

原招标文件中第五部分用户需求书中需求清单一览表:

序号	子项/模块	用途说明	采购品目明细	基本规格要求	单位	数量	备注
1	子项一: 实训室及 工作室改 造	实训楼 406 网络 对抗综合 实训室项 目建设 160 平米 的防静电 地板购置 及 54 套桌 子更新; 2 教副楼 302 攻防 战队工作 室 6 套高	工作室 攻防专 用终端	<ol style="list-style-type: none"> <li>▲处理器不得低于 Intel I7 十二代处理器, 不低于六核六线程;</li> <li>内存容量不低于 32GB; 提供不少于 1T 的 SSD 存储空间;</li> <li>GPU: 不低于 Intel HD Graphics 620 显示芯片;</li> <li>I/O 端口: 不少于 6 个 USB 端口, 不少于 1 个 COM 端口, 不少于 1 个 HDMI 端口, 不少于 1 个 RJ45 端口, 不少于 1 个音频输入口, 不少于 1 个音频输出口;</li> <li>至少支持 Spice、RDP 虚拟桌面等连接协议;</li> <li>支持统一设置终端分辨率, 也可以设置自适应显示器最佳分辨率;</li> <li>支持虚拟教室功能, 支持手动将终端划分到对应的教室, 同时支持根据终端设备 IP 地址自动将终端纳入到不同的教室进行统一管理;</li> <li>支持远程统一唤醒, 实现终端的批量管控;</li> <li>按需交付相应的操作系统和应用软件, 以数据流方式智能传输到终端本地进行保存。</li> </ol>	台	6	
2			终端配 套键鼠	USB 光电键鼠套件	套	6	

3	性能终端设备购置及桌椅文件柜等配套。	终端配套显示器	21.5"宽屏 16:9 LED 背光 TN 液晶显示器, VGA, HDMI 1.4 接口, 无 HDMI 线缆, 250nits, 1000:1, 8 百万:1 (动态对比度), 5ms, 1920x1080, 100x100 壁挂标准 (允许误差±5%)	台	6	
4		工作室定制桌椅	工作室定制双人位, 尺寸 2400mm*600mm*750mm, 办公桌面材: 表面树脂保护膜; 基材: 采用优质的实木颗粒板材; 封边: 2mm 加厚封边条, 专业热熔封边; 桌面 25mm 厚, 承重 300KG, 耐高温, 耐污染, 耐划痕, 防水渍; 钢制下架: 日子型加厚烤漆金属架; PVC 线孔设计轻松走线, 前置挡板设计私密性高, 可移动活动柜。 配套办公椅: 520mm*480mm*960mm, 人体工学设计, 舒适坐感, 适应腰部, 调节身高, 135° 后仰调节, 10cm 升降 360° 旋转, 透气微弹网布, 网布耐受力强, 耐冲击, 不易变形, 结合人体工学椅背, 更好承托的腰部, 尼龙混合玻纤, 强度高, 韧性足, 静压测试可达 1000KG 万向尼龙滑轮, 滑动声音小, 呵护地板。	套	10	
5		工作室文件柜	通体对开玻璃门, 尺寸不低于 1800*850*390 (允许误差±5%), 全钢柜体, 加厚冷轧钢板; 强力承重加厚层板, 层板可调节, 层板可根据需求随意调节或拆卸; 静电喷射, 绿色环保。	个	2	
6		实训室防静电	采用 600*600*35mm 防静电瓷砖作为面层、上 0.4mm/下 0.5mm 复合全钢地板或水泥刨花板、四周导电胶条封边加工而成。	平米	160	

			地板	具有防静电性能稳定、环保、高耐磨、高寿命、高承载、防水、防潮、装饰效果好等优点，适用于各类机房。 含安装调试服务。（含实验室文化墙建设和综合布线）			
7			实训室定制桌子	实训室定制可折叠培训桌，采用冷轧钢材质，表面高温烤漆工艺，加厚稳固钢架，可承重至少 100KG 不变形；桌面不低于 25mm 厚三聚氰胺板面板，厚实耐用全方位支撑，E1 级环保材质，防潮耐高温，耐磨防刮蹭；配静音万向脚轮，可固定设计 360° 旋转；前置挡板设计，手动一键折叠。	张	54	
8	子项二：平台系统软硬件及服务购置 模块一：实验实践教学平台	为高职阶段信息安全技术应用专业及本科阶段网络安全与执法专业人才培养方案中的实验实	在线网络安全实验实践系统	1. 平台在线提供服务，每年支撑账号数量：不少于 80 个；每年提供实验数量：不低于 45 个。主要支撑《windows 操作系统安全》、《linux 操作系统安全》、《web 安全基础》、《病毒分析技术》、《运维安全》、《运维应急响应》、《web 漏洞实战》、《取证分析》、《数据库安全实战》、《信息安全基础》等人才培养方案中的专业基础课、技能课和核心课程；主要性能指标为满足高职阶段和本科阶段 80%以上专业课教学支撑，并能快速更新，可以根据后续专业建设及课程体系的优化需求进行课程更新。配套服务为 5 年内免费提供上述课程的技术支持和服务，帮助课任教师完成对学生的授课支撑。 1.1▲实验实践教学平台：为高职阶段信息安全技术应用专业及本科阶段网络安全与执法专业人才培养方案中的实验实践类课程提供实验实训教学环境及	年	5	

	<p>践类课程 提供实验 实训教学 环境及资 源</p>	<p>内容资源，平台包括在线网安实验实践系统服务，提供为期 5 年每年不少于 80 个账号使用，实验数量不少于 45 个且保证持续更新；以及课程资源包-线上职业技能培训资源课程不少于 4 套。平台需满足高职阶段和本科阶段至少 80%以上专业课教学支撑，可以根据后续专业建设及课程体系的优化需求进行课程更新。配套服务为 5 年内免费技术支持和服务，帮助课任教师完成对学生的授课支撑。</p> <p>1.1.1 系统全面支持远程实验实践教学，支持 Web 方式访问操作实验环境，支持同时并发在线人数不少于 80 人。</p> <p>1.1.2. 系统功能包括但不限于：针对教师提供预约排课、组建课程、上传课件及分配实验环境等教学功能。预约排课可根据具体教学计划进行上机计划安排；支持教师在实验库中选择实验自主组建课程；支持教师上传课件供学生在线浏览，课件类型支持 doc、docx、ppt、pptx、pdf、txt 等；支持教师教学实验自动开放、自动调度分配实验环境、自动停止实验与销毁实验环境功能。</p> <p>1.1.3. 系统功能包括但不限于：针对学生提供详细的实验指导书，学生可根据实验指导书的内容自主完成实验；支持视频学习功能，视频学习支持全屏播放；实验场景支持刷新、销毁、靶标切换、剪切板功能；支持学习过程中的在线提问、回答、笔记、评价等功能；支持上传、下载实验报告功能；支持课后作业</p>			
--	--	---	--	--	--

		<p>的布置、提交及查看等功能。</p> <p>1.1.4 系统功能包括但不限于：支持基本的教学管理功能，学生可通过扫描二维码添加班级；支持教师对实验过程中学生的终端进行监控；支持以日历的形式将以往和正在进行的排课、作业、考试进行展示。</p> <p>1.1.5. 系统支持线上考试功能，提供不少于 800 题的理论考试题库。包括但不限于：支持教师创建和修改试题，支持根据知识点自动生成试卷功能；支持考试开放及关闭功能；支持自动阅卷及成绩统计功能。</p> <p>1.1.6. ▲实验实践教学资源包括：CTF 习题集、渗透测试训练营、渗透综合场景演练、使用 FirewallD 构建动态防火墙、SQL 注入原理与实践、MySQL 盲注、MSSQL 注入提权、Mssql 报错注入、取证分析、XSS 跨站脚本攻击原理与实践、XSS 常见的防御方法、rmap 的网络信息扫描原理与设计、Python 爬虫简单实践、wireshark 数据抓包分析之 ARP 协议、BGP 路径劫持攻击、漏洞扫描之 Nessus、数据恢复原理实验、Linux 系统安全审计、CSRF 攻击实验、漏洞扫描、SSRF 漏洞分析与实践、文件上传漏洞概述、破壳漏洞实践、网页防篡改实验、WAF 渗透攻防实践、Windows Server 2008 系统加固、Linux 网络服务配置与安全、PHP 函数漏洞审计、NAT 配置、区块链安全入门最佳实践、恶意代码分析实战-高级、Python 编程进阶(上)、Python 爬虫-多线程、熊猫烧香病毒剖</p>			
--	--	--	--	--	--

