

附件 1

政府采购项目 采 购 需 求

项目名称：平顶山学院能源互联网信息安全实训

平台项目

采购单位：平顶山学院

编制单位：平顶山学院

编制时间：2026 年 5 月

编 制 说 明

一、采购单位可以自行组织编制采购需求，也可以委托采购代理机构或者其他第三方机构编制。

二、编制的采购需求应当符合《财政部关于印发政府采购需求管理办法的通知》（财库〔2021〕22号）要求及政府采购的相关规定。

三、下划线部分属于提醒内容，编制时应删除。

四、对不适用的内容应删除，并调整相应序号。

一、需求调查情况

为贯彻国家网络安全与能源安全新战略，落实河南省新型电力系统与数字经济发展部署，围绕能源互联网信息安全实训平台建设开展专项需求调研，全面对接国家、省级战略及行业人才培养需求。

从全国战略需求看，能源互联网作为“双碳”目标下新型电力系统的核心载体，已纳入国家战略性新兴产业体系。国家能源局明确要求强化电力监控系统安全防护，落实“安全分区、网络专用、横向隔离、纵向认证”原则，筑牢关键信息基础设施安全防线。当前，能源互联网呈现设备泛在互联、数据海量交互、边界动态开放特征，工控漏洞、网络攻击、数据泄露等安全风险频发，国家多次强调需加强实战化人才培养，补齐能源领域网络安全实训短板，构建“产学研用”一体化安全保障体系。

从河南省战略需求看，我省是能源消费大省与新能源发展重点区域，正加速推进传统电网向新型电力系统转型。《河南省护航新型工业化网络和数据安全 2026 年工作方案》明确提出，要强化工业领域网络安全保障，培育网络安全技术应用场景，提升能源等重点行业安全防护能力。调研显示，省内能源企业、电力场站普遍存在安全防护体系不完善、专业人才缺口大、实战化演练不足等问题，部分新能源场站甚至违反安全分区、横向隔离等核心防护要求。同时，省内高校相关实训资源匮乏，难以匹配行业对复合型安全人才的需求，亟须建设专业化、实战化的能源互联网信息安全实训平台。

建设能源互联网信息安全实训平台，既是响应国家能源安全

与网络安全战略的必然举措，也是支撑河南省新型电力系统建设、破解行业人才瓶颈、提升区域能源安全保障能力的迫切需要。该平台可有效填补省内能源互联网安全实训空白，为行业培养实战型安全人才，助力国家与河南省能源安全新战略落地见效。项目可满足信息安全、物联网工程、电子信息工程、通信工程以及飞行器控制与信息工程等五个专业的相关课程的实验实训教学和实战技能训练任务，能够大幅提升我校能源互联网安全方向办学水平和教学质量，疏解平顶山地区电力、煤炭等能源企业招募网安复合型人才难题，为河南地区持续稳定地输送高素质的能源互联网安全技能人才，并共享教学经验资源，形成示范作用。

在本建设项目中，主要建设能源互联网信息安全实训室。

通过咨询、论证等方式开展需求调查。

了解各子项目均有三家及以上供应商有类似产品，如能源互联网信息安全实训室设备有奇安信、启明星辰、绿盟科技、深信服、博智科技、热月教育等供应商。

● 需求调查结果

1. 相关产业发展情况

相关高校和科研机构已投入使用类似产品

2. 市场供给情况

市场有成熟整套平台供给，总体满足需要系统集成

3. 同类采购项目历史成交信息

天津理工大学：网络信息安全教学及实训平台采购项目，86.85 万元，成交时间：2025.11；云南能源职业技术学院：网络安全运维实训平台建设项目，125.339 万元，中标时间：

2025.12；辽宁科技大学：网络攻防实验室建设项目，69.3万，
2023.7；西安理工大学：网络空间安全人才培养实验与实训平台
采购项目，94.85万元，2026.4；江苏安全技术职业学院：工业
互联网安全实训室建设项目，69.97万元，2024.11。

二、需求清单

（一）项目概况

项目对接河南省能源电子信息特色行业学院，可满足信息
安全专业及信息学部其他相关专业的实验教学需求，支撑学生创
新创业与课外科技活动，同时能为本地能源互联网企业提供认证
培训、安全竞赛、技能演练及应用安全测试等服务。项目有力支
撑信息学部相关学科建设，助推能源电子信息特色行业学院“高
水平、特色化、示范性”发展，并为物联网、通信工程、飞行器
控制等专业提供实训资源，提升整体教学水平和人才培养质量。

（二）采购项目预（概）算

总 预 算： 100 万元

预算： 100 万元

（三）采购标的汇总表

包号	序号	标的名称	品目 分类编码	计量 单位	数量	是否 进口
	1	高性能服务器		台	3	否
	2	交换机		台	3	否

	3	信息安全数字孪生靶场平台		套	1	否
	4	网络安全基础资源包		套	1	否
	5	实网攻防资源包		套	1	否
	6	工控能源安全场景演练资源包		套	1	否

(四) 技术商务要求

(1) 技术要求

序号	设备名称	技术要求
1	高性能服务器	1.性能指标 1) 产品类型: $\geq 2U$ 机架式服务器, 性能满足 120 人实践教学同时使用, 国产品牌, 标配原厂导轨; 2) 处理器: 配置 2 颗 Intel 6252 处理器, 单颗处理器 ≥ 24 核, 主频 $\geq 2.1\text{GHz}$; 3) 内存: 配置 ≥ 8 条 32G DDR4 内存, 支持 ≥ 24 内存插槽; 4) 存储: 配置 ≥ 6 块 960GB SSD 硬盘, 最大支持 ≥ 8 块 2.5/3.5 英寸热插拔硬盘; 5) 网卡: 本次配置 ≥ 4 个千兆网口, ≥ 2 个万兆光口(含多模模块),支持 OCP3.0 网卡模块; 6) RAID 卡: 配置 8 通道 RAID 卡, $\geq 2\text{G}$ 缓存, 支持 RAID0/1/5/10/50/60; 7) IO 扩展: 支持 ≥ 8 个 PCIE 插槽, 支持 1 个 OCP 专用 PCIE 插槽;
		8) 电源风扇: 配置 ≥ 2 个热插拔电源, 功率 $\geq 900\text{W}$, 配置 ≥ 4 个冗余双转子风扇, 风扇转速自动调节。 2.服务指标 三年硬件保修服务; 提供投标商加盖公章的售后服务承诺函。

