合 同 书

合同编号： 豫财招标采购-2026-36

甲方： 河南工业职业技术学院

项目名称： 河南工业职业技术学院电子信息工程技术专业群-信息安全综合实训室（双高）项目

乙方： 杭州安恒信息技术股份有限公司

签约地点： 河南.南阳.宛城区

甲乙双方根据 豫财招标采购-2026-36 号“ 河南工业职业技术学院电子信息工程技术专业群-信息安全综合实训室（双高）项目 ”项目中标通知书和招投标文件，根据《中华人民共和国政府采购法》、《中华人民共和国民典法》等法律法规规定，经双方协商一致，订立本合同。

一、项目清单及合同金额

1. 项目清单及报价：

序号	名称	品牌	型号和规格	数量	原产地	制造商（服务商）名称	单价	总价	备注
1	教学平台	安恒信息	DAS-NGCR-S4900-EDU05	1	杭州	杭州安恒信息技术股份有限公司	326800.00	326800.00	无
2	教学内容资源	安恒信息	DAS-NGCR-S4900-Base05	1	杭州	杭州安恒信息技术股份有限公司	231500.00	231500.00	无
3	实训平台	安恒信息	DAS-NGCR-S590RS	1	杭州	杭州安恒信息技术股份有限公司	316300.00	316300.00	无
4	实训内容资源	安恒信息	DAS-NGCR-S500TR	1	杭州	杭州安恒信息技术股份有限公司	212800.00	212800.00	无
5	服务器	超聚变	2288H V5	4	郑州	超聚变数字技术有限公司	68300.00	273200.00	无
6	核心交换机	新华三	S5500V3-28S-SI	1	杭州	新华三技术有限公司	2900.00	2900.00	无
7	汇聚交换机	新华三	S5130V2-52P-SI	2	杭州	新华三技术有限公司	4900.00	9800.00	无
8	仿真环境设备	安恒信息	DAS-CR-SL-ZY05	1	杭州	杭州安恒信息技术股份有限公司	161900.00	161900.00	无
9	仿真靶标资源	安恒信息	DAS-CR-AB-HC5	10	杭州	杭州安恒信息技术股份	24400.00	244000.00	无

扫描全能王
3亿人都在用的扫描App

						有限公司			
10	学生靠背椅	阿美	定制	48	郑州	河南阿美家具有限公司	485.00	23280.00	无
11	多媒体讲台	定制	定制	1	郑州	河南阿美家具有限公司	1900.00	1900.00	无
12	实训 LED 显示屏	海康威视	DS-D4125CA-1PM	8	杭州	杭州海康威视数字技术股份有限公司	5800.00	46400.00	无
13	演示显示屏	海康威视	DS-D5165TS/GA	4	杭州	杭州海康威视数字技术股份有限公司	3800.00	15200.00	无
14	机柜	鑫华恒	6042	1	天津	天津鑫华恒金属制品有限公司	2330.00	2330.00	无
15	教学终端	联想	慧天 M5	1	联想	联想智慧科技(天津)有限公司	7800.00	7800.00	无
16	教师靠背椅	阿美	定制	1	郑州	河南阿美家具有限公司	490.00	490.00	无
17	学习终端	联想	慧天 M5	48	联想	联想智慧科技(天津)有限公司	7800.00	374400.00	无
18	学生六角形实验桌	阿美	定制	8	郑州	河南阿美家具有限公司	950.00	7600.00	无
19	备品备件	安恒信息	备品备件	1	\	杭州安恒信息技术股份有限公司	0.00	0.00	无
20	专用工具	安恒信息	专用工具	1	\	杭州安恒信息技术股份有限公司	0.00	0.00	无
21	运输(含保险)	安恒信息	运输（含保险）	1	\	杭州安恒信息技术股份有限公司	0.00	0.00	无
22	安装、调试、检验	安恒信息	安装、调试、检验	1	\	杭州安恒信息技术股份有限公司	0.00	0.00	无
23	培训	安恒信息	培训	1	\	杭州安恒信息技术股份有限公司	0.00	0.00	无
24	技术服务	安恒信息	技术服务	1	\	杭州安恒信息技术股份有限公司	0.00	0.00	无
总价：		大写：贰佰贰拾伍万捌仟陆佰元整				小写：	2258600.00		

扫描全能王
3亿人都在用的扫描App

2.项目具体参数：详见附件；

3、合同含税金额：¥2258600.00（大写：贰佰贰拾伍万捌仟陆佰元整）

4. 合同价为含税全包价，包含项目实施过程中所有的制作费、版权费、税费、差旅费、售后服务费、培训等一切费用。该价在合同履行期间固定不变。

二、合同履行

1. 服务期限：自本合同签订之日起60日内完成全部服务内容并调试完成交付甲方验收。

2. 交货地点：河南省南阳市宛城区孔明路1666号河南工业职业技术学院孔明路校区。

3.保证货物及时运到指定地点，保证产品的质量稳定，包装完好，解答用户在应用中遇到的实际问题。

4.质保期内,中标人负责保养和维修本次所供的所有软硬件,对任何因产品设计、材料、产品质量和部件造成的设备或不见损坏进行无偿更换和维修,范围包括维修所需的零配件、人工费、交通费等所有维修费用和产品使用培训和调试费用。

5.采购人反映的软硬件系统故障，中标人承诺在接到采购人报修起，1小时到达现场，24小时解决问题；若不能解决，负责免费提供备用软硬件，以保证系统正常运行。

6.在产品安装部署时根据招标文件要求和货物及服务技术状况提供设备安装调试、远端运行管理调试所有必要材料，以满足现场实施需要为准。

7.应制定详细的培训计划，提供相关培训教材等培训用品，确保采购人的技术人员能够在30日内熟悉货物的各项特性，具备初步的维护和使用能力。提供至少30人日的培训课程，培训期间场地可有采购人安排，但培训讲师的交通、食宿等与培训相关的费用均由投标人承担。

