合同编号：(豫财招标采购-2025-811)

郑州大学政府采购货物合同

甲方（全称）：郑州大学

乙方（全称）：河南尔享科技有限公司

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 10月 10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 10月 17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：**壹佰肆拾捌万玖仟陆佰元整（小写：¥1489600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 21 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）：河南省郑州市高新技术产业开发区银屏路 15 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：河南尔享科技有限公司

地址：河南省郑州市高新技术产业开发区银屏路15号

签字代表：

电话：0371-63288507

开户银行：中国建设银行郑州文博支行

账号：4105 0167 2835 0000 0130

合同签署日期：2025 年 9 月 30 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	网站内容监测系统	奇安信网神网站监测系统 V5.0 (QAXWS-ESM-ESOP-MONITOR-CSL)	奇安信网神信息技术（北京）股份有限公司	中国	1	套	281800	281800	免税
2	网络流量采集探针	奇安信网神威胁监测与分析系统 V4.0 (TY-TSS10000-S89-PA)	奇安信网神信息技术（北京）股份有限公司	中国	1	套	302600	302600	免税
3	网络流量分析系统	奇安信网神威胁监测与分析系统 V4.0 (TY-TSS10000-S80V)	奇安信网神信息技术（北京）股份有限公司	中国	1	套	292400	292400	免税
4	安全能力中心综合运营系统	奇安信网神安全分析与管理系统 V4.0 (S-NGSOC-BD-AQZX)	奇安信网神信息技术（北京）股份有限公司	中国	1	套	329300	329300	免税
5	安全能力中心综合运营系统支撑平台	奇安信网神安全分析与管理系统 V4.0 (S-NGSOC-PT-01)	奇安信网神信息技术（北京）股份有限公司	中国	3	台	59860	179580	免税
6	堡垒机	奇安信网神运维安全管理系统 V6.0	奇安信网神信息技术（北京）	中国	1	台	63700	63700	免税

		(C6100-BH-TF8P)	股份有限公司						
7	终端安全管理系统	奇安信天擎终端安全管理系统 V10.0 (ESM-FL)	奇安信网神信息技术（北京）股份有限公司	中国	1	套	11200	11200	免税
8	数据在线迁移保护系统	英方系统迁移软件 V8.1	上海英方软件股份有限公司	中国	1	套	19100	19100	免税
9	半自动化工具	DAS-TBT-S300	杭州安恒信息技术股份有限公司	中国	1	套	9920	9920	免税
合计：小写：￥1489600 元　　大写：人民币壹佰肆拾捌万玖仟陆佰元整									

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	网站内容监测系统	1.基于云架构方式部署，无需本地部署任何软硬件，通过账号可以直接进行管理，提供 100 个域名授权。 2.支持对录入资产进行 IPv4/IPv6 检测，并根据检测结果对资产进行可用性监测。 3.支持发现网站存在的 SQL 注入、XSS 跨站脚本、目录遍历、文件包含、备份文件、敏感文件等漏洞，检测内容覆盖 WASC 分类的多种 Web 应用漏洞和 OWASP TOP10 网站漏洞；支持定期跟踪漏洞的修复情况从而使网站的漏洞得以快速修复，降低网站被入侵的风险。 4.支持针对常见漏洞进行程序自动化验证，并可将自动验证漏洞生成安全告警。 5.支持按资产维度查看漏洞扫描任务的时间、进度、状态等；漏洞扫描结果可以同步至安全能力中心综合运营系统，实现资产漏洞自动关联分析。 6.支持针对行业漏洞情报进行同步预警，展示最新漏洞情报关联的资产信息。 7.支持发现网站黑链，支持图片暗链的检测，支持全站对于潜藏在页面深处的第三方黄赌毒广告类链接进行监测并告警，可定位源代码黑链的位置和内容，支持配置监测频率，支持任务并发量配置，支持用户自定义黑词。 8.支持结合海量词库及人工识别，通过机器学习手段，提供敏感词发现的技术手段，支持全站监测，可定位敏感词位置和内容。涉及敏感词样本 7000+，支持配置监测频率，支持任务并发量配置，支持用户自定义敏感词，支持网页附件内容检测 9.支持对网页敏感数据进行监测及告警，包括身份证、手机号码、邮箱、ip 地址等信息 10.支持对指定页面进行内容变更监测，当页面发生变更即产生告警，变更类型包括外链、黑词、body 标签为空、HTML 之外内容、其他。 11.支持采用特征分析技术对网站进行木马检测分析，实现快速、准确的发现和定位网页木马，支持对木马威胁进行报警、通知、处置管理，确保用户在第一时间发现感染的木马并及时消除。 12.支持针对黑链、违规内容、漏洞、内容变更告警内容一键生成报告。 13.支持日报、周报、月报、季报的生成；支持自定义周期性报告内容，包括自定义报告覆盖的资产、告警类型等。 14.支持自动添加网站责任人信息、自定义通知转发对象功能。	套	1

