

政府采购项目

市财采计【2026】00839号

西安文理学院
多学科交叉融合的
网络空间安全实验室建设项目
供 货 合 同

甲 方：西安文理学院

乙 方：西安四叶草信息技术有限公司

2026年6月

中国 西安

供货合同

甲方：西安文理学院

乙方：西安四叶草信息技术有限公司

在西安市财政局政府采购管理处的监督管理下，按照政府采购程序组织竞谈采购，确定西安四叶草信息技术有限公司为中标供应商。依据《中华人民共和国政府采购法》、《中华人民共和国招标投标法》、《中华人民共和国民法典》，经甲、乙双方协商，确认方确认，达成如下条款。

一、合同标的物内容及数量

产品名称	品牌	型号	配置参数	数量	单价	总价
万兆交换机	中锐	S6120-20XS4VS2QXS	见附件1	1	8,000.00	8,000.00
千兆交换机	中锐	S2910-24GT4XS-E		1	4,000.00	4,000.00
实验平台计算节点	航天联诚	SD2108-HL		2	135,000.00	270,000.00
实验平台存储节点	航天联诚	SD2112-HL		2	125,000.00	250,000.00
洞镜异常行为（APT）实时监测平台V4.0[软著登字第10718272号]	四叶草安全	CLS-DJ V4.0		1	170,000.00	170,000.00
网络仿真靶场平台V4.0[软著登字第13877988号]（教学实训系统）	四叶草安全	CLS-ADP-SR 1.0		1	164,700.00	164,700.00
网络仿真靶场平台V4.0[软著登	四叶草安全	CLS-ADP-SR 1.0		1	80,000.00	80,000.00

产品名称	品牌	型号	配置参数	数量	单价	总价
字第13877988号] (考核评估系统)						
网络仿真靶场平台V4.0[软著登字第13877988号]] (竞赛系统)	四叶草安全	CLS-ADP-SR 1.0		1	125,000.00	125,000.00
网络仿真靶场平台V4.0[软著登字第13877988号]] (虚拟化仿真引擎系统)	四叶草安全	CLS-ADP-SR 1.0		1	45,000.00	45,000.00
网络仿真靶场平台V4.0[软著登字第13877988号]] (场景拓扑管理系统)	四叶草安全	CLS-ADP-SR 1.0		1	65,000.00	65,000.00
信息技术安全基础课程资源	四叶草安全	CLS-ADP-SR 1.0		1	15,000.00	15,000.00
渗透测试课程资源	四叶草安全	CLS-ADP-SR 1.0		1	15,000.00	15,000.00
SQL注入漏洞脆弱性分析实验课程资源	四叶草安全	CLS-ADP-SR 1.0		1	15,000.00	15,000.00
XSS漏洞脆弱性分析实验课程资源	四叶草安全	CLS-ADP-SR 1.0		1	15,000.00	15,000.00
CSRF漏洞脆弱性分析实验课程资源	四叶草安全	CLS-ADP-SR 1.0		1	15,000.00	15,000.00
逻辑安全漏洞脆弱性分析实验课程资源	四叶草安全	CLS-ADP-SR 1.0		1	15,000.00	15,000.00

产品名称	品牌	型号	配置参数	数量	单价	总价
目录遍历漏洞脆弱性分析实验课程资源	四叶草安全	CLS-ADP-SR 1.0		1	15,000.00	15,000.00
文件管理漏洞脆弱性分析实验课程资源	四叶草安全	CLS-ADP-SR 1.0		1	15,000.00	15,000.00
文件上传漏洞脆弱性分析实验课程资源	四叶草安全	CLS-ADP-SR 1.0		1	15,000.00	15,000.00
文件包含漏洞分析实验课程资源	四叶草安全	CLS-ADP-SR 1.0		1	15,000.00	15,000.00
源码审计技术实验课程资源	四叶草安全	CLS-ADP-SR 1.0		1	15,000.00	15,000.00
密码实验课程资源	四叶草安全	CLS-ADP-SR 1.0		1	15,000.00	15,000.00
网络攻防竞赛课程资源	四叶草安全	CLS-ADP-SR 1.0		1	15,000.00	15,000.00
智能安全实验课程资源	四叶草安全	CLS-ADP-SR 1.0		1	15,000.00	15,000.00
网络仿真靶场平台V4.0[软著登字第13877988号]（攻防工具库与漏洞资源）	四叶草安全	CLS-ADP-SR 1.0		1	30,000.00	30,000.00
多维智显仪	大眼橙	定制		1	12,000.00	12,000.00
合计	税率：13% 不含税价格：壹佰贰拾陆万捌仟柒佰陆拾壹元零陆分（¥1268761.06） 含税总金额：壹佰肆拾叁万叁仟柒佰元整（¥1433700.00）					

二、合同价款

(一) 合同总价款为人民币 (大写) 壹佰肆拾叁万叁仟柒佰元整 (¥ 1433700.00)。

(二) 合同总价包括: 设备费、税费、运杂费 (含保险费)、安装调试费及其它一切相关费用。

(三) 合同总价一次包死, 不受市场价格变化因素的影响。

三、款项结算

(一) 履约保证金缴纳

1、乙方应在本合同生效后【5】个工作日内, 向甲方足额提交履约保证金。履约保证金金额为本采购包合同总金额的 5%, 即人民币柒万壹仟陆佰捌拾伍元整 (¥71,685.00)。

2、履约保证金须以银行转账等非现金方式提交。乙方以银行、保险公司出具的合法有效保函作为履约保证金的, 甲方不得拒绝接收。

3、本采购包项目通过最终验收且合格满一年后, 经甲方核查确认乙方已完全履行本合同各项义务、无违约赔偿责任及其他未决遗留问题的, 甲方在【15】个工作日内将履约保证金无息退还至乙方指定银行账户。

4、若乙方违反本合同约定, 给甲方造成经济损失的, 甲方有权直接从履约保证金中扣除相应的损失赔偿金额; 履约保证金不足以弥补甲方损失的, 甲方有权就差额部分继续向乙方追偿。

(二) 支付方式:

