采购需求

一、采购项目概况

1.本项目为郑州航空工业管理学院网络攻防技术教学与研究平台建设项目。

2.本项目共分 1 个包，具体情况如下：

序号	包号	包名称	包预算（元）	包最高限价（元）
1	豫政采(2)20251631-1	郑州航空工业管理学院网络攻防技术教学与研究平台建设项目	2110000	2110000

3.采购内容：

郑州航空工业管理学院网络攻防技术教学与研究平台建设项目，具体内容包括专用服务器 3 台、专用计算机 43 台、入侵防御平台 1 台、漏扫平台 1 台、日志审计平台 1 台、网络空间安全实训子系统 1 套、网络空间安全靶场子系统 1 套、网络空间安全竞赛子系统 1 套、路由器 2 台、交换机 2 台、下一代防火墙 2 台、Web 应用防火墙 1 台、基础环境集成实施服务 1 项、多媒体教学套件 1 套等设备和软件及相关配套产品的供货、运输、保险、安装、调试、检测、验收及售后服务等合同约定的所有内容。

4.交付期限：自合同生效之日起 90 天内。

5.交货地点：采购人指定地点。

6.质量标准：满足采购需求，符合国家和行业规定的相关标准。

7.质保期：本项目免费质保期不低于 3 年（自正式验收合格之日起开始计算）。

8.合同履行期限：至合同全部权利义务履行完

9.本项目是否接受联合体投标：否

10.是否接受进口产品：否

11.是否专门面向中小企业：否

二、采购产品清单和技术要求

（一）采购产品清单表

1. 采购产品清单表

包号	序号	标的名称	计量单位	数量	是否进口
1	1	专用服务器	台	3	否
	2	专用计算机	台	43	否
	3	入侵防御平台	台	1	否
	4	漏扫平台	台	1	否
	5	日志审计平台	台	1	否
	6	网络空间安全实训子系统	套	1	否
	7	▲网络空间安全靶场子系统	套	1	否
			点	60	否
	8	网络空间安全竞赛子系统	套	1	否
	9	路由器	台	2	否
	10	交换机	台	2	否
	11	下一代防火墙	台	2	否
	12	Web 应用防火墙	台	1	否
	13	基础环境集成实施服务	项	1	否
	14	多媒体教学套件	套	1	否

备注：上表中标注“▲”号的为核心产品；核心产品提供相同品牌产品且通过资格审查、符合性审查的不同供应商参加同一合同项下投标的，按一家供应商计算，评审后得分最高的同品牌供应商获得成交人推荐资格；评审得分相同的，报价得分最高的获得成交人推荐资格，其他同品牌供应商不作为成交候选人。

（二）采购产品技术要求表

1. 技术参数部分

序号	设备名称	数量	单位	技术要求
1	专用服务器	3	台	1.外观尺寸≤2U。
				2.处理器:配置≥2 颗 Intel 至强处理器，单颗核数≥20 个，主频≥2.4GHz；内存：配置≥8*64GB DDR4 内存，配置≥24 个内存槽位。
				3.硬盘：配置≥1 块 3.84TB SSD 硬盘,≥2 块 2.4TB 10K SAS 硬盘,支持≥40 块 SAS/SATA/SSD 硬盘。
				4.阵列控制器：配置≥1 个 SAS 2G 缓存 RAID 卡，支持 RAID 0/1/5/10/50/6/60。
				5.PCI I/O 插槽：支持≥10 个 PCIe3.0 插槽，可选支持≥3 块双宽 GPU 或≥8 块单宽 GPU。
				6.网卡：配置≥4 个千兆网卡；电源：配置≥2 个 550W 热插拔冗余电源，≥6 个热插拔冗余风扇。
				*7.温感控制：支持 3D 图形化的机箱内部温度拓扑图显示，精准模拟服务器内部温度、提供温度展示功能，并以 3D 温度海洋形式展示各组件温度传感器的分布图（提供功能截图）。
				8.管理：配有远程管理控制端口；支持虚拟 KVM 功能配置,可实现与操作系统无关的远程对服务器的完全控制，包括远程的开机、关机、重启、更新 Firmware、虚拟光驱、虚拟文件夹等操作，提供服务器健康日记、服务器控制台录屏/回放功能。
				9.硬件安全性：为满足国家信息化等级保护的要求，服务器可选择提供插卡式安全智能模块，实现关键业务防护，外观与普通网卡一致，可以保障主机网络安全，提供可选的该安全智能模块彩页。
				10.软件特性（提供功能截图证明材料）：
				（1）支持快速扫描，快速对终端系统目录、启动项、注册表、内存、易感染区等进行扫描，快速检查终端是否存在常见病毒；
				（2）支持防感染模式，当扫描到感染型病毒时，自动进入防感染模式，重新开始全盘扫描并阻止恶意样本反复感染文件；
				（3）支持隔离区病毒的恢复，快速、批量恢复企业内部被误杀的文件，可对终端被隔离的文件进行指定时间段、路径、文件名的危险文件进行隔离和回复；
				（4）具有流量控制功能，可以检测每一台终端的网络流量情况，对任意终端执行限速操作，避免在办公区域有终端下载大容量文件而影响整个网络的速度。
2	专用计算机	43	台	一、硬件部分要求：
				1.机型：分体式台式机；处理器：≥12 核/主频 2.1GHz/缓存 25MB 处理器。
				2.主板：≥Intel B760 芯片组，终端具有故障报警检测功能。
				3.内存：≥16GB DDR5 5600MHz，≥2 根内存插槽，最大支持 64GB DDR5 5600MHz 内存。
				4.硬盘：≥512GB M.2 NVMe 固态硬盘 PCIE Gen4，同时加配一块 1T、7200rpm 机

