

政府采购合同

【网络安全实训室建设项目（第三次）】

合同编号：

甲方（买方）：北京市商业学校(北京祥龙资产经营有限责任公司党校)

法定代表人或授权代表：马丽

地址：北京市昌平区北七家镇曹八西路 28 号

联系电话：13520225385

乙方（卖方）：北京铜牛奇安科技有限公司

法定代表人或授权代表：杨帆

地址：北京市东城区天坛东路 31 号铜牛信息大厦 6 号楼二层 201

联系电话：18500197222

根据《中华人民共和国民法典》《中华人民共和国政府采购法》及相关法律法规的规定,就甲方向乙方购买网络安全实训室建设相关货物及服务事宜,经甲、乙双方协商一致,订立本合同。

第一章 合同标的

第 1 条 合同标的

本合同标的为网络安全实训室建设项目（第三次）所需货物、软件系统及集成安装调试服务,具体包括:

（一）网络安全综合演练系统（核心产品）：管理子系统、实训子系统、考试测评子系统、竞赛子系统、虚拟化组件（智慧防火墙）、虚拟化组件（上网行为管理）、定向课程资源包、基础课程资源包、竞赛题库；

（二）网络空间安全实战对抗系统：仿真引擎、系统管理、网络仿真、资源库、漏洞库、态势控制、人员能力评估、攻防演练；

（三）精密空调 2 台、桌面工作站 41 台、多媒体音箱、多媒体功放、多媒体教学软件、机房管理系统、多媒体教学中控；

（四）系统集成、安装调试及三年质保服务。

详细技术规格见投标文件。

第2条 质量标准

乙方所提供的货物须为在售全新设备，不得为停产型号或翻新机，须符合以下标准：

- (一) 国家标准（GB 系列）；
- (二) 行业标准；
- (三) 北京市地方标准；
- (四) 乙方所投产品制造厂商的产品标准；
- (五) 乙方投标文件中所承诺的技术参数和质量标准。

其中，精密空调须符合 GB 21455-2019《房间空气调节器能效限定值及能效等级》二级能效标准；桌面工作站须持有中国强制性产品认证（CCC）证书（认证类别：0901 微型计算机）。

第3条 技术标准。

本合同项下软件系统须满足：

- (一) 网络安全综合演练系统：支持 B/S 架构，具备教学实训、考试测评、攻防竞赛、场景演练功能；
- (二) 网络空间安全实战对抗系统：支持 B/S 架构，支持网络仿真、漏洞库、攻防演练、态势控制。

乙方须确保所提供的软件系统与甲方现有网络环境和教学平台实现对接兼容。

第二章 合同价款与付款条件

第1条 合同总价。

(一) 本合同总价为：人民币 1718940.00 元（大写：壹佰柒拾壹万捌仟玖佰肆拾），该价格包括合同货物价款、软件系统价款、系统集成及安装调试费用、培训费用、税费等全部费用。

(二) 分项价格见投标文件《分项报价表》。

(三) 以上价格为甲方指定地点统一交货价（含税价）。除甲乙双方签订补充协议另有约定外，甲方有权拒付本合同约定合同价款以外的任何费用。

第2条 付款条件。

合同签订生效后，甲方向乙方支付合同总额 75% 的首付款，余下款项需第二年财政拨款后并经甲方验收合格后付清。甲方每次付款前乙方应当开具等额正式发票，开具发票后十个工作日内付款。

第 3 条 履约保证金。

合同签订生效后 7 天内，中标人向采购人提交合同总金额 5% 的履约保证金，质保期届满，中标人已完全履行质保期内全部义务、货物无未解决的质量问题、无任何未结清的违约索赔及维修费用的，采购人将保证金全额无息退还中标人。

第三章 履约要求

第 1 条 交货期

（一）总工期：指自合同签订之日起 120 个日历日内完成项目全部设备到货交付、安装调试、试运行和终验。

（二）设备到货：合同签订后 30 个日历日内，设备到货并完成到货验收

（三）安装调试：设备到货后 30 个日历日内完成设备部署、联调与测试工作，具备试运行条件。

（四）试运行：安装调试完成后进入 3 个月试运行期，试运行期间系统正常运行，且期满乙方须向甲方提交《试运行报告》及《终验申请》，甲方在收到申请后 15 个工作日内组织最终验收。若验收不合格，乙方应在甲方限定期限内完成整改并重新申请验收，相关费用由乙方承担。

第 2 条 交货地点。

交货地点：甲方指定地点。

第四章 验收标准

第 1 条 验收节点。

（一）方案规划验收：自合同签订之日起 15 日内，乙方提交项目实施集成方案详细规划，经甲方审核通过后视为通过方案规划验收。

（二）到货验收：自合同签订之日起 30 个日历日内，设备到货并完成到货验收。甲方对设备数量、外观、型号规格进行核对，乙方提供产品合格证、出厂检验报告等证明材料。

（三）安装调试验收：设备到货后 30 个工作日内完成设备部署、联调与测试，乙方提交调试报告，经甲方确认后视为通过安装调试验收。

(四) 试运行验收：上线试运行期为三个月。试运行期间，系统应稳定运行，无 P1 级以上故障。如发生 P1 级以上故障，试运行期相应顺延。

(五) 终验：试运行期结束后，乙方可甲方提交《试运行报告》及《终验申请》进行项目终验。终验须满足以下全部条件：

1. 软件平台功能验收：对照投标文件中的技术参数表逐项验收，全部条款均满足投标参数指标；

2. 硬件集成验收：对照采购清单逐项验收，设备数量、规格型号均符合合同要求；

3. 试运行验收：自试运行期满验收之日起连续运行 30 日无 P1 级以上故障；若验收不合格，乙方应在甲方限定期限内完成整改并重新申请验收，相关费用由乙方承担。

4. 终验签字：终验合格，甲乙双方在验收报告上签字确认。

(六) 验收依据：以本合同、投标文件、附件技术规格书为验收依据。

第 2 条 验收费用。

(一) 到货验收、安装调试验收费用由乙方承担。

(二) 终验时，如需第三方专业机构对检测，检测费用由乙方承担。

第五章 质保与售后服务

第 1 条 质保期。

安装调试完成并终验合格后，须保证成套设备或整个系统能够正常使用，并提供 3 年质保服务。

第 2 条 售后服务。

(一) 质保期内，乙方须按照以下标准提供售后响应支撑服务：故障维修服务（三年）：接到设备报修故障后：

1. P1 级（重大系统故障）：15 分钟内响应，2 小时恢复；
2. P2 级（严重系统故障）：1 小时内响应，4 小时恢复；
3. P3 级（一般系统故障）：4 小时内响应，24 小时内恢复。

(二) 如遇特殊情况 24 小时内无法及时维修，须提供同品牌型号备用设备保障甲方使用。

(三) 培训服务：乙方负责免费为甲方培训操作及维修人员，包括：基本原理、操作使用和维修保养。培训时间与方式由双方另行协商确定。

(四) 质保期后：质保期结束后接到报修信息仍需 24 小时内到场维修，维修费用由双方协商确定。

第六章 违约责任

第 1 条 乙方延期交货

(一) 乙方须按本合同约定时间完成交货、安装调试和终验。

(二) 乙方延期交货的，每逾期一日应按合同总价的万分之五向甲方支付违约金；逾期超过 30 日的，甲方有权解除合同。

(三) 乙方因延期交货向甲方支付的违约金总额不超过合同总价的 5%。

第 2 条 甲方延期付款

(一) 甲方须按本合同约定时间向乙方支付款项。

(二) 甲方逾期付款的，每逾期一日应按逾期付款金额的万分之 0.84（不低于合同订立时 1 年期 LPR，当前为年利率 3%）向乙方支付逾期利息。

第 3 条 乙方其他违约责任。

(一) 乙方所提供的设备不符合合同约定的质量标准或技术规格的，甲方有权要求乙方免费更换或修复，乙方须在甲方提出更换或修复要求后 15 日内完成更换或修复，并承担因此产生的全部费用。

(二) 因乙方原因造成安全事故或第三方损失的，由乙方承担全部赔偿责任。

(三) 乙方将合同转包、分包的，甲方有权解除合同。

第七章 知识产权

第 1 条 知识产权归属。

(一) 甲方为本合同项下所开发软件系统的知识产权所有人。乙方须在终验前向甲方移交全部源代码、技术文档、系统运维手册等。

(二) 乙方所交付的通用设备（桌椅、空调等）原有的知识产权归属于乙方原制造商，不在本合同转让范围内。

(三) 乙方须保证其所提供的软件系统不侵犯第三方知识产权。如因乙方所提供软件侵犯第三方知识产权导致甲方损失的，乙方须承担全部赔偿责任（包括但不限于经济赔偿、诉讼费、鉴定费、律师费等）。

第2条 保密条款。

(一)甲乙双方应对合同执行过程中知悉的对方商业秘密和技术秘密负有保密义务,未经对方书面同意,不得向第三方披露。

(二)本合同保密义务在合同终止后继续有效,期限为三年。

第八章 争议解决与其他

第1条 争议解决方式。

(一)本合同适用中华人民共和国法律。

(二)因本合同引起的任何争议,双方应首先通过友好协商解决;协商不成的,任何一方可向甲方所在地有管辖权的人民法院提起诉讼。

(三)诉讼期间,除争议事项外,双方应继续履行本合同其他条款。

第2条 不可抗力。

(一)因不可抗力(包括但不限于:自然灾害、政府行为、社会异常事件等)导致一方不能履行本合同的,该方应在不可抗力发生后5日内书面通知对方,并提供相关证明。

(二)因不可抗力导致合同无法继续履行的,双方可以协商解除或部分解除合同,已完成工作量按合同约定单价结算。

第3条 合同变更与解除。

(一)本合同经甲乙双方协商一致,并签订书面补充协议后方可变更。

(二)合同实质性内容(金额、货物数量、技术规格、履约时间)不得随意变更;因客观原因确需变更的,须经政府采购监管部门批准。

(三)一方严重违约的,守约方有权解除合同。

第4条 合同的组成及生效。

(一)本协议书与下列文件一起构成合同文件,互相补充和解释,如有不明确或不一致之处,以次序在先者为准:

- 1、本协议书及附件;
- 2、中标通知书;
- 3、投标函及投标函附录、澄清文件;
- 4、招标文件
- 5、已标价工程量清单;