2	交换机	1. 性能指标 1) 硬件性能：整机交换容量$\geq 672\text{Gbps}$；转发性能$\geq 171\text{Mpps}$（以官网最小值为准）； 2) 单台端口：≥ 48个千兆电口，≥ 4个万兆 SFP+口； 3) 支持 SPAN/RSPAN 镜像和多个镜像观察端口，可以对网络流量进行分析以采取相应管理维护措施； 4) MAC 地址表$\geq 32\text{K}$，IPv4 路由表容量$\geq 8\text{K}$，整机最大 ARP 地址表$\geq 4\text{K}$； 5) 安全：支持 CPU 保护功能，支持防止 DOS、ARP 攻击功能、ICMP 防攻击，支持端口隔离、端口安全、Sticky MAC，保护交换机在各种环境下稳定工作，提供证明截图； 6) 支持 VRRP、OSPF、OSPF v3、BGP、ISIS、BGP4+等增强三层路由协议，提供证明截图； 7) 支持 ERPS 以太环保护协议，切换时间$\leq 50\text{ms}$，提供证明截图； 8) 支持智能运维管理功能，可通过图形化操作的方式实现对网络的统一运维及管理，提供证明截图。 2. 服务指标 三年硬件保修服务；提供投标商加盖公章的售后服务承诺函。
3	信息安全数字孪生靶场平台	一、实训教学功能 1. 实训平台基础系统（管理员用户） 1) 用户与权限管理 ①系统具备用户与权限管理功能，能够完成教师和学生账号的创建、批量导入及统一管理操作； ②系统具备账号增、删、改、查及密码重置功能； ③系统具备角色权限配置功能，能够设置学生、教师、管理员等不同角色权限。 2) 资源管理 ①系统具备教学资源管理功能，能够完成课程资料、实验手册、PPT、视频等资源的上传、更新与管理操作； ②系统具备资源分类管理功能。 3) 课程管理 ①系统具备课程管理功能，能够为教师账号授予课程创建权限； ②能够完成课程计划制订、课程公开或私有模式切换设置。 4) 系统监控与维护 ①系统具备平台运行状态监控功能，能够实时监测服务器性能、网络状况、用户并发数等关键指标； ②系统具备日志查看与分析功能，能够追溯用户操作记录。 5) 考试管理

		①系统具备考试管理功能，能够完成试卷模板创建、试卷公开或私有属性设置、题目分值设置、考试时间设置及考场安排操作； ②系统具备成绩统计与报表生成能力。 2. 实训学习子系统（学生端用户） 1) 课程学习功能 ①系统具备课程筛选与查询功能，能够依据关键字完成课程筛选操作； ②系统具备分类查看功能，能够清晰地展示课程名称、课程作者、课程简介、理论及实验数量等信息； ③系统具备实验指导书查阅功能，指导书内容能够包含实验目的、实验内容、实验步骤等。 2) 实验操作功能 ①系统具备实验环境操作功能，能够在 Web 虚拟桌面中完成文本双向复制粘贴操作及文件上传操作； ②系统具备多种虚拟化仿真模板调用功能，包括虚拟防火墙、路由器、交换机等； ③系统具备实验报告编辑功能，能够完成实验图片插入操作。 3) 学习进度与能力展示功能 ①系统具备学习进度查看功能，能够支持学生实时查看课程学习进度； ②能够通过雷达图等图形化方式展示学生学习情况。 4) 考试参与功能 ①系统具备考试参与管理功能，能够在试卷页面展示已答、未答、当前进度等状态； ②系统具备成绩授权查看功能。 3. 授课管理子系统（教师端用户） 1) 教学资源与课程管理子系统 ①系统具备课程体系管理功能，能够完成课程体系的配置与管理操作； ②系统具备岗位体系管理功能，能够完成职业岗位体系课程的设置与管理操作； ③系统具备实训课程管理功能，能够完成课程体系管理、课程管理及章节管理操作。 2) 网络安全资源库管理子系统 ①系统具备知识库管理功能，能够完成知识库资源的新增、删除、修改、查询操作，知识内容能够涵盖前沿技术、攻防技术、安全技术等多维度网络安全资源； ②系统具备漏洞库管理功能，能够完成漏洞库资源的新增、删除、修改、查询操作；漏洞信息内容能够包括漏洞风险评级、漏洞类型、漏洞介绍、漏洞利用方式、POC 及受影响产品等信息。
--	--	--

		3) 教学过程管理子系统 ①系统具备教学任务下发功能,能够支持教师将课程、班级、作业等学习任务分配至指定目标; ②系统具备考核管理功能,能够支持教师阶段性下发考核任务,并能够完成考核内容及方式设置; ③系统具备班级与人员管理功能,能够支持教师对班级及学生进行新增、删除、修改等操作。 4) 教学质量审核管理子系统 ①系统具备考核任务审核功能,能够完成学生考核或评估任务的审核操作; ②系统具备实验审核功能,能够完成学生实验结果的批改操作。 5) 网络安全仿真实训子系统 ①系统具备场景仿真管理功能,能够完成虚拟场景创建、管理及运行操作,并能够构建仿真网络环境、安全设备及靶机环境。 二、靶场管理系统 1) 资源监控管理子系统 ①系统具备资源统计功能,能够对系统中主机、网络、虚拟机等资源进行统计; ②系统具备资源存量监控功能,能够监控 CPU 存量、内存存量、存储量、虚拟机存量、容器存量及 IP 存量等资源信息。 2) 虚拟化环境管理子系统 ①系统具备虚拟机配置功能,能够完成虚拟机内存大小及 CPU 核数配置操作; ②系统具备虚拟机磁盘配置功能,能够完成磁盘容量及驱动模式配置操作。 3) 平台运维与权限管理子系统 ①系统具备后台任务管理功能,能够查看后台任务、执行进度及执行结果;系统具备后台任务筛选与查询功能; ②系统具备登录日志管理与操作日志管理功能; ③系统具备用户与角色权限管理功能,能够完成用户信息与角色权限配置操作。 4) 攻防裁决管理子系统 ①系统具备目标裁决功能,能够编辑评估裁定规则,能够执行判定操作,能够将随机 Flag 推送至靶标指定磁盘位置,并具备防作弊机制。 5) 靶场平台竞技任务管理子系统 ①系统具备比武演练任务配置功能,能够根据实训任务要求完成参赛队伍与配套比武演练资源的配置操作,配置内容包括竞赛名称、竞赛开始时间及持续时长、竞赛 LOGO、竞赛模式、竞赛规则、竞赛场景(试卷)、参赛队伍
--	--	--