		析、PE 病毒之病毒编写、脚本病毒、引导型病毒原理剖析、利用单次追踪法进行脱壳、利用 ESP 定律进行脱壳、木马攻击实验、Metasploit 制作木马后门、MySQL 提权/条件竞争漏洞分析和利用、破壳漏洞实践等，上述 45 个课程实践资源资源包厂家应标应至少满足 85%以上类别需求。			
9	课件资源包一 线上职业技能培训课程资源包	<p>提供《渗透测试工程师》、《CTF-WEB》、《CTF-Reverse》、《CTF-PWN》不少于四套职业技能培训课程账号。</p> <p>1. ▲提供《渗透测试工程师》线上职业技能培训资源课程学习支撑，支撑账号不少于 3 个，支撑不少于 80 个课时的视频学习，课程内容涵盖但不限于：1 信息收集、2 渗透测试框架 Metasploit 实战、3 WEB 漏洞攻击利用集合、4 漏洞扫描、5 密码破解、6 渗透测试框架 CobaltStrike 实战、7 内网渗透、8 后渗透权限提升、9 后渗透权限维持等渗透测试岗位核心知识体系。</p> <p>2. 提供《CTF-WEB》线上职业技能培训资源课程学习支撑，支撑账号不少于 3 个，支撑不少于 40 个课时的视频学习，课程内容涵盖但不限于：1 SOL 注入、2 文件操作、3 命令执行、4 反序列化、5 服务端模板注入、6 服务端请求伪造、7 跨站脚本攻击、8 XML 外部实体注入、9 CTF 技巧-PHP、10 CTF 技巧-Node、11 CTF 技巧-Python 等知识体系。</p> <p>3. 提供《CTF-Reverse》线上职业技能培训资源课程学习支撑，支撑账号不少</p>	个	3	

			<p>于 3 个，支撑不少于 50 个课时的视频学习，课程内容涵盖但不限于：1 C 语言、2 X86 架构、3 IDA 使用、4 C 语言逆向、5 杂项、6 C++、7 python、8 Golang 等知识体系。</p> <p>4. ▲提供《CTF-PWN》线上职业技能培训资源课程学习支撑，支撑账号不少于 3 个，支撑不少于 30 个课时的视频学习，课程内容涵盖但不限于：1 汇编语言、2 ELF 文件格式、3 LINUX 延迟绑定机制、4 函数调用流程、5 栈溢出原理以及利用、6 ROP 编写、7 LINUX 动态内存管理机制、8 堆漏洞分析与利用、9 iofle 利用手法、10 线下赛 AWD 模式的 patch 技巧等知识体系。</p>			
10	子项二： 平台系统 软硬件及 服务购置  模块二： 竞技及比 武演练平 台	为高职阶 段信息安 全技术应 用专业及 本科阶段 网络安全 与执法专 业提供竞 技比赛、攻	比武演 练系统	<p>以国产自主研发的虚拟云技术、网络复现技术、平行仿真技术为基础，集攻防演练、竞赛运维、场景管理、攻防可视化、考核选拔于一体，通过在线夺旗(CTF)、攻防兼备(AWD+)、场景渗透(ISW)等多种演练模式，依托于高度贴近实战的比赛场景以及赛程可视化，快速检验和发现网络安全实用人才，复盘和推演各种演习态势。平台应包括但不限于：演练任务配置、演练资源及战队管理、演练过程监管、演练结果评估、可视化攻防效果展示等功能模块。攻防演练及赛事可以依靠智能训练效果评估功能进行打分和评判。为教员、裁判和观众提供友好、直观、准确的参考，人员操作同步播放、参赛人员赛程节点路径播放。配套服务为免费提供至少 60 本由厂商自编、正式出版的《内网渗透体系建设》</p>	套	1

		<p>防演练类综合实践课程提供实训环境及资源;为学生网络安全竞赛社团提供日常训练支持。</p>	<p>教材,包括但不限于:内网渗透的基础知识,以及 Kerberos 专题、NTLM Relay 专题和 Microsoft Exchange 专题,和免杀技术等内容。支持课任老师联合开发《内网渗透体系建设》精品课程至少 1 门。</p> <p>1. ▲为高职阶段信息安全技术应用专业及本科阶段网络安全与执法专业提供竞技比赛、攻防演练类综合实践课程,提供竞技及比武演练支撑系统、演练环境及内容资源;为学生网络安全竞赛社团提供日常训练支持。平台包括但不限于:本地部署竞技及比武演练系统 1 套;在线网安竞赛服务系统,提供为期 5 年每年不少于 60 个账号使用;本地部署攻防工具资源包 1 套、竞赛题目资源包 1 套及仿真靶标资源包 1 套。配套服务为免费提供至少 3 个 CISP-PTE 渗透测试工程师的认证培训。另支持提供 2 次省级以上规模(300-500 人)的网络安全大赛驻场支持,内容包括但不限于:赛前准备(比赛设备支持)、赛中支持(赛中全程运维)、赛后管理(比赛复盘)等安全大赛技术支持及指导运维等工作,使用户了解并掌握赛事举办的重点流程。</p> <p>1.1 包括但不限于:具有基于国产自主的虚拟云技术、网络复现技术、平行仿真技术的攻防演练、竞赛运维、场景管理、攻防可视化、考核选拔功能,可提供在线夺旗(CTF)、攻防兼备(AWD+)、场景渗透(ISW)等多种演练模式,具有贴近实战的比赛场景,赛程可视化,可复盘和推演各种演习态势。</p>			
--	--	---	---	--	--	--



			<p>1.2. 包括但不限于：演练任务配置、演练资源及战队管理、演练过程监管、演练结果评估、可视化攻防效果展示等功能。</p> <p>1.3. 包括但不限于：可对攻防演练及赛事进行打分和评判。可为教员、裁判和观众提供友好、直观、准确的参考，可同步播放参赛人员赛程节点、路径及人员操作等。</p> <p>1.4. ▲CTF 攻防场景（包括但不限于：1 Web 安全、2 PWN、3 逆向、4 MISC、5 密码等）不少于 100 个；AWD Plus 攻防场景（包括但不限于：1 代码审计、2 漏洞利用、3 漏洞修补、4 SQL 注入、5 文件遍历、6 爆破、7 溢出、8 后门的发现、9 利用、10 隐蔽等）不少于 15 个。（需提供攻防场景清单）</p> <p>1.5. 系统具备动态 FLAG 反作弊机制，即每个轮次题目 FLAG 均不同；竞赛管理员、裁判能够依据“烽火台”的反作弊机制监控队伍/选手作弊行为，包括但不限于：登录作弊、多队提交同一答案、一队提交多个答案等；裁判能够针对某队伍/选手的制定题目提交答案，以应对队伍/选手答案正确但无法自行提交的情况；</p> <p>1.6. 竞赛管理员、裁判可以对所有队伍/选手的虚拟机环境进行开机、关机、创建快照、重启等操作；竞赛管理员、裁判能够手动开启模拟攻击数据，展示界面将会模拟页面的所有动画效果，并不改变队伍/选手的实际分值，以此保</p>		
--	--	--	--	--	--