6、其他合同文件

在合同订立及履行过程中形成的与合同有关的文件均构成合同文件组成部分。

(二) 本合同自甲乙双方法定代表人或授权代表签字、盖章之日起生效。

(三) 本合同一式四份，甲乙双方各执两份，具有同等法律效力。

(四) 本合同附件为本合同不可分割的组成部分，与本合同正文具有同等法律效力。附件包括但不限于：

1. 技术规格书；

2. 分项报价表；

【以下无正文，为合同签署部分】

甲方：

(盖章)



法定代表人/授权代表(签字)：马丽

日期：2026年8月24日

乙方：

(盖章)



法定代表人/授权代表(签字)：[Signature]

日期：2026年8月24日

附件1：技术规格书；

采购一览表					
序号	产品名称	子系统模块	功能要求	数量	单位
1	网络安全综合演练系统	虚拟化组件(智慧防火墙)	1. 产品支持路由、透明、交换以及混合模式接入，满足复杂应用环境的接入需求。支持旁路模式； ▲2. 支持VTEP (VxLan Tunnel EndPoint) 模式接入VxLAN网络，并可作为VXLAN二层、三层网关实现VxLan网络与传统以太网的相同子网内、跨子网间互联互通；支持通过绑定VLAN、VNI (VXLAN Network Identifier)、远程VTEP，手动管理VxLan网络；支持MAC、VNI、VTEP静态绑定；（提供功能截图并加投标人盖公章） 3. 支持静态路由、策略路由。策略路由支持用户自定义其优先级；必须支持静态和动态多播路由，动态多播路由必须支持PIM-SM（稀疏模式） 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. 支持基于不同安全区域防御SYN Flood、UDP Flood、ICMP Flood、IP Flood、DNS Flood、HTTP Flood攻击，并支持警告、丢弃、普通防护、增强防护、授权服务器防护等多种防护措施。（提供功能截图并加投标人盖公章） 6. 能够对HTTP/FTP/POP3/SMTP/IMAP/SMB六种协议进行病毒查杀； 7. 支持自定义TCP、UDP、HTTP协议的漏洞特征，漏洞特征可通过多个字段以文本或正则表达式的形式进行有序和无序匹配，并可自定义漏洞的源、目的端口范围；同时可标识自定义漏洞的CVE编号或CNNVD编号。 8. 支持将告警信息以SNMP Trap、邮件、等形式通知管理员，告警信息的范围至少包括配置变更、病毒事件、攻击事件、异常事件、CPU利用率、内存利用率、硬盘利用率、接口带宽利用率、NAT端口池利用率等；	1	套
2		虚拟化组件(上网行为管理)	1. 可集中呈现上网行为风险等级和状态。行为风险等级包括安全等级、业务防护等级、合规等级和数据防护等级。行为状态包括管控效果、运行状态、安全状态、业务风险状态、外发状态和应用使用状态。 2. 为覆盖工作无关应用，移动应用不少于1000种，即时消息应不低于150种；为规避外发类风险，论坛发帖应不低于3000种，网络存储不低于100种，代理隧道不低于100种。 3. 根据关键字管理搜索引擎访问；一条策略实现搜索	1	套

		关键字的阻断、记录、告警，方便维护；支持配置免监控域名，用户在认证前即可访问免监控域名。 4. 支持对QQ、微信和百度网盘的PC客户端外发文件进行关键字过滤和封堵。 ▲5. 支持数据库审计，可审计、控制Oracle, MySql, SqlServer, PostgreSQL等数据库的访问与操作，包括添加、删除、修改、查询等。（提供功能截图并加盖投标人公章） 6. 支持通过DNS审计策略对DNS通信内容进行审计和控制；通过SNMP审计策略对SNMP通信内容进行审计和控制；通过NFS审计策略对NFS访问和传输文件进行审计和控制；通过NETBIOS审计策略对NETBIOS通信、登录名及文件、目录进行审计和控制。 7. 支持本地、LDAP、Radius、邮件认证方式的WEB认证。支持在界面上通过配置，将一台设备作为独立的认证服务器配合审计设备使用，提升认证性能。 9. 支持通过FTP和SFTP方式将日志导出到指定服务器，日志支持SSL加密和ZIP压缩，支持自定义导出数据的时间段和数据定时上传的频率。支持定义导出日志数据的范围、用户、位置和工具。 ▲10. 支持≥1.5 亿条 URL 数据。（提供功能截图并加盖投标人公章）		
3	基础课程资源包	1. 通过该课程包中所含课程的学习，使学生掌握计算机信息处理包括Linux操作系统、Mysql数据库的基本概念及应用，了解网络安全的威胁，掌握入侵检测、网络安全防护以及应急响应等基本安全技术。使学生具备Linux操作系统的应用能力，具备常用网络安全工具的使用能力，具备对实际数据库系统主要功能的实验验证能力，可以为信息系统的设计和实现提供网络安全防御机制，从系统的整个生命周期考虑网络安全问题，从而提高信息系统的安全性； 2. 包括不少于400个Linux操作系统及应用、Python开发技术、Windows Server系统管理、密码学基础、Mysql数据库、密码学应用、密码学算法编程、路由交换基础、数据库及系统加固、数据结构与算法、计算机网络、Web中间件漏洞实战、Web安全综合实战、Web渗透测试平台DVWA、Metasploit漏洞利用、Kerberos域安全、网络安全技术基础、Linux防火墙技术、Python安全脚本开发、入侵检测基础、网络攻防技术基础、网络攻防技术课程的实验或理论教学内容，可覆盖不少于700课时的教学。每个实验均须有对应知识点的实验环境及详细的实验指导手册，学生可自主地通过实验指导手册完成实验的操作练习。每个理论课程均需有连贯的理论讲解视频。	1	套

4	竞赛子系统A	1. 系统支持竞赛管理员对赛题的增删改查操作，支持单选题、多选题、判断题、CTF题、攻防题多种类型，支持单选题、多选题、判断题批量导入，支持对题目类型、难度、分类、能力点、题目内容描述和答案等进行编辑； 2. CTF题和攻防题环境支持容器和KVM两种虚拟化技术，自定义上传环境镜像，支持题目环境的参数配置，包括CPU、RAM、访问端口、管理端口、登录账号密码等；CTF题和攻防题支持自定义解题思路； 3. 攻防题支持自定义检测规则设置，支持检测协议和检测脚本上传两种方式，根据需求可使用HTTP、TCP检测协议从服务端口、期望输出、URL等方面设置，也支持使用脚本方式； 4. CTF题支持动态flag，可根据需求使用关联路径、修改变量、命令执行、curl、脚本执行等方式进行设置，CTF题目支持多附件上传，不同附件不同答案； 5. 系统支持管理员对竞赛任务的增删改查操作，竞赛任务配置主要包括竞赛名称、竞赛开始及结束时间、竞赛LOGO、竞赛形式、竞赛规则、竞赛题目、参赛团队或个人、计分规则、环境部署、展屏配置、协作管理人等信息； 6. 系统支持管理员自由组合理论赛、CTF赛和攻防赛模式，对赛前、赛中、赛后三个阶段的维护管理，实现对竞赛全流程的掌控，支持多场竞赛同时管理，支持多人协作管理一场竞赛； 7. 理论赛题目支持固定选题、随机选题、团队内分配三种选题下发策略，固定选题指每个参赛人员题目相同，随机选题指参赛人员每人题目不完全相同，团队内分配团队内成员题目不同，各团队之间题目相同； 8. 支持按题目类型、难度、分类和能力点筛选，同时支持排除已发布至训练的科目，避免比赛泄题； ▲9. 系统支持科目、竞赛双策略计分规则，CTF科目支持基础分和附加分规则设置，攻防赛支持初始分、固定得失分或零和机制设置；竞赛计分规则支持所得分值、所得分值/第一名所得分值两种基数计算方式，并分别设置理论赛、CTF赛和攻防赛分值系数，在比赛结束后按照系数相加实现相对合理的总分统计； （提供功能截图并加盖投标人公章） ▲10. 系统支持科目环境一键快速部署，根据参赛人员、科目类型自动分配虚拟机IP，并以拓扑和列表两种样式展示科目部署情况，支持CTF题和攻防题分开启动/关闭，支持单个科目环境重置；竞赛选手访问科目环境支持系统内置VPN和局域网两种方式；（提供部署前后功能截图并加盖投标人公章）	1	套
---	--------	--	---	---

		▲11. 系统支持赛前测试，管理员可将自己添加为竞赛选手进行答题测试，支持竞赛数据一键重置，清除赛前进行的答题记录、公告、成绩等一系列数据。（提供功能截图并加盖投标人公章）		
5	实训子系统	1. 课程小节内容支持设置关联能力点、建议学习时长、实验手册、实验拓扑、课件资料（PDF\MP4）、学习任务等信息，学习任务支持理论题的课后习题、探针任务和flag任务、附件任务四种类型；手册支持Markdown在线编辑和上传文件两种类型，Markdown类型的手册支持分步式实验手册设计，每一步可关联至学习任务，学员完成关联的学习任务后才能解锁手册的下一步，实现互动式学习。 ▲2. 支持课程资源重组，编辑课程时可引用公开的课程/小节，重新排列组合形成新的课程，可将所引用的小节另存后进行编辑，对原课程无影响；支持根据能力模型从课程库中将能力点相关小节快速重组成新课程。（提供功能截图并加盖投标人公章） 3. 支持云端课程更新，系统在联网情况下，支持通过云仓库下载/更新已购课程的最新版本，可查看已授权课程和未授权课程目录。 4. 教员可对当前课程学习模式进行个性化设置，自定义对学员开启/隐藏实验手册、实验环境、课件资料、学习任务等学习资源； 5. 支持自定义创建学习方案，也可继承系统内已有的方案进行修改，方案自定义多个学习阶段，每个阶段关联课程和测评试卷。系统支持以时序图的形式展示每阶段的课程间的关联关系。 6. 实验环境支持关闭和销毁两种方式，关闭实验环境在虚拟机中的操作自动保存，下次启动实验时可在上次实验操作基础上继续实验，支持教员统一销毁学员的环境和系统定时自动销毁环境两种销毁机制；	1	套
6	考试测评子系统	▲1. 支持多道仿真题共用一套题目环境，支持静态flag、动态flag、探测任务等多种答案形式；探测任务通过探针执行命令检测用户在虚拟机中的操作结果，动态flag通过关联路径、修改变量、命令执行或脚本执行等多种方式生成不同flag；（提供功能截图并加盖投标人公章） 2. 系统支持试卷管理，设置试卷名称、难度、分类、合格分值和组卷方式，组卷方式支持题库自选、策略组卷和模型组卷三种；题库自选组卷模式从题库中选择题目组成固定试卷，支持批量和单独设置题目的分值；策略组卷模式通过设置试卷题目出题范围，如选择题目类型、分类、能力点、难度和出题数量，根据策略规则从题库中自动选题生成试卷；模型组卷根据	1	套