三、履约验收

1.乙方提供的硬件和软件以及附件为最新生产的原装正品，各项指标符合国家检测标准和出厂标准，各项技术参数符合招标文件要求和乙方投标文件承诺。

2.乙方提供的产品不符合规定或质量不合格，由乙方负责更换，并承担换货而发生的一切费用。乙方不能更换的，按不能交货处理。

3.乙方应保证所提供硬件及软件不侵犯第三方专利权、商标权、著作权或其他知识产权。若侵犯了第三方上述权利，并导致第三方追究甲方的责任，甲方受到的损失，应由乙方承担。

4.乙方履约完成并提交验收申请后7个工作日内，甲方按国家相关标准和招投标相关文件自行组织有关专业人员进行验收。

5.验收内容为软件和硬件的数量，运行情况和人员培训情况。

扫描全能王
3亿人都在用的扫描App

四、付款方式及期限

1. 采用人民币转账结算方式。乙方开具以“河南工业职业技术学院”为客户名称的合法有效全额增值税专用发票。

2. 乙方在合同签署前5个工作日内，向甲方指定账户支付合同总价款5%的履约保证金。该履约保证金在项目验收合格满一年且无质量问题后无息退还。

3. 付款方式为项目验收合格后30个工作日内学校向中标人支付合同金额的100%。

五、保修条款、售后服务

1. 自项目验收合格之日起5年内，乙方免费提供小修服务，对甲方提出的合理内容调整需求2个工作日内响应并完成。

2. 乙方保证所交付资源永久使用权归甲方所有，乙方保留署名权，但不得在未取得甲方书面同意的情况下将相同或相似资源提供给第三方使用。

3. 乙方提供7×24小时电话及微信技术支持，联系人：刘鹏，电话：13271586216。

六、相关权利及义务

1. 甲方在验收时发现资源不符合合同约定、技术要求或投标承诺的，有权拒绝验收并要求乙方限期整改。

2. 甲方有义务按合同约定及时支付款项、退还履约保证金，并对乙方的技术秘密予以保密。

3. 乙方不得将本项目整体或部分转包、分包给第三方，否则甲方有权立即解除合同并没收履约保证金。

4. 乙方必须保证所有资源为原创，不得抄袭或使用未经授权的素材，否则承担全部侵权责任并赔偿甲方损失。

七、违约责任

1. 若乙方未在本合同约定的期限内完成设备交付，每逾期1日，应向甲方支付合同总金额1%的违约金；逾期超过15日的，甲方有权解除合同，乙方需退还已收取的款项（若有），并支付合同总金额10%的违约金，同时甲方没收履约保证金。

2. 若乙方提供的货物质量不合格，经两次整改后仍未达到验收标准的，乙方应返还甲方已支付的全部款项（若有），支付合同总金额10%的违约金，并赔偿甲方因此遭受的实际损失，甲方有权没收履约保证金。

3. 若甲方未在验收合格后30个工作日内支付合同费用，每逾期1日，应向乙方支付合同总金额1%的违约金。

4. 乙方违反知识产权约定，擅自使用或泄露项目成果的，应向甲方支付合同总金额10%的违约金，并承担由此引发的一切法律责任及赔偿甲方损失。

5. 因不可抗力造成违约，甲乙双方另行协商解决。

扫描全能王
3亿人都在用的扫描App

八、争议

双方本着友好合作的态度，对合同履行过程中发生的违约行为及时进行协商解决，但技术参数不得低于招标文件要求和投标文件承诺。如不能协商解决可向合同签订地人民法院诉讼。相关费用由过错方支付。

九、其他

1、本合同经双方代表签字盖章后生效。本合同一式陆份，甲方肆份，乙方贰份。

2、其他未尽事宜，由甲乙双方友好协商解决，并参照《中华人民共和国民典法》有关条款执行。

甲　方：	河南工业职业技术学院	乙　方：	杭州安恒信息技术股份有限公司
开户行：	中国银行南阳仲景北路支行	开户行：	杭州银行股份有限公司科技支行
账　号：	2649 9999 9168	账　号：	2201810000000385
委托代理人：		统一社会信用代码：	913301086623011957
		委托代理人：	
联系人：	王培培	企业规模	大型企业
		联系人：	徐军伟
地　址：	南阳市宛城区杜诗东路 1666 号	地　址：	浙江省杭州市滨江区西兴街道联慧街 188 号
电　话：	0377-63270288	电　话：	18838063301
签约时间：	2026 年 5 月 14 日	签约时间：	2026 年 5 月 14 日

扫描全能王
3亿人都在用的扫描App

附件：详细参数

序号	主要内容	基本技术要求
1	教学平台	1.平台功能模块和资源：内含教学云管理、统一身份认证、课程管理、学生管理、考试管理、安全研究、统计分析、教学终端检测、教学工具调用、开发管理等10套教学系统，支持云端部署与本地实体设备对接，实现“虚实结合”教学场景搭建。 2.具备教学场景编排（模拟网络攻防演练流程、设备联动教学流程等）、多角色用户管理(区分教师端课程发布/学情管控、学生端学习实操、管理员系统配置等权限)、多资源库整合（内置课程资源库、工具库、漏洞案例库等，关联实操平台与教学内容资源），通过 Web 端、客户端等形式，为网络安全教学提供一体化管理入口。 3.平台支持角色管理与权限管理功能，内置管理员、教员和学员角色，支持自定义角色，可以为角色划分不同功能和接口权限；支持注册申请教员、学员等角色账号，支持对用户信息进行禁用、启用、修改密码等操作，管理员可对申请账号进行审批，支持批量审批，支持设置账号所属部门及过期时间。 4.平台支持查看软硬件资源创建情况的统计数据信息，包括已创建交换机总数、路由总数、场景总数、主机总数等。平台支持用户自定义编排课程，支持将课程设置为公开课；设置为公开课的课程，所有人均有权进行使用；当为非公开课时，课程为用户私有课程，只有创建者才能使用。 5.课程可以设置多个知识点并关联相关课程，通过关联课程功能可以建立多个课程之间的关联管理；单个课程可以包含理论知识、实验、考试、作业等内容，课件资源支持 PDF、Word、MarkDown、视频、实验靶机、场景等类型。 6.平台支持关联和引用知识库和考试中的资源，同时支持快速创建课程，课程支持统计当前参与学习人数和完成学习人数。平台提供路径学习统计功能，能针对人员的参与、完成、学习时长等情况进行数据的统计展示。 7.课程支持随堂笔记和作业功能，学员可以提交和查看自己的学习笔记和作业，教员可以查看课程中所有学员的课堂笔记。 8.提供实习就业分析模块，实现学生能力画像评估，根据实习就业分析可动态调整相关教学平台课程内容。支持留言板功能，教员、学员能够针对开放的课程进行留言，支持教员、学员查看并回复留言信息，实现学习沟通与分享。 9.平台可支持与线上网络安全在线教育平台类云服务系统结合，支持从教学、安全研究、考试等多个维度对所有人员、单个部门以及个人的学习情况进行分析；每年提供100课时线上平台学习内容。投标人每年提供400课时量的教学平台现场支撑，教学期间30分钟内现场响应，非教学期间2小时内现场响应。同时每年提供由正规出版发行的信息安全类实训书籍100份。