				械硬盘。
				5.显卡：≥4G 独立显卡,≥128Bit 位宽；网卡：集成 10/100/1000M 自适应千兆网卡；音频：集成 5.1 声道声卡，支持前 2 后 3 音频接口。
				6.接口及拓展槽：≥1 个 PCIe x16，≥2 个 PCIe x1,≥1 个 PCI；≥10 个 USB 接口，其中不少于 4 个 USB3.2 Gen1、1 个 USB3.2 Gen2 及 1 个 USB3.2 Gen2 Type-C。
				7.电源：≥300W 节能电源；机箱：≤10L，顶置电源开关，前置可拆洗防尘罩；键盘鼠标：标准 USB 商务键盘鼠标。
				8.显示器：≥23.8 英寸低蓝光液晶显示器，VA 技术，分辨率≥1920x1080、VGA+HDMI+DP 接口，带原厂 HDMI 线缆、VESA 标准安装孔，具备 TUV 低蓝光认证。
				*9.认证证书：符合国家级 GB/T 9813.1-2016 标准中噪声检验，噪声声功率级≤3.63Bel(A)，提供满足技术参数的证明材料；符合国家级 GB/T 9813.1-2016、GB/T 34986-2017、GB/T 5080.7-1986 标准中的可靠性检验要求，MTBF 不低于 110 万小时，提供满足技术参数的证明材料。
				二、软件部分要求：
				1.支持 B/S 管理架构，可通过移动设备通过网页方式对机房进行远程管理，包括远程开关机、时间同步、系统切换、消息广播等操作（提供第三方检测机构出具的具备 CNAS 标识的产品功能测试报告）。
				2.预装正版 Windows 11 及以上操作系统。
				3.支持对客户端内多块硬盘进行分区、系统装载、还原、还原方式设置，满足多硬盘系统还原和管理,提供软件著作权或产品制造厂商针对本项目的售后保障声明。
				4.支持差异拷贝接收端网络环境检测，可检测接收端网卡连接速度，提前发现问题网点，排查处理影响差异拷贝的终端。
				5.支持网络限制策略，能够设定禁用外网或禁用全部网络，并支持设置例外，例外类型包括 IP 地址、网址、端口，并设置生效时间区间，能够精确到秒，支持按天执行、按周执行、按月执行。
				6.能够针对学生软件使用、上网操作进行记录，并支持按照应用、访问网址进行查询，能够根据时间段进行搜索，搜索时间精确到秒，针对上网操作，能够展示网址及网站标题信息，支持表格导出。
				7.支持程序限制策略，支持黑名单、白名单两种模式，能够根据手动添加、游戏进程、应用进程、系统自带进程进行设置，并能够通过客户端实时识别操作系统进程进行控制，并设置生效时间区间，能够精确到秒，支持按天执行、按周执行、按月执行。(提供功能界面截图)
3	入侵防御平台	1	台	1.要求所投产品为多核 CPU 硬件架构，≤2U，1+1 冗余电源，硬盘≥1T 10K，千兆电口（2 组 bypass）≥12 个，SFP 千兆光口≥12 个，SFP+万兆光口≥2 个，扩展槽≥2 个；网络层吞吐≥15Gbps，IPS 吞吐≥8Gbps，每秒新建数≥14 万个，并发连接数≥450 万；三年 IPS 特征库升级及软硬件质保服务。
				2.要求支持智能应用级的负载均衡，负载策略可配置：线路优先级、按运营商负载、带宽比例、平均分配等负载策略。
				3.支持接口虚拟化功能，VRF 功能可以从系统层面隔离不同 VRF 组里的流量信息和路由信息，使用 VRF 功能可以作为 MPLS 组网里的 MCE 设备。

				4. 要求系统定义超过8500+条主流攻击规则，可针对8种协议自定义入侵攻击特征，自定义特征可设定拓展协议字段，设置数据包中的匹配内容，可选择包含、等于、不等于、大于、正则匹配等匹配方式:同时可选择多种匹配条件，支持设置"与和“或”的匹配顺序；
				5.要求支持弱口令扫描能力，可针对IP、IP端、端口等对象，扫描监控空密码、用户名密码相同、预置弱口令、自定义弱口令等规则，弱口令字典可自定义设置。
				6.要求支持数据下钻至单资产风险详情，可自动关联该资产所有安全信息，安全信息包括但不少于：入侵防御、威胁情报、WEB防护、病毒防护、防暴力破解、非法外联防护、弱密码防护、扫描攻击防御和行为模型等。
				7.要求支持记录QQ、TIM、钉钉、企点、企业微信、微信、skype、MSN等主流IM聊天行为和内容；支持审计用户通过HTTP、FTP、Email等方式外发的文件内容；支持审计用户通过U盘操作的行为动作和文件内容，支持文件本地备份。
				8.要求支持Portal逃生，支持选择不逃生、全部用户逃生和已认证用户逃生等方式。
				9.要求支持本地认证、Portal认证、Radius认证、LDAP认证、POP3认证、AD域单点登录、短信认证、微信公众号认证、APP认证、IC卡认证、二维码认证、互联网钉钉认证、混合认证和免认证，其中微信公众号认证支持通过小程序获取手机号；支持用户自注册，支持设置专门的管理员进行认证审核，支持邮件通知审核提醒；支持对接AC Controller、IMC、AAS、SMP、深澜、城市热点、PPPOE、安美等常见认证服务器。
				10.要求设备旁路部署可提供本地WEB认证、Portal Server认证、短信认证、微信认证；短信认证支持HTTP、SOAP通用短信网关，管理员可基于业务需求，自定义报文内容和格式。
				11.要求支持文件缓存，支持安卓和IOS形式的文件，主动缓存文件形式不限于视频、APP等；针对内网域名或者文件请求模糊匹配，推送文件至终端，实现文件下载加速的效果。
				12.要求提供访问控制策略智能分析，可发现访问控制策略中隐藏策略、冗余策略、冲突策略、可合并策略、过期策略、空策略等不合理的策略配置，并在web页面分析呈现。
4	漏扫平台	1	台	1.要求≤2U机架，≥6个千兆电口+4个千兆光口、≥3个扩展槽，1+1冗余电源，≥32G内存 DDR4，≥4T 10K机械硬盘，要求最大并发扫描地址数量≥128个IP，不限制扫描IP地址类型。
				2.要求系统支持部署在IPv4、IPv6环境下，且系统扫描、Web扫描、数据库扫描、弱口令扫描、基线配置核查等各类型任务均支持添加IPv6扫描目标。
				3.要求支持主机漏洞扫描、Web漏洞扫描、数据库漏洞扫描、基线检查、弱口令扫描、工控漏洞扫描、POC扫描多个漏洞扫描能力；能够检测出IT资产开放的端口、服务信息。
				4.支持多种资产扫描参数细化调整，包括但是不限于：并发扫描的资产数、并发的进程数量、资产发现方式、端口范围、发包率、超时时间、重试次数等。
				★5.要求支持漏洞分类不少于70个，漏洞库数量不少于30万个（提供功能视频演示证明材料）。