		能力模型的能力点和权重要求自动生成出题策略和试卷； ▲3. 考试任务的配置信息包括设置考试难度、使用试卷、考试时间和考试对象；支持考试答题次数的设置，在开放时间段内可多次答题考试；支持填空题平台阅卷、人工阅卷两种方式；自定义设置是否允许考生在提交试卷后查看成绩或答案；支持同一场考试配置多套试卷，系统随机为每位考生独立分配试卷；针对同套试卷支持题目乱序功能；（提供功能截图并加盖投标人公章） 4. 考试任务中教员可查看考试人员提交状态和每个考试人员的试卷答题情况；支持教员清除已答题学员的答题记录，让学员重新答题；系统统计考试人员每次答题成绩及详情，支持教员修改学员答题成绩、导出成绩和试卷； 5. 考试任务中支持教员查看该场考试数据统计，包括实际考试人数、合格人数、平均分、平均答题时长、成绩分布、错误率前十题目统计等； 6. 学员统一在任务中心查看考试任务，学员进入相应考试任务进行答题，答题后在答题卡区域显示已答未答标识，可手动标记题目方便查看。		
7	定向课程资源包	▲7.1 数据安全课程资源包应对数据全生命周期实现全流程覆盖，包括获取、处理、分析、备份、监控、审计等。包含实验指导手册、实验场景、源码、视频、PPT、数据集、题库等。（需提供数据安全系列课程（包括但不限于《数据资产管理》《业务数据安全实践》《个人隐私数据安全实践》《企业数据安全保障与实践》《分布式系统数据安全保障与实践》《新一代信息技术对数据安全保障的实践》《隐私计算》等课程）的软件功能截图，以及课程详细目录的软件界面截图（加盖投标人公章）。要求所提供的软件界面截图清晰可见，并能够证明该产品的功能。） 1. 《数据资产管理》课程知识点包括但不限于： (1) 数据资产概述 (2) 数据资产分级分类 (3) 数据资产入表 (4) 数据资产管理系统应用 (5) 数据资产系统安装与设置 (6) 数据资产系统库设计 (7) 数据资产系统表设计 (8) 数据资产系统存储格式设计 (9) 数据资产系统数据加密策略 (10) 数据资产系统网络安全配置	1	套

		(11) 数据账户权限安全 (12) 数据资产密码策略安全 (13) 数据资产动态授权 (14) 数据资产日志监控 (15) 数据资产攻击日志分析 (16) 数据资产可视化地图 提供配套的源码脚本≥ 7套、数据集≥ 3套；每个知识点提供教学 PPT≥ 1个、教学视频时长$\geq 20\text{min}$、练习题≥ 10道、考核题≥ 5道； 2. 《业务数据安全实践》课程知识点包括但不限于： (1) 数据灾备与恢复 (2) 数据销毁策略 (3) 分布式存储安全 (4) 数据加密与数字水印 (5) 数字隐写技术 (6) 数据合规与审计 (7) 数字摘要与签名及时间戳 (8) 电子数据篡改 (9) 数据静态脱敏 (10) 数据动态脱敏 (11) 数据访问控制 (12) 数据访问接口认证 提供配套的源码脚本≥ 10套、数据集≥ 10套；每个知识点提供教学 PPT≥ 1个、教学视频时长$\geq 20\text{min}$、练习题≥ 10道、考核题≥ 5道； 3. 《个人隐私数据安全实践》课程知识点包括但不限于： (1) 个人数据隐私概述 (2) 个人隐私保护技术 (3) 身份验证 (4) 强密码策略 (5) 指纹及生物特征认证技术 (6) 多因子认证 (7) 人为加密传输 (8) 痕迹隐藏技术 (9) 交互数据流隐藏 (10) 数据匿名化 (11) 隐私数据备份与存储 (12) 隐私数据清理策略 提供配套的源码脚本≥ 12套、数据集≥ 12套；每个知识点提供教学 PPT≥ 1个、教学视频时长$\geq 20\text{min}$、练习题≥ 10道、考核题≥ 5道； 4. 《企业数据安全保障与实践》课程知识点包括但不限于：	
--	--	---	--

		(1) 企业数据安全概述 (2) 企业数据安全保障措施 (3) ELK 环境搭建 (4) Logstash 日志搜集配置 (5) Kibana 日志数据可视化		
		(6) ELK 日志安全分析 (7) 日志搜集与合规性 (8) 系统日志监控技术 (9) 文件完整性监控技术 (10) 系统性能监控技术 (11) 系统异常负载监控技术 (12) 访问控制审计 (13) 数据加密审计 (14) 数据库审计 (15) 灾备策略审计 (16) 安全日志集成告警 提供配套的源码脚本≥ 12 套、数据集≥ 12 套； 每个知识点提供教学 PPT≥ 1 个、教学视频时长$\geq 20\text{min}$、练习题≥ 10 道、考核题≥ 5 道； 5. 《分布式系统数据安全保障与实践》课程知识点包括但不限于： (1) 分布式与大数据系统安全风险概述 (2) 大数据安全保障关键技术 (3) ApacheRanger 环境搭建、策略配置与访问控制 (4) 大数据分布式文件系统安全认证 (5) 数据仓库 Hive 的安全认证 (6) HBase 服务的安全认证 (7) Hbase 服务安全认证 (8) Kafka 的多用户访问控制与数据加密 (9) 分布式资源调度平台集成 YARN 服务的安全认证 (10) Storm 集成 Ranger 的实时计算安全认证 (11) Solr 的文档级安全认证与加密 (12) Apache Ranger 的审计与合规性管理 提供配套的源码脚本≥ 10 套、数据集≥ 6 套； 每个知识点提供教学 PPT≥ 1 个、教学视频时长$\geq 20\text{min}$、练习题≥ 10 道、考核题≥ 5 道； 6. 《新一代信息技术对数据安全保障的实践》课程知识点包括但不限于： (1) 人工智能技术在数据安全中的应用 (2) 区块链技术在数据安全中的应用 (3) 基于系统可执行文件的防护分类 (4) 基于多分类的恶意软件处理 (5) 基于深度学习的恶意软件分类		

- (6) 基于 DGA 恶意域名的分类处理
- (7) 基于注入的分类处理
- (8) 基于 SWF 文件的分类处理
- (9) 浏览器指纹聚类分析
- (10) 基于可执行文件的聚类分析
- (11) 基于区块链交易的异常检测
- (12) 基于文件加密勒索软件行为分析

提供配套的源码脚本 ≥ 10 套、数据集 ≥ 10 套； 每个知识点提供教学 PPT ≥ 1 个、教学视频时长 $\geq 20\text{min}$ 、练习题 ≥ 10 道、考核题 ≥ 5 道；

7.《隐私计算》课程知识点包括但不限于：

- (1) 隐私计算概述
- (2) 联邦学习
- (3) 同态加密
- (4) 零知识证明
- (5) 多方计算
- (6) 可信执行环境

7.2上网行为管理课程提供不少于40个实验任务可覆盖不少于50课时的实验教学，包含功能验证型实验、场景实验和综合实验，功能验证型实验与理论课程一一对应，帮助学生通过简单的场景理解和掌握上网行为管理的主要安全功能，包括：部署方式、用户管理、行为管理、流量管理、日志分析、系统维护六个方面，使学生了解上网行为管理的基础安全功能，具备基础的配置管理能力。场景型实验基于客户的真实使用场景，结合客户上网行为管理的方法，通过设计实验场景、业务需求和任务目标，尽可能真实的模拟金融、大企业、中小企业、高校四类客户使用上网行为管理设备的思路和方法。在学生对上网行为管理的基本安全功能有了一定的理解之后，通过四个场景将前序所学的独立安全功能进行有机串联，通过分析实验中所描述的客户需求，整理出实验的目标，设计实现思路和步骤，达成实验目标，加深学生对上网行为管理底层逻辑、技术原理的理解。为了尽可能真实的模拟客户的使用方法，场景实验中所涉及的部分安全功能可能尚未包含在功能验证型实验中。目的在于让学生能够切实的感受不同的客户所面临的不同的问题，以及上网行为管理系统所提供的不同的解决方法。综合实验则是对功能验证型实验中所涉及的重要安全功能进行综合运用，检验学生的学习效果。通过合理的实验场景、实验需求、实验目标的设置串联相关安全功能，具备场景实验的所有特点，即可做为课程学习完成后的综合运用训练适用，也可作为课程评

		价中上机实操考试使用，根据实际授课需求决定适用场景。 7.3. 通过上网行为管理课程的实践教学，培养学生学习上网行为管理的相关知识，理解行为安全管理技术产生的背景、意义、价值和实现思路。通过学习上网行为管理设备的基本功能、配置方法、工作原理，包括识别技术、控制技术和分析技术，理解上网行为管理相关的理论知识与配置技术。通过高度仿真的教、学、做一体化的情境教学模式，通过功能验证型实验、场景实验和综合实验，使得学生了解行为安全管理的基本思想，具备对上网行为日志的数据分析能力，具备典型网络场景下的上网行为管理设备部署能力。学生通过对上网行为管理的实验、实践操作，积累解决实际问题的工作经验，加深对理论知识的理解，在学生的实践能力培养和综合素质培养方面起到重要的支撑作用； 7.4智慧防火墙课程资源包 1. 智慧防火墙课程需提供不少于10个实验任务可覆盖不少于30课时的实验教学，采用循序渐进的模式，学生通过任务制模式阶段性对防火墙安全产品的功能和技术进行应用，主要涉及“三大模块，十个场景”，三大模块包括防火墙初始化配置、防火墙网络功能部署和防火墙安全功能应用，其中防火墙初始化配置模块涉及防火墙基本配置场景，涵盖知识点包括防火墙部署方式、初始化配置、安全域等相关内容，解决用户对于防火墙在出厂零配置状态下需要进行的初始化配置操作等相关问题；防火墙网络功能部署模块涉及路由通信、透明部署、网关多出口与流量管理、DNS域名解析、目的NAT映射共5个实验场景，涵盖知识点包括三层路由模式、二层透明网桥模式、DHCP服务、地址转换、QoS、DNS透明代理等内容，解决防火墙在信息系统网络边界出口关键位置需要发挥的网络通信功能和访问控制能力；防火墙安全功能应用模块涉及安全防护、访问控制、安全认证与审计和SSL VPN搭建共4个实验场景，涵盖知识点包括安全配置文件（行为管控、关键字过滤、内容过滤、文件过滤、邮件过滤、URL过滤）、安全认证、攻击防御（恶意扫描防御、流量型攻击防御、应用层Flood攻击防御）等相关内容，解决企业网络内部应用管理、敏感信息管控、网络安全威胁等安全风险，实现提高企业信息系统安全性的目的； 2. 智慧防火墙课程通过高度仿真的教、学、做一体化的场景化教学，培养学生学习企业网最典型的边界安全设备——防火墙的相关知识、技术，使学生掌握企业	
--	--	--	--