扫描全能王
3亿人都在用的扫描App

2	教学内容资源	1.课程及数量：信息安全类课程教学内容课时数 1500 课时，数据安全理论课程 15 门，课时数 150 课时；涵盖网络安全、系统安全、安全意识、等级保护、安全术语、保密培训、网络安全法律法规、信息安全协议、Web 安全、渗透测试、二进制安全、物联网安全、云计算安全、数据存储安全、编程技术、数据库技术、安全加固、安全防护技术、应急响应、渗透工具等方向。 2.网络安全基础需涵盖网络安全的基础概念、协议和形势分析，包括 DDOS 详解、HTTP 协议概述、当前网络安全形势分析、等级保护法律法规如计算机信息网络国际联网安全保护管理办法、技术标准如信息安全技术网络基础安全技术要求以及政策规范如信息安全等级保护管理办法。这些内容帮助学员理解网络威胁、安全合规要求和基础防御理论。 3.网络安全设备配置需专注于网络安全设备的原理与配置，包括防火墙基础知识如安全区域、状态检测和会话机制、安全策略概述如 Local 区域的安全策略和 ASPF 配置、入侵检测概念，以及日志审计工具的使用如综合日志审计平台功能讲解和邮件告警配置。内容强调设备部署、策略管理和故障排除。 4.Web 应用安全与防护需涉及 Web 应用的安全开发、测试与防护，包括 JavaWeb 应用安全开发与测试如常见安全评估方法和代码审计基础、业务逻辑漏洞如重置密码和竞争条件漏洞、Struts2 漏洞详解、Web 安全部署如服务器安全和中间件加固，以及 XML 外部实体注入基础。内容覆盖漏洞原理、安全编码规范和防护措施。 5.★网络安全应急响应课程需提供网络安全应急处置检测工具（满足教学实训相关服务要求，提供五年服务期），用于网络安全事件应急处置分析，具备应急所需检查流程、课程知识库。聚焦安全态势分析和应急响应流程，包括互联网安全报告如年度网络安全态势综述、工控安全报告、情报分析如评估，定期安全通告。内容帮助学员掌握安全事件分析、风险评估和响应策略。 6.信息安全工具开发需涵盖安全工具的使用和开发基础，包括安全测试工具实战指南如 Burpsuite、Kali Linux 和 Metasploit 指南、安全代码编写如 C/C++、JAVA、PHP 和 C#的安全编码规范、软件安全开发生命周期介绍如安全需求分析与设计测试，以及自动化代码分析工具的使用。内容强调工具操作和安全开发实践。 7.网络安全攻防技术需包括安全攻防基础初级和进阶如欺骗攻击和缓存溢出防御、渗透测试基本概念如信息收集和攻击手段、Web 框架漏洞挖掘如静态和动态分析方法，以及自动化渗透测试技术，提供 Web 应用安全扫描系统，可发起无限 IP 的扫描。 8.数据库安全需包括数据库安全基础如数据库安全概述、数据库安全攻防如攻击手段和防护措施、数据库取证基础如 SQL Server 日志管理与分析和 Sybase 日志配置，以及 Hbase 日志配置与分析，教学资源需提供数据库类审计系统系统资源及数据库扫描类教学展示资源，满足无限制学生数同时发起扫描策略设置及构建数据库审计日志分析场景。 9.安全运维需涵盖安全运维的核心概念和实践，包括防火墙原理与技术、入侵检测系统、日志审计工具配置、电子取证基础、安全加固指南如网络设备 Cisco 和 HuaWei 加固规范、操作系统 Windows 和 Linux 加固规范、数据库 Oracle 和 SQL Server 加