		等信息； ②系统具备比武演练任务常规管理功能，能够完成任务的新建、删除、编辑、查询、下发等操作。 6) 靶场平台试卷赛题管理子系统 ①系统具备赛题常规管理功能，能够完成赛题新增、删除、编辑、查询、预览等操作； ②系统具备赛题信息编辑功能，能够完成赛题名称、类型、题目入口、宿主机、场景等信息的编辑操作； ③系统具备宿主机管理功能，能够完成宿主机的上传、查询、编辑、删除等操作； ④系统具备试卷创建与配置功能，能够通过整合赛题完成试卷创建操作，试卷信息能够包含名称、描述及试卷内题目配置等内容。 7) 靶场平台人员队伍管理子系统 ①系统具备队伍信息常规管理功能，能够完成队伍信息新增、删除、编辑、详情查看、查询等操作；队伍信息能够包含队伍名称、描述、队伍 logo、队伍成员列表等； ②系统具备队伍信息批量处理功能，能够完成队伍信息批量导入或批量删除操作； ③系统具备队伍数据导入导出功能，能够完成队伍信息导入、导出操作，并能够在界面提供导入模板下载功能，导入文件格式为 Excel。 8) 竞赛接入与环境隔离子系统 ①系统具备参赛指引与访问保障功能，能够使参赛队伍/选手依据“参赛手册”访问选手 Web 客户端及赛题环境； ②系统具备实体终端接入能力，能够支持参赛队伍/选手通过实体 PC 接入竞赛环境； ③系统具备队伍隔离功能，能够为每支队伍提供专属题目场景，实现队伍之间环境隔离。 9) 选手竞赛交互子系统 ①系统具备选手端竞赛信息展示功能，能够在选手 Web 客户端界面展示竞赛倒计时、公告信息、实时战况信息、竞赛轮次及时长信息、所在队伍得分及排名信息、所有参赛队伍积分榜单信息； ②系统具备赛题查看与提交功能，能够使参赛队伍/选手通过 Web 客户端查看题目并提交答案或 Flag； ③系统具备动态 Flag 反作弊功能，能够实现题目 Flag 动态生成。 10) 赛事管理与公告发布子系统 ①系统具备公告管理功能，能够支持管理员完成公告新增、删除、编辑、查询、发布等操作； ②系统具备公告定向发布功能，能够支持管理员对所有队伍发布全员可见公告，或对指定队伍单独发布信息；
--	--	--

	③系统具备赛题状态监控与维护功能,能够支持管理员对赛题开启/关闭状态进行监控,并能够完成赛题详情查看与编辑操作;编辑内容能够包括题目名称、题目内容描述、题目附件配置等。 11) 裁判判分与竞赛管理子系统 ①系统具备人工判分与调整功能,能够支持管理员对队伍/选手分数进行人工判定与调整,并能够在调整时记录操作原因及调整后的分数值; ②系统具备赛题批改与人工补交功能,能够支持裁判针对指定队伍/选手的指定题目进行批改,以应对答案正确但无法自行提交的情况; ③系统具备违规处置功能,能够支持管理员对正在参赛且违规的队伍/选手进行禁赛处置。 12) 竞赛环境运维管理子系统 ①系统具备竞赛环境运维管控功能,能够支持管理员对队伍/选手虚拟机环境进行开机、关机、创建快照、重启等操作。 13) 竞赛展示与数据分析子系统 ①系统具备大屏展示功能,能够展示比武演练基本信息、赛题攻克情况、赛队得分情况、排行榜、队伍得分详情、整体分数走势等信息; ②系统具备竞赛数据统计功能,能够统计答题记录、队伍得分记录、失分记录等信息。 14) 网络拓扑场景构建子系统 ①系统具备构建过程分步骤管理与独立保存功能,能够实现构建过程各步骤独立保存; ②系统具备可视化网络拓扑构建功能,能够支持管理员通过网络拓扑构建组件以拖拽方式构建多级网络场景,并能够同步编辑场景基本信息、附加信息等; ③系统具备多人协同场景构建功能,能够支持管理员多人协同构建场景并进行拼接组网,以满足大规模复杂网络构建需求。 15) 靶标资源配置管理子系统 ①系统具备靶标环境动态调整与场景分发功能,能够动态调整靶标环境并实现一键场景分发; ②系统具备场景编辑与资源关联功能,能够对靶标资源、拓扑资源进行调用与相互关联,并能够完成场景的增删改查操作; ③系统具备拓扑节点与靶机资源关联配置功能,能够在关联及模板制作环节将节点关联至靶机,并能够完成基本属性、网卡信息、服务信息等相关信息配置。 16) 场景验证与运行管理子系统 ①系统能够在场景自测及保存环节对建立的场景进行单
--	---

