合同编号(校内)：HW337230203

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一期采购项目

甲　　方：郑州大学

乙　　方：河南尔享科技有限公司

生效日期：2023.11.14

合同编号：（豫财磋商采购-2023-946）

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 11 月 15 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：

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 2023 年 12 月 15 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，而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：**壹佰柒拾捌万玖仟陆佰圆整（小写：¥1789600 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__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 34 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：41050167283500000130

合同签署日期：2023年11月14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	漏洞挖掘分析系统运行基础平台	绿盟远程安全评估系统 V6.0 TVMNX1-SNG	北京神州绿盟科技有限公司	中国	1	套	497800	497800	免税
2	基础挖掘子系统	绿盟远程安全评估系统 V6.0 TVMNX1	北京神州绿盟科技有限公司	中国	1	套	338000	338000	免税
3	固件逆向分析子系统	绿盟工业网络安全合规评估工具系统 V1.0 ISCAT	北京神州绿盟科技有限公司	中国	1	套	458100	458100	免税
4	终端安全管理平台	绿盟终端安全系统 V9.0 ESSNX1-SN	北京神州绿盟科技有限公司	中国	1	套	31650	31650	免税
5	漏洞挖掘算力调度云平台	思腾合力 SCM 人工智能云平台 V6.0	思腾合力（天津）科技有限公司	中国	1	套	25200	25200	免税
6	漏洞挖掘检测工具平台	安恒 DAS-TBTOOL-WSSCAN	杭州安恒信息技术股份有限公司	中国	1	套	28800	28800	免税

7	工业互联网靶标一	和利时 LK220	北京和利时系统工程有限公司	中国	1	台	35700	35700	免税
8	工业互联网靶标二	施耐德 TM262L10MESE8T	施耐德电气（中国）有限公司	中国	1	台	32200	32200	免税
9	工业互联网靶标三	西门子 6ES7 288-1ST20-0AA0	西门子（中国）有限公司	中国	1	台	37100	37100	免税
10	智能终端靶标一	科瑞康 PC-66B	深圳市科瑞康实业有限公司	中国	1	台	12830	12830	免税
11	智能终端靶标二	爱奥乐 G-427B	爱奥乐医疗器械(深圳)有限公司	中国	1	台	6890	6890	免税
12	智能终端靶标三	上禾 SH-X60	郑州上禾电子科技有限公司	中国	1	台	16830	16830	免税
13	云服务器	浪潮 NF5280M5	浪潮电子信息产业股份有限公司	中国	1	台	78280	78280	免税
14	科研训练授权云终端	锐捷 RG-CDC-TCI-Lic-EDU	北京星网锐捷网络技术有限公司	中国	55	套	1130	62150	免税
15	科研训练教学管	噢易计算机实验室智慧服务	武汉噢易云计算股	中国	1	套	25860	25860	免税

	理软件	系统 V5	份有限公司						
16	实验室配套桌椅	阿美家具定制	河南阿美家具有限公司	中国	30	套	1260	37800	免税
17	实验室配套环境建设	尔享定制	河南尔享科技有限公司	中国	1	项	64410	64410	免税
合计： 小写：￥1789600 元 大写：人民币壹佰柒拾捌万玖仟陆佰元整									

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	漏洞挖掘分析系统运行基础平台	**1、总体要求：** 基于对研究人员可见的业务功能点，可以提供人机交互访问能力（HMI），可实施各系统的控制指令下发、进度指示、结果查询查看以及在线的图形化数据分析和离线文件报告导出的服务。通过数据面、控制面和管理面的协同组织，能够用于配置、模板管理、角色管理、权限管理、知识库、综合展示、运行资源配置等方面。 **2、满足运行环境：** 软硬一体式设备，其中系统节点支持扩展部署在独立的服务器和云环境； CPU：逻辑核，60 核及以上； 内存：256GB ECC DDR 及以上；硬盘：2*500GB SSD，10*4TB 机械硬盘； 网卡：2 张千兆 4 端口网卡；Raid 卡：带有读写缓存的 Raid 卡；光驱：内置光驱； 电源：热插拔冗余电源（1+1）1100 瓦。 **3、漏洞挖掘过程可视化：** 支持靶标资产的系统漏洞、网站安全漏洞整体态势的图表统计大屏展示模式。支持仪表盘展示，仪表盘包括靶标资产仪表盘、系统漏洞风险仪表盘、web 漏洞风险仪表盘、情报预警仪表盘以及系统运行资源仪表盘。支持挖掘任务进度仪表盘，展示漏洞挖掘任务的总数、进度、负责人等信息。支持总体靶标漏洞分布态势大屏模式展示，支持风险等级、风险评分、发现漏洞数量最多的系统和应用类型 TOP5、漏洞数量趋势情况统计等。 **4、靶标管控：** 支持通过 DAST 子系统、IAST 交互式检测子系统作为探针的方式，由平台创建漏洞挖掘任务，发现潜在漏洞和收集靶标信息。支持通过文件导入或手工录入的方式，录入靶标研究对象信息。支持创建靶标研究对象	套	1

		发现任务，单次任务、周期任务、定时任务。靶标研究对象信息包括操作系统类型、版本、设备类型、厂商及型号，开放的端口、服务、协议及版本信息；Web 站点的关联域名信息、ICP 备案信息、地理位置信息、Web 站点使用的组件信息。 5、支持在挖掘任务中主动进行存活网站探测，可进行开关启停，开启后对于存在 web 服务的靶标也会同步进行网站探测扫描；支持添加靶标自定义属性，支持多级属性，可设置属性名称和属性类型（文本、树）。支持靶标发现结果自动入库，可配置自动入库策略，支持不同状态的靶标，按照类型自动入库操作；可配置优先入库策略；仪表盘自定义：可自定义显示图标项，可手动拖拽展示顺序； 6、支持时间维度对比：可选择不同靶标对象，基于不同日期的风险结果比对，可展示风险值变化、风险等级变化，支持漏洞环比修复率、漏洞总数、未处置漏洞数、已处置漏洞数的变化；支持新增靶标、减少靶标、不变靶标数统计分析； **7、科研任务管理** 支持手动添加新的漏洞处置单，可录入漏洞类型、描述、影响资产、端口、协议、服务等各类信息。支持从文件导入漏洞处置单，可以批量录入多个漏洞处置单信息进入系统进行闭环处置。支持以漏洞视角、资产分类视图、端口视角、服务视角查看漏洞处置单，视图中提供端口漏洞列表、服务漏洞列表、资产维度的漏洞风险、漏洞维度风险、以及漏洞处置维度的漏洞风险管理能力。 支持靶标的定期梳理和持续监控，扩展了靶标漏洞情报匹配预警、快速漏洞分析环节的靶标漏洞演示场景建立过程。靶标管理支持多用户、角色权限控制，支持研究人员挖掘靶标协同。支持挖掘任务创建，支持挖掘任务基本信息录入和挖掘进度数据录入。支持挖掘引擎实例管理，可新建挖掘引擎并进行注册，包含引擎实例 ID、引擎实例名称、实例名称、实例地址、实例状态、引擎类型、引擎版本、插件数量、实例描述、引擎名称。支持新建 POC 挖掘任务，选择引擎后，查看其插件能力，并指定插件进行挖掘，并获取任务进度和挖掘结果。支持利用靶标数据指纹信息，结合权威漏洞库，自动判断和筛选出该漏洞可能影响的靶标列表，可自动或者人工选择进行预警。 支持异常靶标规则配置，可配置规则名称、对象范围、异常条件规则（包括端口、服务、应用、操作系统等），支持多条件组合规则；对于靶标库中的靶标进行异常标签标记。支持异常靶标白名单配置，对于白名单中的靶标不进行异常分析。支持按属性和标签查询靶标，支持在全部靶标或用户靶标集合中查询，查询条件包括：IP 地址/URL、靶标名称、标签、联系人、靶标类型、操作系统类型、版本、应用版本、厂商、		