扫描全能王
3亿人都在用的扫描App

		固规范、以及中间件 Apache 和 IIS 加固规范。内容覆盖运维中的安全监控、事件响应和系统强化。 10. 安全加固需涉及系统和应用安全加固指南，包括 OPSEC 安全加固指南如网络设备 Cisco、HuaWei 和 Juniper 加固规范、操作系统 Windows、AIX、HP-UX、Linux、RedHat 和 SUSE 加固规范、数据库 DB2、Oracle、Sybase 和 SQL Server 加固规范，以及中间件 Apache、IIS、Tomcat、WebLogic 和 WebSphere 加固规范。内容强调安全配置标准、漏洞修复和系统强化。 11. ★渗透测试需涵盖渗透测试的全流程，包括渗透测试基础讲解如信息收集、攻击手段和漏洞利用、工具介绍如扫描器使用和攻防实战，以及 Web 漏洞测试技术如 SQL 注入和文件上传漏洞原理。课程针对不同场景（Web 测试、二进制分析、CTF 取证）设计 50 +专用 AI 代理讲解内容，不同代理实现漏洞情报分析、自动化利用等。 12. 等级保护需提供提供等级保护相关课程（涵盖：等级保护详述、等级保护 2.0 基本要求解析、等级保护 2.0 教学之国家政策解读、等级保护 2.0 与分级保护的区别、等保工作内容和拓扑实验分析、等级保护 2.0 教学之等保检查程序、 等级保护 2.0 教学之等保建设（三级）、等级保护 2.0 教学之网络安全（网络全局与路由器知识体系）、等级保护 2.0 教学之网络安全（身份鉴别技术）、等级保护 2.0 教学之网络安全（交换机知识体系）、等级保护 2.0 教学之网络安全（强制访问控制体系技术）、等级保护 2.0 教学之网络安全（入侵防御知识体系）、等级保护 2.0 教学之网络安全（防火墙知识体系）、等级保护 2.0 教学之云计算安全与风险评估、级保护 2.0 之工控安全、等级保护 2.0 教学之大数据安全、等级保护 2.0 教学之无线安全、等级保护 2.0 教学之可信计算）； 13. ★等级保护与风险评估课程投标人需提供等级保护管理类平台及等保检查类工具进行课程内容资源更新和根据教学情况进行随时调整。平台内容涵盖等级保护基本要求、计算机信息安全概述、等级保护第一级基本要求、等级保护第二级基本要求、等级保护第三级基本要求、等级保护第四级基本要求、等级保护定级指南、等级保护定级方法、等级保护定级报告、等级保护备案表、等级保护实施概述、等级保护测评的逐级要求、等级保护测评基础、等级保护测评项目管理、等级保护测评探讨、风险评估基础、整体评估、信息系统生命周期各阶段风险评估、风险评估与管理工具、信息安全整改、数据备份与数据恢复技术、密码技术、认证技术、信息隐藏技术、计算机病毒防范技术、网络攻击与防范技术、防火墙技术、入侵检测技术、操作系统安全、数据库安全、软件保护技术、云计算安全、工控安全、未知威胁检测、安全防护技术等。 14. 密码测评需依据《信息安全技术信息系统密码应用基本要求》，投标人需自备密码安全检查类系统，为密码检查、测评工作提供专业检查知识和检查方法课程，促使学生掌握密码检查、测评工作的标准化、规范化和专业化。支持对测评数据的关联分析、统计比对、处理流转等功能。
3	实训平台	1. 平台功能模块和资源：内含实训管理、实训赛事监控、实训竞赛、实训对抗、防作弊、实训可视化大屏、竞赛数据统计、实训考核、实训安全检测、实训漏洞管理

扫描全能王
3亿人都在用的扫描App

		等10余套系统业务功能，支持提供分步实训指引，通过实训视频（演示工具使用、攻击/防御流程）、电子实操手册（拆解每一步操作逻辑、命令代码），引导学生完成从“基础漏洞复现”到“综合攻防演练”的实训任务，支持实时操作校验、过程记录与结果评测。投标人每年提供400课时量的实训平台现场支撑，实训期间30分钟内现场响应，非教学期间1小时内现场响应。 2.支持物理设备的添加与删除，支持设定物理设备的接入方式，支持通过单一设备接入与网络接入等方式实现物理设备的接入；能够根据接入方式提供网络选项配置，支持二层接入与三层接入，二层接入模式接入不限制物理设备本身使用的VLAN，三层接入模式支持NAT接入和路由接入等形式。 3.接入平台的物理设备能够通过拖拽的形式与虚拟设备实现物理与虚拟仿真节点网络互联的能力，并能够实现虚实节点间协议数据的透明交互； 4.支持虚拟网络设备类型包含交换机、路由器、防火墙等；虚拟安全设备类型包含数据库审计、日志审计、流量分析、主机安全、应用安全、堡垒机等。支持将实体设备接入平台，实体设备类型包含计算终端、路由器、交换机、安全防护设备等类型；支持实体设备的注册与删除，支持设定实体设备的接入方式；具备WEB事件及内容检测场景，实现构建网页暗链、坏链、挂马、挖矿脚本、黑页、不良信息等内容的检测分析，构建数据收集与安全验证实训。 5.实验环境支持开机、关机、重启、重置、生成快照、恢复快照、回收资源等操作，同时具有实验环境超时自动回收、延长实验时间能力。支持展示物理设备被引用场景拓扑，物理设备接入场景采用独占的形式，即限制单台物理设备同一时刻只能被同一套场景所引用。 6.支持以平台、个人两种视角展示镜像、工具、漏洞（包含复现环境漏洞数量）、知识（包含视频、实验课时数量）、场景等资源的统计数据，并支持展示各类资源三级标签下排名前十的资源数量及贡献度情况，能够按照一定时间范围进行筛选展示，并通过对比了解实际资源有效利用情况；个人视角支持以图表形式展示个人创建的所有资源贡献情况及每日更新情况。 7.支持以上传或平台内直接制作镜像的方式进行镜像的创建，镜像类型支持虚拟机和容器两种:虚拟机支持qcow2格式,容器支持可以上传Docker镜像及Docker File+源码两种方式；虚拟机镜像支持配置CPU、内存、端口、数据盘等配置信息，容器镜像支持配置CPU、内存、端口等配置信息，支持下载私有镜像资源； 8.平台支持创建解题实操、综合实操类型试题，支持批量导入或手工的方式创建实操试题，实操试题支持关联场景版本、镜像等资源，可配置环境共享、独占的访问方式，支持设置场景和靶机的账号密码、场景中靶机的可见性。 9.支持场景的多版本管理，支持通过新建和已有版本复制的方式创建新的场景版本；场景版本支持设置版本号及编辑场景拓扑，版本列表中支持拓扑预览等功能；平台支持创建学期竞赛实训，一场竞赛可以包含多个阶段，每个阶段可以添加不同赛制类型，同时支持依据人数、分值、排名等设置阶段的准入条件；支持多场赛事并行运行且相互之间不干扰，每场竞赛均支持独立首页展示。