		节点开机、联网开机、资源释放、设备重启等验证操作，并能够将验证通过的场景持久化保存至系统场景库； ②系统具备场景全生命周期管理功能，能够对系统现存场景完成查询、浏览、启动、复制、编辑、删除等操作。 17) 场景扩展与模板管理子系统 ①系统具备场景动态构建与增量式构建功能，能够实现对场景的动态扩展与增量调整； ②系统具备模板克隆与拓扑数据管理功能，能够完成模板克隆、拓扑数据管理与调用操作。 18) 实验场景管理子系统 ①系统支持管理员根据培训要求，自定义创建个性化的实验场景； ②系统支持对实验场景的虚拟机进行设置，以及对场景内不同区域的网络连通性进行设置； ③系统具备环境隔离功能，实验环境满足完全隔离，即学员在进行实验操作时场景之间不可进行数据交换。 19) 虚拟资源管理子系统 ①系统支持 KVM 虚拟机资源和容器类虚拟资源等虚拟资源类型，并支持不同类型虚拟资源的混合组网； ②系统具备虚拟机资源监控功能，能够监控虚拟机的内存使用率、CPU 使用率、磁盘使用率、网络 I/O 等资源占用情况； ③系统具备虚拟机管理功能，支持创建、删除、查询、重启、关闭、克隆、远程桌面连接及接入、虚拟机网卡配置、虚拟机磁盘配置等操作。 20) 靶标资源管理子系统 ①系统支持为靶机设置 Flag 信息，包括 Flag 值、分类、附件、描述等其他信息； ②系统支持对系统中存储的靶机进行常规管理，包括查看、开机、关机、重启、克隆、编辑、删除等操作； ③管理员能够对靶标母版进行克隆和继承改造，形成新的靶标母版。 21) 资源库与镜像管理子系统 ①系统支持对靶标资源库进行常规管理，包括新增、查看、删除、编辑、检索； ②系统支持对 QCOW2 格式的虚拟机镜像及 docker 容器镜像进行管理； ③系统支持虚拟镜像常规管理，包括镜像上传、镜像删除、镜像查看等。 22) 镜像生成与终端管理子系统 ①系统支持虚拟机镜像生成，包括两种生成方式：一是基于系统已有虚拟机模板，快速生成新的虚拟机镜像；二是用户自定义镜像；
--	--	--

		②系统支持查看指定账号下所注册的所有终端（操作机）的列表，并可对其进行开机、关机、重启、打开控制台、删除等操作； ③系统支持通过浏览器接入到终端内部，可对终端内部的软件、文件等进行操作，并保存终端状态。 23）虚实结合设备管理子系统 ①系统具备网络安全设备的虚实结合功能，支持在场景中添加实体设备； ②系统支持添加、查看和删除实体设备信息； ③系统支持配置实体设备的基本信息，包括设备名称、设备型号、设备参数、IP 地址、MAC 地址、网关、操作系统、登录用户密码等信息。 24）攻防工具资源管理子系统 ①系统内置攻防工具库，支持对工具进行常规管理操作，包括新增、删除、编辑、查询等； ②系统支持对工具内容、工具分类、工具简介等信息进行编辑； ③系统支持对工具进行分类管理，并能够自定义工具的种类。 25）任务管理子系统 ①系统具备理论试题、CTF 任务、场景任务等单一类型或多种任务类型的综合管理功能，能够完成网络靶场挑战与任务的规划、设计与执行，并能够提供单人训练与团队训练模式； ②系统能够完成虚拟环境设计与配置，包括网络拓扑、虚拟机设置、靶标环境部署、应用程序和服务配置等； ③系统能够完成复杂环境布置，以实现多场景、多维度挑战设置，覆盖 Web 漏洞类、协议类、密码学及特定行业场景等。 三、系统资源包 1）靶标资源： ①系统内置白板操作系统及应用服务靶标，包含操作系统、网站服务器组件、邮件服务器组件、数据库软件和数据库的连接工具等； ②系统内置公共漏洞靶标，包括但不限于文档类漏洞、浏览器类漏洞、数据库类漏洞、网络设备类漏洞、移动终端类漏洞、web 类漏洞等； ③系统内置安全设备靶标，包括 VPN、IPS、WAF、防火墙、交换机、IDS 设备、安全审计等。采购人在使用过程中，不存在任何形式的隐性消费或二次收费。 2）漏洞库资源： ①内置漏洞信息库，支持对 POC、EXP 管理； ②提供 1000 个高质量漏洞数据（包含漏洞验证代码，远
--	--	---

		程代码执行验证 poc，本地代码执行验证 poc，web 漏洞代码验证 poc，DDOS 相关漏洞验证 poc 等）。 3）知识库资源： ①系统内置 400 篇高质量信息安全及网络攻防相关知识文章，如 Bypass 绕过、内网渗透、渗透技巧、工具技巧、经验总结知识类方向，配合用户快速开展基础知识累积； ②系统内置 40 篇最佳实践领域与实战技战法，包含红队技战法（全域信息收集与攻击面测绘、高精度漏洞利用与权限获取、内网穿透与权限体系控制、社会工程学专项攻击和 AI 赋能的自动化攻击）和蓝队技战法（互联网暴露面收缩与加固、全流量与多维度威胁检测、自动化事件响应与溯源反制、反社会工程学与安全意识建设和 AI 赋能的新一代防御体系）。 44）工具库资源： ①系统内置 100 个工具资源，覆盖 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、信息搜集工具、资产探测工具、子域名搜集工具、字典生成工具等资源。采购人在使用过程中，不存在任何形式的隐性消费或二次收费。 5）理论任务资源： ①提供理论任务不少于 4000 个，覆盖云安全、密码学、工控安全、安全防护、安全运维、主机安全、法律法规、网络安全等网络安全理论知识，其中工控理论任务资源不少于 200 个。 6）CTF 竞赛任务资源： ①提供 100 道 CTF 题目，题目类型包含：Web、Crypto、misc、PWN 和 reverse 等主要方向。 7）可视化展示管理 ①系统支持按需展示实时攻防信息、成绩趋势、实时排行、能力标签、攻防日志、所得分数等信息，支持活动开始倒计时功能，支持成绩趋势查看要求以折线图方式展示得分趋势变化。 四、平台系统更新与故障响应服务 1）故障响应服务 ①产品提供方承诺至少提供 3 年的平台系统运维与更新服务，并出具盖有产品提供方公章的承诺函； ②产品提供方承诺在接到故障通知后 30 分钟内进行远程响应，技术人员通过电话、远程登录等方式初步判断故障原因；若无法远程解决，技术人员将在 4 小时内到达现场进行处置；由平台系统故障导致的核心业务完全中断，产
--	--	---