		15.支持短信、邮件将通知发给网站负责人；快捷生成短 URL 分享链接，供用户随时随地登陆通知进行处理；支持勿扰配置，可以按需设置接受通知的时间。 16.支持 URL 登陆查看通知，并支持快速转发通知，可跟踪告警处理进度、发表告警处理意见和与监管方互通信息。 17.提供云端 7x24 小时告警人工运营服务，并提供问题处置建议和咨询；具有重大活动运营支撑服务。		
2	网络流量采集探针	1.采用软件方式部署，能提供 20GGbps 吞吐网络流量的采集能力，支持 IPv4 和 IPv6 网络环境下的部署，可同时对 IPv4 和 IPv6 网络流量分析检测。 2.支持通过 ip、ip 段、端口、协议、VLAN 等进行流量过滤，过滤条件支持 and、or、not 等逻辑运算创建的 BPF 过滤语法过滤数据。 3.支持手动和 FTP 方式批量导入 PCAP 包对离线流量采集，文件大小不低于 1 个 G；并记录 PCAP 包导入记录及检测状态。 4.支持多层 VLAN、VXLAN、MPLS、GRE 等网络流量的解析检测。云场景下，支持 GENEVE 协议双层隧道封装流量的解析检测。 5.支持常见协议识别并还原网络流量，用于取证分析、威胁发现，支持：tcp、udp、icmp、http、dns、dhcp、smtp、pop3、imap、webmail、db2、oracle、mysql、mssql-db、PostgreSQL、sctp、sybase、smb、sip、ftp、snmp、telnet、nfs、ssl、ssh、ldap、radius、kerberos、netbios、ntp、vnc、ipv6 等。 6.支持外发的网络日志的类型包括：TCP 流量、UDP 流量、异常流量、SSL 加密协商、登录行为、域名解析、文件传输、FTP 控制通道、LDAP 行为、web 访问、邮件行为、数据库操作、telnet 命令、旁路阻断、MQ 流量、Radius 行为、Kerberos 行为、ICMP 流量、syn 流量等 19 种网络日志。每种网络日志，都支持自定义配置外发的字段。 7.支持常见攻击行为检测，支持 HTTP 双向流量动态检测，检出类型包括：SQL 注入，命令执行，代码执行，跨站脚本攻击，权限绕过，暴力破解，扫描工具，数据库攻击，敏感信息泄露，挖矿检测，蠕虫传播，目录遍历，文件包含等。 8.支持基于工具特征的 WebShell 检测，检出类型包括但不限于：中国菜刀、蚁剑、冰蝎、哥斯拉、小马生成器等 webshell 上传攻击检测，HTTP 代理程序等； 9.支持网络攻击检测，检出类型包括：各种协议的帐号暴力破解，Mysql UDF 提权攻击、Microsoft Windows NetLogon 权限提升漏洞攻击，向日葵、TeamViewer，psexec 远程执行、smbexec 在目标上远程执行命令，DCSync_DCShadow 疑似攻击、域用户口令爆破行为、域内密码喷洒攻击，njRat 后门程序变种通信行为、Cobaltstrike HTTPS beacon 通信等； 10.支持的远程工具检测，工具类型包括：向日葵、ToDesk、Sorillus、Stowaway、CcRemote、DWservice 等； 11.支持灵活开启机器学习模型，增强检测精度，模型包括：ICMP 隧道检测、DNSTunnel 检测、HTTP 隧道检测、CS 流量检	套	1