扫描全能王
3亿人都在用的扫描App

		10.具备信息安全实训考核实训场景模块，实训考核数据可以双向同步；实现学生单次和分阶段实训的考核管理，支持按学期以及学年进行实训的考核以及横、纵向比较；考核管理系统支持对接微信公众平台实现系统类通知消息自动通过微信下发到学生组队长，消息类型包括系统通知、考核任务通知、评分通知及考核过程其他通知。消息通知下发后系统自动记录学生是否查看。 11.具备终端审查辅助分析实训场景模块，支持审查主机系统配置信息，内容包括不限于：计算机名、用户名、操作系统、内存大小、磁盘大小、系统路径、共享目录。支持审查主机硬件信息，内容包括不限于：CPU 信息、主板信息、内存信息、显卡信息、硬盘信息、网卡信息。支持审查主机所有开机自启动项程序。支持审查主机密码安全策略配置。支持审查主机所有系统账号。支持扫描系统弱口令，字典库需加入 CSDN 事件中的 top 100 口令，如发现则显示高风险。支持 xml 等格式的输出报。 12.具备信息安全流量检测实训场景模块，支持全流量多协议威胁检测，网络威胁攻击检测引擎，包含 WEB 攻击、远程控制、网站后门、DDOS 攻击、漏洞利用、弱口令、暴力破解、远程溢出、挖矿等其他威胁安全威胁的实时检测实训。 13.具备工控安全监测审计实训场景模块，支持在不引入任何风险的前提下对工控环境进行安全监测，如实完整记录网络行为，实时检测网络攻击、异常操作、非法设备接入、病毒、关键工控行为等安全威胁。 14.具备显示屏内容播放管理实训场景模块，实现文字显示屏终端提供访问控制和入侵防护功能；支持基于 AI 技术对发布信息中的播放画面进行深度剖析的能力，能够快速、精准地识别其中的不良内容；能够充分防御从中心到终端整条信息链路上的各类风险，包括网络入侵风险、不良内容播放风险等。具备 WiFi 热点隐性劫持与检测实训模块，实训环境临时 WiFi 热点模拟、隐性劫持及劫持检测全流程实训，配套攻击端、被攻击端模拟终端及网络嗅探、ARP 检测工具，可捕获实训操作日志、简易文件传输数据等目标信息，支持劫持行为定位、攻击源追溯实训，适配实训终端及虚拟机环境，满足场景化攻防实训教学需求。 15.具备系统漏洞检测实训模块，支持两高一弱专项检测，包含两高一弱中的高危漏洞。支持检测物联网设备的漏洞，支持国内主流摄像头、打印机、路由器。 16.★实训平台需提供网站安全检测实训、数据库安全检测实训、弱口令检测实训实训、恶意代码检测实训、病毒木马检测实训、安全配置检测实训，并提供相应检测工具五年服务期。
4	实训内容资源	1.平台功能模块和资源：实训内容资源为实训平台配套的实战化数字资源集合，主要包含漏洞库，工具库，镜像库，知识库，场景库以及题库，公共漏洞靶标，为相关学习和实操供全面资源支持。提供智能家居类漏洞实训资源包、RFID 门禁克隆与防护类实训资源包、 2.安全知识分类方向包含信息安全基础、应用安全、安全运维、安全编程、安全工具、数据安全、攻防竞赛等 7 大类，共计 2000 多课时的实训理论与实训资源；实训理论资源具有 PDF 课件、视频等资源类型；实验资源具有实验介绍、实验指导书、实验靶机环境、实验工具等资源类型；

扫描全能王
3亿人都在用的扫描App

		3.工具库支持用户自定义创建工具，工具类型可以支持虚拟机型及下载型，创建工具时可以关联工具相关教程，虚拟机型工具支持在详情页面中直接进行启动和使用； 4.镜像数量600个，镜像类型应包含Windows、Linux两种类别，其中涵盖Windows7、Windows10、Windows XP、Windows Server 2003、Windows Server 2008、Windows Server 2012、Windows Server 2016、CentOS6、CentOS7、Ubuntu12、Ubuntu14、Ubuntu16、Ubuntu18、Debain8、Kali2.0、Kali2017等操作系统类型，可以根据镜像类型进行筛选； 5.知识库支持用户自定义创建安全知识，安全知识内容可包含视频、PDF、Word以及MarkDown等类型资源，同时支持关联工具、实验场景、镜像等资源； 6.实训内容资源工具数量1000款，工具类型包含应急响应、日志分析、电子取证、病毒检查、渗透测试、通用工具、逆向工程、Pwn等8种类别，工具不得捆绑具有木马后门、病毒程序； 7.题库的攻防对抗赛题包含缓冲区溢出漏洞、栈溢出漏洞、弱口令、反序列化漏洞、删除后门代码、SSRF漏洞、代码执行、后台文件上传、格式化字符串漏洞、UAF漏洞、文件上传漏洞、代码审计、任意文件读取、弱口令密码、整数溢出漏洞、文件包含漏洞、越权、模板渲染漏洞等多种题型；公共漏洞靶标的漏洞数量应80000个，带复现环境CVE漏洞200个； 8.提供AI安全辅助分析智能体资源支撑教学实训，通过AI辅助分析以人机对话为核心，提供人机对话告警分析、配置变更、规则创建、自然语言转AIQL等智能运营能力，打造一站式高效协作的网络流量安全分析智能中枢平台。 9.提供恶意邮件检测智能体资源，支持精准检测包括钓鱼邮件、木马邮件、踩点邮件、泄密邮件等多种恶意邮件类型，可结合本项目实训平台构建钓鱼邮件风险聚合展示实训，通过邮箱账户、传播方向、协议、处理状态等条件查询某时间段内钓鱼邮件告警信息； 10.支持数据安全智能体开发资源实训包提供基于Web的一体化实训资源，集成代码编写、任务调度、流程设计、实验监控和结果分析功能的智能体系统，可构建安全智能体的“条件-推理-动作”链条能力；支持连接多种教学所用的数据源，如MySQL、PostgreSQL等教学数据库，以及CSV、JSON、PDF、Word等格式的文件样本；学生可通过拖拽组件构建复杂的数据安全处理流程，也可编写代码进行深度定制，同时提供图形化流程设计器和Python/SQL脚本编辑器，满足不同难度和方向的实验需求。 11.提供10个专项信息数据安全类智能体场景实训资源，支持将数据分类分级政策、安全法规、操作手册等文档上传，作为智能体决策的依据；支持将脱敏算法（如替换、哈希、加密）封装为可供LLM智能体调用的工具。
5	服务器	*1.CPU16线程 32线程×2，内存256G，硬盘容量4T×4，可用硬盘空间7T，固态盘960G SSD×2，Raid卡4GB SAS 12Gb 8口RAID卡；该服务器对教学和实训平台（各2台）进行数据存储与管理，集中存放信息并保障其安全与完整性，同时保证100人同时在线学习。 *2.供应商提供的货物配置不能低于《通用服务器政府采购需求标准（2023年版）》

