河南物流职业学院
网络及信息安全基础设施建设项目
采购合同书

甲方（需方）：河南物流职业学院

乙方（供方）：河南育安科技有限公司

甲乙双方依据河南物流职业学院网络及信息安全基础设施建设项目（采购项目编号：豫财磋商采购-2025-585，包号：豫政采(2)20250973-2）中标通知书，根据《中华人民共和国民法典》等有关规定以及甲方采购文件和乙方投标文件的内容，甲乙双方经友好协商，现达成以下条款:

一、合同标的与价款

本合同所指货物为河南物流职业学院网络及信息安全基础设施建设项目（包号：豫政采(2)20250973-2）货物（主要技术参数及配置见附件一、二），合同总价款为人民币大写：捌拾肆万玖仟伍佰元整（小写¥849500.00 元）（该价款已包含所采购货物的成本、利润、税金、包装、运输、安装、人工、材料、保修、人员培训等乙方为履行本合同约定义务发生的所有费用），本合同执行期间合同总价款不变，不因通胀、汇率变动等因素调整。

二、货物质量要求与售后服务要求

（一）货物质量要求

1.乙方应保证货物是全新、未使用过的，并完全符合强制性的国家技术质量规范和本合同附件一、二规定的质量、规格、性能及技术规范等要求。货物符合实行国家“三包”规定的，应执行“三包”规

定。

2.乙方提交的货物应符合响应文件中所记载的详细配置、技术参数、参数及性能，并应附有此类货物完整、详细的技术资料、产品说明书、合格证等。

3.乙方应保证将货物按照国家或专业标准包装、确保货物安全无损运抵合同规定的交货地点，并进行安装、试运行。

4.乙方保证货物不存在危及人身及财产安全的产品缺陷，否则应承担全部法律责任。

（二）售后服务要求

1.质量保证期为自货物通过最终验收之日起36个月。

2.在货物质保期内，乙方应对由于设计、工艺、质量（含环保节能要求）、材料和的缺陷而发生的任何不足或故障负责，并解决存在的问题。

3.乙方提供的货物应包括本合同规定的全部货物及其附（辅）件、资料。

4.货物安装调试完成后，乙方应继续向甲方提供良好的技术支持。应当由专门队伍从事此项工作，并提供全天候的热线技术支持服务，应当对甲方所反映的任何问题在10分钟之内做出及时响应，在2（小时）之内赶到现场实地解决问题。若问题、故障在检修4（小时）后仍无法解决，乙方免费提供不低于故障货物规格型号档次的备用货物供甲方使用，直至故障货物修复。

5.乙方应当建立健全售后服务体系，确保货物正常运行。乙方应当遵守甲方的有关管理制度、操作规程。

6.乙方应负责货物及主要部件、配件维修更换。质保期内，乙方对货物（人为故意损坏除外）提供全免费保修或免费更换；质保期后，

收取维修成本费（备品备件乙方应以响应文件承诺的优惠价格提供）。

7.乙方未及时到达维修，甲方有权聘请第三方进行维修，其产生的所有费用由乙方承担，若因此造成甲方损失，乙方应承担违约赔偿责任。技术电话：17337327396 。若乙方提供的售后服务有书面文件，可作为合同附件。

三、交货期及交货地点

乙方应于本合同签订之日起 30 日内将合同条款中的全部货物运送到河南物流职业学院指定地点，向甲方提供纸质及电子的施工方案、质量控制规范，完成货物的安装、调试和人员培训，并提供项目建设相关纸质及电子版技术文档，所发生的费用由乙方负责。甲方应在货物到达指定地点后，提供符合安装条件的场地、电源、环境等必须的基础工作条件。货物完成验收并交付使用前由乙方保管并自行承担一切责任。

四、技术资料

乙方交货时应提供一套完整的设备技术资料（如目录索引、操作手册、使用指南、维修指南（或）服务手册；或国标装箱要求配置的标准资料）包装好随同每批货物一起交付。乙方不能完整交付货物及本款规定的设备技术资料的，视为未按合同约定供货，乙方必须负责补齐，因此导致逾期交付的，由乙方承担相关的违约责任。如货物外包装完好无缺，但箱内设备有短缺或损伤，甲方及设备最终用户有权在设备质保期内提供有关质量验收证明提出补足或更换，相关费用由乙方承担。补足或更换设备的交货期为接到甲方或设备最终用户通知 7 天内，若乙方未在该期限内进行补足或更换，乙方应向甲方支付合同总价 5%的违约金。

五、使用合同文件和资料

1.事先未经甲方书面同意，乙方不得将由甲方或代表甲方提供的有关合同或任何合同条文、规格、计划、模型等提供给与履行本合同无关的任何其他人。即使向与履行本合同有关的人员提供，也应注意保密并限于履行合同所必需的范围。

2.双方对在合作过程中所获知的对方单位涉密信息、技术情报和资料均必须保密，任何一方不得向第三方泄露或以本合同之外的目的使用，保密信息包括但不限于：学生数据、技术文档等。