1、项目完成交付并验收无异议, 达到付款条件起30日内, 支付合同总金额的100.00%。乙方申请付款前, 应向甲方提供合法有效的增值税专用发票。发票不符合财税规定或无法认证抵扣的, 甲方有权暂缓付款且不承担违约责任。

2、结算方式: 银行转帐。

3、结算单位: 发票开西安文理学院。

四、双方的权利和义务

(一) 甲方的权利和义务

1、甲方应按约定支付合同款项。

2、甲方应为乙方提供施工所需的水、电、网络接入及现场协调，配合乙方进行系统对接。

3、甲方有权对乙方的履约情况进行监督，如发现乙方人员不称职或违规作业，有权要求乙方更换。

4、甲方有权依据合同约定的技术标准组织验收，对不符合要求的部分，有权要求乙方整改直至退货。

（二）乙方的权利和义务

1、质量保证：

（1）硬件：必须为全新原厂正品，符合国家质量检测标准。

（2）软件：必须为正版授权，无病毒、后门，不包含恶意代码。乙方保证对其提供的软件拥有合法的知识产权或授权，不存在任何侵权纠纷。

2、交钥匙责任：乙方负责项目实施的全过程，包括但不限于硬件安装、软件部署、数据迁移、接口开发等，确保系统最终可用。

3、人员要求：乙方指派的项目经理和技术负责人须经甲方认可，未经甲方同意不得随意更换。

4、培训义务：乙方应在项目验收前，免费为甲方操作人员和管理人员提供操作使用培训。

5、保密义务：乙方对在项目实施过程中接触到的甲方相关数据、业务信息负有严格的保密责任，不得向第三方泄露。

五、交货条件：

（一）交货地点：西安文理学院，具体地点（楼、房）由文理学院确定。

（二）交货期：自合同签订之日起30个工作日。

六、运输

乙方负责所有设备及材料的运输。确保设备安全、完整到达使用地点，运杂费用包含在总价内，包括设备从供货地点到使用地点的运输费、保险费、搬运费、上楼费等。

七、质量保证

（一）质量保证期内，非人为原因造成的产品故障由乙方免费保修。乙方在接到甲方的维修通知后24小时内上门为甲方提供免费维修服务。如乙方未及

时处理，甲方可另行选择第三方处理，相关费用甲方可直接从履约保证金中双倍扣除。

(二) 质量保证期内，乙方无法修复非人为原因造成的产品故障或经2次修理，机器仍然无法正常使用，甲方可选择让乙方更换或退货，且不再退还质量保证金。

(三) 乙方应严格按照国家有关标准和规定进行制造和检验，货物及零部件均为全新未用过的，且符合本合同附件中规定。

八、售后服务

(一) 产品质量保证期和售后服务期：从安装调试验收合格之日起 36 个月。

(二) 售后服务

- 1、甲方享有产品生产厂家的一切品牌售后服务；
- 2、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等；
- 3、乙方应在售后服务内容保证书（详见附件2）中明确售后服务内容、响应时间、范围、方式、收费标准等，并进行其他售后服务工作。
- 4、设备投入正常运行后，乙方应定期回访甲方。

九、技术与服务

(一) 技术资料：

乙方应向甲方提供完整、准确、清晰的技术资料，且所有资料均须提供中文版本。具体包括但不限于：

- 1、产品合格证：硬件原厂出厂合格证及防伪查询标签。
- 2、产品使用说明书（中文）：
 - (1) 硬件：提供原厂中文安装手册、操作手册、维护保养手册、故障诊断指南及备品备件清单。
 - (2) 软件：提供详细的功能说明书、用户操作手册（含截图）、系统管理员手册、API接口开发文档。
- 3、调试记录，调试报告：包括软件功能联调报告。

4、其它资料：

(1) 知识产权证明：软件著作权证书复印件、原厂授权函（OEM）。

(2) 培训资料：培训课件（PPT/PDF）、培训签到表及考核记录。

(二) 服务承诺：以附件2售后服务承诺为准。

十、验收

(一) 设备到货后，乙方进行自检，合格后准备验收文件，并书面通知甲方。

(二) 甲方根据合同要求对设备进行外观验收，确认设备的产地、规格、型号和数量。

(三) 乙方按照合同要求完成设备的安装调试及必要操作培训后，提请甲方进行验收，甲方结合设备安装情况及操作人员培训情况验收合格后，乙方填写验收单，并向甲方提交所有资料，以便甲方日后管理和维护。

(四) 验收依据：

- 1、本合同文本；
- 2、招标文件及乙方的投标文件；
- 3、国家相应的标准、规范。

十一、违约责任

(一) 未按合同要求提供产品或设备质量不能满足技术要求，甲方会同监督机构、采购代理机构有权终止合同并对乙方的违约行为进行追究，同时按政府采购供应商管理办法进行相应的处罚。

(二) 甲方应按照合同约定的时间和比例向乙方支付货款。甲方逾期付款的，应按照逾期未支付货款金额的同期银行贷款利率向乙方支付违约金。因财政资金拨付、财政审批、国库集中支付等非甲方原因导致付款延期的，不视为甲方违约。

(三) 乙方交付的标的物为数物，其中一物不符合约定的，甲方可以就該物解除合同，并要求乙方按照合同中该物的 20 %支付违约金。由此给甲方造成损失的，乙方还应当赔偿损失。

(四) 乙方交付的标的物为数物，其中一物不符合约定的，但该物与其他物分离使标的物的价值显受损害的，当事人可以就数物解除合同，并要求乙方按照合同总价款的 20 %支付违约金。由此给甲方造成损失的，乙方还应当赔偿损失。

(五) 乙方逾期交货的，每逾期一日按合同价款的 3‰ 向甲方支付违约金。逾期达 5 日，甲方有权解除合同，乙方应按合同价款的 20 %向甲方支付违约金，并赔偿由此给甲方造成的相关经济损失。

(六) 乙方未在约定的期限内完成安装调试并经甲方验收合格的，每逾期一日按照合同总价款的 3 ‰向甲方支付违约金。逾期达 5日，甲方有权解除合同，并要求乙方按照合同总价款的 20 %支付违约金。由此给甲方造成损失的，乙方还应当赔偿损失。