				6.要求具备对 Docker 容器及其镜像进行深度漏洞扫描的能力，覆盖广泛的主流操作系统（如 Linux 发行版）以及各种应用服务（如 Web 服务器、数据库等），帮助用户及时发现并修复潜在于 Docker 环境中的安全漏洞。
				7.要求至少支持对 Windows 和 Linux 操作系统、各类安全设备（如防火墙、入侵检测系统等）、网络设备（如路由器、交换机等）；中间件（如 Web 服务器、应用服务器等）、数据库（如 Oracle、MySQL 等）、大数据组件（如 Hadoop、Spark 等）等设备对象的脆弱性扫描。
				8.要求可以根据漏洞的类型或分类来浏览和查看漏洞库中的信息，可根据实际需求自定义扫描模板，可根据漏洞的分类来查询特定的漏洞信息，支持通过漏洞的编号（如 CVE 编号）来精确查询漏洞的详细信息。
				9.要求支持对多种常见协议进行口令强度检测，协议至少包括：SSH、TELNET、FTP、SMB、RDP、MYSQL、POSTGRES 协议;要求支持扫描结果中至少可展示弱口令用户名、密码、协议信息、风险级别。
				10.要求支持允许用户自定义扫描参数配置，具体可配置项至少包括：任务的优先级设定、并发扫描的主机数量限制以及并发执行的插件数量控制等。
				11.要求具备全面的 web 脆弱性检测能力，涵盖多种常见的安全威胁检测方式，包括但不限于 SQL 注入、CRLF、XSLT 注入、服务器端代码注入、缓冲区溢出漏洞、参数篡改攻击以及跨站脚本攻击（XSS）等。
				12.要求可识别工控协议至少支持 modbustcp、s7、opc、dnp3、ethernet/ip、bacnet、mqtt、FINS、igss、pcworx、proconos、codesys 等。
5	日志审计平台	1	台	1.事件综合处理性能≥5000EPS，≤2U，≥1 颗 4 核心 8 线程 CPU，≥32GB DDR4 内存，≥8 个千兆电口，≥2 个接口扩展槽，≥4T 10K*2 硬盘，1+1 冗余电源；至少包含日志源接入、存储、检索、分析等功能，不少于 100 个数据源接入授权。
				2.根据使用的采集协议或方法不同，对接入数据源可配置不同的采集轮询时间、超时时间、处理上限、并发个数等频率参数。
				3.数据解析规则支持规则嵌套和逻辑组合方式，能够对一组事件进行多层规则解析处理，添加、删除、重命名、合并、拆分与裁剪现有字段，对范式化后字段再解析处理。支持多种数据解析，包含精准匹配、包含再解析、正则匹配后从数据头、尾进行二次解析等处理。
				★4.支持解析字段可以通过映射关系进行别名显示，映射方式有：文本、时间、URI 解码、IP 解码、重定义、正则、映射表等。同时还可以对某个或某些字段进行加密，无对应权限的用户不能显示该字段，但其他字段不影响（提供功能视频演示证明材料）。
				5.支持内置包括 IP 类、时间类、数字类和字符类的不低于 300 种常用的安全信息，如办公区 IP、工作时间段、黑名单 IP、常见服务端口、cmd 进程白名单、可疑进程列表等。
				6.支持仪表盘和报表模板对 BI 分析结果的直接引用，BI 分析所用的查询条件和 BI 图例一起保存和发布。
				7.支持研判分析过程中在线解码，无需使用其他工具即可实现 BASE64\HEX\URL\JSON 等常见编码和解码转换功能，提高分析效率。

				8.仪表盘的图形位置和大小可自由拖拽，同时支持丰富下钻功能，可下钻至具体事件、告警，也可跳转到自定义的其它仪表盘，实现仪表的嵌套，方便安全人员定制化的快速分析。
				9.支持通过 SNMP 协议监控交换机、路由器等设备可用性，监控指标包含 CPU 使用率、内存使用率、上下行流量。
				10.支持自定义报表图形化结果展示，包括但不限于柱状图、折线图、区域图、环形图、明细表格、聚合表格、统计量、环比量、同比量等。
				11.支持在线对接同品牌云端情报平台、离线导入情报云情报。
				12.支持等级保护工作电子流程化管理，按基础信息录入、定级、备案、差距分析、整改、测评、监督检查等流程化管理电子文档，并支持等保知识库管理功能。
6	网络空间安全实训子系统	1	套	1.为保障平台使用稳定性及易维护，要求所投产品为集群部署，包含出厂集群计算软件和虚拟化软件，要求平台整体至少满足 40 名学员同时在线并发学习及实验。
				2.提供学生个人学习项目的列表，以及个人的今日课表。
				3.课程模块提供课程介绍，包括课程学习目标、前置课程、课程概述，提供课程目录，支持点击目录快速跳转相应课时进行学习。
				4.实操演练课程的操作视频和实验文档支持显示和隐藏功能，管理员和教员可在后台自主控制学员端是否显示该实验课的视频和文档，且实验文档和实验要求分开进行展示，隐藏实验文档后，不影响学员正常完成实验。
				5.实验场景提供自动回收机制和延时功能，实验场景默认启动时间临近时，提醒用户进行延时操作并支持多次延时操作。
				6.不同学员的实验网络环境完全隔离，相互不影响，无数据交流。
				7.系统内置 Windows10、Kali Linux、Parrot OS 等多种配备网络安全工具的实验操作机，并支持自定义制作实验操作机。
				8.技能训练内容按难易程度分为初级、中级、高级三个级别。
				9.提供渗透测试、安全运维、应急响应等多种训练方向。
				10.专项训练提供内网专项、注入训练、提权训练等多个训练专题。
				11.平台内置实战训练资源不少于 70 个。
				12.支持多人同时进行考核，且提供答题时间、答题总数等统计功能。
				13.支持分数显示、答案显示、考试回顾功能，教员可设置在交卷时是否显示分数，回顾试卷时是否显示答案。
				14.提供试卷管理功能，支持随机组卷和人工组卷两种形式，教员可在各类型题目中挑选题目进行组卷，选题时支持题目筛选。
				15.组卷时支持批量设置每类题目分值和单独设定每道题目的分值。
				16.支持通过灵活配置起止时间、答题限时，面向学员提供按照起止时间统一开考和按照答题限时随到随考的考试形式。
				17.支持防作弊功能，支持题目和选项的乱序。
				18.支持教学计划的制定，可根据院校教学大纲制定每学期的教学计划，编排计划课程，设定教学计划目标，设置学习期限，将教学计划下发到某班级或下发到班级内具体学员，有明确的学习目标和教学计划安排。
				*19.教学计划下可监控学员的实操情况，可查看学员的学情数据，可以针对学员提的问题进行在线答疑等（提供产品功能截图）。