3.上述保密义务不因本合同的无效、终止或被解除而终止。乙方员工泄密视为乙方违约。

六、检验和测试

1.货物抵达目的地后，乙方及时向甲方提出检验申请，由甲方按招投标文件要求、合同要求对货物的质量、规格、数量进行检验，如果发现质量、规格、数量或其他有与合同规定不一致的地方；或对成套货物安装调试、人员培训有异议的；或证实货物是有缺陷的，包括潜在的缺陷或使用不符合要求的材料等，甲方有权拒收所有货物，及时通知乙方。乙方在收到通知后最迟应于24小时内解决问题，采取补交或更换等措施，由此造成的损失由乙方承担，由此造成的逾期交货按照逾期违约交货处理。

2.如果乙方在收到通知后7天内没有解决问题，甲方可采取必要的补救措施直至解除合同另行采购，但由此引发的风险、损失和费用均由乙方承担。

3.如甲乙双方对货物的质量发生争议，可委托具有国家规定相关资质的第三方检验机构检验，检验和测试不论在何处发生，一切费用均由乙方承担。

4.安装过程中若发生安全事故由乙方承担。

5.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。

七、验收

1.本项目完成软硬件产品（产品/服务内容第 1-10 项）安装调试后，乙方书面提出验收申请，甲方按学校验收程序组织验收。

2.甲方验收标准为满足国家或行业规定的标准及采购人的验收要求，乙方不得变更合同中的货物品牌、型号、规格等。如因特殊原因需要变更，则必须向甲方递交书面变更申请，并经同意后方可更换，乙方应承担因更换而支付的一切费用。未经甲方同意而进行变更，甲方有权不予验收，并视为违约行为，同时要求乙方按原合同执行。因更换而造成逾期交货，仍按逾期交货处理。

3.甲方可以视项目规模或复杂情况聘请专业人员参与验收，大型或复杂项目，以及特种货物应当邀请国家认可的第三方质量检测机构参与验收。

4.乙方所交的货物安装、调试完毕，正常运行 15 日内，书面形式向甲方提出验收申请，由甲方或其聘请的专业机构依据采购文件、投标文件的技术规格要求及承诺和国家有关质量标准对货物进行现场验收，第一次验收不通过，给予 7 日的整改期，再行组织验收，验收合格后由甲乙双方签署货物验收单并加盖公章。甲方在收到产品设备后可以在合理期限内提出异议。

八、人员培训

乙方免费对甲方人员进行技术培训，培训的时间、地点、方式等以甲方要求为准。

九、付款方式及期限

1.乙方开具以河南物流职业学院为客户名称符合财政要求的正规

发票。

2.付款期限：本项目完工经甲方验收合格并收到乙方的正规发票后，经双方确认后，甲方执行财政资金支付程序，按 100% 一 次支付合同总价款，即人民币大写：捌拾肆万玖仟伍佰元整（含税），小写¥849500.00 元。甲方支付以财政资金及时足额到位为前提，逾期支付不视为违约。

3.乙方账户信息:

乙方（开户名）：河南育安科技有限公司

开户行：中国银行股份有限公司郑州龙子湖智慧岛支行

银行账号：255984945254

统一社会信用代码：91410100MA9NH4B40E

4.乙方企业规模：微型（微型/小型/中型/大型）

十、甲乙双方应严格遵守甲方招标文件中的投标要求和投标人须知，如有违反，按投标要求和投标人须知规定予以处理。

十一、采购文件及其修改、投标文件及其修改、澄清以及本合同书的附件一、二均为本合同的组成部分。其效力顺序为：首先，本合同书及其附件一、二，其次，采购文件及其修改，再次，投标文件及其修改、澄清。

十二、违约与索赔

1.乙方未按合同约定交付货物物和履行合同项目的，应向甲方偿付违约金，违约金按每周合同总价款的 0.5%计收。该违约金的最高限额为合同总价款的 5%。一周按 7 天计算，不足 7 天按一周计算。如果达到最高限额，甲方有权解除合同，合同解除后，乙方应在 5 日内退还甲方已支付的全部款项及合同金额 5%的违约金，并赔偿甲方因此遭受的全部损失。

2.乙方不能交付货物的，应向甲方偿付合同总价款 5%的违约金，同时甲方有权解除合同。合同解除后，乙方应在 5 日内退还甲方已支付的全部款项及并赔偿甲方因此遭受的全部损失。甲方无正当理由拒收货物，应向乙方偿付拒收货物款额总值5%的违约金。

3.乙方所交付的货物不符合本合同规定的，甲方有权拒收，乙方在得到甲方通知之日起5个工作日内采取补救措施。

4.除竞争性磋商文件事先说明、且经甲方事先书面同意外，乙方不得分包、转包其应履行的合同义务。若乙方分包或转包，应向甲方偿付合同总价款5%的违约金，同时甲方有权解除合同。合同解除后，乙方应在 5 日内退还甲方已支付的全部款项及并赔偿甲方因此遭受的全部损失。