十二、合同争议解决的方式

本合同在履行过程中发生的争议，由甲、乙双方当事人协商解决，协商不成的提交甲方所在地法院诉讼。

十三、合同生效

本合同一式玖份，本合同甲、乙、确认各方签字盖章后生效，合同执行完毕后，自动失效（合同的服务承诺则长期有效）。

十四、其他事项

(一) 招标文件、投标文件、澄清表（函）、中标通知书、合同附件均成为合同不可分割的部分。

(二) 合同未尽事宜，由甲、乙双方协商，经确认方确认后，作为合同补充，与原合同具有同等法律效力。

(三) 合同一经签订，不得擅自变更、中止或终止合同。对确需变更、调整或中止、终止合同的，应重新签订补充协议。如未签订补充协议则仍以原合同为准。

(四) 本合同按照中华人民共和国的现行法律进行解释。

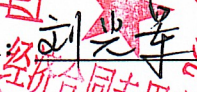
以下无正文

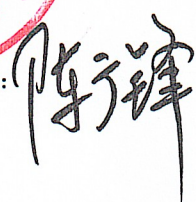
甲 方（法人公章）

单位名称：西安文理学院

地 址：西安市太白南路168号

法定代表人：  (签字)

代理人：  (签字)

项目管理单位负责人： 

联系电话：

签订日期：2026年 6 月 26 日

见证方：陕西正信招标有限公司

日期： 2026 年 6 月 26 日

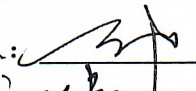
乙 方（法人公章）

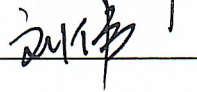
单位名称：西安四叶草信息技术有限公司

地 址：陕西省西安市高新区鱼化街办软

件新城天谷八路156号云汇谷C2楼

1701室

法定代表人：  (签字)

代理人：  (签字)

开户银行：浦发银行西安分行营业部

帐 号：72010078801700004298

联系电话：

签订日期：2026年 6 月 26 日



1. 附件 1 主要技术指标参数

序号	采购项 目名称	主要内容 / 主要技术参数
1	万兆交换机	1、支持并实配10G/1G接口数20，25G/10G接口数量4，40G接口数2，整机可扩展支持10G接口数32； 2、交换容量2.56Tbps。包转发率570Mpps； 3、支持硬件健康状态可视化，可以对风扇状态、电源、温度、板载电压进行监控，尤其是在日常巡查中发现电压异常前兆，可及时处理，避免出现电压异常宕机； 4、支持硬件层级双boot，采用两个FLASH芯片存储boot软件（系统引导程序），实现硬件级boot冗余备份，避免因FLASH芯片故障导致交换机无法启动； 5、设备支持故障隔离技术，用于监测光模块状态，一旦出现故障，可马上识别、并将故障模块隔离； 6、支持RIP，OSPF，BGP，RIPng，OSPFv3，BGP4+； 7、支持多虚一技术，可将多台物理设备虚拟化为一台逻辑设备统一管理； 8、支持CPU保护功能，能够针对发往CPU处理的各种报文进行流区分和优先级队列分级处理，保护交换机在各种环境下稳定工作； 9、支持专门基础网络保护机制，能够限制用户向网络中发送数据包的速率，对有攻击行为的用户进行隔离，保证设备和整网的安 全稳定运行； 10、提供150W交流电源模块，万兆LC接口模块，适用于SFP+接口。
2	千兆交换机	1、交换容量670Gbps，包转发率170Mpps； 2、固化10/100/1000M以太网端口24，固化1G/10G SFP+XS接口4个； 3、产品端口浪涌抗扰度10KV；

		4、支持IPv4和IPv6的静态路由、RIP/RIPng、OSPFv2/OSPFv3等三层路由协议； 5、支持专门针对CPU保护机制功能，保障CPU安全； 6、支持专门基础网络保护机制，能够限制用户向网络中发送数据包的速率，对有攻击行为的用户进行隔离；（需提供第三方检测机构出具的检测报告） 7、支持虚拟化功能，支持OpenFlow 1.3协议，设备MAC地址16K。
3	实验平台 计算节点	1、CPU满足国产信创，不低于2颗CPU、16核32线程，基础主频2.5GHz，双路均衡部署，支持国产操作系统与虚拟化平台。 2、内存：64GB DDR4*8，支持内存热备、镜像、插槽扩容功能。 3、固态硬盘（SSD）：960GB 2.5英寸企业级 SSD，SATA/SAS接口，3DTLC颗粒。 4、机械硬盘（HDD）：8TB 3.5英寸企业级 HDD，7200转，满足数据存储。 5、阵列支持：板载/外接RAID支持 0/1/5/10/JBOD，保障数据安全。 6、盘位：兼容准系统标准 2.5"/3.5" 盘位，支持热插拔。 7、规格：800W1+1冗余双电源，CRPS工业级模组。 8、特性：热插拔、冗余备份，单电源故障不宕机，支持在线更换。 9、效率：92%白金效率，节能降噪，支持宽幅电压输入。 10、扩展：提供标准PCIe扩展插槽，满足网卡、RAID卡、HBA 卡等扩展需求。
4	实验平台 存储节点	1、CPU：配置2颗国产处理器；单颗处理器主频2.20 GHz，核数32核，缓存64MB，TDP140W。 2、内存：64GB* 4 DDR4-3200MHz内存 3、硬盘：1*8TB 7.2K SAS盘，1*3.84T NVME-SSD固态硬盘 4、Raid卡：1张，8通道，2GB缓存，支持raid 0,1,5,6,10,50,60,JBOD。 5、网卡：配置4口千兆以太网卡