扫描全能王
3亿人都在用的扫描App

		（财库〔2023〕32号）实质性指标的最低要求（安全可靠测评除外）。
6	核心交换机	1.整机交换容量826Gbps；转发性能228Mpps；24个千兆电口，4个万兆SFP+口； 2.支持VRRP、OSPFv1/v2、OSPF v3、BGP、ISIS等增强三层路由协议；本次实配智能管理中心，支持图形化操作的方式实现对网络的统一运维及管理。
7	汇聚交换机	1.整机交换容量672Gbps；转发性能166Mpps；48个千兆电口，4个千兆SFP口； 2.内置智能图形化管理功能：支持通过图形化界面设备配置及命令一键下发和版本智能升级；支持进程分布优化功能，允许用户将不同的进程指定到不同的CPU上运行，最大程度地利用CPU和内存资源。
8	仿真环境设备	*1.基础要求：内存256G，硬盘64T；可稳定支持多节点虚拟化部署与大规模网络场景模拟。能够结合各类教学管理平台与实训演练类系统，提供高度灵活的虚拟实验环境，支持同时模拟终端设备、路由器、交换机、防火墙等多种网络与安全设备，适用于网络安全演练、网络工程实验、攻防对抗训练等实践教学场景，实现从理论到实操的一体化支撑。 2.可选取仿真设备，搭建拓扑，虚拟安全设备类型包含数据库审计、日志审计、APT攻击预警、主机安全、Web应用防火墙、堡垒机等。 3.多层次防御场景构建：支持在版本中快速部署并配置下一代防火墙、入侵检测系统、Web应用防火墙等虚拟安全设备。并提供主流的防御规则模板（如入侵检测库、WAF防护策略），让学生能直接在真实的防御体系上进行策略分析和优化演练。 4.接入仿真环境的物理设备能够通过拖拽的形式与虚拟设备实现物理与虚拟仿真网络互联的能力，并能够实现虚实间协议数据的透明交互。支持展示物理设备被引用场景拓扑，物理设备接入场景采用独占的形式，即限制单台物理设备同一时刻只能被同一套场景所引用。 5.支持高仿真网络服务与流量模拟，平台可预置常见的网络服务模拟器（如仿真的Web服务器、数据库、邮件系统），可以引入背景流量生成功能，模拟出正常用户访问流量与攻击流量混合的网络环境，训练学生在复杂网络中精准发现和识别威胁的能力。 6.支持关联场景版本及镜像环境，支持配置靶机类型为共享或独占，共享类型靶机支持配置负载能力。 7.在场景拓扑图上，可实时显示关键链路的数据流量大小、设备CPU/内存利用率等健康状态指标，平台自动记录所有网络连接和关键配置变更事件，实训结束后，可生成“攻击路径动画”，清晰展示攻击者从初始入侵到达成目标的完整链路。 8.仿真环境设备支持融入AI技术实训，集成一个自动化攻击框架，教师选择攻击模式（如“SQL注入获取Webshell”）后，平台能自动按步骤执行攻击，展示每一步的攻击原理、利用工具和产生的系统日志。作为教学演示工具，也能作为红队评估蓝队检测能力的自动化手段。 9.★为保障仿真环境设备全面融入AI安全技术仿真实训的全周期，需提供部署的大模型计算资源与环境支撑，五年课程实训服务期间其计算能力需支持参数量72B的大模型稳定运行与调优，以满足课程对AI安全分析核心能力的深度实训要求。

扫描全能王
3亿人都在用的扫描App

		10. 支持 AI 安全模型对抗性攻击与防御演练仿真，可结合配置的大模型生成图像、文本分类等典型 AI 模型，提供白盒与黑盒环境下对抗样本的生成工具，并支持对抗训练、输入净化等防御策略的部署对比。具备在配置仿真环境设备时，支持勾选指定的常见漏洞：反序列化漏洞、任意文件写入漏洞、垂直权限绕过漏洞、文件上传漏洞、后台 getshell 漏洞等；支持勾选指定的常见攻击手法：SQL 注入、远程代码执行、Docker 提权、身份验证绕过等。教师可灵活提供多个仿真靶标、仿真工具，为学生提供一个多样化、全面化的仿真环境，提升教学实训效果。
9	仿真靶标资源	1. 平台功能模块和资源：提供生产企业仿真靶标资源、政府门户仿真靶标资源、电子商务仿真靶标资源、公安案例案件仿真靶标资源、AI 安全仿真靶标资源、云计算平台安全仿真靶标资源、区块链攻防仿真靶标资源、APT 攻击事件仿真靶标资源、物联网虚拟攻防仿真靶标资源、数据空间安全共享靶标资源等 10 套不同场景的仿真靶场资源。包含简单、中等、困难三个难度等级的场景，简单难度 5 个有效靶标；中等难度 7 个有效靶标；困难难度 10 个有效靶标；总计涵盖 20 个典型漏洞，同时漏洞类型需包含通用 Web 应用漏洞、中间件漏洞、操作系统漏洞、数据库漏洞；总计涵盖 10 种攻防手段，需包含信息收集、漏洞扫描、漏洞利用、权限提升、内网穿透、内网横向渗透等手段。 2. 生产企业仿真靶标资源：需包含和生产企业业务相关的靶标，包括企业门户网站、办公系统、运维系统、打印服务等常见典型靶标，包含域环境及相关攻防手段。 3. 政府门户仿真靶标资源：需包含和政府门户业务相关的靶标，包括办公系统、运维系统、邮件系统、打印服务、VPN 等典型靶标，包含域环境及相关攻防手段。 4. 电子商务仿真靶标资源：需要包含和电子商务业务相关的靶标，包括办公系统、客户关系管理系统、运维系统、邮件系统、客服系统、研发系统等典型靶标，包含域环境及相关攻防手段。 5. 金融系统仿真靶标资源：需包含和金融业务相关的靶标，包括企业门户网站、办公系统、堡垒机等常见典型靶标，包含域环境及相关攻防手段。 6. 公安案例案件仿真靶标资源：需包括 APT 反制场景、钓鱼网站场景、裸聊诈骗场景、杀猪盘场景等常见案件场景，其中钓鱼网站场景可以模拟红包钓鱼，需要有模拟红包领取的相关界面；杀猪盘场景能清楚描述网站、论坛、信息系统架构和基本业务，场景关键部位需要放置 flag 等关键信息，用于提交以验证演练进度，该值可提取用于阶段及能力评估。 7. AI 安全仿真靶标资源：AI 模型训练平台仿真:平台面向算法安全验证场景，构建一体化仿真环境，实现 AI 平台从模型注入、故障演练到漏洞攻防的全生命周期安全能力闭环。具备以下专业化能力： 全栈模型孪生:等比例还原训练环境复杂噪声、数据漂移等 12 类扰动工况；基于轻量化框架，在秒级内完成梯度更新、后门植入检测与轨迹跟踪；内置对抗样本引擎，动态生成中毒数据、提示注入等干扰，验证算法鲁棒性阈值； 多模威胁特征库:覆盖 5 种模型类型（CNN、RNN、GAN、Transformer、联邦学习）以及 3 类异常注入（数据投毒、模型窃取、解释性攻击）等；