		服务端口、服务名称、协议、设备类型、厂商、型号、开发语言、版本、组件名称、版本。支持按靶标安全视角对靶标进行分类展示。 8、支持自定义展示靶标列表表头，提供基本字段展示，可选择需要列表展示项，展示内容包括不限于：靶标风险值、IP、靶标组、重要性、标签、操作系统、端口、服务、联系人、设备类型、自定义属性等；兼容现有挖掘设备、调度设备任务的执行，包括给设备下发挖掘任务，获取任务执行状态，收集挖掘结果，设置设备可挖掘范围、DNS、执行并发数等； **漏洞应急响应** 9、厂商具备漏洞挖掘情报库及威胁情报分析云平台，能够通过收集、交换、购买获得最新的漏洞挖掘情报信息；支持手工录入、批量导入、情报系统自动获取新披露的漏洞挖掘情报信息；支持预警结果标记是否支持漏洞挖掘设备直接进行验证，对于支持验证的可直接对挖掘设备下发验证任务；支持手动发布预警，支持预警设置通知方式、通知范围、预警等级、可能后果及解决方案； 10、平台支持基于资产库的漏洞智能分析，支持功能启停操作，同时可配置开启智能分析的资产范围，支持资产组视角的快速配置，支持多资产组/全部资产组选择；支持基于白名单的漏洞智能分析，可配置协议、软件、及软件版本白名单；支持单个/批量白名单添加、删除操作；平台会在漏洞扫描原始结果基础上针对用户已配置的智能分析规则进一步修正最终漏洞结果信息，可在原始任务结果中查看修正明细，包括修正资产数、漏洞数、详细资产漏洞列表等信息； **11、科研规划管理** 支持科研流程自动化：平台支持按科研流程类型和需求，针对用户输入的参数，自动划分创建科研流程，跟踪科研流程中的各类任务执行，在完成后实施任务结果的自动科研流程回填。 支持代办科研流程、已办科研流程、已完结科研流程、我的申请、草稿箱等科研流程分类管理； 支持查看科研流程详情，包括列表字段取值，环节数据详情、以及科研流程流程图（高亮当前环节），以及支持增、删、改、查科研流程等操作。 支持流程管理，内置产品漏洞验证、产品漏洞核验、漏洞专项排查、漏洞排查验证、漏洞处置修复、漏洞修复核验、漏洞排查闭环、漏洞跟踪闭环等流程；支持流程操作包括启用、禁用、复制、查看详情、导出等操作；支持流程自定义：以图表方式支持创建流程开始、结束、流程分支、操作、审核、同意、驳回等操作；支持按照自定义流程创建对应科研流程。		

		12、支持优先级依据设置：按照资产因子、脆弱性因子、威胁因子、运维因子等不同维度，设置优先级分析维度，可分别设置各维度的因子启停、及相关权重、可为具体因子设置启停和不同级别设置，包括：资产重要性、资产位置、资产防护情况、漏洞分值、热度、交叉验证、漏洞 poc、利用方式、攻击成本、忽略比、修复难易程度等，重新设置依据后自动重算优先级； **13、风险信息管理** 支持新建、管理挖掘设备的非授权登录、授权登录的系统漏洞挖掘、Web 网站漏洞挖掘、弱口令挖掘、配置核查、靶标发现、渗透测试、产品漏洞预警、漏洞验证、POC 挖掘、靶标探测等各类型任务。 支持批量任务策略定义，支持从文件导入批量任务策略，可按照任务配置完成批量任务下发。 支持挖掘策略配置，支持挖掘任务的手动、自动下发给挖掘、监测设备，挖掘任务下发支持选择靶标视图的节点，进行数据筛选。支持产品漏洞预警任务管理，（1）支持新建预警（关联分析）任务，填写任务名称、任务来源、查询选择产品漏洞（展示列表）、查询选择或输入靶标范围（展示列表）（2）支持提供系统中的预警任务列表，包括任务 ID、任务名称、任务类型（产品漏洞预警）、任务来源（本地、跨级）、任务状态（初始化、分析中、已完成、异常终止）、产品漏洞列表、靶标列表、任务报表；支持各类任务操作，包括删除、查看/导出报表、启动、停止。（3）支持漏洞预警结果详情展示及漏洞标记是否支持漏洞扫描设备直接挖掘验证，对于支持挖掘验证的可直接对扫描下发挖掘验证任务。 14、支持渗透测试结果数据的录入，包括渗透测试任务信息、漏洞信息、附件信息的录入，录入后的风险信息能够融入系统其它风险数据统一评估展示； 支持 POC 挖掘管理：提供连接到平台的 POC 引擎节点信息，如 POC 引擎名称、POC 引擎类型（原理挖掘、登录挖掘、版本检测、靶标识别、服务识别）、IP 地址、插件数量、运作状态（离线、在线）。支持新建 POC 挖掘任务，选择引擎后，查看其插件能力，并指定插件进行挖掘，并获取任务进度和挖掘结果； 15、支持选择不同靶标分组进行统计分析，统计概览列表展示主机网站靶标统计、漏洞高中低统计、弱口令统计、不合规检查项统计、已修复、已忽略统计； 16、平台支持输出靶标风险报告、主机挖掘综合报表、网站挖掘报表、配置核查报表、口令猜测报表、网站挖掘报表、靶标发现、预警任务、POC 挖掘、漏洞验证、主机靶标探测、网站靶标探测等各类型报表，支持选择靶标范围、任务范围、时间范围、漏洞状态等输出报表； 17、支持对各类离线挖掘结果数据导入，导入后的风险信息能融入融入系统其它风险数据统一评估展示。		