5.如果乙方对货物的偏差负有责任，而甲方在规定的检验、安装、调试、验收和质量保证期内提出了索赔，乙方应按照甲方同意的下列一种或几种方式解决索赔事宜:

（1）乙方同意退货并用合同规定的货币将货款退还给甲方，并承担由此发生的一切损失和费用，包括利息、银行手续费、运费、保险费、检验费、仓储费、装卸费以及为看管和保护退回货物所需的其它必要费用。

（2）根据货物的偏差情况、损坏程度以及甲方所遭受损失的金额，经甲乙双方商定降低货物的价格。

（3）用符合合同规定的规格、质量和性能要求的新零件、部件和（或）货物来更换有缺陷的部分和（或）修补缺陷部分，乙方应承担一切费用和风险并负担甲方蒙受的全部直接损失费用。同时，乙方应延长所更换货物的质量保证期。

6.如果在甲方发出索赔通知后三十（30）天内，乙方未作答复，

甲方所选择的上述索赔方式之一应视为已被乙方接受。如乙方未能在甲方发出索赔通知后三十（30）天内或甲方同意的延长期限内，按照甲方同意的上述规定的任何一种方法解决索赔事宜，乙方承担违约责任，并赔偿甲方的全部损失以及甲方为维权所支出的诉讼费、律师费、差旅费等费用。

7.甲方将根据违约严重程度视情况将乙方列入甲方的不良诚信记录名单，并向政府有关部门报送不良诚信记录。

十三、知识产权

乙方需保障甲方在使用采购货物或其任何一部分时不受到第三方关于侵犯专利权、商标权或工业设计权等知识产权的任何指控。如果任何第三方提出侵权指控，乙方需与第三方交涉并承担可能发生的一切费用。如因此而给甲方造成损失的，乙方应全额赔偿甲方损失。

十四、通知和送达

1、本合同确定双方的联系人和通讯地址如下:

甲方联系人：姓名：李伟 电话：18530737471

甲方通讯地址：河南物流职业学院平原校区

乙方联系人：姓名：张涛 电话：13838276246

乙方通讯地址：郑州市郑东新区中道东路6号创意岛大厦B-6-020号

上述联系人和通讯地址如发生变化应及时书面通知对方，否则应承担不利的法律后果。

2、本合同在履行过程中所有法律文书的送达均采取书面形式，均应签字确认；如任一方拒绝签收或无法送达的，则另一方可直接采取邮寄的方式送达，一方按照上述地址邮寄送达后，无论对方是否签收，均自邮寄信件交寄出后第三日即视为已经有效送达给对方。

十五、本合同签订和履行适用中华人民共和国法律，因履行合同发生的争议，由甲乙双方直接协商解决，如协商不成向甲方住所地人民法院诉讼。在法院审理期间，除有争议部分外，本合同其他部分可以履行的仍应按合同条款继续履行。

十六、本合同未尽事宜，甲乙双方可签订补充协议，与本合同具有同等法律效力。

十七、合同生效及其它

1.本合同一式 陆 份，甲方 肆 份，乙方 贰 份。具有同等法律效力。自甲乙双方签字、盖章之日起生效。

2.乙方要指定不少于一人全权全程负责本项目服务的落实，包括服务的咨询、执行和后续工作。项目负责人姓名： 张亚 ；联系电话：13939037093 。

3.甲、乙方中任何一方，因不可抗力不能按时或完全履行合同的，应及时通知对方，并在15个工作日内提供相应证明。未履行完合同部分是否继续履行、如何履行等问题，可由双方初步协商，并向主管部门和政府采购管理部门报告。确定为不可抗力原因造成的损失，免予承担责任。

【以下无正文】

【签章页】

甲方（盖章）

单位名称：河南牧业经济学院

法定代表人（或委托代理人）签字：

地址：

电话：0373-7193306

签订时间：2025年7月28日

乙方（盖章）

单位名称：河南育安科技有限公司

法定代表人（或委托代理人）签字：张涛

地址：郑州市郑东新区中道东路 6 号创意岛大厦 B-6-020 号

电话：13838276246

签订时间：2025年7月28日

附件一

货物规格价格一览表

人民币（单位：元）

序号	项目	品牌型号	制造商名称	数量	单位	单价	总价	服务期
1	堡垒机	安恒信息 DAS-USM290-PRO-Z3	杭州安恒信息技术股份有限公司	1	套	70000	70000	3 年
2	运维 VPN	天融信/TopVPN 6000	北京天融信网络安全技术有限公司	2	套	17500	35000	3 年
3	WEBVPN	天融信/TopVPN 6000	北京天融信网络安全技术有限公司	1	套	80000	80000	3 年
4	僵木蠕监测系统	天融信/TopTVD	北京天融信网络安全技术有限公司	1	台	147500	147500	3 年
5	防火墙防病毒功能升级	天融信/AVPRO-SMT-LIC-D-NG-1Y	北京天融信网络安全技术有限公司	1	套	60000	60000	3 年
6	入侵防御设备特征库升级	天融信/IDP-LIC-D-1Y	北京天融信网络安全技术有限公司	1	套	50000	50000	3 年
7	漏洞扫描设备特征库升级	天融信/TSC-SUP-1Y-EP	北京天融信网络安全技术有限公司	1	套	50000	50000	3 年
8	上网行为管理特征库升级	天融信/ACM-LIC-1Y	北京天融信网络安全技术有限公司	1	套	50000	50000	3 年
9	新乡校区防火墙特征库升级	启明星辰 USG-FW-4000-NF-IPS-3Y	北京启明星辰信息安全技术有限公司	1	套	23500	23500	3 年