扫描全能王
3亿人都在用的扫描App

		历史漏洞靶标库:内置 3 类真实历史漏洞场景；每项漏洞场景均提供完整利用链、取证日志及补丁回归测试脚本。 8. 云计算平台安全仿真靶标资源：需包含 K8S、NAS 云存储、Hadoop 计算集群、Spark 大数据引擎等云计算场景下的常见靶标，使用 Docker、负载均衡等技术构建场景。 9. 区块链攻防仿真靶标资源：需包含区块链安全中的溢出攻击、重入攻击、访问控制缺陷、拒绝服务攻击、随机数安全问题；要满足离线环境可正常运行，随开随用。 10. APT 攻击事件仿真靶标资源：需包括 APT 组织渗透场景、APT 组织 C2 回连告警场景、APT 组织钓鱼攻击场景、某业务系统劫持场景、某勒索病毒传播场景等；场景中涵盖 Telnet 服务器、Zimbra 服务器、数据库主服务器、数据库备服务器、文件备份服务器等业务机器。 11. 物联网虚拟攻防仿真靶标资源：需包含路由器或摄像头设备，并将其应用在攻防演练过程中；路由器设备需要包括 MIPS 架构和 ARM 架构；工控系统靶标能并将其应用在攻防演练过程中。 12. 数据空间安全共享靶标资源：以“数据孪生 + 风险靶场”为核心，构建覆盖联邦节点、区块链、访问控制的全要素数据安全演练环境，具备以下专业化能力：全链路数据孪生:支持 12 类数据要素（隐私标签、共识哈希、密钥协商、差分噪声、合规审计、零知识证明、侧信道、智能合约溢出、联邦漂移、访问滥用、元数据泄露）秒级渲染；触发即自动推送隔离、审计、恢复指令；支持分级预警（低/中/高/危急）与日志、警报、仪表盘等多通道发布；3 个高危害安全场景，每项均提供完整检测链、脚本及补丁回归测试等。 13. 边缘计算基站监控系统仿真靶标资源：面向 5G 网络安防教学与科研场景，构建高保真、高威胁、可演进的数字靶场，通过仿真先进的切片隔离技术，对环境的基站、UE、MEC 的等重点区域的全方位、全天候监控； 支持 20+ 5G 网络真实高危漏洞场景库:系统内置覆盖“RAN-核心-边缘”全栈的 20 余种已验证的高危漏洞与测试链，每项均配套利用脚本、测试路径、取证痕迹及处置建议； 教学与实战双模交付:教学模式：分层次实验包（认知、加固、应急），附带 ATT&CK 映射与能力画像；实战模式：红蓝对抗、护网演练、案件复盘，支持多角色并发（运维、厂商、院校师生等）。 14. 密钥分发网络监测系统仿真靶标资源:面向通信安全与网络安全联合演练场景，全栈孪生监测链路:等比例还原 QKD 节点核心部件：光源、探测器、纠缠源、密钥蒸馏器、侧信道传感器等；支持多站多链并发仿真场景：可同时模拟 2 个节点、6 条链路、20 个密钥池的分布式监测网络；高危漏洞风险场景（3 类真实场景，每项均配套完整 PoC 脚本、检测链、补丁验证脚本等）。 15. 仿真场景链路支持特性仿真，支持拓扑绘制时选择节点间的链路，实现光纤和双绞线类型的仿真配置，也可自定义参数进行配置；并支持带宽、丢包率、延迟等特征的配置；能够提供高性能的链路特性。支持仿真节点资源类型包含虚拟终端、虚拟网络设备、虚拟安全设备、物理接入设备等；节点支持 KVM 虚拟机和 docker 容器