		6、电源：配置800W（1+1）冗余电源 7、服务器硬件经过物理老化处理测试，MTBF无故障运行时间超50000小时 8、具备勒索功能模块，支持特殊格式病毒检测率应达到100%、流行病毒检测率和清除率应达到98。3%以上。
5	洞镜异常行为（APT）实时监测平台V4.0[软件著作权第10718272号]	1、标准机架式，2*8核CPU（信创），128GB内存，系统盘：240GB SSD，数据盘：1TB，板载2个千兆电口，6个空闲PCI-E可扩展槽位，双电源。 2、综合安全态势，全局总览整体安全态势，展示用户最关心的告警层风险内容，包括告警分析和风险主机分析，支持2D/3D风险威胁地图切换； 3、威胁事件态势，监控整体威胁事件态势，从内对内，外对内和对内三个方向进行描述；具备威胁事件类型、事件总数、热点事件、事件趋势等内容的统计与展示功能； 4、内置威胁情报检测，APT情报检测能力，内置IOC数据库覆盖主流的APT家族覆盖240个家族； 5、APT通信特征检测，APT威胁情报关联恶意文件； 6、支持DNS隐蔽隧道通信检测：基于隧道工具的DNS隐蔽隧道；DNS直连隧道；APT32利用DNS隧道通信；基于DNS隐蔽隧道关联分析发现受控主机； 7、支持僵尸网络流量通信检测：基于同源僵尸网络通信发现受控主机；基于流量特征检测僵尸网络通信； 8、支持webshell检测：基于机器学习方法检测PHP/ASP/JSP动态脚本的webshell上传；检测冰蝎、蚁剑等加密webshell通信；检测webshell通信行为； 9、支持基于智能模型（人工智能模型）检测DGA域名、恶意代码加密外联通信流量、网络内暗网Tor流量、DNS隐秘隧道通信、ICMP隐秘隧道通信等； 10、具备从流量中还原文件并进行威胁检测的能力，文件类型应包括docx、xlsx、pptx、wps、doc、xls、ppt、rtf、pdf、exe、elf、zip、7z、rar、gzip、tar、pyc、py、html、php、xml、bat、swf、jpeg、png、pcap、class、jar、js、jsp、asp、

		torrent、apk等； 11、支持威胁检测白名单，支持类型包括威胁事件的源/目的IP、包含的域名/URL、威胁类别、规则ID。
6	网络 仿真靶场 平台 V4.0[软 著登字第 13877988 号]（教 学实训系 统）	1、支持按学员专业（如信息安全、计算机学科与技术）、岗位（安全运维、应急响应、渗透测试等）、级别（初/中/高）定制不同梯度学习路线（投标文件中提供软件功能截图证明）。 2、学习路线支持创建多阶段，每个阶段支持关联课程专题、科目训练资源。 3、学习路线阶段及资源可通过鼠标拖动以移动顺序及位置。 4、支持制定学习任务，管理员可下发任务，也可查看任务详情，学习任务支持设置学员完成率指标。 5、学习任务包含专题学习、学习路线、任务排行，注重基础知识的理解和掌握，为后续的实践和考核打下基础。支持动态扩展的接口，能够导入新的课程。支持学生基于PPT、PDF、Word文档等知识课件学习，支持课件内容在线预览，支持操作文档和视频演示的学习模式（投标文件中提供软件功能截图证明）。 6、支持学习生命周期私有网盘功能，可分享文件、上传文件、下载文件和自定义创建文件夹功能。 7、理论教学手段支持4种，包括课件、视频、实验、练习。 8、支持资源共享，查看管理员或他人的共享资源；支持上传资源信息，根据资源关键字、资源分类检索资源（投标文件中提供软件功能截图证明）。 9、支持学习路线的制定，学习路线可关联专题，学生可根据学习路线进行学习，支持查看任务参与人员排行。 10、课程专题支持编辑模式，编辑模式下拖动专题小节名称可调整节顺序，双击节名称可以编辑。支持专题资料上传共享，用户相互讨论交流。 11、视频小节支持上传视频及讲义文件，讲义支持的格式包含PPT、PDF、Word，视频及讲义支持在线预览功能。 12、实验小节支持关联实验工具、实验视频、实操环境、实操自测题、实验手册。 13、学习任务支持从人员维度、课程专题维度、专题小节维度查看学员学习情况。

		14、支持参训人员对视频播放的次数、学习的时长、学习的时间进行记录。 15、支持参训人员基于训练的视频进行笔记记录，能够截取视频播放的画面以及当前视频播放的时间点进行笔记记录，并支持输入文字对当前记录的点进行文字说明。 16、视频笔记支持统一查看功能，能够基于视频笔记自动定位到视频播放记录点并进行播放。 17、支持当前学习视频内容同类知识视频的推荐并进行列表展示，能够点击列表进行视频学习内容的切换。 18、学员用户支持实验台功能，可自主拖拽的方式绘制拓扑。 19、实验台支持流量监控功能，可在网络拓扑中标记采集规则。 20、实验台支持选择开放的场景拓扑进行二次绘制。 21、课程专题、实操科目支持关联知识体系和技能体系中的知识点和技能点。 （演示项）22、实操科目支持一键启动、一键释放，可设置延时启动与释放。 （演示项）23、实操科目支持两种模式：可新建自定义场景拓扑，也可关联已创建拓扑，适配不同实操需求。 24、实操科目支持创建多阶段任务，每个任务支持关联自测点、操作手册、视频、资料文档。 25、实操科目支持开放给学员用户自主练习。 26、开放课程专题、开放渗透测试科目支持学员学习过程记录，包含学习进度、完成时间。 27、每年提供配套课程服务64个学时，提供配套线下教学服务，包含理论授课、现场实操指导、案例复盘分析、小组协作演练、一对一答疑解惑等教学环节，授课讲师需提供在职证明。
7	网络仿真 靶场平台 V4.0[软 著登字第	1、支持对考试训练所使用的试卷进行管理，包括但不限于理论题目、实操题目、场景题目； 2、支持对试卷总分、及格分数进行管理，支持智能组卷、题目库导入和自建题目等多种组卷方式； 3、可针对实操题目、场景题目灵活配置开放资源状态，开放之后学员可在前台进行自主实操练习； 4、支持个人考核与分组考核两种考核模式，可自定义考核时间、考核类型；