				20.课表管理支持根据教学计划给学员合理安排每天、每周的学习时间和计划课程，方便学员提前预知学习时间合理安排预习课程。
				21.支持教学看板总览，可以看到计划课程下学员的总体进度、完成情况、课时的完成率等，直观体现学生学习进度及学习成果，监督教学计划正常有序进行。
				22.统计分析支持考试名称、考试人数、参加人数、题目数量、试卷总分、平均成绩、创建人统计。
				23.支持在线靶机测试，对靶机执行重启，关机，重置操作，保存靶机，另存靶机，延时功能；支持接入终端和虚拟机文件传输功能；支持查询靶机基础镜像和增量镜像的关联。
				24.实例运维支持集群设备节点不同实例状态的分类查看。列表显示包含实例名称，所属场景，个人/队伍场景的关联关系等数据。
				25.提供用户登录平台的信息查询，用户对平台访问和操作行为记录的查询，以及用户在 linux 系统下通过 SSH、RDP 终端登录实例的会话日志记录、监控视频播放、操作命令历史的查询。
				26.支持软件名称、版本、版权、logo 的系统信息设置；支持面向前台展示的平台功能模块的权限管理；支持系统许可信息的查看及管理；支持云平台管理的调度模式的切换；支持平台离线升级。
				27.支持分类管理功能，提供课程分类、镜像类型、操作系统、题目方向、工具分类、训练分类的增删改查功能。
				★28.课程内容资源包提供总课时不低于 1300 课时，其中理论课时不少于 700 课时，实验课时不低于 600 课时（提供功能视频演示证明材料）。
				29.提供网络安全基础课程：包含网络安全意识、Python 编程从入门到实践、PHP 编程基础课程、网络数据包分析、Wireshark 数据包分析实战、计算机网络及协议安全、网络攻防技术实战、DDOS 攻击与防御、Linux 操作系统安全、Windows 操作系统安全、操作系统安全实践、Web 安全基础、Web 安全进阶、web 安全进阶与实战、web 漏洞分析-XSS、web 漏洞分析-CSRF&SSRF、web 漏洞分析-SQL 注入&XXE 注入、web 漏洞分析-文件包含、web 漏洞分析-文件解析及上传、web 漏洞分析-命令执行漏洞、web 漏洞分析-敏感信息泄露、web 漏洞分析-逻辑漏洞、web 漏洞分析-反序列化漏洞、密码学应用、密码学应用、代码审计基础、PHP 代码审计、数据库系统概论等课程。
				30.提供网络安全实战课程：包含 Metasploit 渗透测试指南、爆破工具详解、渗透测试流程、渗透测试环境搭建、渗透测试工具使用、综合渗透靶场实战、中间件渗透实例讲解、常见漏洞靶场实践、web 安全训练靶场、webGoat 训练靶场等课程。
				31.提供 CTF 课程：包含 CTF 基础知识与常用工具、CTF-Misc 综合应用、CTF-密码学详解、CTF-web 深入剖析、CTF-密码学（Crypto）、CTF-web 安全（web）、CTF-二进制（PWN）、CTF-逆向（Reverse）等课程。
				32.提供企业网络安全课程：包含网络安全应急响应、网络安全应急响应工程师、内网安全基础、内网渗透技术、企业安全建设、等级保护、等级保护体系建设、等级保护测评、无线安全、移动安全等课程。
				33.提供创新网络安全课程：包含区块链安全、人工智能安全课程。
				34.提供技能训练资源包：实战训练不低于 70 个，专项训练不低于 50 个。
				35.提供能力考核资源包：理论基础题目数量不低于 3500 个。