		网络安全域的划分、防火墙的网络部署、防火墙的策略配置、防火墙安全防护与运维等操作技术。该课程在实验操作部分中提供了丰富的知识点内容补充，可以加强学生对于防火墙技术的理解 and 应用。学生通过对防火墙设备的配置操作，积累解决实际问题的工作经验，学习深入的专业理论知识，培养和提高学生的安全能力和综合素质； 7.5应急响应课程资源包 1. 应急响应课程的设计从应急响应准备工作开始，逐步介绍系统备份、系统安全加固、webshell分析与检查、日志分析、流量分析、恶意软件分析与扫描以及网页篡改应急响应等方面的内容，提供全面的网络安全应急响应的学习环境，帮助学生掌握处理紧急情况、保障系统安全的必要知识和技能。包含不少于16个实验可覆盖不少于30课时实验教学； 2. 为了便于教学的开展，课程除以上实验内容外，需提供可编辑版本的教学大纲及配套教学PPT，并可在系统中直接下载，教学PPT按照章节分多个文件。		
8	竞赛题库	1. CTF题支持动态flag，可根据需求使用关联路径、修改变量、命令执行、curl、脚本执行等方式进行设置，CTF题目支持多附件上传，不同附件不同答案； 2. 包含不少于280道CTF题目、40道攻防题、1200道理论题。其中CTF题目中包含CRYPTO题目≥50道、MISC题≥50道，PWN题≥60道，REVERSE题≥60道，WEB题≥60道。攻防题目中包含PWN题和WEB题各不少于20道。理论题中包含单选题≥500道、多选题≥500道、判断题≥200道。	1	套
9	竞赛子系统B	▲1. 系统支持竞赛管理员对竞赛开始/暂停状态进行控制，支持准备模式、全通模式、解题模式、解题+加固模式、加固模式、攻防模式的网络控制，各模式之间一键配置，分别对系统、题目进行访问控制、环境隔离控制；（提供功能截图并加盖投标人公章） 2. 系统支持对题目状态进行管控，可设置题目是否下发/收回，是否对比赛人员显示/隐藏； 3. 支持管理员查看参赛人员的题目环境，对题目环境进行启动、关闭、重置操作，记录环境启动、关闭和重置次数； 4. 系统支持多种防作弊机制，包括竞赛各阶段的网络控制、动态flag、攻防赛题目环境异常状态检测、参赛人员来源IP验证、赛后提交Writeup等多个方面。 5. 系统支持来源IP段输入验证、登录绑定，实现各团队题目环境隔离，支持来源IP启用/不启用、清除IP等操作； 6. 支持对个人/团队进行加减分作为奖励或违规处	1	套

		罚，特殊人员/团队给予禁赛处理； 7. 支持竞赛公告管理，支持向全员或指定对象发布公告，支持一般、中等、重要多级别设置，重要公告弹窗提醒参赛人员； 8. 系统支持竞赛中题目答题详情、团队答题详情的管理，CTF题支持基础分、附加分、正确率、提交次数、提交时间、提交答案等数据记录展示，攻防题支持攻击成功次数、防守失败次数、答题状态、得分、失分等数据记录展示； 9. 系统支持实时排行榜展示，分值默认由高到低展示，支持积分得失分数据及得失分原因统计； 10. 系统支持竞赛结果管理，展示个人榜单、团队榜单、writeup，支持数据导出，各竞赛阶段成绩分开统计，并依据各阶段系数合算总得分； ▲11. 系统支持B/S和C/S两种架构且不同风格的CTF赛和攻防赛3D可视化大屏展示，展示数据主要有答题动态、攻击路径、排行榜、得分趋势、得分详情等，布局上适用不同团队数量、不同题目分布，支持16：9和32：9两种规格展示效果。（提供功能截图并加盖投标人公章）		
10	管理子系统	1. 系统采用B/S架构，支持账号密码登录；多个业务模块如教学实训、考试测评、攻防竞赛、场景演练等共用底层服务及硬件资源； 2. 支持账号管理，录入账号信息（如用户名、姓名、组织机构、团队、角色、性别、证件号、手机号、邮箱、密码等），支持按组织机构和角色筛选账号，账号批量启用/禁用、批量导入账号，批量导出账号信息，查看在线/离线用户，针对每个账号设置IP白名单，支持一键下线在线人员； 3. 支持多层级组织机构管理，组织及其下级的创建、删除、编辑，各级组织可自定义移动实现层级切换； 4. 支持团队管理，上传团队logo、添加、删除团队成员，可启用/禁用团队，团队数据可批量导入、导出； ▲5. 支持自定义角色管理，自定义角色名称及模块权限配置，支持用户角色为维度的计算资源权限配置，针对不同角色设置最多启动拓扑环境数量，保障虚拟计算资源的合理分配；（提供功能截图并加盖投标人公章） 6. 支持系统日志管理，日志记录信息至少包括时间、用户名、访问IP、操作详情等； ▲7. 支持系统安全管理，密码相关配置包括密码输入错误次数限制、密码输入错误导致账号冻结时间、密码复杂度要求、密码有效期、密码过期前提醒、历史密码验证次数、首次登录是否需要修改密码等；其他	1	套

		配置包括系统日志保留时间、登录有效时间、实验环境自动销毁时间、硬盘容量告警比例、使用内存告警比例和虚拟机控制台文件管理功能开放控制等；（提供功能截图并加盖投标人公章） 8. 支持系统配置管理，配置服务器IP、修正服务器时间，配置可访问系统的IP白名单，SSH端口支持在WEB管理界面开启和关闭，支持在WEB管理界面中通过开关控制禁用root账号直接登录SSH，系统中SSH登录每次成功或失败的记录，记录在系统日志中； ▲9. 支持系统状态检测，检测集群中每台服务器CPU\VCPU\内存\磁盘的使用情况，检测关键服务的运行状态，包括但不限于虚拟化服务、探针服务、存储服务；（提供功能截图并加盖公章） 10. 支持性能管理，展示各任务对系统性能的占用情况，统计来源模块、任务名称、占用人员、占用VCPU、占用内容等信息，并提供批量关闭及销毁功能用于资源释放； 11. 支持页面上传软件升级包实现系统版本升级； 12. 支持仪表盘统计展示，展示系统各种任务和资源数量，包括但不限于课程任务数、考试任务数、竞赛任务数、演练任务数、课程资源数、考试题数、竞赛题数、工具数、能力点数、虚拟机数、漏洞靶标数、系统用户数等；支持可视化图表展示能力模型能力覆盖率各阶段人数统计； ▲13. 支持为每个学员生成能力画像，以雷达图形式展示展示学员能力等级测评达标情况；统计学员在全平台完成任务获得的能力点，并以可视化形式展示学员所掌握能力在各能力模型中的覆盖率情况。（提供功能截图并加盖投标人公章）			
11	网络空间安全实战对抗系统	攻防演练	1. 功能要求： （1）支持课程库管理，提供个人模板和公开模板两种管理形式，公开模板数据支持全部用户调度使用，个人模板数据仅用户自己可见，支持将个人模板数据转换为公开模板数据以实现分享或将公开数据转为个人模板数据进行个性化编辑。 （2）支持实操类课程关联多个拓扑，可为不同的实验绑定不同拓扑，满足不同实验的独特业务需求，从而缩小课程绑定单拓扑规模。提供实验指导书，支持进行分步设计，提供强制校验功能，开启后学员需按步骤完成不可略过。 （3）支持预览测试，实现对已编排完成的课程的查看和测试，管理员通过生成的URL链接可以体验学员进入课程的学习效果，实现对课程的检查和测试。 （4）教师可查看统计分析的教学数据，包括课程数	1	套

		量、自由学习及排课课程数量、学员数量。支持通过各类图表对教学数据进行分析，包括不限于饼状图、环状图、条形图、表格等。支持展示自由学习热门课程TOP10、展示各个学员学习课程数量及课程完成率情况。 (5) 学员可通过交流讨论功能进行信息发布，并支持上传附件。教员可对学员交流讨论功能进行回复。学员可将发布的信息添加到笔记，支持笔记删除功能，学员可在用户中心查看笔记内容。 (6) 支持创建教师教学模式的课程，支持教师进行课程排课日程的创建，支持查看相关排课信息，排课信息支持按照月、周两种日历形式查看，也支持列表形式查看。 ▲ (7) 创建教学模式的实验课程时，支持开启环境自动部署选项，开启后将根据教师配置的提前部署时间，在课前自动启动学员实验环境，有效避免课堂等待，确保流畅教学；支持开启屏幕录像选项，开启后对学员操作终端界面进行实时录屏，录屏文件支持教师在线查看，便于教学指导。（提供功能截图并加盖公章） (8) 支持教师排课冲突校验，提供冲突提示信息，支持根据冲突情况重新修改排课信息或支持忽略冲突继续创建。 (9) 排课支持设置可参加的学员，被选定的学员方可进入该课程进行学习，未加入的学员看不到该课程。 (10) 支持教师对场景实例进行资源监控及资源回收。支持从已关联拓扑中选取要启动的拓扑进行启动，启动过程中支持展示启动进度和启动状态，支持查看已启动实例清单、网络清单及启动日志。实例清单包括靶标名称、节点名称、实例IP、设备类型、启动时间、状态和操作等内容，操作包括对实例进行重启、重置、错误日志、可视化查看（开机、暂停、恢复、重启、强制重启、关机、强制关机、重置、复制、粘贴、文件导入、文件下载）；网络清单包括实例网络、实例网段、关联靶标数、状态以及操作；启动日志包括阶段、信息、时间、用时、状态以及操作。支持批量回收学员拓扑实例。 (11) 提供操作日志查看功能，包括不限于课程创建、课程发布、启动拓扑、进入课程等关键操作。操作日志记录了操作用户及角色、操作内容、操作时间、操作结果等信息，确保操作可追溯。 (12) 提供屏幕共享功能，支持教师将操作机共享给全部学员进行课程讲解。提供屏幕接管功能，教师能		
--	--	--	--	--