			<p>障展示界面有充足的攻击效果，提升用户体验度；</p> <p>1.7. 系统支持不少于 5 种竞赛展示界面（含 2D、3D 格式），每种展示功能支持竞赛实时攻防信息的显示，提供竞赛公告的显示；</p> <p>1.8. ★支持包括全国职业院校技能大赛、全国大学生信息安全竞赛、公安系统网络攻防大赛等竞技类赛前训练课程；支持包括但不限于：《CTF 基础》、《CTF-WEB》、《CTF-reverse》、《CTF-PWN》等 CTF 大赛实战进阶训练课程；支持主流竞技赛事模拟演练实训课程；能够支撑学生网络安全竞赛社团的日常训练。系统支持 CTF、ISW、AWDPLUS 等更多赛制，历经各大网络安全赛事支撑考验，能支撑学院网络攻防大赛、省部级以上的攻防大赛与网络安全演练等需求。能同时支撑至少 60 人同时在线竞技。提供不少于 5 年的免费升级服务。</p> <p>1.9. 系统应具备承办公安系统网络安全相关比赛或其他行业中大型网络安全攻防赛的运营支撑能力，可提供省部级或以上级别的赛事运营证明材料。</p> <p>1.10 投标方提供参数确认函及售后服务承诺书。</p>			
11		<p>在线网络安全竞赛服务系统</p>	<p>平台在线提供服务，每年支撑账号数量：不少于 60 个。支持不少于 60 人同时并发参与仿真竞赛云端服务，页面加载小于 1 秒；数据交互耗时小于 1 秒，全年服务可用性不低于 99.9%。理论知识不少于 50 道，场景实操不少于 180 道，独家资源不少于 30 道，月度更新不少于 5 道。精选历届比赛真题，构建海量</p>	年	5	

			<p>CTF 题库,更全面的覆盖知识点内容。将 CTF 需要掌握的技能按类型进行归类,按知识点融入知识竞赛训练,通过场景实操的方式巩固知识点;包含 WP 不少于 110 个,月度更新不少于 3 个。帮助学生更好的进行题目练习,平台题目训练模块提供赛题 WP(解题思路),帮助学员解除答题困惑,攻克技术难点,突破认知范围。</p> <p>1. ▲系统在线提供服务,方便学生在实训室之外的环境中配套使用。支持不少于 60 人同时并发参与仿真竞赛云端服务,页面加载小于 1 秒;数据交互耗时小于 1 秒,全年服务可用性不低于 99.9%。学员可基于仿真环境了解和熟悉比赛整体流程,通过实践操作,巩固技能,提升学员实战技能,培养学生赛事思维。</p> <p>2. ▲精选历届比赛真题,构建海量 CTF 题库,更全面的覆盖知识点内容。将 CTF 需要掌握的技能按类型进行归类,按知识点融入知识竞赛训练,通过场景实操的方式巩固知识点;默认提供理论知识不少于 50 道,场景实操不少于 180 道,历届网络安全赛事真题资源不少于 30 道,月度更新不少于 5 道。包含 WP 不少于 110 个,月度更新不少于 3 个。帮助学生更好的进行题目练习,系统题目训练模块提供赛题 WP(解题思路),帮助学员解除答题困惑,攻克技术难点,突破认知范围。(需提供系统内历届网络安全赛事真题截图或列表)</p>			
--	--	--	---	--	--	--

12		攻防工具资源包	提供不少于 400 个攻防工具，包括但不限于：1 arp、2 webshell 管理、3 xss、4 代理工具、5 代码审计、6 子域名、7 批量采集、8 抓包改包、9 指纹识别、10 数据管理、11 无线攻击、12 暴力破解、13 注入工具、14 漏洞利用、15 目录扫描、16 社工辅助、17 端口扫描、18 综合扫描、19 编码解码、20 远程控制、21 逆向、22 动态调试工具、23 反病毒、24 反编译工具、25 安卓和 net、26 程序资源编辑、27 算法工具等。	套	1	
13		竞赛题目资源包	<p>1. 提供不少于 130 道 CTF 题目，题目类型包含但不限于：1 安全入门、2 数据隐写、3 取证分析、4 逆向分析、5 编程技术、6 Web 安全、7 密码学等；提供不少于 15 道 AWD+ 题目，题目知识点涉及但不限于：1 代码审计、2 漏洞利用、3 漏洞修补、4 SQL 注入、5 文件遍历、6 爆破、7 溢出、8 后门的发现、9 利用、10 隐蔽等；提供不低于 6 套场景渗透题目，关卡为 10 关，题目知识点涉及但不限于：1 注入、2 社工、3 获取网站权限、4 代码审计、5 信息泄露、6 木马上传、7 漏洞检测等。</p> <p>2. 质保期内每年更新不少于 20 道 CTF 题目，题目类型包含但不限于：1 安全入门、2 数据隐写、3 取证分析、4 逆向分析、5 编程技术、6 Web 安全、7 密码学等；</p> <p>3. 质保期内每年更新不少于 5 道 AWD+ 题目，题目知识点涉及但不限于：1 代</p>	套	1	

			码审计、2 漏洞利用、3 漏洞修补、4 SQL 注入、5 文件遍历、6 爆破、7 溢出、8 后门的发现、9 利用、10 隐蔽等。				
14		仿真靶标资源包	<p>1. 提供不少于 300 套白板操作系统及应用服务靶标,其中操作系统包括但不限于: 1 Windows XP、2 Windows 7、3 Windows 8、 4 Windows server 2003、5 Windows server 2008、6 Windows server 2012、7 Windows server 2016、8 Windows server 2019 、9 RedHat、10 CentOS、11 Ubuntu、12 Debian、13 KaliLinux、14 openSUSE。应用服务包括: 网站服务器种类不少于 10 种, 邮件服务器种类不少于 8 种, 数据库软件种类不少于 8 种, 其中 MYSQL、SQLServer、Redis 和 SQLite 等数据库的连接工具不少于 10 种。</p> <p>2. 提供不少于 100 套公共漏洞靶标,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。</p> <p>3. ▲提供不低于 6 套场景渗透靶标,包括但不限于涵盖电信运营商、电力、水利、机场、学校等关键信息基础设施应用场景, 平均拓扑规模不小于 10 个节点。(附不少于 6 套大型场景靶标说明)。</p>	套	1		
15	子项二: 平台系统软硬件及	为攻防战队培养专项课程提	安全实训系统	1. ▲为攻防战队培养专项课程提供平台支撑。平台包括本地部署安全实训系统不少于 1 套; 专业实践课程包不少于 2 套, 分别为战队能力培养专项课程资源包及赛前培训专项课程资源包。配套服务为免费提供不少于 3 次战队攻防能力	套	1	

	<p>服务购置</p> <p>模块三： 攻防战队 培养实训 平台</p>	<p>供平台支撑,快速强化战队专业技能,能够代表学校出战各类赛事并争取取得好成绩,为我校的专业建设形成良好口碑及影响力。</p>	<p>培养实训,每次培训时长为不低于4周,总计不低于12周约至少500课时的培训,包含指导教师及学生培训。免费提供不少于3次赛前专项培训,每次培训时长为不少于1周。由高级讲师针对大赛的历届比赛整理相关易考难点知识点,结合最新竞赛模式的解题思路 and 技巧进行深入讲解。充分利用企业的优势和条件为学校提供校外实训基地,为学校提供每年不少于5名以上学生的实习就业机会。</p> <p>1.1. ★可提供典型网络安全与管理、网络应用及编程安全、安全攻防等层次互动仿真实验环境,支持学生通过一系列的单项、综合类型实验实践和攻防演练、竞技等训练方式,强化对网络与信息安全防护知识的理解掌握和技能的灵活运用,支持学校安全相关实验实践教学和学生动手能力养成。</p> <p>1.2. 提供教员、学员、管理员三类角色。包括但不限于:教员能够对课程、学员、学习计划进行管理,并按照培训要求下发考核任务;学员可以按照培训要求或者个人兴趣选择课程内容进行学习,并完成相应的考核任务;管理员可对系统用户角色、系统资源等进行配置管理。</p> <p>1.3. 包括但不限于:实训任务配置、资源管理、过程监管、效能评估等功能。</p> <p>1.4. 包括但不限于:支持批量导入学员信息(包括学号、姓名、用户名、班级、性别、单位、邮箱、电话等信息),支持班级及学员信息导入导出;可对学员</p>			
--	--	--	--	--	--	--