10	新乡校区入侵防御特征库升级	启明星辰 NT3000-VPSB2S	北京启明星辰信息安全技术有限公司	1	套	23500	23500	3年
11	网络安全运营服务	定制服务：1.安全运营服务（SaaS模式）2.对接河南省教育系统网络和数据安全监测与保障服务平台	河南省鼎信信息安全等级测评有限公司	1	项	260000	260000	3年
合计						849500		

附件二

产品/服务参数一览表

序号	产品名称	产品参数	数量	单位
1	堡垒机	1、授权资产数 300，并发字符连接数 300 个；3 年维保，永久使用； 2、支持多种用户角色:超级管理员、部门管理员、审计管理员、运维员、审计员、系统管理员、密码管理员，每种用户角色的权限都不同，为用户设立不同的角色提供了选择，满足合规对三权分立的要求，并提供灵活的角色自定义能力。（提供截图证明）。 3、系统支持风险运维审计实时告警，并通过企业微信或钉钉自动下发，提供相应的技术功能呈现证明材料；支持与 get、post、soap 发送方式的 http 短信网关平台联动，实现短信动态口令双因素认证机制； 4、支持常用的运维协议；可通过应用发布的方式进行协议扩展，如数据库、浏览器等客户端工具；支持主流数据库协议代理运维，可直接调用本地 windows 系统的数据库客户端工具，支持自动登录、无需应用发布前置机； 5、支持 ssh、telnet、rlogin、rdp、vnc 协议的 H5 运维，无需本地运维客户端工具；支持对运维操作会话的在线监控、实时阻断；保存 SSH 的 sz/rz 命令（zmodem）传输的原始文件； 6、支持通过基于时间、IP/IP 段、用户/用户组、设备/设备组、设备账号、命令关键字、控制动作、黑白名单等组合访问控制策略，授权用户可访问的目标设备。 7、运维报表支持自动定期发送，提供一键导出符合等级保护、SOX 法案要求的综合分析报告； 8、投标人提供系统用户、资产、授权的增删改查等 API 接口，允许任何第三方平台安全调用堡垒机的 API 接口，实现用户、资产、权限自动同步到堡垒机，简化配置工作量。（提供接口调用证明材料）； 9、提供集中的命令控制策略功能，支持字符协议及数据库协议的命令级策略控制，支持通配符和正则表达式两种方式，实现阻断会话、阻断命令、审批、直接放行 4 种动作。（提供截图证明） 10、支持对 Web 应用的自动改密功能，并且支持随堡垒机提供的改密插件录制向导，通过改密插件自动生成 web 应用的改密脚本。（提供相关截图证明和承诺函）； 11、支持灵活的文件传输双向控制，支持传输文件留存，有效防止数据泄漏风险。内置 SSLVPN 功能，实现远程运维的安全接入，保证数据传输安全。（提供截图证明）。	1	套

		11、支持灵活的文件传输双向控制，支持传输文件留存，有效防止数据泄漏风险。内置 SSLVPN 功能，实现远程运维的安全接入，保证数据传输安全。（提供截图证明）。 12、支持国密 TLS 双向认证通信，开启后同时使用支持国密算法的浏览器、国密 USBkey 才能访问堡垒机，只使用国密浏览器无法访问堡垒机，以此种方式对发起连接的客户端身份进行验证。（提供相关截图证明并提供证明材料，提供第三方密码产品的《商用密码产品认证证书》及第三方密码产品授权函）。 13、具备自动化编排能力，通过编排动作流的方式，对目标资产进行定时或周期性的自动化运维。动作流可包括：上传文件、执行命令、下载文件等。动作流会按设定好的顺序进行执行，对于常见的运维工作，如升级、巡检等，均可通过此能力快速执行。（提供截图证明）； 14、投标人所投产品全周期满足信息系统等级保护安全相关要求，提供产品服务包含 3 年内每年度不少于 2 次为学校提供监管部门认可的等保工具箱现场检测服务并出具检测报告； 15、提供所投产品 3 年质保升级服务。提供 24 小时支持热线；本地应急响应时间 2 小时内。		
2	运维 VPN	1.硬件参数：1U,内存：4G，CF 卡：1G，4 个千兆电口,单电源。 2.性能参数：,整机吞吐 600M 并发连接 50 万 IPSEC 吞吐 60MSSL 吞吐 120M 最大并发用户数 300 默认含 10 个 SSLVPN 的客户端许可；3 年硬件维保。 3.★具备静态用户名口令、数字证书、短信、硬件特征码绑定、图形码、人脸识别认证方式；（提供截图证明），具备两种或两种以上组合认证方式；（提供截图证明）。 4.具备 Web 方式单点登录，用户登录 VPN 后无需二次输入用户名口令即可登录应用系统； 5.具备可信接入分级授权； 6.具备 PC 终端病毒检查功能； 7.具备 WebCache、图片优化技术，对 web 页面、图片数据进行优化； 8.具备移动 APP 自动封装 SSLVPN 的 SDK； 9.具备虚拟门户功能，具备虚拟门户中使用用户名口令、数字证书、人脸识别认证方式，具备虚拟门户双因子认证； 10.具备国家商密专用的 SM2、SM3、SM4 算法；； 11.具备设备的运行状态、设备资源状态、并发用户数、客户端类型分布、IPSEC 隧道状态、用户流量、安全事件、中国任意省市区县的接入用户数监控，并通过图表展示；（提供截图证明）；	2	台