		支持选择两个或多个任务进行对比分析，支持对任务结果中任务基本配置、目标、端口漏洞、弱口令等信息的对比；保证对比新增、减少、变化等情况； **18、科研知识库** 支持知识库数据各维度统计分析，可统计漏洞（主机、WEB），口令字典、插件（POC、指纹插件），资产标记，情报等各个知识数据量；支持产品漏洞近期新增趋势、产品漏洞数近期来源、配置模板数量趋势、口令字典近期新增来源分布、资产标记数量趋势、插件近期新增来源分布等维度统计分析及可视化展示。支持科研漏洞知识库管理；支持手动添加、导入科研漏洞，可设置各个字段值信息，并支持对已有漏洞库数据的修改及修复建议添加。 支持列表展示：漏洞标识 ID、本地 ID、漏洞名称、脆弱性值、发布时间、发布 ID、发布组织、来源厂商，来源方式(录入、同步、报告提取、情报提取、挖掘)、漏洞状态（初始提交、已验证有效、已验证无效、已核验有效、已核验无效)、操作（表单详情、修复建议)。 19、支持按照服务、应用归并漏洞修复建议，对于相同服务类型的给出影响资产数、漏洞数、建议升级版本，可通过统一升级完成对多个漏洞的修复操作；支持可归并修复的漏洞列表展示，和批量处置，以及升级状态标记；支持按照应用类型、升级状态的统计分析呈现；支持选择多个漏洞处置单进行批量复扫、批量归档、批量验证，支持选择多个或者全部漏洞处置单进行导出，可批量导出到 Excel 文档中下载留存； 20、资产漏洞 支持查看产品漏洞的字段详情，包括漏洞标识号、本地编号、标准组织、描述和修复建议、关联 POC 插件等。支持漏洞分类树的筛选视图，区分主机漏洞（资产类型如系统、组件和应用)、WEB 漏洞（OWASP-2010/WASC1.0)；支持综合的 CWE-TOP25 漏洞原理分类。支持漏洞时间轴，以时间维度展示漏洞新增、融合（谁、厂商、来源方式等)、编辑（展示核心变更项)、状态更新等记录，保留历史数据可追踪当前时间点记录。 支持资产标记库管理，1.内置资产标记库，支持资产名称 CBB 中资产标记库数据，支持产品分类分布、产品族分布；列表字段包含：ID、资产数据来源、产品族、产品名称、产品分类、厂商、产品版本；2.支持创建资产标记任务，支持列表展示，字段包含 ID、任务名称、属性分类（多选)、执行方式、当前状态、任务次数、执行结果（已纠偏、纠偏失败、标准)、创建人，操作（编辑、详情、启动、停止、删除、重扫)； 21、支持漏洞指纹插件库管理，支持添加 POC 插件，可以设置 POC 名称、类型、描述、对应的产品漏洞及 POC 文件上传；支持提供 POC 列表展示，字段包括 POC ID，产品漏洞 ID、名称、POC 类型（漏洞 POC/漏洞 E		

		XP/漏洞指纹）、状态、内容描述，POC 文件附件、文件 HASH、POC 插件文件列表、插件 HASH 列表、引擎 ID 列表； 22、支持以任务结果展示目标属性纠偏结果，列表支持：ID、任务 ID、目标类型、目标属性名称、源值、纠偏状态（已纠偏（展示对应相似度）、待纠偏、标准（相似度：100%）、纠偏失败（相似度：低））、相似度、标准值、操作（删除、恢复、纠偏）； 23、支持基础漏洞知识库内置超过 230000 条漏洞，能够覆盖主流操作系统、软件、数据库、网络设备，能够覆盖网站系统的通用组件、第三方软件以及各类 Web 组件漏洞； **挖掘工具集** 24、工具库中包含 300 种以上相关的靶标安全验证工具；覆盖漏洞检测工具、漏洞利用工具、后门和远程管理工具等多个类别。 25、包含验证工具库相关 300 种以上工具的中文测试验证教程，以指导用户如何进行安全测试；		
2	基础挖掘子系统	**1、能力标准要求：** 支持自动筛选出有价值的异常信息，迅速定位漏洞并分析漏洞的成因； 具有良好的数据流和控制流分析能力，能够分析控制流可控性，实现漏洞可用性判定。 **2、高级反汇编分析引擎** 支持汇编指令逆向分析：能够对可执行文件进行汇编指令级的逆向分析。 支持函数名称解析：能够分析并显示出部分函数名称。 支持文件结构解析：能够解析可执行文件的结构数据，包括加载基址、需要加载的模块名称等内容。 支持 C 伪代码逆向分析：输出类 C 伪代码或 IR 中间表示数据。 **3、动态调试引擎** 支持断点设置与记忆：支持设置断点及断点自动记忆功能。 支持汇编与内存数据显示，当程序被中断时，能显示被中断的汇编指令和前后部分指令，同时可以显示相关地址的内存数据。 支持指令与数据追踪：支持指令流单步追踪、条件追踪和数据流读写追踪功能。 支持环境上下文信息：具备完整的环境上下文信息显示。 线程与模块追踪：支持线程和模块的指定追踪模式。	套	1

		支持调试事件显示：支持调试事件的实时显示功能。 支持安全监视：支持缓冲区溢出监视和 SEH 链表监视。 **4、横向扩展功能要求** 支持扩展支持漏洞模式匹配库，通过分析程序出错点的上下文环境，追踪部分数据流，回溯相关指令流，对漏洞的可用性进行初步分析。 支持扩展支持污染数据回溯功能，自动分析污染数据在内存中的传播路径。 5、为保证业务系统安全性，系统生产商具备较强的漏洞分析能力。		
3	固件逆向分析子系统	**1、能力标准要求** 支持系统提供固件提取、模拟仿真、逆向分析、动态调试等功能，可以实现固件在模拟环境下的执行、调试和漏洞复现。 **2、运行环境要求** CPU：四核八线程（主频：2.8GHz，睿频：4.7 GHz）及以上； 内存：16GB，DDR4 及以上； 硬盘：1TB，SSD 操作系统：支持统信等主流科研环境适配操作系统； 接口：千兆网口 2 个、电源接口 1 个、RS232\422\485 串口 1 个(可调)、USB2.0(Type A)接口 1 个、USB3.2(TypeA)接口 2 个、USB3.2(Type C)接口 1 个、HDMI 接口 1 个、VGA1 个、具有音频接口等； 电池：单块 4700mAh 锂电池及以上；电源：220V/19V 交流电源适配器与交流电源线；防护等级：IP53 及以上； 指示灯：具备但不限于电源指示灯、电池指示灯、硬盘指示灯、大小写指示灯、数字键指示灯、无线指示灯； 其他：内置喇叭、安全 U 盘等； **3、其他性能指标要求：** 漏洞扫描单 IP 时长 3 分钟； 5GB 流量分析时间 15 分钟； 固件检测已知 CWE 检测；	套	1