		品提供方承诺在 48 小时内解决，若无法按时解决，产品提供方提供备用机直至问题解决。 2) 平台系统更新 ①在服务期内，服务商至少提供每年 4 次的平台系统更新服务，包含安全更新、质量与性能更新、兼容性更新等。
4	网络安全基础资源包	1.网络安全课程资源包 网络安全课程资源包（内含课程讲授视频、课程 PPT、课程练习题、教学案例资料等课程资源）覆盖以下课程，总学时不低于 1000 课时，具体课程至少包括：（交付时至少包含如下课程的 80%，交付一年内如下课程需要 100% 包含） 《信息安全导论》：不少于 40 课时 《应用密码学》：不少于 60 课时 《Web 安全》：不少于 60 课时 《渗透测试技术》：不少于 40 课时 《内网渗透测试技术》：不少于 30 课时 《逆向工程》：不少于 60 课时 《电子数据取证技术应用》：不少于 40 课时 《网络安全编程》：不少于 40 课时 《运维开发与自动化》：不少于 60 课时 《编程基础与代码安全》：不少于 30 课时 《网络安全设备配置与管理》：不少于 30 课时 《网络安全攻防演练技术》：不少于 30 课时 《漏洞挖掘与代码审计技术》：不少于 60 课时 《Linux 与网络运维》：不少于 60 课时 《Linux 系统管理》：不少于 40 课时 《网络协议安全》：不少于 30 课时 《数据库基础与安全》：不少于 30 课时 《Linux 系统架构》：不少于 90 课时 《AI 大模型与安全攻防》：不少于 30 课时 《应急响应实战》：不少于 30 课时 《工业控制系统与工业网络基础》：不少于 30 课时 《工控系统漏洞分析与安全防范》：不少于 30 课时 《数据安全治理》：不少于 30 课时 《零信任与新型网络安全架构》：不少于 30 课时 《网络安全攻防实践（CTF）》：不少于 60 课时 2.网络安全实验资源包 实验资源包括不少于 250 套活体漏洞配套实验，实验内容涵盖以下类型：SQL 注入、跨站脚本攻击、文件上传漏洞、文件包含漏洞、RCE 漏洞、逻辑漏洞、反序列化漏洞等，其中具备 CVE 编号的实验不少于 150 套。（每年根据一线应用实际，对资源包进行扩展与更新不少于 2 次。）
5	实网攻防	1.金融行业安全防护综合实验场景

资源包	1) 行业化网络环境仿真指标 ①实验场景应包括金融行业典型网络环境,能够模拟金融科技企业业务架构; ②实验场景网络架构分域不少于4级; ③实验场景应包括DMZ区、生产区、办公区和子公司区等多种功能区域,并支持区域间网络隔离与访问控制配置。 2) 业务系统与漏洞风险仿真指标 ①实验场景DMZ区部署Windows Server服务器以及门户网站,并预留后台登录入口,设置弱口令、Shiro反序列化漏洞及接口未授权访问漏洞; ②实验场景生产区部署多台服务器,集成数据库弱口令及中间件漏洞等风险点,便于后续信息获取; ③子公司区域主机配备有安全防护措施,需通过免杀技术绕过后,开展后续操作。 3) 内网渗透与攻防路径训练指标 ①实验场景办公区模拟员工使用的终端设备,包含Windows 7/10/11混合终端以及AD域,设置浏览器插件漏洞、弱口令终端、凭证泄露、漏洞提权、永恒之蓝等风险点; ②实验场景可实现从门户网站入手,结合Web漏洞拿下首个入口,尝试利用跳板主机进入AD域,获取基础权限后深入内网测试环境,利用漏洞或其他弱点实现横向移动,最终通过办公终端渗透到子公司,实现完整网络控制的完整攻击路径; ③实验场景应包括对信息收集、漏洞利用、权限提升、横向渗透及持久化控制等能力的综合训练内容。 4) 验证评价与资源配套指标 ①实验场景应包括多级Flag校验机制,用于验证渗透链路的完整性和攻击效果。场景内置Flag数量不少于10个,分布在各功能域; ②场景配套提供场景描述、Flag获取任务描述、网络拓扑、演示视频、标准答案及复现报告等资料。 2.政府系统安全防护综合实验场景 1) 行业化网络环境仿真指标 ①实验场景应包括政府门户系统及其配套网络环境的仿真; ②实验场景网络架构分域不少于4级; ③实验场景应包括DMZ区、生产区、办公区、核心区等多种功能区域,并支持区域间网络隔离与访问控制配置。 2) 业务系统与漏洞风险仿真指标 ①DMZ区部署政府门户网站,内置后台弱口令、文件上传GetShell漏洞,暴露管理入口; ②生产区部署生产服务器,内置Fastjson反序列化、RCE
-----	---

	漏洞、容器环境逃逸等漏洞； ③核心区模拟政府办公环境，部署运维终端，存在密码保存、RDP 登录凭证泄露风险； ④办公区存储敏感信息，部署 SQLServer 数据库、域控服务器、邮件服务器，存在数据库弱口令、zerologon 域控漏洞、域内 hash 横向移动风险，从而扩大战果。 3) 内网渗透与攻防路径训练指标 ①实验场景可实现以门户网站 Web 漏洞作为起点，通过生产服务器的漏洞扩大战果，最后尝试解密 RDP 凭证侵入办公区，跳板进入核心区，实现重要数据获取； ②实验场景应包括对信息收集、漏洞利用、权限提升、横向移动及持续控制等攻防能力的训练内容。 4) 验证评价与资源配套指标 ①实验场景应包括多级 Flag 校验机制，用于验证渗透链路的完整性和攻击效果。场景内置 Flag 数量不少于 8 个，分布在各功能域； ②场景配套提供场景描述、Flag 获取任务描述、网络拓扑、演示视频、标准答案及复现报告等资料。 3.教育行业安全防护综合实验场景 1) 行业化网络环境仿真指标 ①实验场景应包括教育机构典型网络环境的整体仿真； ②实验场景网络架构分域不少于 4 级； ③实验场景应包括 DMZ 区、生产区、分校办公区、分校生产区等多种功能区域，并支持区域间网络隔离与访问控制配置。 2) 业务系统与漏洞风险仿真指标 ①DMZ 区搭载校园门户系统，内置文件上传漏洞及后台弱口令风险； ②生产区存放 web 业务系统，预置 RCE 漏洞及容器逃逸环境； ③生产区模拟学校人员使用的电脑，包含 Windows7/10/11 混合终端，部署 OA 系统，存在文件上传 GetShell 漏洞、浏览器凭据泄露及 SMB 弱口令风险； ④分校区办公区存在最终靶标，可能存在弱口令及 SMB 溢出漏洞。 3) 内网渗透与攻防路径训练指标 ①实验场景从校园门户后台弱口令突破外围，结合容器逃逸获取内网权限，利用域内弱口令横向移动至核心生产区，实现横向渗透，最终攻入分校区的关键系统，实现完整网络控制的完整攻击路径； ②实验场景应包括对信息搜集、漏洞利用、权限提升、横向移动及持续控制等攻防能力的训练内容。 4) 验证评价与资源配套指标
--	---