		测、MSF 检测、挖矿流量检测、代理流量检测、暗网流量检测、弱口令检测、SSH 爆破登录成功检测；支持与学校现有探针集群部署，实现流量负载分担； 12.支持门罗币、莱特币、以太坊、比特币、斯特币等币种的检测。 13.支持根据正则/机器学习来判断告警详情是否包含身份证号、用户名、密码等敏感信息，敏感信息加密展示。		
3	网络流量分析系统	1.2U 机箱，吞吐量 40Gbps，配置 4 个千兆光口，8 个万兆口，3 个扩展槽，内存 256G；硬盘 960G SSD+8TB SATA 硬盘，冗余电源。 2.支持 IPv4 和 IPv6 网络环境下的部署，支持对 IPv4 路由监控和对 IPv6 路由监控，可同时对 IPv4 和 IPv6 网络流量分析检测。 3.支持记录 TCP，UDP，HTTP 等协议流量日志中的负载信息：TCP,UDP 的上下行负载支持可配，不低于 10KB。HTTP 协议的请求头，请求体，响应头，响应体支持长度可配，不低于 8KB。 4.支持常见协议识别并还原网络流量，用于取证分析、威胁发现，支持：tcp、udp、icmp、http、dns、dhcp、smtp、pop3、imap、webmail、db2、oracle、mysql、mssql-db、PostgreSQL、sctp、sybase、smb、sip、ftp、snmp、telnet、nfs、ssl、ssh、ldap、radius、kerberos、netbios、ntp、vnc、ipv6 等。 5.支持对 HTTP、FTP_DATA、SMB、SMTP、POP3、WEBMAIL、IMAP、TFTP、NFS 等类型协议流量中出现文件传输行为进行发现和还原，并记录文件 MD5 发送至分析设备。 6.新增规则产生的告警进行单独展示和标注。 7.支持检测模式的标准模式、精简模式、自定义模式的切换；支持手动配置各类检测引擎、机器学习模型的开关。 8.支持常见攻击行为检测，支持 HTTP 双向流量动态检测，检出类型包括：SQL 注入，命令执行，代码执行，跨站脚本攻击，权限绕过，暴力破解，扫描工具，数据库攻击，敏感信息泄露，挖矿检测，蠕虫传播，目录遍历，文件包含等。 9.支持基于工具特征的 WebShell 检测，检出类型包括：中国菜刀、蚁剑、冰蝎、哥斯拉、小马生成器等 webshell 上传攻击检测，HTTP 代理程序等； 10.支持网络攻击检测，检出类型包括：各种协议的帐号暴力破解，Mysql UDF 提权攻击、Microsoft Windows NetLogon 权限提升漏洞攻击，向日葵、TeamViewer，psexec 远程执行、smbexec 在目标上远程执行命令，DCSync_DCShadow 疑似攻击、域用户口令爆破行为、域内密码喷洒攻击，njRat 后门程序变种通信行为、Cobaltstrike HTTPS beacon 通信等； 11.支持隐秘信道检测。检测类型包括：ICMP、DNS 协议等隐蔽隧道攻击检测，恶意软件加密通信的检测，加密 web 应用的流量检测，非法应用加密通信的检测，SSL 加密协议相关的漏洞与攻击的检测，加密通道攻击行为检测，支持 JA3 指纹检测； 12.支持基于自定义正则表达式以及自定义弱口令字典的弱口令登录行为检测， 同时要支持不同协议弱口令分析。自定义弱	套	1