				*36.具备 SaaS 服务能力（提供功能截图证明材料）：
				（1）提供 SaaS 服务能力，通过互联网即可接入学习平台进行理论和实验操作学习，提供人工智能、AI 科普、AI 工具、AI 进阶课程、玩转办公等课程；
				（2）提供实战靶场，包含 WordPress 实战、Joomla 实战、weblogic 实战、Jenkins 实战等训练，提供 SQL 注入、反序列化、命令执行、文件下载等专项训练。
7	▲网络空间安全靶场子系统	1	套	1.参训人员可以查看训练基本信息、训练拓扑、操作机接入场景、虚拟节点管理、实装设备管理、任务考核。
				2.任务运维和导调人员可以查看训练基本信息、训练拓扑，管理公告、虚拟节点、实装设备，任务评判、流量采集、主机采集，任务复盘、人员管理等。裁判可以查看训练基础信息、训练拓扑，公告管理、流量采集、主机采集，并对任务考核进行评判。
				3.提供流量采集功能，根据拓扑区域进行节点流量查询，包括源地址、源端口、目标地址、目标端口、协议、时间、下载等。
				4.训练拓扑编排：操作机接入点配置、流量采集配置（全局流量采集、攻击流量采集）、主机采集方案配置、流量仿真配置、战争迷雾配置。
				5.要求至少提供 15 个内置场景，至少包含：轨道交通典型网络攻击、电子支付数据篡改攻击、企业办公系统内网攻击景、医疗行业数据泄露、数字化电商平台网络攻击等。
				6.测试验证功能提供对用户真实业务场景进行仿真，开展各项安全测试。根据要测评的网络实际部署情况，依托各种靶标元素，采取虚实结合的方式，构建高仿真的网络环境，检测和发现网络中存在的风险和漏洞，测试原有安全加固设备的有效性和稳定性，提高系统的安全性。
				7.提供靶标创建功能，包括靶标名称、操作系统、靶标类型、镜像类型、镜像文件、系统架构、系统语言、CPU、内存、磁盘大小、系统账号、系统密码、Cloud-init、Qemu-guest-agent、靶机描述、服务信息等。靶机服务信息包括服务或协议名称、端口号、账号、密码等。
				8.支持在线靶机测试。KVM、Docker 镜像格式的靶机支持文件上传，重启，关机，重置。支持对 KVM 镜像格式的靶机进行保存靶机，另存靶机操作。
				9.支持设置靶标接入方式，远程连接协议包括 RDP、VNC、SSH，支持同时设置多个接入并可以为每个接入方式单独设置是否允许终端连接。
				10.提供操作系统靶标不少于 50 个，包括 Windows Server2008/2012/2016、Windows7/8/10、Ubuntu、openSUSE、CentOS、OpenBSD、Debian、Fedora、NetBSD、freeBSD 等；
				11.提供应用服务类靶标不少于 500 个，包括 AdaptCMS、AnchorCMS、ArtmedicCMS、b2evolution、beescms、BigTreeCMS、ClipperCMS、cmseasy、Codiad、Croogo、CSZCMS、CubeCart、dnetCMS、DBHcms、DeDeCMS、Dolibarr、DrakeCMS、Drupal、EngineersOnlinePortal、EskolarCMS、e-VisionCMS、ExeroCMS、FamilyCMS、fowlcms、GazelleCMS、GeniXCMS、Hedgehog-CMS、ICEHrm、iGamingCMS、ImpressCMS、JetboxCMS、Joomla、LaniusCMS、LibrarySystem、MiaCMS、MonstraCMS、OpenEMR、OpenSNS、osCommerce、Pbootcms、PHPMBBCMS、PHPBack、phpCollab、PHPIPAM、Piwigo、PixieCMS、PliggCMS、Rukovoditel、Semcms、SeoPanel、ShareCMS、SOPlanning、TestLink、TuguxCMS、webERP、WEBInstaCMS、Webtareas、WordPress、XOSShop、YCCMS、yunyecms、ZeroCMS、快排 CMS 等。

				12.靶场实装设备管理，用户需要根据任务需要从实装设备库中申请借用对应实装设备，当任务完成后可以归还设备。
				*13.拓扑绘制包括网络区域创建、设备添加、链路类型、链路带宽、节点配置，绘制时支持暂存场景，保存拓扑信息、并支持预览场景（提供产品功能截图）。
				14.新增工具包括工具名称、上传工具、工具 logo、工具分类、系统平台、授权方式、工具语言、使用手册、工具 Markdown 介绍等。
				15.提供工具不少于 200 款，包括无线安全、渗透测试、加密解密、脱壳工具、数据库攻击、漏洞扫描、漏洞利用、系统安全、安全运营、云安全等。
				16.技战法管理包括技战法名称、技战法编号、状态、技战法描述、选择关联的战术；战术管理包括战术名称、战术标号、应用领域、战术描述、选择关联的技术。
				17.提供至少一套攻击技战法,包括不少于 14 个战术和 680 个以上技术或子技术。
				18.提供至少一套防御技战法，包括不少于 15 个战术和 100 个以上技术。
				19.漏洞复现提供完整的漏洞验证环境，用户可以使用自定义操作机接入漏洞仿真环境后开展漏洞挖掘和利用，平台提供完整的验证手册辅助用户研究。同一个场景漏洞验证环境，支持不同操作机接入，如 Kali、Windows 操作机、Parrot OS 等。
				20.提供创建漏洞功能，包括漏洞编号、漏洞名称、关联编号、发布时间、漏洞类型、漏洞成因、漏洞等级、威胁类型、漏洞描述、参考链接、POC、EXP、验证环境、验证手册、受影响产品、官方解决方案、补丁解决方案等。
				*21.提供漏洞复现场景不少于 100 个，漏洞总数不少于 32 万条（提供产品功能截图）。
				22.提供账号批量创建功能，包括账号名称、姓名、角色、所属组织、启用/禁用、密码设置、个人头像、手机号、工号/学号、单位/学校、个人邮箱、身份证号等信息的配置。
				23.已删除账号提供账号还原和注销的功能，账号还原后用户可以正常访问平台且历史数据可用，账号注销后该账号及账号相关数据会从数据库永久删除。
				24.支持个人密码修改，需要输入旧密码、新密码、新密码二次确认后完成修改。
				25.提供虚实结合管理功能，包括虚实结合控制器和虚实结合交换机，每类设备支持多台接入；虚实结合交换机连接实装设备的多个网络接口，支撑任务拓扑的虚实互联。
				26.提供终端安全神经元功能：
				（1）支持用户收藏夹、选项页配置等数据同步管理，可实现切换设备后数据云端同步，支持由用户个性化设置与管理平台同步的数据类型；
				（2）支持特定情景下以用户和设备组成的虚拟组，并绑定到组织架构中。当用户端以账号模式或设备模式获取策略时,优先其登录模式所在组织的包含的策略时才会去尝试命中组策略。
				*27.为保障教学所使用网络空间安全靶场系统匹配国家攻防演练能力,以培养社会实际攻防人才需要，要求靶场系统具备支持国家级实战攻防演习能力（如国家护网，强国杯，强网杯，网鼎杯等活动），提供有效证明文件。