扫描全能王
3亿人都在用的扫描App

		类型。支持对场景中的仿真节点进行监控，支持仿真节点的无感知监控与基于 agent 的节点监控形式；无感知监控：即无需于节点中内置任何代码即可获取节点的 CPU 等资源的使用情况；agent 节点监控，能够获取节点内的进程、端口等情况。
10	学生靠背椅	1.单层网布，尼龙塑胶扶手；定型坐垫，海绵双层 3D 网格面料，一次成型免安装设计钢制椅架，塑料脚垫；颜色定制。
11	多媒体讲台	1.可放多种教学设备:电脑主机、纯平或液晶显示器、键盘鼠标、笔记本电脑、实物展示台、功放等设备；接口配备:电源，笔记本 VGA、HDMI 接口、USB、音频、视频、网口、话筒，并提供满足教学与实训运行所需的标准化环境建设及配套基础设施。
12	实训 LED 显示屏	1.彩色，LED 像素点间距 2.5mm;像素密度 160000 点/㎡；支持信源接入状态显示，可通过设备上的 source 按键、客户端、遥控器的快捷键或菜单键、设备自带 Web 浏览器进行信源切换；可将输入信号进行缩放，以匹配 LED 的分辨率进行输出。 2.显示屏幕峰值亮度 600cd/㎡,峰值功耗 440W/㎡ ，平均功耗 148W/㎡；具有 2 个控制网口，支持 TCP/IP 网络协议，双网口均可用于控制设备或设备网络级联，其中一个接口用于控制设备时，另外一个网口就用于设备网络级联。
13	演示显示屏	1.整机屏幕采用 65 英寸液晶显示器，整机采用 UHD 超高清 LED 液晶屏，显示分辨率 3840*2160，可视角度 178°；用于教学演示投屏，分列教室左右两侧，更利于学生观看。整机屏体无需操作即可实现蓝光防护，具备物理防蓝光功能；整机采用硬件低蓝光背光技术，在源头减少有害蓝光波段能量。整机支持 windows 系统和 android 系统之间进行串口通信，android 系统可获取 OPS 的 CPU 型号，内存以及网卡型号，序列号等信息，android 系统下可一键还原 windows 操作系统，控制 OPS 的开关机。 2.整机内置支持 2.4GHz 和 5GHz 双频 WiFi，支持蓝牙 5.4；Wi-Fi 和 AP 热点工作距离 15m，AP 热点支持 50 个用户终端在线网络连接；整机支持锁屏，并具有多种解锁方式，USB key 插入后解锁，密码解锁，刷 IC 卡解锁，扫二维码解锁，通过手机应用程序扫描二维码解锁并自动登录教学软件账号，老师无需二次登陆；在整机没有网络的情况下，也可以支持手机扫码解锁。
14	机柜	1.42U，颜色：黑色，配置 8 位 10A PDU 插排 1 个，固定板 3 块，内嵌风扇部件 1 组，4 只两英寸重型脚轮，M12 支脚 4 只，M6 方螺母钉 40 套，内六角扳手一只。
15	教学终端	*1.CPU：14 核，20 线程；内存：32GB DDR4；硬盘：1TB 固态硬盘；接口：USB 接口 11 个（其中一个为 USB Type-C）；显卡：集成显卡；自适应千兆网卡；扩展槽：1 个 PCI-E*16、1 个 PCI-E*1、3 个 M.2 接口(其中 2 个支持扩展 SSD)；机箱：标准立式机箱，机箱 15L，顶置电源开关键，方便使用；电源：200W；键鼠：防水抗菌键盘、抗菌鼠标；操作系统：出厂预装正版操作系统；安全特性：USB 屏蔽技术，可设置为仅识别 USB 键盘、鼠标，无法识别 USB 读取设备，有效防止数据泄露。 支持通过微信服务平台提供全天候自助服务和 12 小时在线人工服务，支持添加单位服务账号，成批添加并绑定设备，实现保修期查询，预约、维修，咨询在线客服及查询服务网点等功能，并提供满足教学与实训运行所需的标准化环境建设及配套基础设施。

扫描全能王
3亿人都在用的扫描App

		*2. 供应商提供的货物配置不能低于《台式计算机政府采购需求标准（2023 年版）》（财库〔2023〕29 号）实质性指标的最低要求（安全可靠测评除外）
16	教师靠背椅	1. 牛皮覆面，厚度 1.5mm，不含禁用偶氮染料；泡棉：内衬优质环保高回弹一次成形泡棉，座密度 35Kg/m³、背密度 30Kg/m³、回弹性能 40%、压缩变形率 6%； 2. 衬板：E1 级环保弯曲木胶合板，厚度 12mm，阻燃、透气、吸音抗收缩特性，长久使用不变形、不塌陷；特优底盘、具备升降，多段倾仰锁定功能、靠背頃仰软硬度可根据不同使用需求自行调节、弯曲实木扶手嵌牛皮软包、靠背加厚有腰托结构，座面舒适型加厚处理、最低座面高 420mm；颜色可选。
17	学习终端	*1. CPU：14 核，20 线程；内存：32GB DDR4；硬盘：1TB 固态硬盘；接口：USB 接口 11 个（其中一个为 USB Type-C）；显卡：集成显卡；自适应千兆网卡；扩展槽：1 个 PCI-E*16、1 个 PCI-E*1、3 个 M.2 接口(其中 2 个支持扩展 SSD)；机箱：标准立式机箱，机箱 15L，顶置电源开关键，方便使用；电源：200W；键鼠：防水抗菌键盘、抗菌鼠标；操作系统：出厂预装正版操作系统；安全特性：USB 屏蔽技术，可设置为仅识别 USB 键盘、鼠标，无法识别 USB 读取设备，有效防止数据泄露。 支持通过微信服务平台提供全天候自助服务和 12 小时在线人工服务，支持添加单位服务账号，成批添加并绑定设备，实现保修期查询，预约、维修，咨询在线客服及查询服务网点等功能，并提供满足教学与实训运行所需的标准化环境建设及配套基础设施。 *2. 供应商提供的货物配置不能低于《台式计算机政府采购需求标准（2023 年版）》（财库〔2023〕29 号）实质性指标的最低要求（安全可靠测评除外）
18	学生六角形实验桌	1. 饰面:三聚氰胺板，基材刨花板密度为 0.68kg/cm3,甲醛:E1 级，游离甲醛释放量 3.0mg/100g。尺寸：2500mm（直径）×775mm（高）、桌面为内切六边形;封边材料:优质 PV 塑胶边，厚度 2.0 毫米热压成型不易开裂，粘合符合剂符合国家标准。台面 2.5cm 厚度板材，侧板 2.5cm 厚度。五金配件:采用冷轧钢板经喷涂处理，开闭灵活无噪音。

扫描全能王
3亿人都在用的扫描App