		口令正则表达式方式支持自定义弱口令强度、复杂度规则。支持配置多条弱口令检测的正则表达式。 13.支持自定义威胁情报，支持根据威胁类型、威胁名称、威胁级别、置信度、情报类型、IP、域名等自定义添加威胁情报，支持 STIX、OPENIOC、JSON、XLSX 等格式的批量导入。 14.支持门罗币、莱特币、以太坊、比特币、斯特币等币种的检测。 15.支持对使用 base64、unicode、url 编码等混淆手段攻击检测。 16.支持攻击特征高亮展示，方便分析人员事件分析。		
4	安全能力中心综合运营系统	1.支持接入学校现有的网络安全态势感知平台，支持下发同步关联分析规则，支持设置数据订阅策略获取平台数据，数据订阅策略类型包括告警订阅、弱口令订阅、配置核查订阅、漏洞订阅和资产订阅。告警订阅策略包括首次告警时间、危害等级、攻击结果、置信度。弱口令订阅、配置核查订阅、漏洞订阅策略包括最近发现时间和危害等级。 2.可实现与学校现有的资产管理平台无缝对接，所产生的开发费用由服务方自行承担。 3.大数据架构要求：系统基于大数据底层架构开发，包含 kafka、yarn、hive、es 等大数据组件。 4.支持对网络设备、安全设备、主机系统的日志、网络流量等多种数据源的采集；支持接入并解析的数据源数量 50 个，支持按需扩容数据源数量。 5.支持接入并管理日志采集器、流量采集器，可支持第三方采集器的数据接入。 6.支持资产风险态势展示功能，能够展示“全局风险态势”、“全局风险趋势”、“资产组风险排行”、“资产组树状展示”信息，具备外部威胁态势展示功能，能够展示“威胁总数”、“受攻击资产总数”、“受攻击 ip 总数”、“受攻击资产 top5”、“外部威胁级别分布”、“攻击地图”、“威胁趋势”、“攻击源 iptop5”、“威胁类型 top5”、“威胁来源国家/地区”、“威胁列表”信息； 7.支持新增日志类型功能，可在线新增字段信息，支持数据存储类型的配置，包括：ES、Hive、Kingbase、mysql，支持存储基础信息的配置：包括数据库名、存储时间、分区方式等基础属性信息，从而达到分类存储日志的目的； 8.支持常见攻击检测功能：具备 SQL 注入、文件上传、目录遍历、文件包含、勒索软件、远控木马、僵尸网络、网络蠕虫、重要资产非法外连行为、非办公时间访问核心资产、未注册 IP 访问核心资产、信息泄露、信息收集、端口扫描、漏洞扫描、APT 等攻击行为的检测能力，已经提供第三方检测机构针对软件功能的检测报告并附与标书中。 9.告警管理功能预置 12 种常见场景的告警快速筛选器，包括今日新增威胁告警、已先陷告警、首次出现告警、IOC 告警、外部攻击告警、横向移动告警、资产外连告警、恶意文件告警、Web 攻击告警、Windows 告警、Linux 告警、自身安全性告警。告警筛选器支持通过安全内容包升级的方式定期自动升级，用户可持续获取到厂家最新的安全经验。 10.具备独立的告警分析管理功能，支持基于多视角进行聚合分析，预置分析视角至少包含告警名称分析、攻击者分析（含	套	1

		外部攻击者、内部攻击者）、失陷情报分析、挖矿木马分析、勒索软件分析、ATT&CK 分析。 11.支持安全运营态势展示功能，能够展示“资产管理情况”、“安全设备部署情况”、“威胁监控”、“安全人员”信息，具备全网漏洞态势展示功能，能够展示“漏洞信息”、“漏洞类型 TOP10”、“影响资产 TOP5”、“安全域”、“漏洞处置分布”、“漏洞平均修复时间”信息。 12.支持业务资产外连态势展示功能，能够展示“资产外连总览”、“资产外连次数 TOP5”、“资产外连趋势”、“被连国家/地区 TOP5”、“被连 IP TOP5”、“资产外连实时监测”信息，具备内网威胁态势展示功能，能够展示“内网威胁概况”、“内网威胁等级”、“威胁类型 TOP5”、“3D 球形图”、“内网威胁趋势图”、“攻击者网段分布”、“跨网段攻击 TOP5”、“攻击者 TOP5”信息。 13.支持通过智能分诊，对告警进行智能化的归类，协助客户快速分析研判，以可视化的方式呈现归类后告警：重点关注告警、低关注告警、不关注告警、未分诊告警，同时提醒告警的智能分诊率。 14.支持关联多个类似告警进行事件创建，事件类型包括：恶意程序事件、网络攻击事件、数据安全事件、信息内容安全事件、设备设施故障事件、违规操作事件、安全隐患事件、不可抗力事件、其他事件 15.支持事件调查管理，支持查看事件详情信息；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、资产及脆弱性信息、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。 16.支持工单管理功能，能够将告警、漏洞通过工单下发给责任人处理，能够查看、结束工单，具备联动功能，能够设置基于内网 IP、外网 IP、域名、URL 的联动处置。 17.工单支持 SLA 配置，按照工单优先级配置 SLA 时限，分为响应时限和处置时限。响应时限：从工单下发到工单状态变成处置中、处置时限：从工单下发到工单状态变成已完成。		
5	安全能力中心综合运营系统支撑平台	1.安全能力中心综合运营系统算力存储支撑平台，提供 3 套算力平台支撑，每算力平台配置要求如下：CPU：2 颗 16 核主频 2.4GHz；内存 256GB；系统硬盘 2 块 960G SSD 固态硬盘；数据硬盘 12*8TB SATA 硬盘，冗余双电源；配置 4 个千兆电口，2 个万兆光口（含两个 SFP+多模光模块）。同时要求实现对现有核心系统平台算力无缝兼容部署，部署不影响安全能力中心平台的正常使用，确保平台各项功能指标不受的影响。 2.支持集群部署，可根据学校需要，水平扩展到多台设备集群。 3.支持数据存储类型的配置，包括：ES、Hive、Kingbase、mysql，支持存储基础信息的配置：包括数据库名、存储时间、分区方式等基础属性信息，从而达到分类存储日志的目的；	台	3