		12.★具备“管理”、“系统”、“安全”、“策略”、“通信”、“硬件”、“容错”、“测试”等多种触发报警的事件类；（提供截图证明）； 13.★提供 IPv6Ready 认证证书；(提供证书复印件） 14.提供所投产品 3 年质保升级服务。提供 24 小时支持热线；本地应急响应时间 2 小时内。		
3	WEBVPN	1.硬件参数：1U,8 个千兆电口，4 个千兆光口,冗余电源,1 个扩展槽位。 2.性能参数：,IPSEC 最大吞吐率：1.5GbpsIPSECVPN 最大隧道数：4000SSL 最大吞吐率：1GbpsSSL 最大并发用户数：4000 最大管理用户数：15000 配置 1000 个 SSLVPN 的客户端并发许可；可扩展 PC 端可信接入模块、可扩展短信认证模块，可扩展入侵防御模块，可扩展应用过滤模块，可扩展 PC 端 Windows 系统病毒检查模块，可扩展人脸识别认证模块；3 年硬件维保。 3.★具备静态用户名口令、数字证书、短信、硬件特征码绑定、图形码、人脸识别认证方式；（提供截图证明），具备两种或两种以上组合认证方式；（提供截图证明）。 4.具备 Web 方式单点登录，用户登录 VPN 后无需二次输入用户名口令即可登录应用系统; 5.具备可信接入分级授权; 6.具备 PC 终端病毒检查功能; 7.具备 WebCache、图片优化技术，对 web 页面、图片数据进行优化; 8.具备移动 APP 自动封装 SSLVPN 的 SDK; 9.具备虚拟门户功能，具备虚拟门户中使用用户名口令、数字证书、人脸识别认证方式，具备虚拟门户双因子认证; 10.具备 SPA 单包认证功能; 11.★具备流量控制，可对链路的速率、最大速率、优先级等进行设定；（提供截图证明） 12.具备设备的运行状态、设备资源状态、并发用户数、客户端类型分布、IPSEC 隧道状态、用户流量、安全事件、中国任意省市区县的接入用户数监控，并通过图表展示; 13.具备网络加速功能；通过网络加速功能动态地调整拥塞窗口大小和发送速率。 14.★具备“管理”、“系统”、“安全”、“策略”、“通信”、“硬件”、“容错”、“测试”等多种触发报警的事件类；（提供截图证明）； 15.具备集群管理，在 SSLVPN 负载均衡模式下 VPN 不需要借助其他负载产品可以完成负载分发工作;	1	台

		16.★需提供 IPv6Ready 认证证书；(提供证书复印件) 17.提供所投产品 3 年质保升级服务。提供 24 小时支持热线；本地应急响应时间 2 小时内。		
4	僵木蠕监测系统	1.硬件参数：2U,内存 32G，机械硬盘 1TB，6 个千兆电口，4 个千兆光口插槽，1 个 CONSOLE 口,冗余电源,5 个扩展槽位。 2.性能参数：最大并发连接数：150W，综合威胁检测能力：3Gbps,含：3 年打包升级许可，包含攻击检测规则库、应用识别库、地理信息库、僵尸主机规则库、威胁情报库、URL 分类库。3 年硬件维保。 3.具备受害者视角分析，按照时间范围、受害主机、事件类型、处置状态、攻击结果、应用协议等条件综合分析受害者信息。 4.具备 DDoS 攻击事件分析，按照时间范围综合分析 DDoS 攻击类型分布、被攻击 IPTop10、被攻击 IP 排名、被攻击 IP 流量排名等信息。 5.具备能够检测包括：扫描探测、暴力猜解、拒绝服务攻击、后门控制、溢出攻击、代码执行、非授权访问、注入攻击、URL 跳转、跨站攻击、WebShell、浏览器劫持、文件漏洞攻击、工控漏洞攻击、车联网漏洞攻击、物联网漏洞攻击、其他类攻击等在内的 17 大类超过 10000 种以上网络攻击事件。 6.具备对攻击逃逸报文进行深度智能检测，包括：IP 分片、TCP 分段、RPC 分片分段、SMB 分片分段、HTTP-Header 折叠、HTTP-BodyUTF-7 编码、HTTP-BodyUTF-16（LE/BE）编码、HTTP-BodyUTF-32（LE/BE）编码、HTTP-Body 压缩、HTTP-Post 数据编码、邮件体编码、URL 多重编码、URL 斜线分隔符、URI 相对目录欺骗、HTTP-Javascript 编码、邮件头折叠等类型。 7.★具备独立的僵尸主机检测引擎，涵盖 11000 种以上的僵尸主机规则库。规则库具备按照攻击类型、操作系统、风险等级、ATT&CK、攻击阶段等方式进行分类。（提供截图证明）。 8.具备 DDoS 自学习模式检测，可设定学习时长，根据周期内流量状态自动学习，设置检测流量阈值。流量异常触发阈值系统自动进行告警。 9.具备恶意程序检测，采用固网恶意程序检测智慧引擎、移动恶意程序检测智慧引擎、虚拟沙箱、YARA 等多种检测方式。 10.★具备通过智慧引擎检测未知威胁，通过威胁情报、僵尸主机检测已知 APT 攻击行为和已知 APT 组织。（提供截图证明）； 11.具备恶意加密流量检测，采用恶意 TLS 流量智慧引擎、异常握手、非法证书和内网流量检测恶意加密流量。	1	台