			<p>进行分组管理，将指定学员添加到相应的班级中，针对班级设置个性化教学计划，管理员可以为班级指派负责教员，指派成功后，该班级即成为该教员的专属班级。管理员可以随时指派或更换班级的负责教员。支持班级批量导入、导出，一键完成班级创建及班级成员的自动添加。</p> <p>1.5. ▲具备多种任务数据可视化的展示形式，包括但不限于：针对各系统的认证访问情况、任务执行情况、系统资源使用情况、仿真场景运行情况、服务器运行状态情况等相关数据进行集中汇总、统计分析，以折线图、柱状图、饼状图、雷达图等形式配合列表，实时反映出靶场平台中各类数据状态趋势，为用户掌握靶场平台的全局态势提供直观的参考。（需提供系统数据可视化展示形式的证明材料）</p> <p>1.6. 提供不少于5年的免费升级服务。</p> <p>1.7. 投标方提供参数确认函及售后服务承诺书。</p>			
16		专业实践课程包一战队能力培养专	<p>▲课程包共分渗透测试攻击及安全运维防御两个侧重点，包括但不限于：1 设置操作系统（Linux）及虚拟化、2 软件安装和网站环境搭建、3 网络协议及网络设备配置、4 代码编程（Web 前端后端）、5 Web 安全、6 SQL 注入漏洞、7 sqlmap 环境题目讲解、8 Oracle 注入、9 代码审计、10 内网渗透、11 域渗透，12 二进制文件防御及修补技巧、13 CTF 进阶、14 AWP 专项提升培训等</p>	套	1	

			项课程资源包	知识内容，支撑战队实战能力的养成。包括但不限于：视频不少于 130 个，战队实训场景不少于 90 个（含单点及多点实训环境）、不少于一套发生于 8 个月内的安全事件仿真场景靶标。（需附课程包目录及场景靶标说明）			
17			专业实践课程包一赛前培训专项课程资源包	▲赛前培训专项课程资源包括 CTF 四大方向课程（Web、Reverse、PWN、Misc），AWDP 两大方向课程（Web、PWN）及 Web 安全、逆向工程、其他杂项等整套课程的环境支持，其中包含视频不少于 90 个，赛题环境不少于 40 个。（需附课程包目录）	套	1	
18	子项二：平台系统软硬件及服务购置模块四：网络安全	▲网络安全对抗靶场平台：为战队培养实训平台、竞技及比武演练平	靶场云系统	1. ▲可为实践教学、赛训演练及科研工作提供基础设施服务，实现对主机资源、网络资源、存储资源、容器资源、模板资源、计算资源等集中管理、统一调度与运行监视。可快速精准地支撑各平台对于实验、实践、竞赛、演练与科研场景的构建需求。（需提供对系统资源集中管理调度运行监视配置界面截图） 2. ▲包括但不限于：计算资源管理、网络资源管理、存储资源管理、虚拟机资源管理、实体资源管理、虚拟镜像管理、VPC 资源管理、数据采集管理以及云系统管理等功能。（需提供界面截图）	套	1	



	<p>对抗靶场平台</p>	<p>台提供必不可少的底层功能支撑;也可用于支撑大中型规模赛事;甚至可为科研工作提供各类仿真场景构建的基础条件。平台包括本地部署靶场云系统1套;本地部</p>	<p>3. 支持网络资源负载控制,支持网络流量均衡。支持计算和存储资源负载控制,能够按照负载策略将虚拟机或镜像分配到不同的计算引擎服务器运行。</p> <p>4. 支持网络资源隔离管理,可利用网络子网隔离技术将不同的虚拟网络进行隔离,同时保障虚拟机资源之间的通信安全、互不干扰。</p> <p>5. 支持虚拟设备与实体设备混合组网,实现虚实设备互联互通,包括但不限于:实体设备检测、实体设备注册、实体设备接入场景、实体设备自动化配置、实体设备运维、实体设备重启等。</p> <p>6. 支持子网资源情况监控,包括但不限于:可监控子网池中的子网资源已分配情况、子网资源剩余情况、子网资源可用情况、位于隔离子网中的虚拟机等设备资源规模及子网的网络 I0 负载情况;支持子网资源预警,能够在检测到子网池中的空闲子网不足、网络 I0 负载过高时进行预警。</p> <p>7. 支持操作系统及应用软件配置信息采集,包括但不限于:能够获取指定路径下配置信息是否存在、配置信息内容、配置信息最后修改时间,操作系统包括但不限于 Windows XP、Windows 7、Windows Server 12、ubuntu 14、ubuntu 16、ubuntu 18、CentOS 6.5、Centos7.4。</p> <p>8. 支持通过内部交换机镜像口全量拷贝流量,并以 pcap 包形式进行本地保存,为后续的审计分析提供数据样本。</p>			
--	---------------	---	---	--	--	--

	署网络复 现系统 1		9. 提供不少于 5 年的免费升级服务。 10. 投标方提供参数确认函及售后服务承诺书。			
19	套;本地部 署综合管 理系统 1 套。	网络复 现系统	1. 基于演训、竞赛、测评及科研任务的实施,通过图形化、拖拽式网络拓扑绘制解决方案,支撑各任务场景设计。能够对各拓扑节点资源模板进行绑定,依托云系统提供的资源调度接口,自动完成任务场景的构建过程,并提供开机校验,确保场景合理有效。支持通过 WEB VNC 的方式访问场景,可提供对于场景总体计算方案控制与虚拟机节点的启停控制。 2. 包括但不限于:网络复现任务配置、靶机资源管理、目标场景构建、虚实混编组网、靶标资源库管理、脚本推演展示及执行终端管理等功能。 3. ▲实验场景由操作区和目标区构成,场景必须支持添加不少于 3 个(含)以上目标区(需附截图证明); 4. 内置虚拟机模板不少于 300 个,包括但不限于: windows 2000、XP、Server 2003、Windows 7、Redhat、Kali、Centos 等操作系统,用于实验环境的虚拟靶机包括漏洞信息。 5. 实验环境可提供虚拟安全防护手段,其中的攻防工具以及漏洞仅限于在实验环境中被使用。 6. 提供安全隔离的独立实验场景虚拟网络,内置虚拟防火墙和路由器,构建各	套	1	

			<p>类具有安全策略的多安全区仿真实验场景，支持场景网络自检，支持静态和动态等多种模式。</p> <p>7. ▲系统提供以 2D、3D 拓扑图模式直观地展示出网络场景全貌、攻防状态以及流量轨迹。场景管理员能够自定义攻防脚本及演示功能。可通过选择一个场景为其创建攻防脚本，包括但不限于：录入的主要元素包括脚本名称、步骤对应节点、步骤对应节点状态、步骤持续时间、数据染色；通过 3D 拓扑图的形式展示脚本模拟的攻防状态以及流量轨迹。</p> <p>8. 能同时支撑至少 60 人在线进行靶场训练，支持启动网络拓扑规模为 30 节点的场景，或者至少 15 支队伍启动场景规模为 4 的赛题环境。虚拟网络构建时间一般不超过 10 秒。</p> <p>9. 提供不少于 5 年的免费升级服务。</p> <p>10. 投标方提供参数确认函及售后服务承诺书。</p>			
20		综合管理系统	<p>1. ▲通过虚拟云资源调度，可为网络仿真复现、网络安全实训、学科竞赛、攻防演练及科研场景搭建等提供指挥调度服务，包括但不限于：具有集中化认证、集中化管理、集中化展示、集中化协调、集中化共享、集中化审计的能力，可整合系统相关业务信息，实现资源的统一调配与共享。</p> <p>2. 包括但不限于：统一身份认证、个人云盘管理、综合任务管理、综合日志审</p>	套	1	

			<p>计以及综合态势展示等功能。</p> <p>3. 支持 CSV 格式批量导入学员信息（包括学号、姓名、用户名、班级、性别、单位、邮箱、电话等信息），包括但不限于：支持班级及学员信息导入导出；可对学员进行分组管理，将指定学员添加到相应的班级中，针对班级设置个性化教学计划，管理员可以为班级指派负责教员，指派成功后，该班级即成为该教员的专属班级。管理员可以随时指派或更换班级的负责教员。支持班级批量导入、导出，一键完成班级创建及班级成员的自动添加。</p> <p>4. ▲具备多种任务数据可视化的展示形式，包括但不限于：针对各系统的认证访问情况、任务执行情况、系统资源使用情况、仿真场景运行情况、服务器运行状态情况等相关数据进行集中汇总、统计分析，以折线图、柱状图、饼状图、雷达图等形式配合列表，实时反映出靶场平台中各类数据状态趋势，为用户掌握靶场平台的全局态势提供直观的参考。（需提供系统数据可视化展示形式的证明材料）</p> <p>5. 提供不少于 5 年的免费升级服务。</p> <p>6. 投标方提供参数确认函及售后服务承诺书。</p>			
21	子项二： 平台系统	为支撑上 述软件平	靶场平 台主控	1. 用途：为经过安全加固的专用服务器，作为平台的主控中心服务器，主要负责管控靶场平台各资源节点的使用情况、人员资源调配、态势整理展示、等功	台	1