13877988	5、考核活动支持配置用户名打码、考核排行是否展示、考核结束之后是否可查看详情； 6、考核活动支持自建试卷和试卷库导入两种模式； 7、考核活动试卷支持另存到试卷库； 8、考核裁决支持自动化裁决和人工裁决； 9、支持根据题目类型、题目数量、题目分值自动组卷试卷； 10、支持一键分配、启动与释放考核环境； 11、支持基于拓扑的场景实操考核功能，每个学员环境逻辑隔离独享； 12、支持考核环境拓扑的设置，支持根据考核模式进行设置，支持开放拓扑和不开放拓扑，支持拓扑是否可编辑配置； 13、支持考核类型包括渗透测试考核（不开放拓扑）、应急响应考核（开放拓扑）、日常运维考核（支持编辑和配置下发考核拓扑）； 14、考核活动支持一键下发、暂停、恢复、结束状态控制； 15、考核活动支持管理员在排行榜修改学员理论得分、实操得分、场景得分，修改后可一键发布成绩； 16、支持从擅长岗位、擅长知识域、擅长技术领域、擅长技术方向多维度展示个人能力画像； 17、支持以雷达图的方式展示学员在所有岗位的各维度的已掌握的知识和技能情况； 18、人员能力画像支持评估画像参数设置，可设置学习、考核权重及技能掌握的熟练程度； 19、支持针对每个学员进行人员画像，包括学习统计、知识画像、技能画像和岗位画像； 20、支持自定义岗位体系，岗位画像支持展示岗位方向、知识点数、技能点数、课程专题数、课时、渗透测试科目数； 21、支持自定义知识体系，知识体系包含三层架构，包括知识域、二级分类、知识点，知识域30个，二级分类160种，知识点700个；
----------	---

		22、支持自定义技能体系，技能体系包含三层架构，包括技能域、二级分类、技能点，技能域20个，二级分类90种，技能点400个。
8	网络仿真靶场平台V4.0[软件著作权第13877988号]（竞赛系统）	1、支持对比赛信息进行配置，如赛事名称、比赛时间、计分模式、比赛模式、比赛类型、报名审核机制，支持对展示模式（真实信息或者编号代替）、排行榜展示、比赛详情、主办方信息等配置。支持自定义赛前宣传页； 2、支持对参赛人员、观光人员进行管理；管理包括人员移出、批量移出、审核、批量审核、添加（从人员管理移入）、一键导出所有人员； 3、支持管理员对场景进行一键下发、一键启动、分批释放等操作； 4、支持管理员对赛事进行赛前测试，可设置测试开始时间，截止时间。支持添加测试人员以参赛人员的身份进行测试。测试数据仅测试人员能看到。测试完毕后，可以一键清除测试数据； 5、支持在竞赛过程中控制每个赛题的开启和关闭状态，实时监控所有参赛队伍的赛题服务状态； 6、支持动态FLAG记录、作弊监控、IP记录和处罚警告等防作弊功能； 7、支持针对参赛人员赛事提交Writeup对应的解答过程进行管理；支持以文件形式提交查看； 8、支持writeup审核和清空； 9、支持统计所有赛段得分、排名和导出排行； 10、支持根据平台资源情况，配置赛题题目环境属性（个人独享、小组共享、全员共享）等； 11、支持管理员实时监控平台参赛人员的访问日志、Flag记录、异常监控，并据此观察攻防行为，防止竞赛过程中的作弊行为； 12、CTF赛段包括赛段时间、计分模式（固定计分、动态计分），是否加成（一血加成5%，二血加成3%，三血加成1%）； 13、支持静态FLAG和动态FLAG两种模式； 14、理论赛支持防作弊机制，包括题目乱序、选项乱序； 15、AWD赛段支持配置赛段时间、回合时长、加固阶段、回合分数、宕机分数信息；

	16、支持理论赛、攻防夺旗赛（CTF）、攻防对抗赛（AWD）赛制任意赛制的混合组合； 17、支持将队伍的得分情况以排行榜形式展示，支持以题目的维度展示成功拿下一血、二血、三血的队伍名称及其得分； 18、支持CTF题目、AWD题目开放给学员自主实操练习。 19、每年提供针对全国大学生信息安全竞赛，赛前连续集中培训64课时，授课讲师团队5人，需提供在职证明。
网络仿真靶场平台V4.0[软著登字第13877988号]（虚拟化仿真引擎系统）	1、支持虚拟机、容器等多种虚拟节点的混合组网，提供多层复杂网络结构的编排和调度能力； 2、能够开展网络环境构建，按需分配资源，灵活柔性配置资源，动态生成满足要求的训练环境；能够快速恢复训练环境；能够按需销毁训练环境，回收训练环境占用资源； 3、具备横向扩容，支持AMD、Intel、ARM等处理器混合构建统一资源池，并支持不同架构镜像环境的自动分配，以便于大规模场景/人数的使用； 4、实现设备虚拟化、网络虚拟化，使用户可以在系统中拖拽自主构建虚拟网络环境； 5、支持安全组功能，能够创建和删除安全组，在安全组下能配置，场景编排时可在虚拟机的网卡上选择和绑定安全组； 6、支持虚实结合组网，将物理设备接入拓扑与虚拟节点构建混合网络，支持实物设备并联和串联两种方式接入场景拓扑中使用； 7、支持对仿真网络指定IP地址功能，可通过平台编辑实例的IP地址，虚拟机启动时自动写入虚拟机实例； 8、支持对启动的虚拟机实例配置端口隔离功能，防止IP欺骗影响同网段主机； 9、启动的场景拓扑支持网络流量抓包分析功能，支持2种方式：实时本地Wireshark远程抓包分析和在线B/S形式抓包分析； 10、支持对启动虚拟实例进行剪贴板、文件上传操作； 11、支持在场景拓扑中进行背景流量模拟，模拟方式两种，包括pcap包重放和脚本模拟； 12、支持无线信号模拟，可对无线通信进行抓包测试； 13、支持虚拟化嵌套功能，支持嵌套启动的虚拟化软件4种：包括VMware、Virtualbox、QEMU等； 14、支持计算方案管理，指定分配给虚拟机的内存、CPU等配置，包括CPU个数、CPU频率以及内存；