		12.具备 URL 检测，检测类型包括：搜索引擎、社交网络、网上购物、科学技术、求职招聘、生活资讯、新闻及门户、休闲娱乐、财经、流媒体、P2P 资源、下载、教育、邮件和存储、传统行业、政策法规、网络安全、成人内容、非法及不良、其它等 20 大类 1000 万条规则。 13.★具备与原有防火墙联动处置，发现威胁事件联动防火墙阻断，具备有与原态势感知系统联动，发现威胁事件信息可上报至平台进行态势分析。（提供截图证明） 14.具备取证功能，取证类型包括：PCAP 取证、样本取证两种形式，PCAP 取证文件具备在线预览。 15.★产品具备《网络安全专用产品安全检测证书》（提供证书复印件） 16.提供所投产品 3 年质保升级服务。提供 24 小时支持热线；本地应急响应时间 2 小时内。		
5	防火墙防病毒功能升级	1.原防火墙设备升级，开通防病毒功能模块，对进出的网络数据流进行病毒、恶意代码扫描和过滤处理，并提供病毒代码库的自动或手动升级，彻底阻断外部网络的病毒、蠕虫、木马及各种恶意代码向网络内部传播，病毒过滤网关与部署在终端、服务器上的防病毒软件相配合，从而形成覆盖全面，分层防护的多级病毒过滤系统，提供 3 年特征库升级许可。 2.★具备 IPv6 域名控制，具备对多级域名进行控制，域名对象具备通配符；（提供截图证明） 3.具备对达梦、人大金仓等数据库应用、P2P、移动应用、迅雷加密流量、向日葵/Teamview 等远程控制软件、Modbus/IEC/OPC 等工控物联网协议进行识别控制，具备自定义应用特征； 4.具备 NTPDDOS 防护，采用阈值检查、源/目的限流、源认证等方式综合进行 NTPREQUESTFLOOD、NTPREPLYFLOOD 攻击防护； 5.内置邮件安全防护功能，具备邮件过滤、邮箱防暴力破解、邮件泛洪攻击防护、邮件黑、白名单检测；	1	项
6	入侵防御设备特征库升级	1.原入侵防御设备升级，针对常见的漏洞利用攻击、SQL 注入攻击、XSS、缓冲区溢出、DOS/DDOS 攻击等恶意破坏方式，综合采用多种安全机制，阻断恶意的网络数据包，有效保证信息系统服务器正常提供服务，提供 3 年特征库升级许可。 2.具备独立的攻击检测引擎，涵盖 12000 种以上的攻击检测规则库。规则库具备按照攻击类型、操作系统、风险等级、应用类型、流行程度等方式进行分类。 3.具备工控漏洞攻击、车联网漏洞攻击、物联网漏洞攻击。如对施耐德、Siemens、SCADA、SERVER-WEBAPPLinksysE 系列、IGSSSCADA 系统、罗克韦尔、华为 HG532 路由产品、Vivotek 智能摄像头、XiaomiMiWiFiR3G 路径遍历漏洞攻击等。	1	项