	软硬件及服务购置模块五：平台的硬件支撑	台的运行及服务内容,需购置的硬件设备	中心	<p>能。提供功能、性能软硬一体化优化产品形态,应能支撑上述本地部署软件系统的业务指标的稳定运行。在 60 人并发实验时,系统响应时间少于 5 秒。</p> <p>2. ▲硬件参数:标准 2U 机架专用设备;并配置≥2 颗 CPU、内存≥64G、存储≥4*2T;配置≥2*千兆双电口网卡。</p> <p>3. 提供服务器售后服务承诺函。</p>			
22			计算引擎服务器	<p>1. 用途:为经过安全加固的专用服务器,作为平台的云计算引擎服务器,主要负责用于负载场景资源、场景防火墙等功能,并受主控中心的控制,提供资源负载。提供功能、性能软硬一体化优化产品形态,应能支撑上述本地部署软件系统的业务指标的稳定运行。在 60 人并发实验时,系统响应时间少于 5 秒。</p> <p>2. ▲硬件参数:标准 2U 机架专用设备;并配置≥2 颗 CPU、内存≥64G、存储≥4*2T;配置≥2*千兆双电口网卡;</p> <p>3. 提供服务器售后服务承诺函。</p>	台	3	
23			存储引擎服务器	<p>1. 用途:为经过安全加固的专用服务器,作为平台的存储引擎服务器,主要负责集中管控平台中所存储的场景模板、平台功能虚拟机、负载均衡、IP 地址池等功能。提供功能、性能软硬一体化优化产品形态,应能支撑上述本地部署软件系统的业务指标的稳定运行。在 60 人并发实验时,系统响应时间少于 5 秒。</p>	台	3	

			<p>2. ▲硬件参数：标准 2U 机架专用设备；并配置<math>\geq 2</math> 颗 CPU、内存<math>\geq 64G</math>、存储<math>\geq 4*2T</math>；配置<math>\geq 2*</math>千兆双电口网卡。</p> <p>3. 提供服务器售后服务承诺函。</p>			
24		主控区交换机	<p>1. 用途：作为靶场平台核心交换机，负责联通各管理中心和引擎节点；负责联通虚拟场景及实体场景；负责联通用户操作终端。作为计算和存储之间的数据交换，满足靶场中频繁构建和回收场景资源、更改虚拟机配置。</p> <p>2. ▲硬件参数：二层千兆以太网交换机，背板带宽 240Gbps，配置<math>\geq 48</math> 个 10/100/1000Base-T 以太网端口，<math>\geq 4</math> 个 1000Base-X 以太网端口，<math>\geq 1</math> 个 Console 口。不少于 2 个千兆光模块。</p>	台	3	
25		场景安全接入模块	<p>1. 用途：为用户使用仿真场景提供了安全接入的通信通道，在保障业务平台和仿真环境安全隔离的条件下，实现同一物理终端可同时访问业务平台和仿真环境。为每个接入仿真环境的用户提供安全链路、分配独有的网络 IP，具备子网隔离能力，保障每个学员或队伍使用的网络环境不同，保障虚拟机资源之间的通信互不干扰，增强安全性。系统使用通信协议、身份验证和数据加密 3 种技术保证数据传输的安全性；可支持任何类型数据流，支持多种类型的传输媒介，同时满足传输语音、图像和数据的需求。</p> <p>2. 规格参数：软硬一体专用设备，每台设备可支持不少于 30 人接入，无论虚</p>	台	2	

				拟终端或远程用户都只需通过一个公用网络端口或 Internet 路径即可接入网络仿真环境。			
--	--	--	--	---	--	--	--

更正为：

序号	子项/模块	用途说明	采购品目明细	基本规格要求	单位	数量	备注
1	子项一：实训室及工作室改造	实训楼 406 网络对抗综合实训室项目建设 160 平米的防静电地板购置及 54 套桌子更新； 2 教副楼 302 攻防	工作室 攻防专用终端	<ol style="list-style-type: none"> <li>▲处理器不得低于 Intel I7 十二代处理器，不低于六核六线程；</li> <li>内存容量不低于 32GB；提供不少于 1T 的 SSD 存储空间；</li> <li>GPU：不低于 Intel HD Graphics 620 显示芯片；</li> <li>I/O 端口：不少于 6 个 USB 端口，不少于 1 个 COM 端口，不少于 1 个 HDMI 端口，不少于 1 个 RJ45 端口，不少于 1 个音频输入口，不少于 1 个音频输出口；</li> <li>至少支持 Spice、RDP 虚拟桌面等连接协议；</li> <li>支持统一设置终端分辨率，也可以设置自适应显示器最佳分辨率；</li> <li>支持虚拟教室功能，支持手动将终端划分到对应的教室，同时支持根据终端设备 IP 地址自动将终端纳入到不同的教室进行统一管理；</li> <li>支持远程统一唤醒，实现终端的批量管控；</li> <li>按需交付相应的操作系统和应用软件，以数据流方式智能传输到终端本地进行保存。</li> </ol>	台	6	

2	战队工作室6套高性能终端设备购置及桌椅文件柜等配套。	终端配 套键鼠	USB 光电键鼠套件	套	6	
3		终端配 套显示 器	21.5"宽屏 16:9 LED 背光 TN 液晶显示器,VGA,HDMI 1.4 接口,无 HDMI 线 缆,250nits,1000:1,8 百万:1(动态对比度), 5ms,1920x1080, 100x100 壁挂标 准(允许误差+-5%)	台	6	
4		工作室 定制桌 椅	工作室定制双人位,尺寸 2400mm*600mm*750mm,办公桌面材:表面树脂保护膜; 基材:采用优质的实木颗粒板材;封边:2mm 加厚封边条,专业热熔封边;桌面 25mm 厚,承重 300KG,耐高温,耐污染,耐划痕,防水渍;钢制下架:日子型 加厚烤漆金属架;PVC 线孔设计轻松走线,前置挡板设计私密性高,可移动活 动柜。 配套办公椅:520mm*480mm*960mm,人体工学设计,舒适坐感,适应腰部,调节 身高,135° 后仰调节,10cm 升降 360° 旋转,透气微弹网布,网布耐受力墙, 耐冲击,不易变形,结合人体工学椅背,更好承托的腰部,尼龙混合玻纤,强 度高,韧性足,静压测试可达 1000KG 万向尼龙滑轮,滑动声音小,呵护地板。	套	10	
5		工作室 文件柜	通体对开玻璃门,尺寸不低于 1800*850*390(允许误差+-5%),全钢柜体, 加厚冷轧钢板;强力承重加厚层板,层板可调节,层板可根据需求随意调节或 拆卸;静电喷射,绿色环保。	个	2	



6			实训室防静电地板	采用 600*600*35mm 防静电瓷砖作为面层、上 0.4mm/下 0.5mm 复合全钢地板或水泥刨花板、四周导电胶条封边加工而成。 具有防静电性能稳定、环保、高耐磨、高寿命、高承载、防水、防潮、装饰效果好等优点，适用于各类机房。 含安装调试服务。（含实验室文化墙建设和综合布线）	平米	160	
7			实训室定制桌子	实训室定制可折叠培训桌，采用冷轧钢材质，表面高温烤漆工艺，加厚稳固钢架，可承重至少 100KG 不变形；桌面不低于 25mm 厚三聚氰胺板面板，厚实耐用全方位支撑，E1 级环保材质，防潮耐高温，耐磨防刮蹭；配静音万向脚轮，可固定设计 360° 旋转；前置挡板设计，手动一键折叠。	张	54	
8	子项二：平台系统软硬件及服务购置 模块一：实验实践教学平台	为高职阶段信息安全技术应用专业及本科阶段网络安全与执法专业人才培养	在线网络安全实验实践系统	1. 平台在线提供服务，每年支撑账号数量：不少于 80 个；每年提供实验数量：不低于 45 个。主要支撑《windows 操作系统安全》、《linux 操作系统安全》、《web 安全基础》、《病毒分析技术》、《运维安全》、《运维应急响应》、《web 漏洞实战》、《取证分析》、《数据库安全实战》、《信息安全基础》等人才培养方案中的专业基础课、技能课和核心课程；主要性能指标为满足高职阶段和本科阶段 80%以上专业课教学支撑，并能快速更新，可以根据后续专业建设及课程体系的优化需求进行课程更新。配套服务为 5 年内免费提供上述课程的技术支持和服务，帮助课任教师完成对学生的授课支撑（课程名称可以	年	5	