				28.要求网络空间安全实训子系统、网络空间安全靶场子系统和网络空间安全竞赛子系统为同一品牌。
		60	点	1.提供虚拟靶标（VM、Docker）授权，保障虚拟场景的正常使用。
8	网络空间安全竞赛子系统	1	套	1.要求平台集成虚拟仿真系统，基于平台一体化部署，无需另外单独配置虚拟化专属资源池。
				2.要求平台整体至少满足40名学员同时在线并发学习，要求每年度提供资源升级包更新服务，包括不低于100个解题题目、10个攻防题目、1套靶场挑战赛题目的内容更新，提供平台终身使用授权，至少提供三年资源升级更新服务。
				3.要求至少支持以提交Flag的方式对学员的训练成果进行评估，单个训练任务支持多训练目标和Flag；支持普通用户上传训练报告，由管理员完成训练成果的判定。
				4.要求至少支持技能训练的管理，至少支持通过关键字检索、训练类型、训练分类、难易程度等方式搜索训练，支持训练文档的显示和隐藏。
				5.要求CTF解题赛题目至少支持静态Flag、动态Flag、随机Flag三种Flag类型。动态Flag题目pushflag方式要求支持路径指定及脚本指定方式。
				6.要求所有竞赛题目支持增删改查及在线题目测试。管理员可访问题目环境，在线调试题目，销毁启动实例，延时使用场景，并管理全局下实例资源的使用。另外，在线测试中解题赛题支持测试Pushflag功能，攻防赛题支持测试Check，Pushflag功能。
				7.要求至少支持线上赛、线下赛两种赛事形式。所有赛事形式下选手题目环境全部采用独享模式进行环境部署。
				*8.要求支持赛事流量管理。开启流量管理可全程记录每个选手、每道题目的解题行为数据，提供管理员下载查看，为赛事争议解决提供有力证据。（提供产品功能截图）。
				9.要求平台支持严格的动态防作弊机制，基于选手token信息动态的为每位选手随机生成唯一Flag信息，实时检测到作弊行为后，立即自动禁赛作弊选手并记录日志。支持管理员解除作弊选手禁赛状态。
				10.要求支持数据统计功能。提供积分总榜，专项排行，题目榜单，答题日志的统计展示。提供3D视觉沙盘态势。使用飞机代表攻击战队，沙盘建筑表示题目，通过机群对沙盘的攻击过程展示完整的比赛态势。
				11.要求支持竞赛运维功能。至少分别从赛事控制，题目运维，实例管理，流量管理，网络详情，公告管理，选手管理，展示管理8个纬度保证运维赛事的精细度。
				★12.要求内置攻防工具至少150款，包含但不限于：漏扫扫描、渗透测试、嗅探欺骗、漏洞利用、加密解密、免杀辅助和信息收集等工具（提供功能视频演示证明材料）。
				*13.要求支持在线靶机测试。提供KVM、Docker格式靶机文件的上传、重启、关机、重置、延时功能。支持对KVM格式靶机的保存、另存操作。（提供产品功能截图）。
				14.要求支持漏洞条目数不少于32万条。
				15.要求实例运维支持按照节点、实例状态、场景分类属性筛选查看实时数据。列表显示至少包含实例名称，所属场景，个人/队伍场景的关联数据信息。

				16.要求技能训练资源包提供CTF训练不低于50个，实战训练不低于50个，专项训练不低于40个。
				17.要求平台内置能力考核题目不低于3000个、CTF解题类题目不低于200个、CTF攻防赛题目不低于15个、CRC靶场挑战赛题目不低于2套。除能力考核题目外均配套完整的解题思路文档。
				18.为保证竞赛实训教学过程中具备实训用病毒库、攻防工具库等资源符合教学及国家相关网络安全法规要求，要求生产厂商具备中国反网络病毒联盟白名单认证甲级认证，提供有效证明文件。
9	路由器	2	台	1.防火墙性能≥4Gbps、包转发率≥35Mpps、加密性能≥2Gbps、IPSec VPN隧道数≥128个、NAT会话数≥50万、带机量≥800个、内存≥2GB。
				2.接口：WAN口≥2*10GE(SFP+)+2*GE Combo，LAN口≥8*GE电(4个可切换三层模式)，≥1个USB3.0/2.0，支持扩展4/5G接入、≥1个CON口。
				3.路由协议：支持静态路由，动态路由协议（等价多路径）；支持组播路由协议：IGMPV1/V2/V3，PIM-DM，PIM-SM，MBGP，MSDP；IPv6：支持IPv6 ND，IPv6 PMTU，IPv6 FIB，IPv6 ACL，NAT-PT，IPv6隧道，6PE、DS-LITE；IPv6隧道技术：手工隧道、自动隧道、GRE隧道，6to4，ISATAP，静态路由，动态路由协议，IS-ISv6，BGP4+；内置网管软件：可实现路由器和交换机一体化网络管理。
10	交换机	2	台	1.性能：交换容量：≥672Gbps，包转发率≥144Mpps（如有多个值，以官网最小值为准）；端口数量：≥48千兆电口+4个千兆SFP。
				2.管理：支持命令行接口（CLI）配置，支持Telnet远程配置，支持通过Console口配置，支持SNMP（EImple Network Management Protocol），支持RMON（Remote Monitoring）告警、事件、历史记录。
11	下一代防火墙	2	台	1.要求1+1冗余电源，≤1U规格，≥4个千兆电口，≥4个Combo（光电复用）口，≥1个CON口，≥1个USB3.0口，≥1个MGT口，≥500G SSD硬盘；网络层吞吐≥2Gbps，IPS吞吐≥1.2Gbps，最大并发连接数≥200万个，每秒新建连接数（HTTP）≥1.9万个，SSLVPN最大用户数≥1000个，IPSec VPN吞吐量≥1Gbps，至少提供60个SSLVPN授权。
				2.要求支持策略预编译技术，在大量防火墙访问控制策略情况下整机性能不受影响。
				★3.要求支持基于IP网段、IP地址范围、ISP地址库、区域地址库等的多种黑名单阻断方式；支持分组功能，可基于分组的一键启停；支持在会话管理界面根据当前会话信息直接设置黑名单（提供功能视频演示证明材料）。
				4.支持网络入侵检测及防御功能，入侵防御事件库事件数量不少于3000条。
				5.要求支持IPS抓包取证，可选择将产生IPS事件的会话所有报文进行存储，并与IPS日志关联一键导出。
				6.基于主流杀毒引擎，支持对文件感染型病毒、蠕虫病毒、脚本病毒、宏病毒、木马、恶意软件等过滤，病毒库数量不少于1200万。
				7.支持对通过设备的SSL流量进行解密。支持代理模式和透明模式两种组网；并支持客户端模式和服务器模式的流量进行SSL解密检查。
				8.至少支持高、中、低三种密码检查强度。
				9.支持对口令频繁暴力破解的检测。检测到暴力破解后可选择告警、精准阻断、阻断源IP等动作。