		支持 WIFI 检测； **系统综合管理** 支具备被检单位管理能力，支持对检查单位的名称、负责人、所属行业、省份、检查周期和更新时间等基础信息管理，支持被检单位信息模板下载及导入，支持批量删除功能。 具备工控系统管理能力，支持对系统名称、所属备件单位、安全保护等级、覆盖范围、服务对象、更新时间、是否备案、是否测评等基础信息管理，支持被检单位信息模板下载及导入，支持批量删除功能。 具备工控资产管理能力，支持将工控资产按照普渡模型分层筛选，并将资产按照工控设备资产、工控工作站资产、工控服务器资产、工控网络设备资产、工控安全防护资产、工控视频监控资产维度分类管理。资产信息包含设备标识、所属工控系统、安全分区、 设备厂商、设备型号、设备固件、设备 IP、设备 MAC、资产类型等字段。支持工控资产信息模板下载及导入，支持批量删除功能。 **检查任务管理** 具备检查计划管理能力，支持对计划编号、计划名称、被检单位、工控检查类型、流程状态、创建时间等基础信息管理和创建检车计划，支持计划来源和检查类型的选择，支持通过检查计划直接生成检查方案的能力，支持批量删除功能。 具备检查方案管理能力，支持由检查计划生成的检查模板，支持检查模板、资产信息、检查内容确认以及检查方案的拟制功能，支持检查记录单编制及打印功能，支持检支持工具调度功能、支持结果处理功能。在检查过程中支持添加前期未收录的新资产的功能；支持对检查方案进行编辑、进度查询等功能。 具备检查结果管理能力，支持检查结果的查看、删除及批量删除功能。 **4、逆向分析工具集** 支持工控系统资产发现支持旁路流量识别和低频无损探测识别的检测方式，旁路流量识别支持流量采集时长的设置，低频无损探测基础配置支持扫描速度的控制及 IP 范围设置，高级配置支持端口访问策略、存活判断策略、扫描策略等参数配置。支持对探测任务的取消、停止、删除以及批量删除。 支持资产安全漏洞检查支持通过录入设备基本信息通过漏洞库比对发现漏洞信息，支持通过低频无损探测方式对资产进行安全漏洞检查。扫描目标支持对厂商、控制器型号、CPU 类型、网络类型维度进行筛选配置；低频无损探测基础配置支持扫描速度的控制及 IP 范围设置，高级配置支持端口访问策略、存活判断策略、扫描策略等参数配置。支持对探测任务的取消、停止、删除以及批量删除。		

		支持固件恶意代码检查支持对导入检音工具的设备固件包,文件进行安全检测的工具，支持恶意代码检查，脆弱性代码检查，CVE/CWE 漏洞检检查等。支持任务创建以及固件上传功能。 支持通讯流量诊断支持通信流量采集、通信流量统计分析、通信流量协议解析、异常流量发现、流量离线分析等功能。可配置流量包文件名、采集时长、采集数据总量等参数，并可根据工业行为、资产检测、流量监测、工业协议、协议对象、故障检测等类型，分类建立检测任务。 5、支持主机信息采集工具通过 U 口插入工控系统上位机设备，完成主机基础信息，文件样本特征值信息、进程信息、网络外联信息，注册表信息等五类信息的采集。U 盘同步支持病毒检测能力。() 6、支持对工控系统中的无线 WI-FI 进行安全检查，支持 wifi6，支持发现所有参与无线通信的设备，并对该无线热点进行弱密码检查。支持设备信息、信道概览、安全事件、弱口令检测、安全策略、密码字典等功能; 支持对工控系统中的服务器、网络设备和上位机设备进行配置核查，包含设备的访问控制策略、身份鉴别策略、安全审计策略等。支持通过模板创立检查列表，模板支持按照等保等级筛选，并通过 SMB、SSH、Telnet、RDP、HTTP、HTTPS、WinRM 等协议登录到设备进行检查。 **7、逆向分析知识库** 支持知识库配置：系统内置工控设备库、经典案例库、威胁情报库、威胁特征库、政策法规库、漏洞情报库、攻击组织库、工控协议库、工控漏洞库、配置模板库，并支持新知识可类型的创建。 支持知识库内容：工控设备库 1640 条；威胁特征库 10370 条；政策法规库 130 条；漏洞情报库 11550 条；组织攻击库 100 条；工控协议库 35 条；工控漏洞库 253030 条；配置模板库 116 条；支持经典案例库和威胁情报库；支持所有知识的导入导出功能；日志管理：支持日志查询和备份。 支持系统配置管理：支持主题配置、系统监控、痕迹清除、证书管理、升级管理、网络配置、登录设置、角色管理、账号管理。		
4	终端安全管理平台	**1、主要性能指标要求：** 支持操作系统适配：Windows XP_SP3 及以上/Windows Vista/Windows 7/Windows 8/Windows 10/ Windows 11/Windows Server 2003_SP2/Windows Server 2008/Windows Server 2012/Windows Server 2016/ Windows Server 2019/SUSE Linux/Red Hat Linux/CentOS/Ubuntu 12 及以上版本。 支持控制中心：采用 B/S 架构管理端，具备设备分组管理、策略制定下发、全网健康状况监测、统一杀毒、	套	1