	<p>养方案中的实验实践类课程提供实验实训教学环境及资源</p>	<p>略有不同，相关技能相同即可）。</p> <p>1.1▲实验实践教学平台：为高职阶段信息安全技术应用专业及本科阶段网络安全与执法专业人才培养方案中的实验实践类课程提供实验实训教学环境及内容资源，平台包括在线网安实验实践系统服务，提供为期5年每年不少于80个账号使用，实验数量不少于45个且保证持续更新；以及课程资源包-线上职业技能培训资源课程不少于4套。平台需满足高职阶段和本科阶段至少80%以上专业课教学支撑，可以根据后续专业建设及课程体系的优化需求进行课程更新。配套服务为5年内免费技术支持和服务，帮助课任教师完成对学生的授课支撑。</p> <p>1.1.1 系统全面支持远程实验实践教学，支持Web方式访问操作实验环境，支持同时并发在线人数不少于80人。</p> <p>1.1.2. 系统功能包括但不限于：针对教师提供预约排课、组建课程、上传课件及分配实验环境等教学功能。预约排课可根据具体教学计划进行上机计划安排；支持教师在实验库中选择实验自主组建课程；支持教师上传课件供学生在线浏览，课件类型支持doc、docx、ppt、pptx、pdf、txt等；支持教师教学实验自动开放、自动调度分配实验环境、自动停止实验与销毁实验环境功能。</p> <p>1.1.3. 系统功能包括但不限于：针对学生提供详细的实验指导书，学生可根据</p>			
--	----------------------------------	--	--	--	--

		<p>实验指导书的内容自主完成实验；支持视频学习功能，视频学习支持全屏播放；实验场景支持刷新、销毁、靶标切换、剪切板功能；支持学习过程中的在线提问、回答、笔记、评价等功能；支持上传、下载实验报告功能；支持课后作业的布置、提交及查看等功能。</p> <p>1.1.4 系统功能包括但不限于：支持基本的教学管理功能，学生可通过扫描二维码添加班级；支持教师对实验过程中学生的终端进行监控；支持以日历的形式将以往和正在进行的排课、作业、考试进行展示。</p> <p>1.1.5. 系统支持线上考试功能，提供不少于 800 题的理论考试题库。包括但不限于：支持教师创建和修改试题，支持根据知识点自动生成试卷功能；支持考试开放及关闭功能；支持自动阅卷及成绩统计功能。</p> <p>1.1.6. ▲实验实践教学资源包括：CTF 习题集、渗透测试训练营、渗透综合场景演练、使用 FirewallD 构建动态防火墙、SQL 注入原理与实践、MySQL 盲注、MSSQL 注入提权、Mssql 报错注入、取证分析、XSS 跨站脚本攻击原理与实践、XSS 常见的防御方法、Nmap 的网络信息扫描原理与设计、Python 爬虫、wireshark 数据抓包、BGP 路径劫持攻击、漏洞扫描之 Nessus、数据恢复原理实验、Linux 系统安全审计、CSRF 攻击实验、漏洞扫描、SSRF 漏洞分析与实践、文件上传漏洞概述、破壳漏洞实践、网页防篡改实验、WAF 渗透攻防实践、</p>			
--	--	--	--	--	--

		<p>Windows Server 2008 系统加固、Linux 网络服务配置与安全、PHP 函数漏洞审计、NAT 配置、区块链安全入门最佳实践、恶意代码分析实战、Python 编程进阶、Python 爬虫-多线程、熊猫烧香病毒剖析、PE 病毒之病毒编写、脚本病毒、引导型病毒原理剖析、病毒脱壳、木马攻击实验、Metasploit 制作木马后门、MySQL 提权/条件竞争漏洞分析和利用、破壳漏洞实践等，上述课程实践资源资源包厂家应标应至少满足 85%以上类别需求（课程名称可以略有不同，相关技能相同即可）。</p>			
9	<p>课件资源包—线上职业技能培训课程资源包</p>	<p>提供《渗透测试工程师》、《CTF-WEB》、《CTF-Reverse》、《CTF-PWN》不少于四套职业技能培训课程账号（课程名称可以略有不同，但是需满足相类似 CTF 技能考核需求）。</p> <p>1. ▲提供《渗透测试工程师》线上职业技能培训资源课程学习支撑，支撑账号不少于 3 个，支撑不少于 80 个课时的视频学习，课程内容涵盖但不限于：1 信息收集、2 渗透测试框架 Metasploit 实战、3 WEB 漏洞攻击利用集合、4 漏洞扫描、5 密码破解、6 渗透测试框架 CobaltStrike 实战、7 内网渗透、8 后渗透权限提升、9 后渗透权限维持等渗透测试岗位核心知识体系（技能模块可以略有不同，但是需要满足本模块核心技能需求）。</p> <p>2. 提供《CTF-WEB》线上职业技能培训资源课程学习支撑，支撑账号不少于 3</p>	个	3	

			<p>个，支撑不少于 40 个课时的视频学习，课程内容涵盖但不限于：1 SQL 注入、2 文件操作、3 命令执行、4 反序列化、5 服务端模板注入、6 服务端请求伪造、7 跨站脚本攻击、8 XML 外部实体注入、9 CTF 技巧-PHP、10 CTF 技巧-Node、11 CTF 技巧-Python 等知识体系（技能模块可以略有不同，但是需要满足本模块核心技能需求）。</p> <p>3. 提供《CTF-Reverse》线上职业技能培训资源课程学习支撑，支撑账号不少于 3 个，支撑不少于 50 个课时的视频学习，课程内容涵盖但不限于：1 C 语言、2 X86 架构、3 IDA 使用、4 C 语言逆向、5 杂项、6 C++、7 python、8 Golang 等知识体系（技能模块可以略有不同，但是需要满足本模块核心技能需求）。</p> <p>4. ▲提供《CTF-PWN》线上职业技能培训资源课程学习支撑，支撑账号不少于 3 个，支撑不少于 30 个课时的视频学习，课程内容涵盖但不限于：1 汇编语言、2 ELF 文件格式、3 LINUX 延迟绑定机制、4 函数调用流程、5 栈溢出原理以及利用、6 ROP 编写、7 LINUX 动态内存管理机制、8 堆漏洞分析与利用、9 iofle 利用手法、10 线下赛 AWD 模式的 patch 技巧等知识体系（技能模块可以略有不同，但是需要满足本模块核心技能需求）。</p>			
10	子项二： 平台系统	为高职阶 段信息安	竞技比 武系统	以国产自主研发的虚拟化仿真云技术、网络场景构建技术、平行仿真技术为基础，集竞技比武训练、竞赛运维、攻防可视化、考核选拔于一体，通过在线夺	套	1

	<p>软硬件及服务购置</p> <p>模块二：竞技及比武平台</p>	<p>全技术应用专业及本科阶段网络安全与执法专业提供竞技比赛、攻防演练类综合实践课程提供实训环境及资源；为学生网络安全竞赛社团提供日常训练支持。</p>	<p>旗（CTF）、攻防对抗（AWD+，也可被描述为AWDP、AWDPLUS，下同）、内网实战（ISW）等多种演练模式，高度贴近实战的比赛场景以及赛程可视化，能及时检验和发现专业实用人才，复盘和推演各种演习态势。平台应包括但不限于：竞技比武配置、资源及参赛队伍管理、比武结果评估、可视化攻防效果展示等功能模块。攻防演练及赛事可以依靠智能训练效果评估功能进行打分和评判。为管理员、裁判和观赛人员提供友好、直观、准确的参考，人员操作同步播放、参赛人员赛程节点路径播放。配套服务为免费提供至少 60 本正式出版的网络安全渗透/网络攻防类教材，包括但不限于：内网渗透的基础知识，以及 Kerberos 专题、NTLM Relay 专题和 Microsoft Exchange 专题，web 安全专题，和免杀技术等内容。支持课任老师联合开发《网络安全渗透/网络攻防》精品课程至少 1 门。</p> <p>1. ▲为高职阶段信息安全技术应用专业及本科阶段网络安全与执法专业提供竞技比赛、竞技比武类综合实践课程，提供竞技比武支撑系统、演练环境及内容资源；为学生网络安全竞赛社团提供日常训练支持。平台包括但不限于：本地部署竞技及比武系统 1 套；在线网安竞赛服务系统，提供为期 5 年每年不少于 60 个账号使用；本地部署竞技比武训练资源包 1 套、竞赛题目资源包 1 套及靶标资源包 1 套。配套服务为免费提供至少 3 个 CISP-PTE 渗透测试工程师</p>			
--	------------------------------------	--	---	--	--	--