		①实验场景应包括多级 Flag 校验机制，用于验证渗透链路的完整性和攻击效果。场景内置 Flag 数量不少于 8 个，分布在各功能域； ②场景配套提供场景描述、Flag 获取任务描述、网络拓扑、演示视频、标准答案及复现报告等资料。 4.医疗行业安全防护综合实验场景 1) 行业化网络环境仿真指标 ①实验场景应包括医院信息系统及基础网络环境的仿真； ②实验场景网络架构分域不少于 4 级； ③实验场景应包括互联网访问域、业务服务域、办公管理域、核心数据控制域等多种功能区域，并支持区域间网络隔离与访问控制配置。 2) 业务系统与漏洞风险仿真指标 ①互联网访问区域部署医院门户网站与远程预约平台，向外部开放提供患者信息交互入口，集成敏感信息泄露、文件上传及 JWT 鉴权等典型 web 漏洞； ②业务区域包含配置内部 OA 办公系统以及内网测试服务环境，具备基本业务操作逻辑； ③办公区模拟企业内部员工使用的办公终端，这些终端分布在独立子网中，与生产区通过部分主机跨网卡联通，用于还原内网深度渗透路径； ④核心数据区配置为 Windows 域控制器，集成永恒之蓝漏洞，获取 DC 域控权限及核心数据是参训人员的最终目标。 3) 内网渗透与攻防路径训练指标 ①实验场景可实现从门户网站入手，结合 Web 漏洞拿下首个入口，进入 OA 系统获取基础权限后深入内网测试环境，利用系统漏洞与中间件弱点实现横向移动，最终通过办公终端渗透到域控系统，实现完整网络控制的完整攻击路径； ②实验场景应包括对信息搜集、漏洞利用、权限提升、横向移动及持续控制等攻防能力的训练内容。 4) 验证评价与资源配套指标 ①实验场景应包括多级 Flag 校验机制，用于验证渗透链路的完整性和攻击效果。场景内置 Flag 数量不少于 8 个，分布在各功能域； ②场景配套提供场景描述、Flag 获取任务描述、网络拓扑、演示视频、标准答案及复现报告等资料。 5.电信行业安全防护综合实验场景 1) 行业化网络环境仿真指标 ①实验场景应包括电信运营商典型网络环境的整体仿真； ②实验场景网络架构分域不少于 4 级； ③实验场景应包括 DMZ 区、生产区、办公区、子公司区
--	--	--

	等多种功能区域，并支持区域间网络隔离与访问控制配置。 2) 业务系统与漏洞风险仿真指标 ①DMZ 区搭载短信服务入口，存在 active-mq 默认口令及后台任意文件上传等多个漏洞； ②生产区搭载 nacos 系统，存在默认口令漏洞； ③办公区部署 AD 域及证书服务环境，存在 ADCS ESC1 漏洞及 SSH 私钥泄露问题，攻击者可获取服务器及域管理员权限，存在内网横向移动及域控沦陷风险； ④子公司区部署应用服务器以及财务数据库，存在敏感信息泄露风险。 3) 内网渗透与攻防路径训练指标 ①实验场景可实现以短信服务入口的文件上传漏洞为初始突破点，获取生产区主机控制权限；随后利用生产区已存在的漏洞横向进入 AD 域环境，并通过 ActiveDirectory CertificateServices (ADCS)ESC1 漏洞获取域管理员权限；进一步通过 SSH 私钥泄露问题获取子公司服务器控制权限，最终访问财务数据库，实现对整体网络环境的全面控制； ②实验场景应包括对信息搜集、漏洞利用、权限提升、横向移动及持续控制等攻防能力的训练内容。 4) 验证评价与资源配套指标 ①实验场景应包括多级 Flag 校验机制，用于验证渗透链路的完整性和攻击效果。场景内置 Flag 数量不少于 8 个，分布在各功能域； ②场景配套提供场景描述、Flag 获取任务描述、网络拓扑、演示视频、标准答案及复现报告等资料。 6.工业控制行业安全防护综合实验场景 1) 行业化网络环境仿真指标 ①实验场景应包括工业控制典型网络环境的整体仿真； ②实验场景网络架构分域不少于 4 级； ③实验场景应包括互联网访问区、DMZ 区、生产控制区、办公区等多种功能区域，并支持区域间网络隔离与访问控制配置。 2) 业务系统与漏洞风险仿真指标 ①互联网访问区搭载 web 访问入口，存在弱口令及后台任意文件上传等多个漏洞； ②DMZ 区放置场景数据库，存在 Redis 未授权访问漏洞； ③生产控制区存在域控环境和 Tomcat 系统，存在弱口令、文件上传漏洞和 Everything 未授权访问漏洞，可通过域控主机进行横向移动； ④生产控制区内置 PLC 程序图纸逆向解密，学生可通过程序解密获取目标；
--	--