		统一漏洞修复、网络流量管理、终端软件管理、硬件资产管理以及各种报表和查询等功能。 支持客户端：与系统控制中心通信，提供控制中心管理所需的相关数据信息；执行最终的木马病毒查杀、漏洞修复等安全操作。支持终端保护密码，设置密码后，终端退出或卸载杀毒都需要输入正确的密码方可执行。支持网页访问部署、离线安装包部署、域推送等部署方式，可自定义部署通知邮件及部署通知公告。支持文件与目录自定义黑白名单的方式来管理全网终端的文件；文件被加入白名单，客户端不再查杀，加入黑名单，客户端不可执行此文件； 2、支持虚拟分级管理，可以实现全省或全市终端都部署在一台服务器上，但不同地市或县市管理员分别管理所属客户端，且不影响同一台服务器上的其他终端支持自主授权分割功能，管理员可以从主系统中心分割授权客户机数量给下级系统中心，限制下级系统中心对客户机的注册数量，阻止非法客户机注册。 3、邮件检测 支持电子邮件内文件检测，可清除隐藏于电子邮件计算机病毒和恶性程序；支持拦截下载器自动下载木马程序、恶意推广程序、黑客远程控制本机、盗号木马；可以提供U盘等移动设备接入电脑自动检测功能，全面拦截和清除在移动设备接入系统可能带来的病毒木马；支持浏览器防护，对篡改浏览器设置的恶意行为进行有效防御，并可以锁定默认浏览器设置 支持邮件报警，可以设定多种触发条件，满足条件后自动发送邮件到相关人。邮件触发条件包括：一定时间内的病毒数量阈值、一定时间内的未知文件数量阈值、重点关注的终端发现病毒、病毒库超期等 具有定时修复漏洞功能，同时可以设置筛选高危漏洞、软件更新、功能性补丁等修复类型；支持补丁验证升级延迟天数设置功能；服务器客户端具备资产管理及运维管理的功能，包括软件资产管理，网络管控、流量管理、密码管控功能； 支持多种分组规则，如IP分组以及支持与AD、LDAP同步功能，可将用户组织架构同步到终端安全管理系统中，依照用户现有架构进行管理。分组支持无限层次分组，支持生成组安装包，安装后自动进入该分组。支持文件、引导区、内存、注册表、服务、进程、进出文件、目录、压缩文件、网页等恶意代码、恶意样本查杀。 4、支持虚拟补丁功能，拦截外部黑客工具通过利用弱口令集和密码表对目标机器的网络共享发起高频率的操作请求，以达到攻破目标机器的密码并在目标机器上释放运行病毒文件的行为。 5、支持通过数字签名或者文件名的方式分别显示文件，方便管理员管理全网终端上报的文件；支持文件解		

		压缩病毒查杀，支持对 zip、rar、7z 等多种格式的压缩文件查杀能力；默认支持 32 层压缩扫描，且用户可以自定义设置扫描层数 6、可以提供对各类即时通讯工具、邮件、网络下载工具、文件，文件类型支持.dll、scr、rtf、pps、zip、MP4、AVI、wmv、RMVB、psd、jpeg、bat、cfg，apk、lnk 等保存到本地文件的查杀功能，并进行文件审计，可查看文件审计列表，并可对任意审计文件进行追溯对勒索者病毒提供防护机制，采用虚拟钓饵方式有效拦截勒索者病毒。		
5	漏洞挖掘算力调度云平台	**1、主要性能指标要求：** 支持资源虚拟化：采用轻量级容器虚拟化技术，实现对 CPU、内存、磁盘等资源的虚拟化和统一管理。针对人工智能领域的特定需求，可以提供 GPU 等异构计算资源管理接口，实现对 GPU 等异构计算资源的虚拟化统一管理，支持为容器以直通方式挂载 GPU 等异构计算资源；容器通信：支持容器间 infiniband 高速通信。算法开发：支持用户在线提交计算资源，支持单机多 GPU 与多机多 GPU 的训练任务。web Terminal：用户无需在容器中安装 ssh 服务，即可通过平台直接访问容器终端。 支持底层使用非 k8s 或解决 k8s 中 pod 因内存或硬盘超过配额限制而重启的问题。资源规格：支持管理员自定义资源规格，降低因用户随意选择资源造成资源碎片化产生在线人数：支持查看当前平台在线人数。角色管理：支持平台上功能权限细分，限制用户越权操作，管理员能更精准的限制用户所使用的功能。登录日志：支持记录用户的登录时间、登录状态、登录 IP、使用浏览器等。 2、支持容器管理：支持快速创建多种深度学习开发调试环境的容器，支持 web Terminal 访问容器，支持将创建的容器在线进行镜像打包，并支持将打包好的镜像上传镜像仓库，实现镜像版本的持续更新。存储管理：支持 NFS 空间修改资源配额。 3、支持数据管理：支持用户使用 FTP 工具进行自定义代码和数据文件的上传下载操作。算法开发：平台整合 jupyter-lab、vscode 功能，用户访问增加权限控制。算法开发： 4、支持 vnc 功能，用户可以在平台上直接访问容器桌面环境。作业管理：可以提供训练作业管理功能，包括查看任务运行状态、作业快速克隆、作业查询、作业日志和作业文件管理等基本功能。 5、支持作业监控：支持输出损失率、准确率等动态可视化监控图表，同时支持输出训练过程日志，并提供日志查看功能：文件共享与隔离：支持数据共享与数据隔离，即同一数据可供多用户同时访问，不同用户有自己的私有空间。也可以设定不同用户的访问权限。镜像管理：支持私有镜像仓库，集中化管理用户的	套	1

		镜像。能够提供新建项目、设置用户权限等功能。 6、使用时长：支持统计用户任务及资源使用时长，并通过 Excel 表格导出。操作日志：支持记录用户操作，包含功能名称、操作人、请求方式、操作状态、时间等。 7、集群管理软件是国产。国产化：集群管理软件支持国产化模块。		
6	漏洞挖掘检测工具平台	**1、主要性能指标要求：** 界面友好，并有详尽的技术支持文档，所有图形界面中文。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。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。硬件支撑：采用安全的 Linux 操作系统，双核或双核以上 CPU，8G 以上内存，1T 硬盘空间；可以提供用户概述功能，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；支持提供离线检测工具； 离线检测工具包含 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。可以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； 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； 4、支持实时结果的展现，展现内容包含扫描对象、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； 5、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；可以提供接口管理功能，能与其他系统进行对接；可以提供引擎管理功能，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；	套	1

7	工业互联网靶标一	**1、主要性能指标要求：** 控制器主频：双核，600MHz 指令执行时间：位运算 15ns；定点运算 15ns；浮点运算 25ns 存储器：集成存储器（程序+数据）64MB；掉电保持区：512KB MRAM 集成接口：以太网接口：2 路 RJ45 接口，10/100/1000M 自适应，双网口冗余，支持 Modbus TCP 协议、Hol liTCP 协议 通信连接资源： Modbus TCP：主、从连接数各 16 个 Powerlink：128 个 PL 从站 Profibus-DP：124 个 DP 从站〞 变量区： 输入变量区（I 区）：空间为 32KB 输出变量区（Q 区）：空间为 32KB 硬全局变量区（N 区）：8MB 自由变量区（M 区）：6MB〞 工作温度： -20～70℃ 诊断：通道级诊断、输出预置功能，支持带电插拔，采用防混销设计 编程平台：PLC 编程平台自主可控，编程语言遵循 IEC61131-3 国际标准 编程语言：LD、CFC、ST、SFC 掉电保持：周期性备份掉电保持数据，并在掉电后，仍能保存这些数据 增量下装：支持增量下装，程序下装时设备不停机 工作模式： RUN（运行） 模式、 PRG（编程） 模式和 REM（远程控制） 模式	台	1
8	工业互联网靶标二	**1、主要性能指标要求：** 电源电压：24Vdc 离散量输入/输出：16 点离散量输入/输出 输入类型及数量：8 个漏型/源型 24Vc 输入，包括 4 个高速输入； 8 个继电器输出；	台	1