		4.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。 5.支持统计规则建模，在指定的时间范围内，对符合过滤条件的日志中数字类字段进行统计，将其与阈值进行比较以发现异常威胁事件；统计方式包括不限于：计数、求和、平均值、最大值和最小值等计算方式； 6.支持序列规则建模，在指定的时间范围内，通过对 2 个及 2 个以符合过滤条件的日志发生，以发现复杂场景下的威胁事件；序列方式包括不限于：A 事件后发生 B 事件、A 事件发生 M 次后发生 B 事件等。 7.提供独立的安全内容包升级，安全内容部包含关联规则、行为基线模型、分诊规则、日志检索预语句、告警筛选器、视图、仪表板、ATT&CK、报表模板等。 8.支持用户角色管理， 可以为不同角色赋予不同系统功能模块及数据的读写权限. 9.支持通过热数据、冷数据方式对存储时间不同的日志进行分类搜索。 10.支持高级模式、Lucene、QAL 等模式进行搜索； 11.支持 QAL 语法检索，通过管道符方式拼接搜索语句，支持 10 种搜索命令，80 种函数。提供语法帮助功能。支持命令联想、常用搜索、如何搜索等指导。 12.搜索结果支持按照全文或结构化（键/值、JSON 串）展示，可筛选展示字段，隐藏不必要字段，支持调整字段展示顺序。 13.支持对字段内容进行快速过滤、排除、新建搜索、复制、查询资产、查询情报、解码操作。 14.支持对日志内容进行编解码，包含 Unicode、UTF-8、URL、ASCII、Hex、Bse64 等解码方式；支持对日志内容进行进制转换，包含 2 进制、8 进制、10 进制、16 进制间的互相转换。 15.支持用户角色管理，可以为不同角色赋予不同系统功能模块及数据的读写权限。		
6	堡垒机	1.1U 机架式，配置 6 个千兆电口，2 个扩展槽，内置 4TB 硬盘，双电源，支持液晶屏，最大支持 150 路图形会话或 400 路字符会话并发，提供授权 100 个被管资源数（资源数计算方式：IP+端口）； 2.支持使用微信小程序生成动态口令，用于用户双因子认证，实现通过账号密码+动态口令的方式登录堡垒机； 3.支持与 AD、LDAP、RADIUS、OIDC、CAS 等认证系统联动登录堡垒机，支持自动同步 AD/LADAP 用户。 4.支持的运维协议包含 SSH、RDP、VNC、Telnet、FTP、SCP、SFTP、DB2、MySQL、Oracle、SQL Server、Rlogin、DM、Redis、PostgreSQL 等； 5.支持云主机资源批量导入，包括阿里云、百度云、华为云、腾讯云、Ucloud、AWS、Azure 云等平台的资源，支持设置优	台	1