		⑤办公区模拟企业内部用户的办公终端，存在黄金票据漏洞。 3) 内网渗透与攻防路径训练指标 ①实验场景可实现从 web 访问区入手，获取 DMZ 区数据库机器控制权，并进一步利用生产控制区的 tomcat 系统相关漏洞获取主机权限进一步攻入域环境，通过域内信息收集利用哈希传递进行横向移动，利用黄金票据获取最终办公区机器权限，实现对整体网络环境的全面控制； ②实验场景应包括对信息搜集、漏洞利用、权限提升、横向移动及持续控制等攻防能力的训练内容。 4) 验证评价与资源配套指标 ①实验场景应包括多级 Flag 校验机制，用于验证渗透链路的完整性和攻击效果。场景内置 Flag 数量不少于 7 个，分布在各功能域； ②场景配套提供场景描述、Flag 获取任务描述、网络拓扑、演示视频、标准答案及复现报告等资料。
6	工控能源安全场景演练资源包	一、场景资源 1.电力领域工控安全综合实验场景 1) 业务场景仿真指标 ①场景以 10kV 配电网远程监测与控制为蓝本，完整复现配电站房内“四遥”（遥测、遥信、遥控、遥调）业务链路，覆盖配变电压监测、线路电流采集、故障跳闸控制及无功补偿投切等典型生产流程； ②实验场景基于 10kV 配电网 SCADA 系统的远程监测与控制仿真环境； ③实验场景可模拟配变电压监测、线路电流采集及故障跳闸控制等核心业务功能； ④实验场景可模拟非法入侵 SCADA 系统的攻击场景； ⑤实验场景可模拟监测数据篡改攻击与控制指令伪造攻击场景。 2) 配电自动化系统架构指标 ①实验场景可采用“管理层—控制层—现场设备层”三级简化架构模型设计或更复杂设计； ②实验场景管理层部署工业控制主机 1 台，负责数据展示和指令下发； ③实验场景控制层设置边缘控制网关，用于实现 Modbus TCP/RTU 协议转换与数据转发； ④实验场景现场设备层部署配变监测终端模拟器，可模拟电压、电流数据采集，兼容 ModbusRTU 协议； ⑤实验场景现场设备层部署断路器模拟器，接收跳闸指令并反馈运行状态。 3) 安全分区与纵深防御指标 ①实验场景管理层与控制层部署工控防火墙，开启工业协

		议白名单防护； ②实验场景管理层与控制层采用工业以太网互联，控制层与现场设备层采用 RS-485 总线连接；工控防火墙划分两个隔离网段； ③配电自动化主站系统按等保 2.0 定级为第三级，须具备访问控制、入侵防范、安全审计、数据完整性校验等技术措施； ④场景采用“安全分区+纵深防御”的架构设计，划分为安全 I 区（生产控制区）、安全接入区、安全 II 区（非控制生产区）和管理信息区四个逻辑区域，各区域之间通过专用安全设备实现边界隔离，内置 6 个及以上核心靶标； ⑤配电网需设立安全接入区作为内外网之间的缓冲地带。 4）工业控制安全攻防训练指标 ①攻击面覆盖从网络边界到物理设备的完整攻击链，包含边界突破与横向渗透、纵向加密认证绕过、工控协议攻击、配电终端恶意控制、勒索病毒、SCADA 服务器权限获取、DoS/DDoS 攻击以及 APT 全链路攻击； ②实验场景可用于演练默认凭据、XAML 组态文件缺乏完整性校验、对异常 Modbus 报文缺乏输入验证等训练内容； ③实验场景可用于演练 Telnet/SSH 弱口令、固件未签名验证、协议转换层缺乏报文合法性校验、无线接入面缺乏设备认证等训练内容； ④实验场景可用于演练验证防火墙规则有效性、绕过 DPI 检测的报文构造技术、规则配置疏漏导致的穿透等训练内容； ⑤实验场景可用于演练缺乏写保护、固件升级接口缺乏认证、支持广播报文等训练内容； ⑥实验场景可用于演练证书伪造攻击、加密隧道中间人攻击、策略配置绕过等训练内容； ⑦实验场景可用于演练验证隔离强度、尝试反向渗透路径、利用摆渡数据残留的攻击面等训练内容。 5）实训教学与资源配套指标 ①实训内容不少于 40 个学时； ②场景配套提供场景描述、Flag 获取任务描述、网络拓扑、演示视频、标准答案及复现报告等资料。 2.煤炭领域工控安全综合实验场景 1）工业控制业务仿真指标 ①实验场景基于煤矿井下胶带输送机启停控制与故障监测仿真环境； ②实验场景可模拟输送机启停操作、速度监测及超温/跑偏报警等核心功能； ③实验场景可模拟非法控制输送机运行、屏蔽故障报警等
--	--	--

		场景。 2) 工业控制架构设计指标 ①实验场景可采用“地面控制层—井下控制层—现场设备层”三级简化架构模型设计或更复杂设计。 3) 地面控制层设备部署指标 ①实验场景地面控制层部署工业控制主机 1 台, 安装组态软件, 用于实现运输机状态远程监控与启停操作; ②实验场景地面控制层部署地面集控服务器, 集成煤炭产量计量、设备运行状态汇总、视频监控联动等功能; 部署调度操作站, 提供皮带机启停操作、故障报警确认、运行参数调整等人机界面。 4) 井下控制层设备部署指标 ①实验场景井下控制层设置井下 PLC 控制器, 用于模拟控制核心, 处理传感器数据与控制指令; ②实验场景井下控制层设置工业环网交换机, 模拟环网架构, 组成 MRP (介质冗余协议) 环网, 用于保障单点故障时的通信连续性, 实现地面与井下数据传输。 5) 现场设备层设备部署指标 ①实验场景现场设备层部署配变监测终端模拟器, 可模拟电压、电流数据采集, 兼容 ModbusRTU 协议; ②实验场景现场设备层部署断路器模拟器, 接收跳闸指令并反馈运行状态; ③实验场景现场设备层部署速度/温度传感器模拟器, 用于监测运输机运行速度与滚筒温度; ④实验场景现场设备层部署声光报警器模拟器, 用于接收故障报警指令并反馈状态。 6) 工业通信与网络安全防护指标 ①管理层与控制层部署工控防火墙, 开启工业协议白名单防护; ②实验场景地面控制层与井下控制层通过 MRP 工业环网 (六台交换机组成环) 互联, 井下 PLC 与现场设备通过总线连接; 环网交换机开启端口隔离, 防范广播风暴; ③实验场景内置 4 个及以上核心靶标, 用于非法登录、远程控制指令注入攻击演练、PLC 漏洞利用、控制逻辑篡改测试、环网拓扑攻击、端口扫描测试、传感器数据篡改、故障信号屏蔽测试等训练内容。 7) 实训教学与资源配套指标 ①实训内容不少于 40 个学时; ②场景配套提供场景描述、Flag 获取任务描述、网络拓扑、演示视频、标准答案及复现报告等资料。 3. 水利领域工控安全综合实验场景 1) 工业控制业务仿真指标 ①场景以某流域小型水库为原型, 复现水位监测—闸门联
--	--	---