		输出连接可拆卸螺钉接线端子可拆卸螺钉接线端子或弹簧接线端子； 离散量输入/输出连接：专用可拆卸接线端子 模拟量输入：7 个 ModiconTM3 扩展模块，带有限数量的输出 可支持最大 I/O 扩展模块数量：限制性合理使用 ModiconTM2 扩展模块；TM221CE 控制器内置 1 个以太网接口；ModbusTCP 协议（客户端&服务器）；ModbusTCP 从站，动态 DHCP 客户端配置、编程、下载、监控 以太网通信：短信和邮件服务；1 个串行通信端口（RS232/485),+5V 电源；一个位于 TM221M…控制器上端串行通信端口（RJ45 接头），RS485； 过程控制：PID 控制； 计数：多达 4 路高速计数输入（HSC），频率为 100KHz 多达 4 路高速计数输入（HSC），频率为 100KHz； 位置控制：对于 TM221M16T/TG,TM221ME16/TG,TM221ME32TK 及 TM221ME32TK 控制器，包含：脉宽调制（PWM）、脉冲发生器（PLS）；2 个 P/D 脉冲串输出，支持梯形及 S 曲线加减速（r），频率为 100KHz；扩展版；支持扩展版数量：显示器、图像显示单元、安装、导轨安装或使用 TMAM2 安装套装。		
9	工业互联网靶标三	**1、主要性能指标要求：** 功耗：14W 可用电流（24VDC）：最大 300mA(传感器电源) 数字输入电流消耗(24VDC)：所用的每点输入 4mA CPU 特征：用户储存器：12KB 程序存储器/8KB 数据存储器/最大 10KB 保持性存储器 板载数字 I/O：12 点输入/8 点输出 过程映像大小：256 位输入(I)/256 位输出(Q) 模拟映像：56 个字的输入(AI56 个字的输出(AQ) 位存储器(M)： 256 位 临时（局部）存储：主程序中 64 字节，每个子程序和中断程序中 64 字节 I/O 模块扩展：6 个扩展模块 信号板扩展：1 个信号板 高速计数器：共 4 个；单相：4 个 200kHz 正交相位：2 个 100kHz 脉冲输出：2 个 100kHz	台	1

		脉冲捕捉输入： 12 循环中断：共 2 个，分辨率为 1ms 沿中断：4 个上升沿和 4 个下降沿（使用可选信号板时，各 6 个） 存储卡：MicroSDHC 卡（可选） 实时时钟精度：+/-120 秒/月 实时时钟保持时间：通常为 7 天，25℃时最少为 6 天（免维护超级电容） 其它性能：布尔运算 0.15μs/指令；移动字 1.2μs/指令；实数数学运算 3.6μs/指令		
10	智能终端靶标一	**1、主要性能指标要求：** 血氧饱和度：SP02 测量范围：100 测量精度：75～100：±2 测量范围：30bpm～240bpm 精度：±2 或±2bpm 取大值 报警限默认值：上限：100-240 bpm 下限：30-60 bpm 测量范围：0.2～20 测量精度：0.2～2 ±02 ～10 ±1 数据存储：每 1/2/4/8 秒钟存储一组数据（SpO2 和 PR），最大可存储 70 小时的数据。 抗自然光干扰能力：在室内自然光及现有照明光源下的血氧测量值与暗室条件下的测量值相比，偏差小于±1 抗工频干扰能力：在脉搏血氧仿真器设有工频干扰（模拟日光灯等干扰光）的测试条件下能正确测量血氧饱和度和脉率值	台	1
11	智能终端靶标二	**1、主要性能指标：（智能终端）** 记忆组数:500 组记忆值，含测试日期及时间 反应时间:5 秒 使用环境:5℃～40℃;相对湿度小于 80%RH 测量范围:1.1-33.3mmol/L	台	1

		传输模式:蓝牙传输 显示：超大背光屏幕显示，时间、日期显示 采血量：约 0.7 微升采血量，只需 5 秒即可快速出结果，自动退试片，避免交叉感染 安全符合 IS015197:2003 中的 GB/T14710-2009 执行标准。		
12	智能终端靶标三	**1、主要性能指标要求：** 测量方式：采用上臂式血压计测量（支持左右血压测量）； 性能：智能加压技术、示波测定法测量高压、低压、心率； 范围：血压：0-299mmHg(0-39.9kpa) 脉搏：40-180times/min； 紧急停止开关：测量中如感觉不适，如果按开始/结束扭，袖带中的空气也无法排出时，请按下[紧急排气]扭，约 4 秒钟后，空气即可排净； 操作系统：可选择单项测量，全部顺序测量等模式，全程智能语音和动画提示操作简单； 通讯方式：可以提供 RS232 接口、WiFi 接口、RJ45 网口，蓝牙（选配），3G/4G（选配）。 可与第三方系统数据通信；兼容与医院、电子病例（EMR）、HIS 健康体检系统数据共享通信； LCD 显示：采用 10.2 寸高清彩色液晶屏，超大字体，醒目清晰显示，日期时间温度，与网络同步，时间准确，显示体型体型偏胖、正常、偏瘦； 打印功能：采用高速热敏易装打印机实现自动打印测量结果，换纸方便，还可设置打印； 自动语音播报：清晰语音报出测量数值并且根据使用情况设置提示语音； 微信推广：设备并提供测量数据和微信公众号的绑定，居民在通过微信扫一扫手机获取测量数据的同时关注公众号； 数据存储：可存储 100 万条以上测量数据，并支持 U 盘导出；电源电压：采用 AC100V-240V/12V 直流电源，输入宽电压适合电压不稳定地区； 消耗功率：待机 10W，工作时平均 15W； 工作环境：温度-10℃至+40℃　湿度：20%-85%PH；	台	1
13	云服务器	**1、主要性能指标要求：** 采用 1U 机架式服务器，配置 1 颗处理器，每颗 CPU 8 核心 16 线，主频 3.0Ghz。 服务器 4 个内存插槽，配置 32G 内存（32G*1）；硬盘：采用硬盘 4 个 2.5/3.5 英寸 SATA 热拔插插槽，2 个	台	1