	够对学生的实验操作进行远程协助，以弹窗的形式展示，支持最大化展示。可对操作机界面进行控制，包括开机、暂停、恢复、重启、强制重启、关机、强制关机、重置、粘贴、文件导入、文件下载。支持屏幕监控功能，可查看学员操作机界面的实时监控。 (13) 学生进行实验课程学习时，支持实验指导书及操作终端同屏展示，学员可根据实验指导书内容，完成实验课程。实验指导书可展开可折叠，也可小窗悬浮展示。支持对操作终端进行全屏展示，支持切换操作机。 (14) 每个用户学习环境隔离，且相同实验课下不同用户的网络配置完全一致，保证是操作的一致性。 (15) 学员能够按照月、周两种日程形式查看课程课表，支持前后切换月份和周次，默认显示当天所有课程，便于学员学习指定课程。 (16) 支持创建学习地图模式的课程，支持教师按照课程体系对学习地图进行课程组织，包括课程顺序调整、添加移除等操作。用户可按照当前学习地图提供的课程进行体系化的课程学习。支持学员学习不同内容的课程，包括但不限于：图文、视频、文档、实验、测验等。支持学员课程测验，测验题型包括但不限于：单选、多选、判断、填空、简答。学生进行实验课程学习时，支持实验指导书及操作终端同屏展示，支持对操作终端进行全屏展示，支持切换操作机，支持实验指导书悬浮展示。 (17) 支持关卡设置，实现不同阶段的学习内容分级，通过逐层关卡学习，低关卡课程学习完成方可进入高关卡课程学习。 2. 性能要求： (1) 实网攻防资源包包括但不限于： 1) 单域安全实战课程实验场景 ①. 实验场景整体设计思路为：通过域成员主机，定位出域控制器IP及域管理员账号，利用域成员主机作为跳板，扩大渗透范围，利用域管理员可以登陆域中任何成员主机的特性，定位出域管理员登陆过的主机IP，设法从域成员主机内存中dump出域管理员密码，进而拿下域控制器、渗透整个内网。 ②. 实验场景需至少包括入口点攻击、SMB中级攻击、缓存票据和攻击域控等4个实战阶段。 ③. 实验场景需具备gitlab漏洞getshell，内网代理、内网渗透、SMB中继攻击、后门远程、权限获取，权限维持等安全技能知识点。 ④. 实验场景需提供配套实验环境和操作指导书。 2) APT-C-36项目实战实验场景	
--	---	--

		①. 实验场景整体设计思路为：主要模拟和复现 APT-C-36组织的攻击过程，包括连接代理服务器、制作带有恶意宏的MHTML格式的OfficeWord诱饵文档、带有密码压缩文档、发送钓鱼邮件等步骤。 ②. 实验场景需至少包括邮箱信息收集、代理服务器、C2远程服务登录、木马生成、构造恶意文档、部署钓鱼邮件、数据渗出等7个实战阶段。 ③. 实验场景需内置大灰狼远程管理软件、proxifier、nginx、winrar、foxmail、7-zip等配套工具资源，方便学生在操作时直接调用使用。 ④. 实验场景需提供配套实验环境和操作指导书。 (3) 医疗行业内网演训实战实验场景 1) 实验场景整体设计思路为：以kali攻击机和win7攻击机作为外部操作机，对邮箱进行钓鱼，通过抓取目标的用户名密码从而远程登陆目标主机，登陆后，再通过目标浏览器保存的账号密码登陆医院的HIS系统，通过医院HIS系统的文件上传漏洞获取医院HIS系统的服务器权限。 2) 实验场景需至少包括MSF钓鱼、权限获取、内网横向等3个实战阶段。 3) 实验场景需内置msfconsole、foxmail邮件系统、python3，代理工具proxifier等配套工具资源，方便学生在操作时直接调用使用。 4) 实验场景需提供配套实验环境和操作指导书。 (4) 高校内网项目实战实验场景 1) 实验场景整体设计思路为：以邮件钓鱼为切入点，获得内网的跳板，通过mimikatz抓取系统密码来远程登录内网系统，然后收集受害者的浏览器书签记录和密码记录，横向到内网服务器和数据库。并且通过UDF提权获得数据库的SYSTEM权限。 2) 实验场景需至少包括钓鱼邮件、内网潜入、内网横向移动、UDF提权等4个实战阶段。 3) 实验场景需内置MSF、mimikatz、proxifier、Navicat Premium 15、蚁剑、burp suit等配套工具资源，方便学生在操作时直接调用使用。 4) 实验场景需提供配套实验环境和操作指导书。 (5) 政务内网实战实验场景 1) 实验场景整体设计思路为：以kali以及win7攻击机作为外部操作机，对其中一台办公机进行钓鱼，远程连接，继续连接到内网中的另一台办公机中，进行FTP渗出。 2) 实验场景需至少包括MSF木马、代理远程登录、文件后门设置、权限维持、FTP文件爆破等5个实战阶段。 3) 实验场景需至少具备CVE-2017-11882的漏洞利用、		
--	--	---	--	--

		以及相关配套工具。 4) 实验场景需提供配套实验环境和操作指导书。		
12	人员能力评估	1. 系统支持对用户岗位匹配进行基于知识和技能画像，包括但不限于展示胜任岗位数据、岗位匹配雷达图、知识和技能获取曲线及日志。 2. 支持基于任务、知识、技能层面的人员评估维度，进行用户岗位匹配的人员能力画像。 3. 支持岗位能力评估模型，系统根据用户完成任务的情况进行知识、技能、能力的分析匹配，结合网络安全从业人员能力基本要求进行岗位模型搭建，支持根据岗位类型调整评估权重，形成岗位能力匹配度画像。 4. 系统支持基于ATT&CK、D3FEND的技术策略值分析个人的多维度能力，可将评估人员的攻击效能、防御效能情况进行“数字化”呈现。 5. 提供岗位能力评估框架，支持用户自定义创建岗位标准，支持自定义岗位、任务、知识及技能，支持用户配置岗位与任务的关联关系、配置岗位对应任务达标值、配置任务与知识、技能的关联关系，支持创建多级知识及技能。 6. 提供评估模型框，支持用户自定义创建自有岗位标准。支持创建标准，定义标准名称及标准编号，并对标准进行描述以说明标准的适用场景。支持自定义岗位、任务、知识及技能，实现岗位与任务、知识、技能之间的定义，完成岗位定义。 7. 支持针对于标准进行知识的基础数据添加，支持对知识添加子知识，以实现知识的归类，支持对技能添加子技能（最多支持三层）以实现技能的归类。 8. 支持针对于标准进行任务的基础数据添加，支持将知识和技能与任务进行关联，实现对完成任务需具备的知识和技能的定义。 9. 支持对标准添加岗位，并赋予岗位需要完成的任务并设置任务达标值，同时支持对岗位设置前置任务，实现对岗位的定义。 10. 提供1套人员能力评估模型，评估模型覆盖GB/T42446《信息安全技术-网络安全从业人员能力基本要求》国家岗位标准中的五大类十五个岗位，网络安全管理类岗位，包含网络安全管理人员、数据安全保护人员、密码应用人员、网络安全咨询人员；网络安全建设类岗位，包含网络安全架构设计人员、网络安全开发集成人员；网络安全运营类岗位，包含网络	1	套

			安全运维人员、网络安全监测分析人员、网络安全应急管理人员；网络安全审计和评估类岗位，包含网络安全审计人员、网络安全测评人员、网络安全认证人员、电子数据调查取证人员；网络安全科研教育类岗位，包含网络安全科学研究人员、网络安全培训人员。		
13		系统管理	1. 支持记录系统日志，涵盖系统内核、中间件服务、基础设施服务、扩展功能服务等日志类型，以时间、级别、主机名、程序名、进程号维度展示，可查看详情，支持一键清除、下载日志。 2. 能够按系统日志级别配置消息推送方式，支持推送至指定的Syslog服务器或发送平台的系统消息给管理员用户两种形式。 3. 支持管理员发送系统公告，系统公告发送后该租户下全部用户可查看。 4. 控制节点磁盘空间不足时，系统将给出醒目提示，并提供快速处理方案供用户选择快速处理。 5. 支持用户管理功能，支持对用户信息进行批量导入、导出操作。支持对账号有效期进行设置。支持账号赋予用户组，从而赋予账号对应的平台权限。提供用户注册入口，可对注册账户信息进行审核，审核未通过用户无法登录系统。 6. 系统采用多因子认证机制，用户登录时，需先通过账号密码完成基础验证，接着输入动态口令，双重校验通过方可进入系统；若为初次登录，需先完成账号绑定，再按上述“账号密码+动态口令”方式登录。 7. 支持对系统进行个性化配置，包括系统展示背景、主题色彩、登录页名称、登录页logo、登录页登录信息布局、浏览器标题及图标等。	1	套
14		网络仿真	1. 功能要求： (1) 支持系统管理员对镜像文件数据进行查看及管理，支持硬盘镜像（qcow2、ova、raw、vdi）、容器镜像、光盘镜像（iso）、LXC镜像（gz、tar）的管理，支持镜像文件的断点续传能力。 (2) 支持虚拟靶标管理，提供两种创建方式，包括向导式靶标设置以及基于模板快速创建。新建靶标时，支持根据靶标类型进行镜像文件的推荐检索。 (3) 支持8种靶标控制操作，包括开机、关机、暂停、恢复、重启、强制关机、强制重启、重置等，支持3种靶标信息输入输出操作，包括复制、粘贴、文件导入等，支持对配置完成的靶标进行远程接入方式切换。 (4) 虚拟靶标支持打开虚拟桌面进行编辑，编辑完成后，使用另存为功能生成基于差分磁盘技术的新靶标模板，减少资源占用。支持对靶标错误日志进行集	1	套

