护”理念，主动实施定时的系统回访、消除系统隐患。并建立有强大的技术支持队伍，确保及时对系统进行专业化维护、升级。安排专业的技术人员，对用户在系统各相关方面提供长期、高质量的技术支持。

免费维修时间：我公司针对本项目提供所投产品提供 3 年质保 。质保期外所有设备免费保修（只收取材料费），免费上门服务。

售后服务响应方式及响应时间：自接到用户报修后，0.5 小时内响应，2 小时内到达用户现场并解决问题，如不能及时解决问题要提供备机服务、直到原设备修复（特殊情况另行商议）。

维修单位名称：北京墨格教育科技有限公司，

售后负责人：梁艳丽

联系电话：010-80653658

我们完全响应贵方的要求，若中标将严格执行投标文件的所有条款，我公司保证服从校方的统筹调度，配合各责任主体职责范围内的工作，在项目过程中，我们将始终信守合，将履行合同条款作为我们的一切行动的中心目标，我公司对本项目承担总包责任，不转包项目，确保项目质量。

公司名称：北京墨格教育科技有限公司

附件 4：

郑州大学仪器设备初步验收单

No.　　年　月　日

<table>
<tr><td>使用单位</td><td colspan="2"></td><td>使用人</td><td colspan="2"></td><td>合同编号</td><td colspan="2"></td></tr>
<tr><td>供货商</td><td colspan="5"></td><td>合同总金额</td><td colspan="2"></td></tr>
<tr><td colspan="9">设备明细（品名、型号、规格、生产厂家、数量、金额等，不够可另附表）</td></tr>
<tr><td>序号</td><td colspan="2">品名</td><td colspan="2">技术参数
（规格型号）</td><td>生产厂家
（产地）</td><td>数量</td><td>单位</td><td>金额</td></tr>
<tr><td></td><td colspan="2"></td><td colspan="2"></td><td></td><td></td><td></td><td></td></tr>
<tr><td rowspan="3">实物验收情况</td><td colspan="8">外观质量（有无残损，程度如何）。</td></tr>
<tr><td colspan="8">清点数量（主机、配件、型号、规格、产地是否与招投标文件、合同、发票、装箱单的数量相同，若有出入，说明缺件名称、规格、数量、金额）。</td></tr>
<tr><td colspan="8">仪器设备安装调试及使用人员培训情况（是否完成整套设备安装、有无安装缺陷，使用人员是否经过培训）。</td></tr>
<tr><td>技术验收情况</td><td colspan="8">依据合同约定技术条款逐一测定设备的性能和各项技术指标，所测结果是否与合同约定技术条款规定的一样，性能是否稳定，配件是否齐全，是否有安全隐患，具体说明。</td></tr>
<tr><td>初步验收情况</td><td colspan="8">☐通过验收　　☐整改后再组织验收
☐不通过验收　索赔要求　　☐其他结论</td></tr>
<tr><td colspan="2">验收小组成员签字</td><td colspan="3"></td><td>供货商
授权代表签字</td><td colspan="3"></td></tr>
</table>

附件 5：

中标通知书

河南省公共资源交易中心

中标通知书

（分包编号：豫政采(1)20250140-1）

北京墨格教育科技有限公司：

贵单位于2025年7月29日参加的郑州大学网络空间安全学院、中原网络安全研究院漏洞挖掘与应用研究分析平台建设项目三期采购项的投标（采购编号：豫财招标采购-2025-595），经评标委员会评审及采购人确定，贵单位为该项目中标人，中标金额为2186000元人民币。

请贵单位收到中标通知书后，按照本项目招标文件的规定及贵单位投标文件确定的事项，与采购人签订书面合同。

特此通知。

采购人（盖章）

集中采购机构（盖章）

2025年7月30日