	15、支持自动识别接入系统的物理USB设备、支持自动识别接入系统的物理无线设备； 16、构建云计算系统仿真环境，支持对关键组件如CPU、GPU和存储的虚拟化技术； 17、支持链路的特性仿真，内容包括带宽、延迟、丢包率，支持自由控制链路特性仿真内容； 18、提供构建多种链路媒介及带宽的仿真，包括光纤、双绞线（可以指定双绞线类型）等； 19、支持配置全局DNS，无需独立的DNS服务器即可完成DNS解析，以方便模拟更为真实的Internet网络； 20、根据场景中设置的靶标和拓扑结构，系统自动计算出场景总体占用的vCPU、内存及硬盘占用数据； 21、场景拓扑搭建支持虚拟机间的链路设置，网速限制配置，支持QoS配置，设置丢包率及延迟时间； 22、支持实物设备通过串联、并联形式加入任意虚拟网络； 23、支持路由器、交换机设备的串口连接，可使用串口连接至终端设备； 24、虚实结合支持实物以RJ45接入、USB接入及WIFI接入等接口进行场景构建； 25、流量监控具备对仿真网络的流量进行抓包、监听、分析的功能，为防御训练、技术研究、科研测试提供可扩展性工具； 26、支持将场景中的指定节点或指定区域节点流量镜像到特定安全分析节点或设备中进行安全分析与研究； 27、设备虚拟化具备启动引擎包含：KVM、Docker、VPCS、Dynamips等4种； 28、网络虚拟化数字设备包含：交换机、路由器、背景流量模拟、数采交换机、防火墙、网络、NAT网络、桥接网络8种； 29、具备镜像终端访问，支持协议：VNC、RDP、Telnet、SSH4种； 30、预置网络设备靶标3种，包括但不限于路由器、三层交换机、二层交换机等，支持Cisco、HUAWEI、Juniper、H3C、锐捷等主流品牌； 31、支持导入的虚拟镜像文件类型6种，包括RAW、VMDK、ISO、IMG、BIN、TAR等； 32、支持安卓操作系统模拟，支持版本6种，包含：Android4.2、Android4.3、Android4.4、Android7.1、Android7.2、Android7.3；
--	--

		33、支持MacOS操作系统模拟，支持类型4种，包含：Ventura、Catalina、Monterey、BigSur； 34、支持工控靶标环境模拟，厂商类型5种，包含：研华、三菱、Modbus、施耐德、西门子； 35、支持30条工控攻击流量，涉及厂商10家，包括3S-Smart Software Solutions GmbH、Advantech、Wellintech、Autodesk、Omron、Conprosys、Rockwell Automation、InduSoft、Schneider Electric、Siemens； 36、支持15种物联网流量样本类型，涉及厂商10家，包括Apache、Dahua Security、D-Link、HP、Cisco、HUAWEI、Samsung、TP-Link、ASUS、H3C、TOTOLINK、Netgear、Tenda。 37、支持协议仿真：包括DNS、DCE/RPC、EIP、Elasticsearch、FTP、HTTP、IEC 104、Memcached、Modbus等主流协议仿真。 38、支持IOT设备模拟：包括但不限于路由器、防火墙、交换机、摄像头（D-link、TP-Link、Tenda、Cisco、TOTOLink、锐捷、华为等）。 39、支持安防设备模拟：包括但不限于bigip、checkpoint、sonicwall、fortigate、juniper、paloalto等。 40、支持数字化节点，可由用户自定义指定文件、协议、启动命令等参数，实现进程级数字化模拟。
10	网络仿真靶场平台 V4.0[软著登字第13877988号]（场景拓扑管理系统）	1、场景中节点可配置的访问协议3种，包括VNC、noVNC、Telnet等。 （演示项）2、场景节点支持9种运维操作，包括重启、关机、编辑、控制台、快照、快照恢复、删除节点、保存镜像、设为流量镜像节点。 3、场景设计支持用户可实时进行编辑操作，多人可同时编辑同一个拓扑场景，轻松调整网络配置，增加或删除节点和连线，配置节点属性和启动参数。 4、支持用户自主设计网络拓扑，用户可以通过简单的拖放操作在网络拓扑编辑器的工作区中快速、方便的配置起自己的仿真网络，也可以对网络中网络设备的属性进行设置。 5、支持管理员建立新的组件或修改已有组件，并支持保存为拓扑模板。拓扑制作过程中支持靶机、安全设备、路由器、交换机等设备进行拖拽式组建自定义拓扑。

		，网络与协议攻击类277个（包含ARP欺骗、流量嗅探、WiFi攻击及各类拒绝服务攻击），渗透测试类42个（覆盖信息收集、初始突破、权限提升、横向移动、凭证获取及权限维持等完整攻击链），所有科目具备独立实验环境、明确攻击路径及可量化考核指标，确保训练内容具备体系化、实战化与可验证性。 2、每学年提供64学时的教学服务，连续5年。
13	SQL注入漏洞脆弱性分析实验课程资源	1、SQL注入漏洞脆弱性分析实验资源包需包含但不限于以下实验内容：SQL注入基础、联合查询注入、报错注入、布尔盲注和时间盲注、delete和limit注入、update和insert注入、HTTP头注入、二次注入、堆叠注入、SQL注入SQLMap工具、Tamper脚本编写、盲注脚本编写、SQL注入常见绕过方式、SQL注入Bypass技巧、Access手工注入、SQL Server注入基础、SQL Server手工注入、SQL Server注入waf绕过、SQL注入练习和巩固。资源包合计包含16个实验环境、16个视频资源，配套资源包含标准化实验手册、体系化PPT课件、习题、工具包。 2、每学年提供32学时的教学服务，连续5年。
14	XSS漏洞脆弱性分析实验课程资源	1、XSS漏洞脆弱性分析实验资源包需包含课程内容对应实验环境、实验手册、PPT、理论视频、实验视频、习题等内容；资源包需包含但不限于以下实验内容：Cookie和Session基础、XSS漏洞基础、存储式XSS、反射式XSS、DOM式XSS、XSS漏洞Bypass技巧、XSS辅助工具、XSS平台搭建、XSS平台的使用、Cookie窃取发送邮件、XSS漏洞防御技巧。每年更新4个实验，每年更新3年。资源包合计包含16个实验环境、16个视频资源，配套资源包含标准化实验手册、体系化PPT课件、习题、工具包； 2、每学年提供16学时的教学服务，连续5年。
15	CSRF漏洞脆弱性分析实验课程资源	1、CSRF漏洞脆弱性分析实验资源包需包含课程对应实验环境、实验手册、PPT、理论视频、实验视频、习题等内容；实验内容为CSRF漏洞、CSRF利用工具、XSS+CSRF组合拳利用、CSRF漏洞添加后台管理员。资源包合计包含16个实验环境、16个视频资源，配套资源包含标准化实验手册、体系化PPT课件、习题、工具包； 2、每学年提供16学时的教学服务，连续5年。