中展示。

(5) 支持配置及展示靶标的服务映射信息，支持TCP/UDP协议映射，支持快速配置常用的应用层协议映射，包括HTTP、HTTPS、RDP、FTP等映射信息，支持用户通过本地主机直接访问虚拟靶标的服务或桌面。

▲(6) 提供网盘功能，实现本机与靶标管理中的任一靶标的数据共享，实现数据的上传下载，每个靶机都可访问这个网盘进行数据交互。（提供功能截图并加盖投标人公章）

(7) 支持通过拖拽的方式进行可视化网络拓扑设计，支持对网络节点的网络接口数量进行动态调整，支持在链路线条的两端显示接口名称及IP地址，可快速查看连接信息。

(8) 支持IPv4和IPv6双栈模式，支持是否开启IPv6模式。拓扑支持连线模式二层、三层模式，二层模式解决小型局域网构建，支持access/trunk两种端口模式的设置；三层模式通过IP路由实现跨网段通讯，支持大型网络构建。支持链路仿真配置，内容包括带宽、延迟、丢包率。

▲(9) 支持在拓扑启动状态下的实时编辑，支持添加或删除网络配置以满足网络连通性测试或验证，支持添加和删除连线以满足网络架构的动态调整，支持替换节点后重新绑定靶标以满足替换设备的需求。

（提供功能截图并加盖投标人公章）

(10) 提供拓扑发布，支持根据实际的用户操作需要进行对应靶机的发布，以避免拓扑实例删除后靶标编辑数据丢失或误删。支持拓扑快照，可将当前拓扑状态保存为快照，并在需要的时候将拓扑恢复到保存快照时的状态。

(11) 支持提供当前拓扑中的靶标节点清单，节点清单支持按照拓扑架构进行分级展示，支持通过节点清单进行整个拓扑节点数据的查看，支持根据节点名称进行快速搜索定位，支持将选中的节点在画布进行同步定位展示，支持对节点进行批量启动等操作。

(12) 提供三种拓扑启动方式，包括全部启动、部分启动及仅启动网络，部分启动支持用户按需选择启动节点。节点启动后，清单中设备的图标及名称会变色，在部分启动状态下以区分哪些靶标已启动哪些未启动。

(13) 支持在拓扑绘制过程中对拓扑中全部靶标的服务映射情况进行集中查看，便于在拓扑调试过程中快速调度使用。支持以列表展示，支持对映射HTTP和HTTPS协议类型映射成功后点击跳转展示。

		▲ (14) 支持可视化配置全局DNS解析, 支持A、TXT、ALIAS、CNAME、MX五种解析类型, 无需在网络中加入独立的DNS服务器、无需为单机或DHCP网络配置DNS地址, 即可由系统自动完成DNS解析模拟真实的Internet网络。(提供功能截图并加盖投标人公章) (15) 支持日志采集、流量采集及通用协议采集, 支持对不同维度数据的采集与查看, 可用于数据分析, 在网络仿真中采集的数据隔离存储。 (16) 支持12种日志采集内容, 包括系统日志、CPU利用率、内存利用率、磁盘利用率、网络流量、开放端口、网络接口、主机信息、进程状态信息、TCP链接信息、UDP链接信息、文件变化信息。 ▲ (17) 支持流量采集设置, 支持用户自定义采集数据范围, 采集完成数据自动存为流量数据包进行展示。支持对流量数据进行可视化查看及下载, 包括数据包列表(包含时间戳采集时间, 源IP, 目标IP, 协议, 长度, 信息)。(提供功能截图并加盖投标人公章) (18) 支持流量生成, 可配置源目的IP及端口, 支持采用2种方式进行流量生成配置, 包括选择内置模板或用户自定义设置, 自定义设置支持选择ipv4、802.1Qtag、tcp、udp、http等协议, 支持对数据包数量、频率等参数设置。 2. 资源要求: (1) 内置硬盘镜像20个, 包含Windows7、Windows10、Windows11、WindowsServer2008、WindowsServer19等Windows系统10个, CentOS、Ubuntu、RedHat、Kali等Linux系列10个; 容器镜像3个, 包含DockerNginx、DockerMysql、DockerAlpinelinux; 光盘镜像20个, 包含Windows和Linux常见版本; LXCUbuntu镜像1个。 (2) 提供基础靶标20个, 涵盖Windows、Linux等常见操作系统类型; 包含Windows7、Windows10、Windows11、WindowsServer2008R2、WindowsServer2012R2、WindowsServer2016、WindowsServer2019、KaliLinux、Centos、Ubuntu、RedhatLinux等常见主流版本操作系统。 (3) 提供漏洞靶标200个, 包含数据库、浏览器、文档、IOT设备、移动终端、应用软件和WEB等类别, 包含身份绕过、代码执行、越权、远程命令执行、缓冲区溢出、SQL命令注入、文件读取、密码重置、拒绝服务、目录遍历、信息泄露、权限提升、反序列化等常见漏洞。 (4) 提供应用靶标60个, 包含数据库、Web、邮件服务、中间件、终端软件、杀毒软件、办公软件和工控	
--	--	---	--

		等类别，包含Mysql、postgres、redis、mongo、finecms、greencms、74cms、taocms、hms、wdjacms、eyoucms、emlogcms、cmseasy、dedecms、seacms、genixcms、wordpress、lcewarp、exchange、apache、nginx、zentaoOA、通达OA、phpstudy、finalshell、火绒安全、360杀毒、openvpn、openpic、kingview等常见应用靶标。		
15	资源库	1. 流量包管理 (1) 支持用户自定义上传流量包，支持对流量包进行标签设置，用于流量的分类划分及便捷筛选。 (2) 支持批量上传流量包。 (3) 支持将公开模板的流量包进行导入、导出操作。 2. 工具管理 (1) 支持工具管理功能，支持创建、编辑、删除、预览等管理能力。支持对工具进行发布操作，发布的工具支持用户进行查看。支持对工具进行收藏。 (2) 支持对工具的软件版本进行管理，支持上传对应版本和支持平台的软件包，用于用户查询筛选下载使用。 (3) 支持对工具进行下载，支持根据平台和系统进行软件包筛选。 (4) 支持将公开模板的工具进行导入、导出操作。 (5) 内置不低于300个常用安全攻防工具，类型包含VPN工具、Webshell管理工具、爆破工具、代理工具、代码审计工具、恶意行为系统检测工具、解密工具、漏洞检测工具、漏洞利用工具、漏洞扫描工具、密码破解工具、免杀工具、目录爆破工具、逆向破解工具、数据库管理工具、网络协议工具、嗅探欺骗工具、溢出提权工具、远程控制工具、资产探测工具、字典生成工具、域名与子域名搜索工具；提供windows、linux、vmware ESX和macOS等常用平台多版本下载地址。	1	套
16	漏洞库	1. 支持漏洞管理，包括创建、编辑、删除等，支持对漏洞进行发布操作，发布后的漏洞支持用户进行查看，支持检索含有利用代码（Exploit）或概念性验证（PoC）的漏洞数据。 2. 内置超过25万条漏洞数据，其中11万条以上具备CVE以及CNNVD标识映射。涵盖近十年CNNVD发布的低、中、高危漏洞，包含攻击向量、攻击复杂度、身份认证、机密性影响、完整性影响、可用性影响的CVSS标准漏洞评分，不少于900多条Category、Base、Variant、Class、Pillar、Composite、Chain等类型的CWE漏洞信息。 3. 内置超过2万个高质量漏洞数据，包含但不限于漏	1	套

			洞利用代码类、远程代码执行利用exp、本地代码执行利用exp、web漏洞代码执行exp、ddos相关漏洞利用代码、shellcode利用代码等类别。		
17		仿真引擎	1. 采用标准B/S架构设计，支持Chrome、火狐、Edge（87.0+版本）等主流浏览器访问，确保跨平台兼容性。 2. 提供离线热升级功能，支持补丁包/版本包静默安装，升级过程中不中断虚拟靶标运行。 3. 支持利用集群的闲置算力对平台中的应用进行扩容，可以在可视化界面选择一台或多台计算节点安装应用，实现应用的性能提升和高可用，可以在可视化界面看到每台计算节点已安装的扩容应用的数量。 4. 系统支持对集群状态进行监控，支持展示集群服务器的IP、节点类型、配置、vCPU占用、内存占用、存储占用、延迟、状态等信息，提供对单个计算节点的详情查看，以折线图形式展示对应CPU占用、内存占用、存储占用以及存储的读取和写入速度的使用趋势情况。 5. 支持对以太网设备接入面板设备的集中管理，支持将接入面板设备与租户进行绑定，实现租户通过网络仿真进行该设备的接入面板使用。	1	套
18		态势控制	1. 支持对图表进行位置自定义编排，可根据实际的展示需求进行图表的可视化配置。支持配置多个展示方案，通过拖拽图表元素的形式对方案进行配置，支持修改图表及方案名称。 2. 支持以2D/3D的方式对仿真环境中的网络拓扑结构、攻击与防护效果等进行可视化展示。 3. 支持在拓扑结构可视化中进行流量数据展示，能够展示真实的恶意流量走向及路径。 4. 提供复盘功能，支持对接各业务以进度条的方式展示已发生的活动全过程，提供播放、暂停、倍速等功能。 5. 支持切换查看视角可使用自动漫游及固定视角两种方式查看态势，在自动漫游模式下支持设置摄像机旋转速度。 6. 大屏选择主题样式支持选择2种，包括：地球、棋盘拓扑。 7. 支持不少于11种特效，包含：重置效果、网络扫描、病毒入侵、木马入侵、DDOS攻击、主机陷落、加固、主机隔离、钓鱼邮件攻击、篡改数据、数据窃取。 8. 提供可配置图表10个，包括事件发生日志、设备类型分布、流量生成趋势、设备攻击情况、效能评估结果、提交问题情况、总得分情况、行为事件日志、排行榜情况、系统运维情况。	1	套