		m.2 SSD 插槽（m.2 仅用于系统盘）；标配整机配置硬盘 2 块 3.5 寸 4TB 7200 转 SATA III，整机配置 1 块 480G 固态硬盘+2 块 240G M.2 SSD。 网口：4 个千兆网口;1 个千兆管理口；电源：1 个电源。 配置云桌面管理平台。管理平台为 B/S 架构，中文界面，同一管理界面中可实现对计算、存储、网络等功能的配置操作。 支持查询主机节点名称、管理 IP、连接状态、描述、创建时间、CPU、内存、硬盘、网卡、主机心跳等信息支持主机性能状态监控，能以小时、天、周、月、季度、半年、一年维度，对主机 CPU 使用率、内存使用率、磁盘速率、磁盘 IOPS、网卡错误数、丢包率、网卡带宽进行性能监控记录。 支持虚拟机性能状态监控，能以小时、天、周、月、季度、半年、一年维度，对主机 CPU 使用率、内存使用率、磁盘 IOPS 进行性能监控记录。为保证分布式存储的性能，三节点集群模式，4KB 块大小全随机 100%读 IOPS 大于 170 万。为保证硬盘故障后，数据可以快速重构，所投产品的分布式存储性能，满足 1T 数据重构时间不超过 15 分钟，为避免用户数据外泄，分布式存储采用块虚拟化技术，将用户的文件切分成多个小数据块，以裸数据的形式分别保存在不同服务器的不同硬盘上。避免硬盘故障维修时，原故障硬盘被第三方公司/人带走，导致数据外泄。 单个数据中心可创建 64 个虚拟机交换机，每个虚拟交换机默认创建 256 个端口，可根据需要自动创建/删除端口；单个虚拟交换机最多可创建 2048 个端口支持查询、下载系统管理员的操作日志，日志包括：管理员账号、IP 地址，操作时间、操作内容。		
14	科研训练授权云终端	**1、主要性能指标要求：** 采用配置云桌面控制平台授权，平台采用 B/S（Broswer/Server）架构，可以提供云桌面管理、镜像管理、用户管理、终端管理、策略管理等功能模块。支持采用远程方式对云桌面进行远程协助。远程协助基于 WEB 页面，无需额外安装客户端。支持用户桌面个性化数据(包括应用程序配置文件、注册表、系统的修改和配置等用户个性化文件)重向至定个人磁盘中，管理员在统一更新、升级镜像后不会影响个人数据。支持 Windows Server 中安装的应用发布，远程交付多个应用。支持通过上传操作系统 ISO 文件、QCOW2 格式文件来制作生成镜像。支持应用程序安装包和共享文件的管理，包括：上传、删除、查询与制作镜像时加载到虚拟机内部。 支持管理 X86 架构的终端，支持将第三方 PC 通过 intel TCI（透明计算)技术云化，纳入平台统一管理。支	套	55

		持将普通 windows 系统的 PC 纳入平台统一管理。 持配置终端无线白名单，确保终端无法接入非法 WI-FI SSID。 支持外设控制策略，包括禁用启用设备、以及读写权限控制，外设设备包括：输入设备、存储设备、摄像设备、办公设备、手机、其他已归类设备等。支持对接 LDAP、AD 域导入用户，支持通过导入 Excel 文件的方式批量新建用户信息。支持定义主题策略，支持自定义终端登录背景、管理界面 LOGO 等内容。支持分级分权管理，可以按需自定义不同角色用户对应的管理权限：可以针对角色指定其可以操作的功能菜单，包括镜像管理、教室管理、用户管理、系统设置等权限设置；可以针对角色指定其可以操作的具体功能按钮，包括镜像模版的删除、创建、复制、快照管理等权限设置；可以针对用户指定其具体可以管理的哪几个镜像模版、哪几间教室。支持精细化配置功能权限，功能权限颗粒度细化到页面的具体功能。		
15	科研训练教学管理软件	1、整体功能指标： 采系统采用 B/S 架构，通过浏览器访问服务器对机房的 VDI 桌面、VOI 桌面，PC 桌面在进行管理；支持展示实验室资源数据使用，包括实验室在线/总数、终端在线/总数、场景在线/总数、桌面在线/总数；展示实验室资产状态，包括终端的风险预警次数、待处理变更数、待处理报修数；展示服务器资源实时使用情况，包括 CPU 使用、内存使用信息、存储使用信息； 支持展示桌面今日并发趋势；管理平台支持在线客服，可直接在平台上咨询客服技术问题，当客服不在线时可进行留言，留言支持上传图片、视频等方式提供给客服进行问题分析。无需安装第三方通讯软件；当终端桌面有多个操作系统时，可通过管理平台远程切换终端桌面系统；支持对实验室的终端桌面进行督导抽查，可批量的对多个桌面进行监看，支持四屏、九屏、十六屏的方式同时监看。可对任意桌面进行远程协助，远程锁定、远程重启和发送消息的管理操作；可统计学生前排就座率、到课率和按时到课率、桌面使用活跃度和广播教学时长占比。并可导出实验教学课堂分析报告，为教务部门评估课程教学质量作决策依据； 支持开启自动审批时指定实验室，当教师新提交的排课申请中填写了实验室，实验室均在自动审批的指定实验室范围内时，没有排课冲突将自动审批通过并排课；系统可以显示实验室排课率、排课节次分布、教师排课量数据，便于合理安排实验室使用时间，均匀排课；管理员可设置哪些实验室是否开放预约，可设置开放预约顺序优先级以及实验室开放预约机位数的占比；并可设置预约时间段；管理员可查课学生的预约情况，包括预约学生的姓名、所属院系专业和班级、预约日期和上机时间、以及预约上机的状态（待上	套	1