		4.具备对攻击逃逸报文进行深度智能检测防御，包括 IP 分片、TCP 分段、RPC 分片分段、SMB 分片分段、HTTP-Header 折叠、HTTP-BodyUTF-7 编码、HTTP-BodyUTF-16（LE/BE）编码、HTTP-BodyUTF-32（LE/BE）编码、HTTP-Body 压缩、HTTP-Post 数据编码、邮件体编码、URL 多重编码、URL 斜线分隔符、URI 相对目录欺骗、HTTP-Javascript 编码、邮件头折叠等类型。 5.★入侵防御系统需提供人工智能模型特征库构建能力，进行 DNS 日志收集；进行去重整理，然后提取特征字段，对异常特征库字段进行不断的向量化处理，从而能够不断训练出更优质的人工智能检测模型，显著降低入侵防御的检测误报率。（提供第三方权威机构颁发的具有法律效力的有效性证明文件及技术支撑材料）		
7	漏洞扫描设备特征库升级	1.原漏洞扫描设备特征库升级，通过对系统漏洞、服务后门等攻击手段多年的研究积累，总结出了智能主机服务发现，深入检测出系统中存在的漏洞和弱点，最后根据扫描结果，提供整改方法和建议，帮助管理员修补漏洞，全面提升整体安全性，提供 3 年特征库升级许可。 2.具备扫描系统漏洞数量大于 370000 种，Web 漏洞数量大于 5000 种,数据库大于 3000 种; 3.具备扫描大数据组件的安全漏洞，如 Spark、Splunk、Kafka、Storm、Cassandra、Ambari、Impala、Solr、Oozie、Hbase、Hadoop 等，可扫描漏洞数量大于 400 条; 4.具备同时下发系统扫描任务、弱口令扫描任务、Web 扫描任务、基线核查任务 5.★具备漏洞生命周期管理，包括未修复、确定、忽略、修复、已验证五种状态（提供截图证明）；	1	项
8	上网行为管理特征库升级	1.原上网行为管理特征库升级，为客户提供安全策略、链路负载、身份认证、流量管理、行为管控、上网审计、日志追溯、网监对接、用户行为分析、等实用功能，提供 3 年特征库升级许可。 2.一键下载设备健康信息，当设备发生故障时如丢包、宕机、异常重启等问题时可以通过设备健康信息获取有效数据，能够快速定位问题。 3.具备对 TCP、UDP、ICMP、TCPSYN 超时时间，无回应 UDP 超时时间设置，并能具备按照新建会话与总会话比例设置老化开始或者结束。 4.具备隐藏设备源地址，替换成可自定义的伪装地址。 5.★具备通过指纹识别用户身份，并对用户做控制。（逐项提供截图证明，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）；	1	项

9	新乡校区防火墙特征库升级	原新乡校区防火墙特征库升级，提供三年入侵防御特征库升级服务，采用基于状态的协议分析和协议树匹配算法，能够实时检测和阻止各种恶意网络攻击行为，保护网络系统和资源的安全。支持安全防护监测能力：系统命令注入、目录遍历、webshell 上传、文件包含、cookie 攻击等攻击方式的防御、web 漏洞和系统漏洞攻击防护、缓冲区溢出检测等功能。支持自动、手动方式的应用特征库升级，特征库更新周期每周一次。	1	项
10	新乡校区入侵防御特征库升级	原新乡校区入侵检测特征库升级，提供三年入侵检测特征库升级服务，支持协议自识别与协议插件技术，可准确识别采用非常规端口的协议和新型协议，对于病毒、蠕虫、木马、DDoS、扫描、SQL 注入、XSS、缓冲区溢出、欺骗劫持等威胁具有高精度的检测能力，并提供相应的处理建议。支持对异常流量的检测，可实时发现流量异常行为；并提供了对入侵威胁事件的 IP 定位系统，可迅速定位威胁源。支持自动、手动方式的应用特征库升级，特征库更新周期每周一次。	1	项
11	网络安全运营服务	一、安全运营服务（SaaS 模式） 服务内容: 1.提供 3 年 7*24 小时整体网络安全威胁检测和响应运营服务。依托远程安全运营中心的专家团队和技术堆栈，结合用户本地安全探针引擎，持续性开展威胁监测、事件分析与处置等运营工作，与用户共同打造流程化、指标化的持续、闭环、有效的安全运营体系。主要内容包括: （1）互联网业务漏洞监测、安全持续监测服务。 （2）高频漏洞专项安全运营服务、安全持续监测服务。 （3）内部网络漏洞监测（WINDOWNS 的 DNS 服务被频繁攻击）、安全威胁分析服务、安全能力有效性评估服务、网络安全培训服务、网络安全运营支撑平台服务。 服务成果: 2.《安全运营服务报告》报告频率：周报/周，月报/月。《安全事件分析及处置报告》报告频率：按需触发，不限次数。《安全预警通告》报告频率：按需触发，不限次数。《安全培训》频率：一年两次。 服务要求: 3.安全运营服务团队具备一线分析师 2 人，二线分析师 2 人，专职交付经理 1 人。所有分析师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分析师。 4.系统内配置服务质量管理的各项质量指标要求，指标项 60 项，以指标项对项目整体、各分析师进行评价，并在系统中提供专用的运营质量可视化管理功能。（提供以上要求相关服务能力截图）	1	项