19	精密空调	★产品匹数	5匹，制冷/制热功率与5匹规格匹配，满足大空间使用需求	2	台
		★能效等级	能效等级：二级能效，符合GB 21455-2019《房间空气调节器能效限定值及能效等级》标准，能效比(COP)≥3.2		
		★冷暖类型	冷暖类型：冷暖两用，支持制冷、制热双向运行，制冷时出风温度可调节范围16℃-30℃，制热时出风温度可调节范围18℃-32℃，切换流畅无故障		
		变频/定频	运行模式：变频，采用直流变频技术，频率调节范围30Hz-120Hz，运行稳定，噪音≤55dB（室内机）、≤60dB（室外机），节能效果显著		
		睡眠模式	睡眠模式：支持按键调节，通过空调面板按键可直接开启/关闭睡眠模式，开启后可自动调节温度、风速，符合人体睡眠舒适需求，具备睡眠节能功能		
		其他基础要求	设备为原厂全新正品，具备3C认证，室内机、室外机配套齐全，安装配件（铜管、支架等）为原厂标配，兼容性良好		
20	桌面工作站	★CPU	CPU型号：8核16线程，基准主频≥3.0GHz，最高睿频≥3.3GHz，二级缓存≥4MB，三级缓存≥16MB，典型功耗≤65W，支持DDR4内存，符合国产处理器相关标准，性能强劲可满足日常商务办公需求。	41	台
		★内存	配置：总容量≥32GB，内存频率≥3200MHz（支持向下兼容），满足多任务运行需求。		
		★存储系统	固态硬盘（SSD）：512GB，接口为SATA 3.0或M.2 NVMe，读速≥500MB/s，写速≥400MB/s；机械硬盘（HDD）：1TB，SATA 3.0接口，7200转，缓存≥64MB		
		★独立显卡	显存容量：≥4GB，接口为PCIe 4.0×16，支持DirectX 12及以上版本，提供HDMI、VGA视频接口，满足日常图形处理、视频输出需求，无硬件故障，兼容性良好。		
		输入设备	标配有线USB键鼠套装，键盘为标准104键，鼠标为光电鼠标，手感舒适、响应灵敏，支持即插即用，与主机兼容性良好。		
		电源	额定功率：≥750W，80Plus认证（铜牌及以上），支持宽电压输入（100V-240V），具备过压、过流、短路保护功能，为原厂标配电源，与机箱、主板完全兼容，无噪音超标问题。		
21	多媒体音箱	★显示器	尺寸：23.8英寸，屏幕比例16:9，分辨率≥1920×1080（全高清），IPS面板，亮度≥250cd/m²，对比度≥1000:1，响应时间≤5ms，提供HDMI、VGA接口，支持防眩光、低蓝光模式，与主机配套原厂出品。	1	台
			1. 频率响应：80Hz—18kHz； 2. 阻抗：8Ω； 3. 功率：80W*2； 4. 灵敏度：90dB；		

		5. 单元类型： 3.5"×2(BASS)，3"×1(TREBLE)；		
22	多媒体功放	1、针对教学扩声需求设计，免维护，低功耗、无风扇，适合长时间工作，无噪音，适合教学环境； 2、数字调节方式，可根据实际需要设置，每次开机可自动恢复音乐和麦克风音量的预设音量，并可限制最大音量，便于管理； 3、具有5路麦克风输入，方便接入不同类型的麦克风。支持为鹅颈话筒幻象电源供电； 4、具有4路立体声混音输入，无需考虑信道切换问题； 5、具有2路音频输出，支持输出到录播或电脑； 6、具有LCD中文菜单显示，清晰直观； 7、支持串口控制功能，可与中控或电脑等设备配合，联动控制； 8、技术指标：频率响应：50 Hz~20 KHz；灵敏度：-82 dBm (1% BER)；信噪比：90dB；输出功率：150W×2；推导阻抗：4-16 Ω	1	台
23	多媒体教学软件	1、支持网络同传/增量同传，网络同传需支持自动同传部署，不用去每台学生电脑上操作，支持同传限速功能。 2、系统集成电子白板和电子黑板，老师可以截取屏幕的任何部分作为绘图背景，老师可灵活的设置学生绘图权限，可以让学生各自独立使用电子白板功能进行练习。电子白板支持文件共享功能，方便师生上传下载自己保存的白板文件。 3、支持自学点播功能，老师可将多个视频教学课件加入到点播列表中，学生可以根据自己的兴趣和进度选择观看不同的视频课件，达到自学目的。 4、系统内置同品牌远程连接工具，当客户使用中需要协助时，不需要安装额外的软件，即可让厂家技术人员通过内置远程工具连接到客户电脑实现远程协助。	1	套
24	机房管理系统	1、系统具备一键监控学生电脑的摄像头内容并支持自动截图保存监控画面，摄像头监控可一键切换到电脑屏幕监控，支持师生间一对一的进行视频、文字和语言交流，支持定时锁定学生电脑。 2、系统具备将老师的教学过程录制下来，并支持对录制文件的再次编辑功能，如剪切，提取，合并等操作。 3、系统需具备电子签到以及人脸识别智能签到两种模式，并支持对多次签到进行统一管理。 4、为了丰富学生的学习生活，系统需集成有打字软件等多种益智类软件，并支持设置组长让学生进行分组讨论。 5. 支持实训室电脑系统同传功能，包括信创电脑和X86电脑。	41	套

25	多媒体教学中控	1. 网络中控主机与面板采用分体式结构，设备低功耗，稳定可靠，无风扇，无噪音，适合长期不间断工作； 2. 包含面板，功能清晰简明，操作简单方便，支持一键开关设备，支持音量控制，支持面板开计算机功能，面板支持状态指示，方便使用者了解当前状态及操作结果； 3. 媒体设备信号源支持4路HDMI信号输入2路输出； 4. 投影机电源和计算机电源具有延时关闭功能，保证设备正常自动关机后断电，延时时间长短用户可自定义； 5. 中控联动控制功能，用户可根据使用习惯设定联动模式，设置灵活； ▲6. 基本接口：HDMI：不低于4路输入和2路输出；AV：不低于4组输入和2组输出；麦克风接口：不低于2路；RS-232：不低于6路（1路可编程）；I/O接口：不低于5路；网络接口：不低于6个10/100M；设备电源：不低于1路；计算机电源：不低于1路（可设定延时）；投影机电源：不低于1路（可设定延时）；幕布控制：不低于1路（可设定延时）； 提供实物照片。	1	套
----	---------	---	---	---

★对于提供强制采购的节能产品，依据品目清单和认证证书实施政府强制采购。
本项目中属于政府强制采购的节能产品的品目编号及名称为：★A02010104 台式计算机；★A02052309 专用制冷、空调设备；

★本项目所采购产品中属于中国强制性产品认证目录（CCC目录）的，须提供所投产品由具有资质的认证机构出具的中国强制性产品认证（CCC）证书。本项目中属于中国强制性产品认证目录（CCC目录）的产品代码及种类为：0901 微型计算机、0703房间空气调节器。

附件 2：分项报价表；

序号	分项名称	制造商	产地 / 国别	制造商统一社会信用代码	制造商规模	制造商所属性别	外商投资类型	品牌	规格、型号	单价 (元)	数量	合价 (元)
1	网络安全综合演练系统 - 管理子系统	奇安信网神信息技术 (北京) 股份有限公司	北京 / 中国	911101087855446996	大型	男	内资	奇安信网神	规格: B/S 架构账号登录, 人员信息录入维护; 按机构、角色筛选账号, 支持账号批量导入导出及状态管控; 可查看在线离线用户, 单账号设置 IP 白名单, 在线用户一键强制下线。 型号: 奇安信网神网络安全综合演练系统 V7.0	35000.00	1	35000.00
2	网络安全综合演练系统 - 实训子系统	奇安信网神信息技术 (北京) 股份有限公司	北京 / 中国	911101087855446996	大型	男	内资	奇安信网神	规格: 教员自定义课程展示模式, 管控各类学习资源显隐; 可新建或复用修改学习方案, 多阶段绑定课程、试卷, 时序图直观呈现阶段课程关联。 型号: 奇安信网神网络安全综合演练系统 V7.0	138000.00	1	138000.00
3	网络	奇安	北京	911101087855446996	大型	男	内资	奇安	规格: 教员可查看考生提交	75000.	1	75000.00

	安全综合演练系统 - 考试测评子系统	信网神信息技术（北京）股份有限公司	／中国				信网神	状态与答题详情，可清空作答记录供学员重答；自动统计历次成绩，支持成绩修改、试卷及成绩导出；可查阅本场实考、合格人数、均分、答题时长、成绩分布、高频错题等考试统计数据。 型号：奇安信网神网络安全综合演练系统 V7.0	00		
4	网络安全综合演练系统 - 竞赛子系统 A	奇安信网神信息技术（北京）股份有限公司	北京／中国	911101087855446996	大型	男	内资	奇安信网神 规格：平台可实现题库与竞赛任务一体化管理，兼容理论及攻防类全品类题型，支持客观题批量导入与题目精细化编辑。支持赛事模式自由搭配，覆盖赛前赛后全流程运维，满足多赛事同步及多人协作管理需求。 型号：奇安信网神网络安全综合演练系统 V7.0	75000.00	1	75000.00
5	网络安全综合演练系统	奇安信网神信息技术（北京）股份有限公司	北京／中国	911101087855446996	大型	男	内资	奇安信网神 规格：支持竞赛网络模式一键切换，管控题目下发与环境启停重置；配备多维度防作弊、IP 隔离、奖惩禁赛机制，可分级发布赛事公	50000.00	1	50000.00

	- 竞赛子系统 B	北京) 股份有限公司							告, 完整记录答题攻防数据、实时排行, 双架构 3D 可视化大屏多比例展示赛事数据 型号: 奇安信网神网络安全综合演练系统 V7.0			
6	网络安全综合演练系统 - 虚拟化组件 (智慧防火墙)	奇安信网神信息技术 (北京) 股份有限公司	北京 / 中国	911101087855446996	大型	男	内资	奇安信网神	规格: 产品支持路由、透明、交换以及混合模式接入, 满足复杂应用环境的接入需求。支持旁路模式; 支持将告警信息通知管理员, 告警信息的范围至少包括件、CPU 利用率、内存利用率、硬盘利用率、接口带宽利用率、NAT端口池利用率等 型号: 奇安信网神网络安全综合演练系统 V7.0	35000.00	1	35000.00
7	网络安全综合演练系统 - 虚拟化	奇安信网神信息技术 (北京) 股	北京 / 中国	911101087855446996	大型	男	内资	奇安信网神	规格: 可配置 DNS、SNMP、NFS、NETBIOS 四类审计策略; 分别实现 DNS、SNMP 通信管控审计, NFS 文件访问传输行为审计管控, 以及 NETBIOS 通信、账号、文件目录全维度审计管控。	45000.00	1	45000.00