		先导入公网和内网 IP 设置，支持导入同时批量新建标签； 6.针对核心设备可配置双人授权，需要管理员现场审批才能访问资源； 7.支持对主机服务器、网络设备、安全设备等进行管理，可根据用户账号、用户/IP/地址(或用户 MAC 地址)、用户访问时间等条件控制用户访问，可根据用户组、用户、设备等信息进行角色划分，并授予不同的管理权限； 8.支持以部门、资源账户、账户组、时间、改密周期、改密方式生成详细的改密计划，到期自动执行。 9.支持关联 IP 与账户名相同，但是协议不同的资源账户，关联后，任一资源账户密码改变，其余资源账密码均同步改变。 10.不限操作系统类型，无需安装任何客户端插件，使用浏览器通过 H5 方式即可直接运维 SSH、RDP、Telnet、VNC、Rlogin 和 SFTP 资源 11.不限操作系统类型，无需安装任何客户端插件，使用浏览器通过 H5 方式即可直接运维 SSH、RDP、Telnet、VNC 和 SFTP 资源。 12.支持基于用户登录账号、用户登录时间、控制对象账号等制定命令控制策略，并支持单点登录功能。 13.支持运维过程中邀请其他用户参与、协助操作；会话协同过程中，协同者可以申请控制会话，创建者可以强制获取控制权。 14.支持以云盘形式在堡垒机上存储常用文件，实现操作端、堡垒机和目标资源三者之间文件共享，并支持对不同用户配置不同大小的网盘空间，支持多文件和文件夹下载，文件展示最近修改时间和权限。 15.支持通过工单向管理员申请需要访问的资源的权限。 16.支持工单审批时，设置多人审批模式或会签审批模式，支持开启终审节点审批，需要系统管理员做最终审批。 17.支持在线和离线回放运维人员对资源的操作过程，并可以对播放速度进行调整，支持拖动、暂停、停止、跳过空闲、重新播放、切换会话等操作。 18.支持采用 OCR 识别技术，可以识别图形操作中的操作系统文字、应用软件文字、浏览器文字等文本信息，支持设置识别精细度和识别间隔时间，以平衡性能开销和识别精度；		
7	终端安全管理系统	1.支持主流操作系统，中英双语界面。可实现对客户端的集中管理，包括终端统一部署、策略配置、任务分发、集中监控、资产管理、防病毒、终端管控、终端审计、日志报表等终端安全管理功能，提供 100 点终端授权。 2.病毒防护概况：终端基础信息、病毒库版本、发现病毒数、未处理病毒数、最后查杀时间、文件防护状态、引擎使用状态、扩展病毒库版本。 3.支持对主机磁盘、主机内存、主机引导区、移动存储介质等的病毒检测，病毒检测类型包含文件感染型病毒、宏病毒、蠕	套	1

		虫、木马程序、间谍软件、脚本恶意程序、后门程序、僵尸程序、勒索软件、RootKit 恶意程序、BootKit 恶意程序等，病毒处理动作包含阻止、删除、隔离、清除还原等。 4.支持对终端当扫描到感染型病毒、顽固木马时，自动进入深度查模式，可设置禁止终端用户管理路径或文件白名单、禁止终端用户管理扩展名白名单、扫描时不允许终端用户暂停或停止扫描任务。 5.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。 6.支持逃避检测防护，包含压缩文件检测、加壳文件检测、格式混淆检测、捆绑文件检测等防护方式。 7.支持未知病毒检测功能：支持基于静态文件二进制特征、动态行为特征未知病毒检测 8.支持按补丁类型和级别修复，补丁级别需包括：安全更新、重要补丁、功能补丁、可选补丁，支持仅安装指定补丁设置。 9.能够按照补丁分发范围、分发时间、安装情况和终端类型等方式进行补丁分发，支持补丁静默和用户提示安装两种方式，可显示终端已安装和未安装补丁信息。 10.支持外设库管理，可统计终端外接的各种设备，包括制造商和设备类型、产品、数量、PID、VID 和设备来源等。 11.支持对网卡进行防护，支持阻止终端修改 IP 地址、使用动态 IP 地址、热点创建和 IPV6 地址使用等，可自定义提示内容和生效时间。 12.支持实时监测终端通过多网卡、无线、代理和拨号等外联行为，并可进行实时阻断。 13.支持主机防火墙功能，通过添加 IP、域名规则、支持允许/拒绝规则、支持任意流向拦截和允许，支持 TCP、UDP、TCP+UDP、ICMP、多播和组播，支持自定义端口范围、支持自定义目标 IP，支持输入 IP 范围，支持对设定进程名称、进程路径，支持模糊规则。 14.支持展示防火墙上报日志，展示终端基础信息、拦截规则名称、拦截时间、操作、协议、源地址，目的 IP/域名、源端口、目的端口。 15.支持根据地址、协议、域名和关键字等监测并记录终端上网行为，能够有效阻断终端违反安全策略行为。 16.支持不依赖日志，还原文档中的电子水印信息，通过审计日志，通过文件唯一 ID 还原文件内部流转轨迹。		
8	数据在线迁移保护系统	1.支持在线迁移，即迁移过程中源端服务器应用无需停止，支持差异数据同步，即在首次完整数据镜像后、整机切换前源端所产生的新数据的同步，支持迁移前检查主机系统、磁盘等信息；支持 MBR、GPT 格式的系统迁移，自动匹配对应格式，支持 BIOS 和 UEFI 引导模式的整机迁移； 2.支持数据传输压缩，提供多个压缩等级，节省带宽消耗；支持 IPv4 和 IPv6 网络环境的部署和运行，支持断点续传，即迁移过程中碰到网络中断或备端不可达等异常情况，环境恢复后续传。	套	1