16	逻辑安全漏洞脆弱性分析实验资源包需包含课程对应实验环境、实验手册、PPT、理论视频、实验视频、习题等内容；资源包需包含但不限于以下实验内容：越权访问基础、水平越权、垂直越权、密码重置漏洞、验证码绕过漏洞、变量覆盖漏洞、接口枚举漏洞、未授权访问。资源包合计包含16个实验环境、16个视频资源，配套资源包含标准化实验手册、体系化PPT课件、习题、工具包；	2、每学年提供16学时时的教学服务，连续5年。
17	目录遍历漏洞脆弱性分析实验资源包需包含课程对应实验环境、实验手册、PPT、理论视频、实验视频、习题等内容；资源包需包含但不限于以下实验内容：目录遍历漏洞、.git文件泄露漏洞、svn源码泄露漏洞、网站备份文件泄露漏洞、.swp文件泄露、DS_Store 文件泄露、WEB-INF/web.xml 泄露、robots.txt目录泄露、任意文件读取漏洞、文件覆盖漏洞。资源包合计包含16个实验环境、16个视频资源，配套资源包含标准化实验手册、体系化PPT课件、习题、工具包；	2、每学年提供16学时时的教学服务，连续5年。
18	文件管理漏洞脆弱性分析实验资源包需包含课程对应实验环境、实验手册、PPT、理论视频、实验视频、习题等内容；资源包需包含但不限于以下实验内容：文件下载漏洞、文件管理主题插件上传漏洞、任意文件修改漏洞、任意文件删除漏洞、任意文件写入漏洞、文件备份getshell、文件编辑getshell、修改配置文件getshell、编辑器模板漏洞。资源包合计包含16个实验环境、16个视频资源，配套资源包含标准化实验手册、体系化PPT课件、习题、工具包。	2、每学年提供16学时时的教学服务，连续5年。
19	文件上传漏洞脆弱性分析实验资源包需包含课程对应实验环境、实验手册、PPT、理论视频、实验视频、习题等内容；资源包需包含以下实验内容：文件上传漏洞基础、文件上传漏洞之工具介绍、各式各样的webshell编写、Windows特性上传漏洞、服务器解析漏洞、条件竞争漏洞、截断绕过、文件上传漏洞常见的过滤方式、文件上传漏洞Bypass技巧、WAF绕过、免杀木马编写、文件包含+文件上传组合拳利用、Tomcat后台部署war包getshell。资源包合计包含16个实验环境、16个视频资源，配套资源包含标准化实验	

		手册、体系化PPT课件、习题、工具包。 2、每学年提供32学时时的教学服务，连续5年。
20	文件包含漏洞分析实验课程资源	1、文件包含漏洞分析实验资源包需包含课程对应实验环境、实验手册、PPT、理论视频、实验视频、习题等内容；资源包包含以下实验内容：文件包含漏洞基本原理、本地文件包含和远程文件包含、文件包含其他利用方式、文件包含漏洞伪协议、文件包含phar&zip、截断包利用、常见CMS文件包含漏洞。资源包合计包含16个实验环境、16个视频资源，配套资源包含标准化实验手册、体系化PPT课件、习题、工具包。 2、每学期提供16学时时的教学服务，连续5年。
21	源码审计技术实验课程资源	1、源码审计技术实验资源包需包含课程对应实验环境、实验手册、PPT、理论视频、实验视频、习题等内容；资源包包含于以下实验内容：php反序列化、typecho install.php反序列化、phar反序列化、反序列化字符串逃逸、反序列化POP链、SSRF漏洞审计、XSS漏洞源码审计、命令执行漏洞源码审计、代码执行漏洞、open_basedir目录限制绕过、disable_function配置绕过、PHP弱类型、常见CMS漏洞代码审计。资源包合计包含16个实验环境、16个视频资源，配套资源包含标准化实验手册、体系化PPT课件、习题、工具包。 2、每学期提供32学时时的教学服务，连续5年。
22	密码实验课程资源	1、提供密码实验课程包含：古典密码算法实现、对称/非对称密码算法实验、哈希与数字签名技术、暴力破解、字典攻击等密码攻击技术实验；资源包合计包含16个实验环境、16个视频资源，配套资源包含标准化实验手册、体系化PPT课件、习题、工具包。 2、每学期提供32学时时的教学服务，连续5年。

23	网络攻防竞赛课程资源	1、提供网络攻防竞赛课程包含：CTF资源1000个，AWD10套（含Web方向SQL注入/文件包含/代码审计解题，Pwn方向栈溢出/格式化字符串/堆溢出漏洞利用，Reverse方向汇编指令分析、PE/ELF文件结构解析、逆向工具实操，Misc方向隐写术/流量分析/编码解码解题）；CTF工具实操与解题技巧（含Burp Suite、IDA Pro、GDB等竞赛常用工具配置与高阶使用，解题思路梳理与快速破题技巧）；团队协作与竞赛策略（含CTF团队分工模式、答题节奏把控、难题攻坚策略）；AWD攻防对抗（含AWD竞赛规则解读、靶机防御配置、攻击漏洞挖掘与利用、漏洞修复与后门植入防护）； 2、提供面向CTF竞赛题目交付的标准化工程化链路设计，提供自研脚本工具，支持自动化构建可直接用于竞赛部署、教学实训、漏洞复现的标准化CTF题目环境，支持构建“提交源码/目录→自动生成合规交付件→一次校验通过→直接上线部署”的全流程闭环体系，可支撑学校网安方向学科建设、竞赛备赛、人才培养及内部赛事运营需求； 3、提供网络安全相关文献资源10万条。 4、提供5年的网络攻防竞赛课程资源更新服务，年更新数量不低于10%。
24	智能安全实验课程资源	1、提供智能安全实验课程资源包含提示词注入、越狱攻击、情景引导攻击、机器学习、数据挖掘、供应链投毒等。资源包含10个实验环境。配套资源包含标准化实验手册、实验视频、习题、工具包； 2、每学期提供8学时的教学服务，连续5年。
25	攻防工具库与漏洞资源库	提供独立的攻防工具漏洞资源库。攻防工具包括信息收集工具、Web工具、漏洞工具、逆向工具、暴力破解工具、密码破解工具、SQL注入工具、横向渗透、端口转发、Socks代理、痕迹隐藏、漏洞利用工具、代码审计、权限提升、取证分析、逆向分析、无线攻防、编码解码、日志分析、社会工程学辅助等各类工具。总数量3500个。