				10.支持通过主动及被动探测方式，识别终端类型（至少包括：PC、网络打印机、网络摄像机、网络设备、防火墙、负载均衡等），支持多种资产异常告警选项包括 MAC 地址、操作系统、厂商、类别、指纹等。
				11.支持手动设置以及一键生成资产黑名单,支持手动设置以及一键生成资产 MAC 地址绑定表。
				12.至少提供超过 1800 种预定义设备指纹，可手工升级，支持自定义指纹添加，并支持根据实时扫描结果一键生成自定义指纹。
				13.支持对资产的行为学习，自动学习资产相关的流量以及网络连接关系，通过连接关系拓扑可以进行抓包、一键生成安全策略操作。
				14.支持并开通基于 DPI 和 DFI 技术的应用特征识别及行为控制，应用识别的种类不少于 2000 种；支持并开通基于 URL 分类库的 Web 访问管理，URL 分类库规模不少于 2000 万条。
				15.支持并开通基于线路和多层通道嵌套的带宽管理和流量控制功能。
				16.支持并开通 IPSec VPN、GRE VPN，并且支持从管控平台查询到每条 gre over ipsec 的实时包、抖动、延迟数据以图形化界面进行展示。
				17.支持静态路由、动态路由（RIP、OSPF、OSPFV3、BGP4）及基于入接口、源地址、目标地址、服务端口、应用类型的策略路由。
				18.支持 VXLAN 功能，支持跨局域网络建立二层转发。
				19.支持设备本地的配置手动和自动备份，自动备份可按照日、周、月定期备份配置，并从任意配置恢复或者导出，支持自动备份配置不少于 32 个。
				20.支持系统快照功能不少于 16 个。支持将版本、配置文件存储为一个快照并备注描述，可以从历史快照中选择一个进行版本回滚。
12	Web 应用防火墙	1	台	1.支持 1+1 冗余电源，≤1U，多核 CPU 硬件架构，内存≥16GB，硬盘≥1T 10K；千兆电口≥16 个（2 组 Bypass 口），千兆光口≥8 个，万兆光口≥2 个，扩展槽≥1 个，防护站点数≥512 个；网络层吞吐≥26Gbps，HTTP 吞吐≥14Gbps，HTTP 新建连接数≥6 万个，HTTP 并发连接数≥250 万个。
				*2.要求支持 SSL 透明代理，可以对 HTTP 网站进行保护，HTTP 站点同时配置商密算法+国密算法（提供产品功能截图）。
				3.要求系统具备注入攻击防御能力，可以对 SQL 注入、LDAP 注入、SSI 指令注入、Xpath 注入、命令注入、远程文件包含以及其他注入进行防御。
				4.要求系统具备信息泄露防御能力，可以防止服务器错误、数据库错误、Web 目录内容、程序代码、关键字（支持中文，已内置大量的关键字，将请求或者响应中的关键字进行脱敏处理（替换为任意指定字符））等信息的泄露。
				5.要求支持 API 的安全检测和防护功能，可基于 OpenAPI 规范文档，实现合规性检测。
				6.要求保护站点可以选择操作系统/Web 服务器/数据库/开发语言信息。
				7.要求产品支持 Web 应用漏扫，支持的扫描各种类型的 Web 漏洞至少包括：SQL 注入漏洞、XSS 攻击漏洞、Web 服务漏洞、信息泄露漏洞、异常访问漏洞。
				8.要求支持抗拒绝服务攻击，包括：Ping of Death、Teardrop 攻击、IP 分片攻击、Smurf 及 Fraggle 攻击、Land 攻击、ICMP 大包攻击等。
				9.要求支持 IPv4、IPv6 双栈部署，可同时添加 IPv4 和 IPv6 地址为保护站点。

				10.要求支持站点自发现（HTTP 和 HTTPS），自动发现网络中的 HTTP 网站，包含服务器 IP/端口/域名/访问次数等信息，并一键添加为保护站点。
				11.要求支持 PCI-DSS 报表，可根据 PCI-DSS 规范，评估保护站点的合规性。
13	基础环境集成实施服务	1	项	1. 实验室（长：15 米,宽：7 米）内部改造：文化氛围建设、智能化改造（至少包含物联网空开、门窗感应、人在感应）。 （1）实验室改造，施工前提供甲方认可的装修方案； （2）文化墙整体形象设计、氛围布置等； （3）同时可根据甲方的实际需求进行定制化改造。
				2.系统集成综合布线安装调试： （1）综合布线：43 个接入点，六类网线、带线签，电源线必须为国标线、满足设备供电功率需要，所有裸露线路必须整理、捆扎、缠绕管线束； （2）安全：所有设施无安全隐患； （3）设备调试：软硬件平台正常运行，满足日常教学使用； （4）其他：施工前提供甲方认可的施工方案。
				3.定制教师讲桌≥1 套；定制配套钢木结构学生桌（尺寸≥1500mm*600mm*750mm）≥21 套； （1）定制教师讲桌≥1 套，要求： ①讲桌尺寸需根据校方具体情况定制。 ②要求采用优质冷轧钢板，桌面耐划，台面实木，橡木扶手。 ③要求包含教师椅。 （2）定制配套钢木结构学生桌≥21 套，要求： ①学生桌子尺寸≥1500mm*600mm*750mm； ②桌面部分：桌面基材采用 25mm 厚度 E1 级高密度三聚氰胺饰面实木颗粒板材，环保三聚氰胺贴面；要求板面光滑平整，防划伤、高强耐磨,集中耐高温 200℃。板材截面采用同色 PVC 封边条经全自动封边机高温粘贴;修边光滑平整,无棱角,且经过抛光处理。 ③钢架部分：桌架主体采用优质冷轧钢材,数控机床磨具冲压，避免焊缝开裂；管壁厚度不低于 1.0mm， 焊接件焊接时采用二氧化碳保护焊接，焊接处应无脱焊、虚焊、焊穿、错位；焊接后要经打磨处理。各钢件经酸洗、磷化、防锈处理采用高压静电喷涂而成，聚酯环氧粉末喷塑等符合国家环保标准规。
				4.标准 42U 服务器机柜，尺寸：≥600mm*1000mm*2000mm，承重≥800kg，配备 PDU。
14	多媒体教学套件	1	套	1.多媒体教学套件：鹅颈线麦≥1 只，音响≥2 只，功率放大器≥1 台，无线话筒≥1 只；智慧黑板≥1 台 86 寸智慧黑板。 （1）鹅颈线麦≥1 只，要求： ①采用轻触开关，开机具有灯环提示； ②采用≥3 针 XLR 插头；采用≥48V 幻像供电； ③换能方式：电容式；频率响应：20Hz-20KHz；灵敏度：-40dB±2dB。 （2）音响≥2 只，要求： ①二分频线路设计，频率响应不低于 50-17kHz；灵敏度（dB SPL）：≥89dB 1 Watt@1m；额定功率：≥8Ω 150W，最大功率：≤300W；覆盖角度：≥70 度（H）×70 度（V）；声压级：≥112dB 连续/118dB 峰值； ②低音单元：≥1×10 英寸锥形振膜低音；高音单元：≥2×3 英寸纸盆高音。