		3.支持提供带宽控制功能，可灵活根据时间段调整带宽，可降低对生产业务网络的影响；完成数据和系统同步后，支持手工切换到灾备机；支持同时执行多个整机迁移操作、互相独立、可单独开启和停止。 4.支持 NodeProxy 代理实现跨网络数据传输，支持跨网络迁移场景；支持批量创建迁移任务和批量进行迁移操作；迁移任务支持从模板创建；支持统一的灾备管理能力和扩展性，必须具备扩展支持其他灾备能力，避免重复建设。 5.目标主机需要提前部署和源端相同版本的操作系统，支持排除指定文件或目录，避免无效数据占用带宽资源，无需处理引导模式不同、驱动兼容性带来的问题，支持迁移目标主机保留原来的网络配置，支持主流操作系统跨小版本的迁移，跨小版本指标准版、企业版、数据中心版。 6.支持备份数据校验，可配置严格校验和时间校验，支持备份数据以 MFT 或普通文件方式打开，支持数据传输加密，支持 AES 和 SM4 国密算法，支持迁移规则可设定立即启动或定时启动。 7.支持在线迁移，即迁移过程中源端服务器应用无需停止。支持手工切换到灾备主机进行接管，支持同时执行多个整机迁移操作、互相独立、可单独开启和停止，支持基于中转代理程序实现跨网络数据传输。 8.支持业务主机和管理主机所在网络隔离的场景，支持批量创建迁移任务和批量进行迁移操作，支持统一的灾备管理能力和扩展性，必须具备扩展支持其他灾备能力，避免重复建设，支持数据传输加密，支持 AES 和 SM4 国密算法，支持迁移规则从模板创建 9.管理人员对帐号的增删改操作均有记录；用户登录系统、注销登录日志均有记录；事件、操作日志和调试日志完整可用于审计。 10.默认开启防暴力破解机制，可配置 允许尝试登录次数和失败锁定时间。 11.支持强口令方案，对密码长度、密码复杂度、密码有效期组合要求。 12.支持任务的实时监控功能，包括但不限于当前备份规则状态、速率、数据复制进度，提供监控报警功能，如任务异常，生产机或目标环境发生改变等影响数据复制成功的警告，支持通过电子邮件、短信、站内消息等方式的日志告警，客户端兼容 x86、ARM 架构服务器，客户端兼容 SUSE Linux 、Redhat、CentOS、Ubuntu、Debian 和 Windows 等主流操作系统，客户端兼容统信、中标麒麟、银河麒麟、红旗和华为欧拉等国产操作系统。 13.支持常见应用系统，包含 Oracle、DB2、MySQL、人大金仓、达梦、GaussDB、Informix、SQL_Server、Exchange、Lotus Notes、Sybase ASE 等应用程序和数据库的整机迁移。 14.支持常见应用系统，包含 Oracle、DB2、MySQL、人大金仓、达梦、GaussDB、Informix、SQL_Server、Exchange、Lotus Notes、Sybase ASE 等应用程序和数据库的整机迁移。		