	组件（上网行为管理）	份有限公司						型号：奇安信网神网络安全综合演练系统V7.0			
8	网络安全综合演练系统—定向课程资源包	奇安信网神信息技术（北京）股份有限公司	北京／中国	911101087855446996	大型	男	内资	奇安信网神 规格：数据安全课程覆盖数据全生命周期，含7套专项课程及全套教学素材，配套足量源码、课件习题；上网行为管理、智慧防火墙、应急响应课程配备多类型实验与充足课时，一体化实训，配套可下载教学资料 型号：奇安信网神网络安全综合演练系统V7.0	200000.00	1	200000.00
9	网络安全综合演练系统—基础课程资源包	奇安信网神信息技术（北京）股份有限公司	北京／中国	911101087855446996	大型	男	内资	奇安信网神 规格：Linux操作系统及应用、Python开发技术、Windows Server系统管理、密码学基础、Mysql数据库、密码学应用、密码学算法编程、路由交换基础等课程的实验或理论教学内容。 型号：奇安信网神网络安全综合演练系统V7.0	120000.00	1	120000.00

									迟、状态等信息，提供对单个计算节点的详情查看，以折线图形式展示对应CPU占用、内存占用、存储占用以及存储的读取和写入速度的使用趋势情况。 型号：综合网络靶场系统 V2.0			
1 2	网络空间安全实战对抗系统－系统管理	广东丈八科技有限公司	广州／中国	91110114MA0205PL3R	小型	男	内资	丈八网安	系统采集多类型日志，多维度检索，支持下载清理；可按日志级别推送至 Syslog 或管理员站内消息，管理员可发布租户全域公告；账号支持批量运维、有效期管控、分组赋权，新用户注册需人工审核。 型号：综合网络靶场系统 V2.0	35000.00	1	35000.00
1 3	网络空间安全实战对抗系统－网络仿	广东丈八科技有限公司	广州／中国	91110114MA0205PL3R	小型	男	内资	丈八网安	规格：可一站式完成镜像运维、靶标管控、网络流量仿真全流程实操支撑，依托差分磁盘技术节约平台存储资源。搭载专属靶机网盘实现跨设备数据交互，全面采集主机运行日志，可灵活仿真真实网络流量。同时预置	75000.00	1	75000.00

	真								丰富镜像与全品类靶标资源，全方位满足网安实训、攻防演练教学需求。 型号：综合网络靶场系统 V2.0			
14	网络空间安全实战对抗系统-资源库	广东丈八科技有限公司	广州／中国	91110114MA0205PL3R	小型	男	内资	丈八网安	支持流量包批量上传、标签分类及模板导入导出；平台工具支持全生命周期管理、多版本维护与跨系统筛选下载，可收藏发布工具；内置300款以上攻防工具，覆盖多类别，适配多操作系统 型号：综合网络靶场系统 V2.0	63000.00	1	63000.00
15	网络空间安全实战对抗系统-漏洞库	广东丈八科技有限公司	广州／中国	91110114MA0205PL3R	小型	男	内资	丈八网安	规格：具备漏洞管理检索功能，快速定位带 PoC、EXP 漏洞；库内二十余万漏洞数据，大量绑定官方漏洞编号，完整收录 CVSS 评估指标与 CWE 分类，储备两万条高质量漏洞利用脚本。 型号：综合网络靶场系统 V2.0	18000.00	1	18000.00
16	网络空间安	广东丈八科	广州／中国	91110114MA0205PL3R	小型	男	内资	丈八网安	规格：图表拖拽编排并保存多套展示模板，2D、3D 立体展示仿真拓	45000.00	1	45000.00

	全实战对抗系统 - 态势控制	技有限公司						扑与恶意流量链路；全流程演练复盘支持倍速回放，双浏览视角、两种大屏风格、十一类安全事件特效，内置十类可视化统计图表。 型号：综合网络靶场系统 V2.0			
17	网络空间安全实战对抗系统 - 人员能力评估	广东丈八科技有限公司	广州 / 中国	91110114MA0205PL3R	小型	男	内资	丈八网安 规格：平台依托国标网安人员能力标准搭建完整人才评测体系，对标十五类细分网安岗位分层评估。结合 ATT&CK、D3FEND 框架量化攻防实操水平，从任务、知识、技能多维度自动生成可视化能力画像，可灵活调整岗位评估权重，为单位人才定岗、梯队培养、人员能力摸底提供数字化量化依据。 型号：综合网络靶场系统 V2.0	42000.00	1	42000.00
18	网络空间安全实战对	广东丈八科技有限公司	广州 / 中国	91110114MA0205PL3R	小型	男	内资	丈八网安 规格：支持公私课程模板流转、课程多拓扑绑定与分步实验校验，可预览课程；具备排课、教学数据分析、师生交流笔记、	150000.00	1	150000.00

	抗系统一攻防演练	司							学习地图关卡等功能，支持课前自动部署环境、课堂录屏与远程教学管控；内置多行业内网实战攻防场景，配套完整实验资源 型号：综合网络靶场系统 V2.0			
19	精密空调	青岛海尔空调器有限总公司	青岛 / 中国	913702122648088392	大型	男	内资	统帅	匹数：5匹，制冷/制热功率与5匹规格匹配，满足大空间使用需求 2. 能效等级：二级能效，符合GB 21455-2019《房间空气调节器能效限定值及能效等级》标准，能效比（COP）是3.2； 3. 冷暖类型：冷暖两用，支持制冷、制热双向运行，制冷时出风温度可调节范围16℃-30℃，制热时出风温度可调节范围18℃-32℃，切换流畅无故障。 型号：KFRd-120LW/5YTF82T	21000.00	2	42000.00
20	桌面	浪潮	济南	91370000706266601D	大型	男	内资	浪潮	规格：1、CPU 型号：海光	7800.00	41	319800.00

工 作 站	电 子 信 息 产 业 股 份 有 限 公 司	/ 中 国					3350, 8 核 16 线程, 基础主频 3.0GHz, 最高睿频 3.3GHz, 二级缓存 4MB、三级缓存 16MB, TDP 65W, 适配 DDR4 内存, 国产海光处理器, 符合国产处理器标准, 满足商务办公运算需求; 2、内存: 32GB 总容量 DDR4 3200MHz, 向下兼容低频内存, 多任务并行运行; 3、存储系统固态硬盘 (SSD): 512GB, 接口 M.2 NVMe, 读速 500MB/s, 写速 400MB/s; 机械硬盘 (HDD): 1TB, SATA 3.0 接口, 7200 转, 缓存 64MB; 4、独立显卡: 4GB, PCIe 4.0 ×16 总线, 支持 DirectX 12+, 标配 HDMI+VGA 双视频输出接口, 满足图文、视频图像处理, 硬件兼容稳定。5、输入设备: 标配有线 USB 键鼠套装, 键盘为标准 104 键, 鼠标为光电鼠标,			
-------------	--	----------	--	--	--	--	---	--	--	--

									手感舒适、响应灵敏，支持即插即用，与主机兼容性良好； 6、电源：额定功率：750W，80Plus 认证（铜牌及以上），支持宽电压输入（100V-240V），具备过压、过流、短路保护功能，为原厂标配电源，与机箱、主板完全兼容，无噪音超标问题。7、显示器：尺寸：23.8英寸，屏幕比例16:9，分辨率1920×1080（全高清），IPS面板，亮度250cd/m²，对比度1000:1，响应时间5ms，提供HDMI、VGA接口，支持防眩光、低蓝光模式，与主机配套原厂出品。型号：CE530H			
21	多媒体音箱	北京华璨电子有限公司	北京 / 中国	91110114697732630U	小型	男	内资	华璨	规格： 1. 频率响应：80Hz—18kHz； 2. 阻抗：8 Ω； 3. 功率：80W*2； 4. 灵敏度：90dB； 5. 单元类型：3.5"×2(BASS)，3"×1(TREBLE)； 型号：AS-80	1500.00	1	1500.00

2 2	多媒体功放	北京华璨电子有限公司	北京 / 中国	911101146977 32630U	小型	男	内 资	华 璨	规格： 1. 具有5路麦克风输入，方便接入不同类型的麦克风。支持为鹅颈话筒幻象电源供电； 2. 具有4路立体声混音输入，无需考虑信道切换问题； 3. 具有2路音频输出，支持输出到录播或电脑； 4. 具有LCD中文菜单显示，清晰直观； 5. 支持串口控制功能，可与中控或电脑等设备配合，联动控制； 6. 技术指标： 频率响应：50 Hz~20 KHz； 灵敏度：-82 dBm (1% BER)； 信噪比：90dB； 输出功率：150W×2；推导阻抗：4-16 Ω 型号：AV-150	2800.0 0	1	2800.0 0
2 3	多媒体教学软件	传奇科软科技（北京）有限公司	北京 / 中国	911101085732 31527Q	微型	男	内 资	传 奇	规格： 系统集成电子白板和电子黑板，老师可以截取屏幕的任何部分作为绘图背景，老师可灵活的设置学生绘图权限，可以让学生各自独立使用电子白板功能进行练习。	3000.0 0	1	3000.0 0

		司							电子白板支持文件共享功能，方便师生上传下载自己保存的白板文件。 型号：传奇电子教室软件 V16.0			
24	机房管理系统	传奇科软科技（北京）有限公司	北京 / 中国	91110108573231527Q	微型	男	内资	传奇	规格： 系统具备一键监控学生电脑的摄像头内容并支持自动截图保存监控画面，摄像头监控可一键切换到电脑屏幕监控，支持师生间一对一的进行视频、文字和语言交流，支持定时锁定学生电脑。 型号：传奇网络还原系统 V9.0	240.00	41	9840.00
25	多媒体教学中控	北京华璨电子有限公司	北京 / 中国	91110114697732630U	小型	男	内资	华璨	规格： 基本接口： HDMI：4路输入和2路输出； AV：4组输入和2组输出；麦克风接口：2路； RS-232：7路（2路可编程）。 型号： HC-S1000 (HD)	3000.00	1	3000.00
总价（元）											/	1718940.00