		<p>的认证培训。另<b>免费</b>支持提供 2 次省级以上规模（300-500 人）的网络安全大赛驻场支持，内容包括但不限于：赛前准备（比赛设备支持）、赛中支持（赛中全程运维）、赛后管理（比赛复盘）等安全大赛技术支持及指导运维等工作，使用户了解并掌握赛事举办的重点流程。</p> <p>1.1 包括但不限于：<b>具有基于国产自主的虚拟化仿真云技术、网络场景构建技术、平行仿真技术的竞技比武训练、赛中全程运维、攻防态势可视化、考核选拔功能，可提供在线夺旗（CTF）、攻防对抗（AWD+）、内网实战（ISW）等多种演练模式，具有贴近实战的比赛场景，赛程可视化，可复盘和推演各种攻防态势。</b></p> <p>1.2. 包括但不限于：竞技比武配置、资源及参赛队伍管理、比武结果评估、可视化攻防效果展示等功能。</p> <p>1.3. 包括但不限于：可对攻防演练及赛事进行打分和评判。为管理员、裁判和观赛人员提供友好、直观、准确的参考，人员操作同步播放、参赛人员赛程节点路径播放。</p> <p>1.4. <b>▲CTF 攻防场景（包括但不限于： Web 安全、PWN、逆向、MISC、密码等）不少于 100 个； AWD+训练场景（包括但不限于： 漏洞利用， SQL 注入， 爆破，漏洞修补，溢出，后门的发现等）不少于 15 个。（需提供详细场景清单）</b></p>			
--	--	---	--	--	--

			<p>1.5. 系统支持动态反作弊机制，比赛过程中管理员以及裁判可依据平台的反作弊机制实时监控参赛队伍和选手的作弊行为，包括但不限于：登录作弊、答案相同等。</p> <p>1.6. 系统支持不少于 5 种竞赛展示界面（含二维、三维格式），每种展示功能支持竞赛实时攻防信息的显示，提供竞赛公告的显示。</p> <p>1.7. ★支持包括全国职业院校技能大赛、全国大学生信息安全竞赛、公安系统网络攻防大赛等竞技类赛前训练课程；支持包括但不限于：《CTF 基础》、《CTF-WEB》、《CTF-reverse》、《CTF-PWN》等 CTF 大赛实战进阶课程（课程名称可以略有不同，但是核心技能点需覆盖）；支持主流网络安全赛事模拟演练实训课程；能够支撑学生网络安全竞赛社团的日常训练。系统支持 CTF、ISW、AWD/AWD+等更多赛制（覆盖三种以上常见赛制），历经各大网络安全赛事支撑考验，能支撑学院院级网络攻防大赛、省部级以上的攻防大赛与网络安全演练等需求。能同时支撑至少 60 人同时在线竞技。提供不少于 5 年的免费升级服务。</p> <p>1.8. 系统应具备承办公安系统网络安全相关比赛或其他行业中大型网络安全攻防赛的运营支撑能力，可提供省部级或以上级别的赛事运营证明材料。</p> <p>1.9 投标方提供参数确认函及售后服务承诺书。</p>			
--	--	--	---	--	--	--



11		在线网 安竞赛 服务系 统	<p>平台在线提供服务，每年支撑账号数量：不少于 60 个。支持不少于 60 人同时并发参与仿真竞赛云端服务。理论知识不少于 50 道，场景实操不少于 180 道，独家资源不少于 30 道，年度更新不低于 10%。精选历届比赛真题，构建海量 CTF 题库，更全面的覆盖知识点内容。将 CTF 需要掌握的技能按类型进行归类，按知识点融入知识竞赛训练，通过场景实操的方式巩固知识点；包含 WP 不少于 110 个，年度更新不低于 10%。帮助学生更好的进行题目练习，平台题目训练模块提供赛题 WP（解题思路），帮助学生解除答题困惑，攻克技术难点，突破认知范围。</p> <p>1. ▲系统在线提供服务，方便学生在实训室之外的环境中配套使用。支持不少于 60 人同时并发参与仿真竞赛云端服务。学生可基于仿真环境了解和熟悉比赛整体流程，通过实践操作，巩固技能，提升学生实战技能，培养学生赛事思维。</p> <p>2. ▲精选历届比赛真题，构建海量 CTF 题库，更全面的覆盖知识点内容。将 CTF 需要掌握的技能按类型进行归类，按知识点融入知识竞赛训练，通过场景实操的方式巩固知识点；默认提供理论知识不少于 50 道，场景实操不少于 180 道，历届网络安全赛事真题资源不少于 30 道，年度更新不低于 10%。。包含 WP 不少于 110 个，年度更新不低于 10%。。帮助学生更好的进行题目练习，系</p>	年	5	
----	--	------------------------	---	---	---	--

		统题目训练模块提供赛题 WP（解题思路），帮助学生解除答题困惑，攻克技术难点，突破认知范围。（需提供系统内历届网络安全赛事真题截图或列表）			
12	攻防工具资源包	提供不少于 300 个攻防工具，包括但不限于：代理工具、抓包改包、指纹识别、数据管理、破解、程序资源编辑等。	套	1	
13	竞赛题目资源包	1. 提供不少于 130 道 CTF 题目，题目类型包含但不限于：数据隐写、逆向分析、Web 安全、密码学等； 提供不少于 12 道 AWD + 题目，题目考点包含但不限于：漏洞利用、SQL 注入、爆破等； 提供不低于 3 套内网实战题目，每套关卡不少于 6 关，题目考点包含但不限于： 社工、 网站权限获取、 漏洞检测等。 2. 质保期内每年更新不少于 20 道 CTF 题目，题目类型包含但不限于：数据隐写、逆向分析、Web 安全、密码学等； 3. 质保期内每年更新不少于 3 道 AWD + 题目，题目考点包含但不限于：漏洞利用、SQL 注入、爆破等。	套	1	
14	仿真靶标资源包	1. 提供不少于 100 套操作系统及应用靶标，其中操作系统包括但不限于：Windows 、 RedHat、 CentOS、 Ubuntu、 KaliLinux、 openSUSE 等。 2. 提供不少于 60 套漏洞靶标，其中包括但不限于 web 类漏洞、浏览器类漏洞、网络实体设备类漏洞等。 3. ▲提供不低于 5 套内网实战靶标，包括但不限于国网、高校、运营商、民航	套	1	

				等关基设施应用场景（可以有其他应用场景，但是场景类型不能过于单一，不得少于三种以上类型），每套拓扑规模不小于 12 个节点。（附不少于 5 套大型场景靶标说明）。			
15	子项二： 平台系统 硬件及服务购置  模块三： 攻防战队 培养实训 平台	为攻防战队培养专项课程提供平台支撑，快速强化战队专业技能，能够代表学校出战各类赛事并争取取得好成绩，为我校的专业建设形	安全实训系统	<p>1. ▲为攻防战队培养专项课程提供平台支撑。平台包括本地部署安全实训系统不少于 1 套；专业实践课程包不少于 2 套，分别为战队能力培养专项课程资源包及赛前培训专项课程资源包。配套服务为免费提供不少于 3 次战队攻防能力培养实训，每次培训时长为不低于 4 周，总计不低于 12 周约至少 500 课时的培训，包含指导教师及学生培训。免费提供不少于 3 次赛前专项培训，每次培训时长为不少于 1 周。由高级讲师针对大赛的历届比赛整理相关易考难点知识点，结合最新竞赛模式的解题思路和技巧进行深入讲解。充分利用企业的优势和条件为学校提供校外实训基地，为学校提供每年不少于 5 名以上学生的实习就业机会。</p> <p>1.1. ★可提供典型网络安全与管理、网络应用及编程安全、安全攻防等层次互动仿真实验环境，支持学生通过一系列的单项、综合类型实验实践和攻防演练、竞技等训练方式，强化对网络与信息安全防护知识的理解掌握和技能的灵活运用，支持学校安全相关实验实践教学和学生动手能力养成。</p> <p>1.2. 提供教师、学生、管理员三类角色（角色类型可以有其他描述，比如教员、</p>	套	1	