9	半自动化工具	1.产品要求界面友好，并有详尽的技术支持文档，所有图形界面要求中文。系统为 B/S 架构，并采用 SSL 加密通信方式，用户可以通过浏览器远程方便对产品访问操作，支持多用户同时登陆操作。 2.支持各类 WEB 编程语言的应用的深度网页后门检测；支持常见的 asp、php、jsp、aspx 等多种 WebShell 的有效扫描；支持实时结果的展现；支持生成统计报表；支持 IIS、Websphere、Weblogic、Apache 等所有的应用服务器；支持 Asp、Jsp、.Net、J2EE、Php、Perl 等所有的 WEB 应用编程语言。 3.支持实时结果的展现，展现内容应至少包含扫描对象、类型、描述、特征、危险等级和修改时间；支持一键导出单个或所有恶意代码，并以相应的形式进行展示；支持从界面直接打开文件所在目录；引擎应支持黑白名单编辑功能，可添加相应的黑名单和白名单；引擎应支持 win2003/win2008/win2012/win2016win7/win8/win10 等类型的 win 操作系统；引擎应支持 Redhat/CentOS/suse/ubuntu 等 unix 操作系统； 4.支持快速扫描功能：支持根据文件类型自动选择内置扫描策略进行扫描，例如当进行扫描 index.ASP 文件时程序会自动选择 ASP 对应的策略进行扫描而 忽略其他的扫描策略； 5.支持全盘扫描功能，支持扫描所有内置的策略以 及用户自定义策略；支持自定义扫描功能，支持文 件类型、优先级、扫描策略等用户自定义。 6.硬件支撑要求：采用安全的操作系统，双核或双核以上 CPU，8G 以上内存，1T 硬盘空间； 提供用户概述功能，详细展示客户端使用登录、使用情况，上传的文件样本数及人工审核确认数； 7.支持对系统参数进行配置，包括网络配置及系统安全参数的配置，如登录失败处理功能、最大并发、用户登录超时时间等；提供接口管理功能，能与其他系统进行对接；提供引擎管理功能，能对引擎进行配置改造；支持对引擎的检测记录进行展示功能；支持对单条检测记录的展示，展示的内容至少包含扫描文件数、威胁数量、扫描 IP、客户端版本号、扫描时间、扫描用时； 8.支持提供离线检测工具； 离线检测工具应包含 windows 和 linux 版本；离线检测工具应支持实时生成检测报告；平台可以对恶意代码的特征进行分析和展示。提供多权分立的账户体系，用户能根据其地域对下属单位进行管理；	套	1

附件 3：

售后服务计划及保障措施

我公司就项目名称：郑州大学网络空间安全学院、中原网络安全研究院安全能力建设采购项目；采购招标编号：豫财招标采购-2025-811 招标活动并投标，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，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。**我公司提供的服务是 7×24 小时响应服务，对于故障要求 1 分钟响应，3 小时内赶到现场并处理，如不能及时修复、24 小时内免费提供备用机满足教学正常需要。**我公司有一整套完备的售后服务体系，包括严密的组织体系、高素质的人才队伍、完整严谨的服务流程等。依靠这套售后服务体系，我公司完成了众多大型项目的策划、组织、实施、维护和服务。

售后服务机构信息：维修单位名称：河南尔享科技有限公司，总部设立在郑州市，并且配备有专业售后服务技术人员。维修单位地址：河南省郑州市高新技术产业开发区银屏路 15 号

售后负责人：程宇锋

联系电话：0371-63288507

我们完全响应贵方的要求，一贯坚持为用户提供高质量、完善的技术支持服务，遵循“全程全面全天候专业化服务”的服务宗旨，秉承长期为广大用户提供优质服务积累的经验，致力于为用户提供精湛的技术和全面周到的服务。

公司名称：河南尔享科技有限公司

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></td><td>使用人</td><td></td><td>合同编号</td><td></td></tr>
<tr><td>供货商</td><td colspan="3"></td><td>合同总金额</td><td></td></tr>
<tr><td colspan="6">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>品名</td><td>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></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td rowspan="3">实物验收情况</td><td colspan="6">外观质量（有无残损，程度如何）。</td></tr>
<tr><td colspan="6">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="6">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="6">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="6">□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>验收小组成员签字</td><td colspan="2"></td><td>供货商
授权代表签字</td><td colspan="2"></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)20250179-1）

河南尔享科技有限公司：

贵单位于2025年8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安全能力建设采购项目的投标（采购编号：豫财招标采购-2025-811），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1489600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9月3日