		5.分析过程通过安全运营服务支撑系统编写分析记录，系统的记录字段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。（提供以上要求相关服务能力截图） 6.安全运营服务团队通过聚合、清洗多源情报，提供可直接使用的有效情报进行威胁分析。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。（提供以上要求相关服务能力截图） 7.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 100 个，每个事件脚本中包含事件确诊、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。（提供以上要求相关服务能力截图） 8.威胁事件的平均检出时长（MTTD）小于 2 小时；事件平均定性时长（MTTA）小于 12 小时。所有事件的 MTTD、MTTA 指标在运营支撑系统中以可视化形态进行展示。（提供以上要求相关服务能力截图） 9.告警及事件通告方式支持邮件、短信、社交媒体（微信群、飞书群、企业微信群、微信服务号等）及电话。（提供以上要求相关服务能力截图） 服务支撑平台要求: 10.安全运营服务提供 SaaS 化 Web 服务门户，接入 3 台核心安全防护设备，并根据需求部署流量分析工具。 11.支持用户登录安全运营服务门户，查看项目交付情况，浏览安全态势、下载成果报告。 12.安全运营服务支撑门户支持展示相关用户的服务成果汇总信息，包括但不限于服务开通情况、服务安全得分、已发现高危资产、已处理告警各级别量、已分析安全事件各级别量、已发现安全漏洞各级别量，已提交报告量等；能够展示至少近 6 个月的高危漏洞的发现数量变化趋势；能够展示至少近 6 个月的安全事件类型分布情况；支持通过点击已发现高危资产、已处理告警各级别量、已分析安全事件各级别量、已发现安全漏洞各级别量，已提交报告量等数字跳转至相应详情页面中。（提供以上要求相关服务能力截图） 13.安全运营服务支撑门户支持以“业务系统资产”与“基础资源资产”两级维度对资产进行展示，能够展示两类资产的安全属性信息，并支持构建“业务系统资产”与“基础资源资产”的包含关系，并以资产关联关系图的形式呈现业务形态。（提供以上要求相关服务能力截图）		

		14.安全运营服务支撑门户支持将用户威胁监测事件分析成果在同一事件窗口内以不同标签页的形式构建事件分析卷宗进行呈现，标签页应包含事件详情、事件分析、事件处置、受影响资产、相关漏洞、可疑对象、告警与报告等。（提供以上要求相关服务能力截图） 15.安全运营服务支撑门户支持展示相关用户的漏洞数据情况，包括已发现安全漏洞、业务系统漏洞、基础资源漏洞；待修复业务系统漏洞、基础资源漏洞；已修复业务系统漏洞、基础资源漏洞；已完成敏感信息泄露测试数量、已完全安全意识评估数量等。能够展示已发现漏洞类型分布、整改情况分布 top10、近 6 个月漏洞变化趋势、漏洞发现/整改态势图等；支持展示安全敏感信息泄露服务成果，包括监测任务名称、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、公众号数量等；支持展示安全意识隐患服务成果，包括评估任务名称、受测邮箱数量、运行附件数量、点击链接数量、提交表单数量等。（需提供以上要求相关服务能力截图） 16.安全运营服务支持将相关用户运营服务报告进行汇总展示的能力，包括且不限于安全测试报告、季度报告、运营月报、运营周报、运营日报、阶段性报告、事件分析报告、安全意识隐患报告、安全敏感信息泄露报告等。（提供以上要求相关服务能力截图） 二、对接河南省教育系统网络和数据安全监测与保障服务平台 3 年服务 17.满足接口适配性要求：严格按照省平台提供的接口规范进行开发和对接，确保接口的兼容性和稳定性，且接口响应时间不超过 500 毫秒。 18.满足数据格式一致性要求：所有上报至省平台的数据，包括资产信息、漏洞数据、告警事件等，严格遵循省平台规定的数据格式标准。 19.满足数据准确性要求：上报的资产信息与单位实际资产情况完全一致，准确率达到 99%以上。事件数据完整记录事件的发生时间、来源、影响范围、处理状态等关键信息，确保数据的真实性和完整性。 20.满足数据及时性要求：资产信息发生变更后，在 8 小时内完成数据更新并上报至省平台。告警事件发生后，在 30 分钟内完成事件信息的上报，并在事件处理过程中实时更新处理进度信息。 21.满足数据传输稳定性要求：建立可靠的数据传输机制，确保在网络波动或异常情况下，数据传输的完整性和可靠性。数据传输成功率达到 99.9%以上，若出现数据传输失败的情况，具备自动重传功能。 22.满足数据传输安全协议要求：在与省平台进行数据传输时，采用 SSL/TLS 等加密协议，确保数据在传输过程中的安全性。		

		23.满足国密加密硬件通信保障：在与省厅数据对接的网络边界处，部署符合国家相关标准的综合安全防护网关设备。采用支持国密算法（如 SM2、SM3、SM4 等）的专用密码硬件，对与省厅平台之间传输的数据进行设备身份认证和通信加解密处理，确保数据在传输过程中的保密性、完整性和真实性。 24.满足访问控制：能够基于 IP 地址、端口、协议、用户身份等多维度设置访问控制策略，严格限制非授权访问，确保只有经过授权的设备和用户能够与省厅平台进行数据交互。		