		动控制—视频监控的完整业务链路，覆盖“信息采集—传输处理—决策控制—执行反馈”四个环节； ②实验场景基于小型水库单孔闸门升降控制与水位监测仿真环境； ③实验场景可模拟水位实时采集、闸门开度调节及超水位报警联动等核心功能； ④实验场景可模拟非法控制闸门启停、篡改水位数据等场景。 2) 工业控制架构设计指标 ①实验场景可采用“控制层—现场设备层”二级简化架构模型设计或更复杂设计。 3) 控制层设备部署指标 ①实验场景控制层部署 PLC 模拟机 1 台，用于逻辑控制与数据处理； ②实验场景控制层部署上位机组态服务器、工程师编程站、操作员站等，提供水位监视、闸门操作、报警管理等人机交互界面。 4) 设备层设备部署指标 ①实验场景现场设备层设置水位传感器模拟器：超声波液位计，用于输出 4~20mA 信号，量程 0-50m； ②实验场景现场设备层设置闸门执行器模拟器：4 台电动闸阀，用于接收升降指令并反馈开度状态。 5) 工业通信与网络安全防护指标 ①实验场景控制层内 PLC 与监控主机通过以太网互联，PLC 与现场设备通过模拟量模块连接； ②控制层依赖 WinCC 的权限管理和 Windows 域策略进行访问控制； ③实验场景内置 4 个及以上核心靶标，用于 PLC 程序上传下载攻击、逻辑篡改测试、监控软件非法登录、画面篡改攻击演练、传感器信号干扰、虚假数据注入测试、非法控制指令下发、设备误动作测试等训练内容。 6) 实训教学与资源配套指标 ①实训内容不少于 40 个学时； ②场景配套提供场景描述、Flag 获取任务描述、网络拓扑、演示视频、标准答案及复现报告等资料。 二、配套课程资源 1.靶场场景与课程资源须实现内容配套，形成理论—实践闭环 1) 课程内容与靶场场景一一对应 ①靶场场景中涉及的工控协议，须提供对应的通信设备和协议交互环境； ②靶场场景中攻击面（如边界突破、协议攻击、终端控制、勒索病毒等），须提供对应的靶标和攻击路径；
--	--	--

		③须提供课程大纲与靶场场景对应关系表，逐项标注每个课程模块对应的靶场设备、靶标编号和攻击/防御科目。 2) 课程资源配套完整性 ①须提供“基础—进阶—实战—考核”四阶段课程体系，总课时≥ 160课时，其中：基础阶段≥ 40课时，进阶阶段≥ 50课时，实战阶段≥ 50课时，考核阶段≥ 20课时； ②每门课程须提供对应的实验指导书、PPT课件（覆盖全部课时）； ③考核试题库（试题总量≥ 500道，含单选、多选、判断、实操题）； ④须提供课程大纲、课时分配表、实验指导书封面及目录页、试题样本。 3) 课程架构设计 ①课程模块：工控安全基础、工控安全进阶、场景驱动实战、专项练习与考核。 4) 理论课件阶段、模块分别制作 ①基础阶段课包含知识点讲解、配套动画、随堂测试题； ②进阶阶段课件：增加案例驱动的教学设计——每个知识点配套一个真实或仿真的安全事件案例； ③实战阶段课件：作为任务书和参考手册使用，包含攻防科目的完整任务描述、操作步骤截图和注意事项。 5) 实训任务手册 ①攻防科目配备独立的实训任务书，统一采用“五段式”结构：任务目标、前置知识、操作步骤、注意事项、考核标准。 6) 配套工具与资源包 ①配套工具资源包：仿真软件、PLC模拟器、协议分析工具、漏洞扫描工具、模糊测试工具、逆向分析工具等； ②攻击脚本库：Modbus攻击脚本集、配电终端交互脚本、辅助工具脚本。
--	--	---

（2）商务要求

1. 现场演示及测试：项目中标后、签订采购合同之前，提供主要设备厂方针对本项目的授权、产品原厂售后服务承诺函、产品授权等材料；业主对任何响应内容存疑时，可随时（原则上为中标通知书生效后的一周内、合同签订之前）要求对所提供的方案的任意功能在项目实施现场进行功能演示与测试，投标方必须无条件配合。如果与投标响应文件存在不符、功能不能实现、不能按要求对接现有系统、要求改变现有系统状态（如整体或部分替换、拆除、改变使用方式、改变配置等）、无法满足设计规范、不符合系统实施方案的要求等情况，任何一种情况均按虚假应标处理，采购人有权终止合同签订流程，追究投标方违约责任，由此所产生的一切费用及项目延误造成的一切损失由投标人全部承担，并可以由后续中标候选人顺序中标。

2. 除明确说明内容外，所有响应细节中有关“支持”等响应描述，当用户方对“支持”等内容有具体需求时，中标方均应当无条件免费提供满足用户方相应需求的服务。

3. 质保服务：本项目须提供 5 年免费质保服务（主要设备及核心软件原则上为原厂质保）。质保期内，中标人负责对软件系统进行维护和迁移，并且保证每学期上门维护一次，不再向用户收取任何费用。质保期后中标人提供的产品，采购人有权永久免费使用、迁移、安装。软件版本、各种升级库终身免费更新；系统漏洞和各种 BUG 终身免费修补。须提供产品原厂使用授权函和售后服务承诺函。

4. 故障处置：一般系统故障（包括漏洞修复）须在 2 小时内做出有效响应，24 小时内解决；特殊复杂的系统故障（包括漏洞修复）须 48 小时内解决；若需现场解决故障的，服务人员必须在 5 小时内到达学校。

5. 技术及使用培训：免费提供所购软件中文版的操作说明书、相关技术资料及培训资料。免费提供每年不少于 2 次的现场培训或集中培训，并提供各种类型培训与个性化指导。

6. 费用范围：本项目为交钥匙工程，项目预算已包含项目实施过程中的所有费用。投标方应充分考虑项目实施过程中各环节的费用，并包含在投标总报价中，项目实施中不得以任何理由增加费用。

7. 交货期：原则上合同签订后 30 天内到货并安装调试完毕。