26	多维智显 仪	1、最大兼容分辨率：≥3840*2160dpi 2、ISO亮度：≥3500lm 3、投影光源：三色激光 4、标准分辨率：≥4K 5、支持自动对焦 6、能效等级：一级能效 7、投射比≥0.9-1.5
----	-----------	--

2. 附件 2 售后服务方案

2.1. 售后服务承诺

- 1、交货时间：合同签订后30天内到货并安装调试交付使用。
- 2、交货地点和方式：西安文理学院指定地点。
- 3、支付方式：一次付清。
- 4、支付约定：付款条件说明：项目完成交付并验收无异议，达到付款条件起30日内，支付合同总金额的100.00%。
- 5、验收标准和方法：按谈判文件、响应文件及合同约定执行。
- 6、包装方式及运输：涉及的商品包装和快递包装，完全符合《商品包装政府采购需求标准（试行）》《快递包装政府采购需求标准（试行）》的要求，包装完全适应于远距离运输、防潮、防震、防锈和防野蛮装卸，以确保货物安全无损运抵指定地点。
- 7、质量保修范围和保修期：质保期内我司提供上门维护和升级，如因产品性能故障连续维护三次仍不能正常使用的，在一个月内更换相同型号及同等功能的全新产品。上述费用含在合同总费用中。
- 8、违约责任及解决争议的方法：按谈判文件、响应文件及合同约定执行。
- 9、产品培训：我司将对软硬件设备的技术运用、操作使用方法、维护管理等进行培训。
- 10、有专门专业技术人员对此项目负责技术支持回应，系统故障响应时间不超过1小时，系统故障解决时间不超过24小时。重大故障或长时间不能远程解决的，现场提供服务直至解决问题，费用包含在报价中。
- 11、针对总体项目应提供终身技术咨询服务。
- 12、质保期以后我司将终身提供广泛优惠的技术支持和维修服务，将对质保期外服务条款及费用的收取另行签署保修协议。服务内容与保修期内的售后服务内容相同，服务方式和响应时间与保修期内售后服务方式和响应时间相同。

2.2. 售后服务内容

2.2.1. 响应时间

我公司将向用户提供快速的技术服务响应。对于甲方提出的技术支持要求，我公司在接到用户通知后30分钟内响应，4小时解决问题。特殊情况24小时内

解决，突发事件响需现场进行故障排除，2小时到达现场。

我公司通过技术支持代表为甲方提供多元化的技术支持，借助我公司多年以来服务用户积累的雄厚的技术力量集及经验，我们的多层次的技术支持队伍共同为维持采购人的最高满意度而努力，即迅速回应用户的疑问和问题，并提供用户需要的适当和准确的解答。

2.2.2. 服务内容

通过免费热线电话029-88894789和现场支持方式向甲方提供支持服务，支持范围包括故障报修、产品功能介绍、配置、安装、调试，升级以及使用中遇到的技术问题的咨询等。

2.2.3. 备品备件服务

我方可根据采购方要求，为用户单位提供备品备件服务，保障故障修复，交付产品后可提供用户所需的相关所需备品备件。如遇备品备件不足情况，在甲方认可情况下，使用技术特性不低于原产品的同类型产品替代。

2.2.4. 系统软件升级服务

协助客户进行软件版本管理，包括：定期核查软件产品的版本情况，及时提供服务范围内所有软件的升级信息，保证客户能够及时获取并使用，保证其合法性、准确性和及时性；提出软件产品版本升级建议，协助制定升级方案，对升级的测试、实施等工作提供技术支持。

2.2.5. 故障维修维护服务

协助客户建立所有系统软件各种故障的恢复流程及应急措施，提供相关技术方案。在故障发生后，尽快修复故障并投入使用。对于维护清单以外的非系统故障造成的问题协助解决，给出合理的建议。

2.2.6. 维修保障相关计划和内容

2.2.7. 售后维修

为适应用户需求，加强市场工作，我公司对销售的所有产品的售后服务工作进行统一管理和评价。组织机构方面，工程调测、安装及售后服务等管理工作组建专门团队负责；各技术开发团队及相关部门负责实施服务工作；质量管理部门负责接收质量问题的举报/投诉；市场部门负责顾客满意程度的归口管理。在公司领导层的直接指挥下，管理部门、技术部门、市场部门，与质量管理

部门相互协调，及时解决用户提出的问题，保证交付系统的正常运行。

本项目所有产品提供售后质保服务是免费维护服务。保修期间由专门人员负责技术支持和维护。在保修期内，如果系统发生故障，承诺调查故障原因并免费维修或更换系统软件，同时承诺免费提供软件版本、规则库、特征库及时更新至最新版本。

在保修期内，如果系统发生故障，免费提供调查故障原因并修复，直至满足最终验收指标和性能的要求，或者免费更换整个或部分有缺陷的材料。

系统运行稳定，没有发生任何系统故障，若因为系统自身问题，发生故障，协助客户及时解决不影响相关考核指标。同时，承诺系统运行效率满足客户单位相关规范的要求和客户单位业务处理的速度要求。

3. 附件 3 产品交付说明

情况说明

我公司交付的网络靶场平台V4.0包含教学实训系统、考核评估系统、竞赛系统、虚拟化仿真引擎系统和场景拓扑管理系统。所交付的产品完全满足招标文件要求。

特此说明。