	成良好口碑及影响力。		<p><b>学员、管理员等</b>)。包括但不限于：教师能够对课程、学生、学习计划进行管理，并按照培训要求下发考核任务；学生可以按照培训要求或者个人兴趣选择课程内容进行学习，并完成相应的考核任务；管理员可对系统用户角色、系统资源等进行配置管理。</p> <p>1.3. 包括但不限于：学习安排配置、学习资源配置等功能。</p> <p>1.4. 包括但不限于：可批量导入学生信息（包括学号、姓名、班级、性别等信息），支持班级定向导入与导出功能，一键完成班级创建及班级成员的自动添加。</p> <p>1.5. ▲系统支持多种可视化的展示效果，方便教师和管理员对数据做集中汇总以及数据分析，需支持不少于4种展现形式，实时反映出系统中各类数据状态趋势。（需提供系统数据可视化展示形式的证明材料）。</p> <p>1.6. 提供不少于5年的免费升级服务。</p> <p>1.7. 投标方提供参数确认函及售后服务承诺书。</p>			
16		专业实践课程包一战	<p>▲课程包共分渗透测试攻击及安全运维防御两个侧重点，<b>包括但不限于：设置Oracle注入、网络协议及网络设备配置、操作系统（Linux）及虚拟化、Web安全、软件安装和网站环境搭建、代码编程（Web前端/后端）、sqli环境题</b></p>	套	1	

			队能力培养专项课程资源包	目讲解、代码审计、内网渗透、域渗透等知识内容，支撑战队实战能力的养成。包括但不限于：视频不少于 130 个，战队实训场景不少于 90 个（含单点及多点实训环境）、不少于一套发生近一年内的安全事件仿真场景靶标。（需附课程包目录及场景靶标说明）			
17			专业实践课程包一赛前培训专项课程资源包	▲赛前培训专项课程资源包括 CTF 四大方向课程（Web、Rerveres、PWN、Misc），AWD+两大方向课程（Web、PWN）及 Web 安全、逆向工程、其他杂项等整套课程的环境支持，其中包含视频不少于 90 个，赛题环境不少于 40 个。（需附课程包目录）	套	1	
18	子项二： 平台系统 软硬件及 服务购置	▲网络安全对抗靶场平台：为战队培养实训平台、	靶场云系统	1. ▲可为实践教学、赛训演练及科研工作提供基础设施服务，具备对主机、模板、存储及网络、容器、以及计算资源等的管理与调度，支持虚实结合以及混合组网。（需提供对平台内置资源集中管理调度运行监视配置界面截图） 2. 提供不少于 5 年的免费升级服务。 3. 投标方提供参数确认函及售后服务承诺书。	套	1	
19	模块四：	竞技及比	网络场	1. 基于演训、竞赛、测评及科研任务的实施，通过图形化、拖拽式拓扑绘制	套	1	

	网络安全对抗靶场平台	武演练平台提供必不可少的底层功能支撑;也可用于支撑大中型规模赛事;甚至可为科研工作提供各类仿真场景构建的基础条件。平台包括本地部署靶场云系统 1	景构建系统	<p>解决方案,支撑各任务场景设计。</p> <p>2.包括但不限于:网络场景构建资源管理、虚实结合混合组网等功能。</p> <p>3.▲实验场景由操作区和目标区构成,场景必须支持添加不少于3个(含)以上目标区(需附截图证明)。</p> <p>4.提供虚拟路由器,构建各类具有安全策略的多安全区仿真实验场景,支持场景网络自检,支持静态和动态等多种模式。</p> <p>5.▲系统支持以二维和三维拓扑图模式展示流量轨迹与攻防态势(需附截图证明)。</p> <p>6.能同时支撑至少60人在线进行靶场训练,支持启动网络拓扑规模为30节点的场景,或者至少15支队伍启动虚拟机并发规模为4的赛题环境。</p> <p>7.提供不少于5年的免费升级服务。</p> <p>8.投标方提供参数确认函及售后服务承诺书。</p>			
20			综合管理系统	<p>▲通过虚拟云资源调度,可为网络场景构建、安全实训、学科竞赛、攻防演练及科研场景搭建等提供指挥调度服务,包括但不限于:具有集中化认证、管理、展示、协调、共享、审计的能力,可整合系统相关业务信息,支持资源的统一调配与共享。</p> <p>2.包括但不限于:身份认证、任务管理、以及综合态势展示等功能。</p>	套	1	

		套;本地部署场景构建系统 1 套;本地部署综合管理系统 1 套。		<p>3. ▲系统支持多种可视化的展示效果,包括但不限于:认证访问、资源占用、任务运行等相关数据进行集中汇总、统计分析,需支持不少于 4 种展现形式,实时反映出系统中各类数据状态趋势。(需提供系统数据可视化展示形式的证明材料)</p> <p>4. 提供不少于 5 年的免费升级服务。</p> <p>5. 投标方提供参数确认函及售后服务承诺书。</p>			
21	子项二:平台系统软硬件及服务购置	为支撑上述软件平台的运行及服务内容,需购置的硬件设备	实验室平台主控设备	<p>1. 用途:作为实验室平台的主控设备,主要负责管控实验室平台各资源的使用情况、人员资源调配等功能。提供功能、性能软硬一体化产品形态,应能支撑本地部署软件系统的稳定运行。在 60 人并发实验时,系统响应时间少于 5 秒。</p> <p>2. ▲硬件参数:标准 2U 机架专用设备;并配置<math>\geq 2</math>颗 CPU、内存<math>\geq 64G</math>、存储<math>\geq 4*2T</math>;配置<math>\geq 2*</math>千兆双电口网卡。3. 提供服务器售后服务承诺函。</p>	台	1	
22	模块五:平台的硬件支撑		实验室平台计算设备	<p>1. 用途:作为平台的云计算设备,主要负责用于负载场景防火墙与资源等功能。提供功能、性能软硬一体化产品形态,应能支撑本地部署软件系统的稳定运行。在 60 人并发实验时,系统响应时间少于 5 秒。</p> <p>2. ▲硬件参数:标准 2U 机架专用设备;并配置<math>\geq 2</math>颗 CPU、内存<math>\geq 64G</math>、存储<math>\geq 4*2T</math>;配置<math>\geq 2*</math>千兆双电口网卡。</p>	台	3	

				3. 提供服务器售后服务承诺函。			
23		实验室平台存储设备		<p>1. 用途：作为平台的存储设备，主要负责集中管控平台中所平台内置的虚拟机、以及负载均衡等功能。提供功能、性能软硬一体化产品形态，应能支撑本地部署软件系统的稳定运行。在 60 人并发实验时，系统响应时间少于 5 秒。</p> <p>2. ▲硬件参数：标准 2U 机架专用设备；并配置≥2 颗 CPU、内存≥64G、存储≥4*2T；配置≥2*千兆双电口网卡。</p> <p>3. 提供服务器售后服务承诺函。</p>	台	3	
24		实验室主控交换机		<p>1. 用途：负责联通各节点以及虚实结合场景。</p> <p>2. ▲硬件参数：二层千兆以太网交换机，背板带宽 240Gbps，配置≥48 个 10/100/1000Base-T 以太网端口，≥4 个 1000Base-X 以太网端口，≥1 个 Console 口。不少于 2 个千兆光模块。</p>	台	3	
25		场景 VPN 接入模块		<p>1. 用途：为每个接入仿真环境的角色提供安全链路，支持不同学生或不同队伍使用的网络环境不同，可支持系统各资源之间的互不干扰。为用户使用仿真场景提供了安全接入的通信通道，在保障业务平台和仿真环境安全隔离的条件下，实现同一物理终端、同时访问业务平台和仿真环境。每台模块可支持不少于 30 人接入。</p>	台	2	