		机、上机中、已失约、已结束、已取消），管理员可以根据实际上课情况强制取消学生的预约；支持断网锁屏功能，终端断网自动锁屏，当网络连通后终端自动解锁；如客户端非正常锁定，管理端可生成解锁密码，解锁客户端； 2、满足登录模式功能指标：可设置实验室电脑终端的登录方式，可设置免登录的完全开放模式和输入帐号密码的登陆模式。登录模式可以选择全校全体师生和部分院系师生；可将上机违规学生手动方式拉入黑名单，拉入黑名单的学生在不能进行登录上机；黑名单可以设置天数自动移除以及手动移除； 3、满足自定义功能指标：可针对每间实验室或每台电脑终端自定义标签，管理员可以按标签的类别来搜索实验室或终端电脑。标签可设置为使用场景、使用班级、单双号等类别；可设置程序限制策略，支持黑名单、白名单两种模式，支持从样机、规则库、文件的方式导入黑白名单； 4、满足管理员功能指标： 支持管理员可定义预约规则，包括可提前多少天预约、预约开始多长间未登录视为失约并自动取消预约、中途下机多长时间未登录则自动释放机位；可编辑预约注意事项，学生预约之前可了解相应的规则；可在计划内排课中设置上课时自动化录制教师机桌面的音视频，资源按课程自动归类。 该课程对应班级学生或教师可以直接在平台上在线观看，管理员也可以设定哪些课程为公开课，公开课所有的学生都可以进行在线学习；可通过楼层间的电子屏查看全部实验室或指定实验室的当日课表安排； 可以统计每个学生什么时间段在哪台终端电脑使用过，包括总体使用时长、上机时间、下机时间。并可将记录以电子表格形式进行导出； 支持可统计按 CPU 类型、内存容量、硬盘容量搜索指定类型的终端电脑，分布在哪间实验室机房；支持跨网段远程开机、关机、重启、场景切换等；支持标记为教师机；自动收集终端硬件信息，并支持对硬件信息编辑；教师和学生可以通过系统客户端上报使用电脑的故障，管理员在平台上收到上报消息之后，可以进行判断处理；平台支持安全学习考试，教师或管理员可在平台上编辑考试试题，指定需要参加考试的学生在登录上机时会自动弹出试题进行考试，通过之后才可正常使用电脑终端。可根据实际情况设置临时跳过考试的次数；为提高学生的网络安全意识和水平，落实文明上网。 支持系统检索搜索引擎或浏览器地址栏搜索的内容，与敏感词库进行匹配并记录，当搜索内容包含敏感词时，可设置在客户端桌面发出提醒警告；可统计每间实验室终端电脑数量、实验室占有率、上机人次、终端利用率以及智能监测捕获风险项，包括 CPU 高负载预警、内存高负载预警、磁盘 IO 高负载预警、系统盘		

		空间不足预警、CPU 高温预警、独立显卡高温预警、异常断电/蓝屏死机预警 、终端网卡链接低速预警； 支持管理员可统计终端报修情况和硬件变更记录，当有报修记录和变更记录时会在平台消息栏中提醒管理员及时处理；可统计一个校区或多个校区的某间实验室或多间实验室实验教学网址次数的前 50 名，并可以统计每个网址具体的访问次数；可通过图形化的方式生成实验室使用报告，并导出报告图片。使用报告包括：实验室数量、终端数量、终端使用时长、服务师生人数和次数、实验室占有率、终端利用率、终端能耗统计、硬件风险趋势以及风险类型占比；可统计每台终端电脑的使用时长、利用率、能耗、开机次数、报修次数、硬件变更次数、风险预警次数； 支持大屏显示大数据看板，可显示实验室使用实时状态，包括终端在线数、登陆上机人数、正在使用实验室数量；风险预警状态图、报修记录、软件使用前 5 的类别。以及服务实验室的总数量、总的师生人数、终端利用率前 5 名的实验室和占用率前 5 名的实验室；为了保障教学过程的稳定，可禁止学生修改系统设置，比如修改 IP 地址、亮度、更新设置等；为方便学校统一形象管理，支持自定义客户端登录页 LOGO 和登录区标识，可变更为学校统一身份认证标识；支持管理员用户分权管理，可设定不同的管理范围和不同的管理权限；系统平台支持启用微信公众号，进入公众号可以视图形式查看实验室排课内容和自己的课表、支持上机预约申请、支持查看预约申请记录、显示个人帐号信息； 5、满足跨校区功能指标：可将用户认证平台的用户信息以增量的方式同步到系统平台，可设置手动同步和自动同步。自动同步可设定每天的具体时间进行同步；可统计一个校区或多个校区的某间实验室或多间实验室软件使用时长前 50 名，并且可以统计每个软件具体使用时长；		
16	实验室配套桌椅	**1、主要性能指标要求：** 采用工位的桌子桌面采用复合木质坚固耐用，形状美观大方凸凹有致，满足灵活多样的使用要求，工位的椅子结构坚固耐用，透气性好。符合人体工程学原理，座面弹性适中。 桌子高度 70 厘米，单个工位长度 120 厘米，宽度 60 厘米，桌子采用隐藏式设计键盘托。 椅子结构坚固耐用，尺寸 50*50*100 厘米。椅子框架使用管壁 2mm 的钢管，透气性好。座面密度>35KG/m3，背密度>30KG/m3.	套	30
17	实验室配套环境建设	**1、实验室配套环境建设要求：** 采用对教室原有线路进行清除，每间教室配置学生点位 45 个，重新进行整体强弱电、网络设施等相关设备的规划布局，内容包含地面开槽、强电布线、通信弱电布线、视频弱电布线、信息插座、强电插座等，所	项	1

		有实施材料严格按照国家相关产品技术标准，确保整体网络、电路、通信等综合环境安全运行。对实验室各个区域进行规划设计，整体风格美观大方，简单实用，特色突出。 实验室所需优化的网线采用品牌六类网线，六类水晶头，网线外护套采用 PVC(聚氯乙烯)，绝缘层采用 PE(聚乙烯)，导体采用优质无氧铜，内部具有弹性十字骨架分隔线对保证传输性能。相关执行标准按 GB/T 3939.1-2004 进行执行； 实验室所需优化的电源线和插座安全、可靠，根据单个实训室电量负载需求，完成强电室内布线和接入楼层强电间，单个实训室要实现可以分组控制电源。相关执行标准按 GB/T 28567-2022 进行执行。 实验室所需优化的强、弱电改造采用不锈钢线槽，全部沿线槽规范布线，有强电和弱电走同一个不锈钢线槽要求分支电缆采用 RVV6mm2 以上铜缆，使用金属穿线管敷设。相关执行标准按 GB/T 28567-2022 进行执行。 实验室综合布线符合国家《综合布线系统工程设计规范》GB/T 38002.2-2022 标准，所有实施材料严格按照国家相关产品技术标准，确保实验室整体网络、电路、通信等综合环境安全运行		

附件 3：

售后服务计划及保障措施

我公司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。

售后服务体系：此次项目我公司客户信息部主要是接收客户的报修信息和反馈信息，进行分类和归档，并根据客户不同的要求落实到相关职能部门，对整个服务过程进行跟踪，保证对客户服务的及时性，同时建立客户档案，定时对客户进行回访。技术服务部主要负责解决在售后服务中出现的技术问题，对客户所提出的技术问题给予及时的处理和解答，并进行现场服务工作。维修部主要负责产品的维修和跟踪。

售后服务内容、形式：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相应时间：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。

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，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：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 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></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：

成交通知书

河南省公共资源交易中心

成交通知书

河南尔享科技有限公司：

贵单位于 2023 年 10 月 23 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一期采购项目（豫财磋商采购-2023-946）的竞争性磋商采购活动，经磋商小组评审及采购人确定，贵单位为该项目成交供应商，成交金额为 1789600 元人民币。

请贵单位收到成交通知书后，按照本项目采购文件的规定及贵单位响应文件确定的事项，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）

2023 年 10 月 27 日