				（3）功放≥1 台，要求： ①具有高、中、低音调节旋钮，延时、节拍、回声调节旋钮。具有输出短路保护/直流保护/越温保护装置，扬声器保护装置，智能多级风扇变速控制散热。支持≥4 路话筒输入，话筒插口采用卡侬/直插二合一万能座，方便接入不同类型接头的话筒，每路话筒均具一个隐藏式音量调节旋钮；≥2 组辅助线路输入,≥1 组混合音频输出。前面板具有≥1 个话筒总音量控制旋钮，≥2 个辅助音量控制旋钮。 ②后面板接口不少于：TRS/XLR 二合一头×4，莲花×4，输出：莲花×2，2 组专用欧姆头输出接口。 ③带+48V 幻象供电，一个幻象开关。 ④输出功率：8Ω ≥2×300W，4Ω ≥2×450W；频率响应：320Hz-20KHz(±2dB)；阻尼系数：>100：1；信噪比：≥71dB；动态压限：＜0.05%。 （4）无线话筒≥1 只，要求： ①具有 LED 液晶屏显示 RF/AF 信号强度，自动选讯，可设定频道/频率，状态一目了然；具有频率自动选定功能，自动回避干扰；灵敏度可调，接收距离从 25 米-60 米之间可以分段设置；全新独特 ID 编码功能，对周围环境或≥10 台叠机多套使用，具备优良的抗干扰能力，支持自动搜索无干扰信道功能，PLL 相位锁定频率合成振荡模式；双频道频道组数，可切换频率数≥ 400 组；接收机有≥7 档 SQ，可调节接收机灵敏度，可适配更多环境；还原性好，天线分集，接收距离达≥160 米远，适用于大型多功能厅、教学、会议、演出等多种场景。 （5）智慧黑板≥1 台，要求： ①采用超高清≥86 英寸 LED 液晶显示屏,显示比例≥16:9,分辨率≥3840×2160,显示区域:≥1895.04(H)×1065.96(V)mm;色彩度:≥1.07B(10bit);色域（Typ）不低于 85%;动态对比度：≥4000：1;亮度不低于 350cd/m² ；可视角度：≥178°(H/V) ；表面钢化玻璃硬度≥9H；玻璃厚度≤3mm;采用全金属外壳，三拼接平面一体化设计，屏幕边缘采用圆角包边防护，整机背板采用金属材质。尺寸：宽≥4200mm，高≥1200mm，厚≤119mm。 ②整机支持 Windows 及 Android 双系统，其中嵌入式系统版本≥Android 14，主频≥1.8GHz，内存≥2GB，存储空间≥8GB。CPU 不低于四核 ARM Cortex-A55，GPU 不低于 Mali-G52。嵌入式芯片内置 2TOPS AI 算力，可用于 AI 图像、音频处理。Windows 系统采用抽拉内置式模块化电脑，可实现无单独接线的插拔。和整机的连接采用万兆级接口，传输速率≥10Gbps。OPS 配置：CPU 不低于 I5 十二代，内存≥16GB DDR4 内存配置，硬盘≥256 GB SSD 固态硬盘。 ③整机内置不低于 2.1 声道扬声器，顶置朝前发声，额定总功率不低于 50W。扬声器均采用模块化设计，无需打开背板即可单独拆卸，便于维护。④为方便教学，整机支持在 Windows 系统下可实现无需点击任意功能入口（不需要通过点击批注及打开白板等操作），当检测到触控笔笔尖接触屏幕时，自动进入书写模式；通过提笔即写唤醒批注功能后，可进行手笔分离功能，使用笔正常书写，使用手指可以操作应用、点击操作，如打开浏览器等。⑤整机支持画中画模式，可对整机 HDMI 通道、内置 PC 通道等非安卓通道进行画面快速预览，在预览画面中可进行触摸点击、应用打开等操作，实现跨通道的双系统联动使用，支持对画中画窗口显示大小、音量进行调节。整机画中画窗口支持大、中、小三个级别调节，且可以在屏幕中的任意位置漫游。 ⑥交互式白板软件支持手写笔迹的智能编辑，支持通过手绘置换符快速置换前后

				文字语序，支持手动涂抹笔迹对象进行快速删除，支持圈选笔迹对象进行手写笔迹缩放，支持文字间手绘竖线进行文字间距的快速调整。

注 1：

（1）供应商须在投标文件中如实响应上述要求，对材料真实性负责，如果存在编制虚假材料情况，采购人将有权按照政府采购相关规定上报上级管理部门。

（2）供应商应如实描述所报产品的技术参数和性能，不得完全复制粘贴上表技术参数和性能描述。因完全复制粘贴上表技术参数和性能描述而产生的不利于供应商的评审风险由供应商自行承担。

注 2：

（1）技术支持资料：对要求提供截图、视频、技术方案文档等的条款，供应商当在如实提供，凡不提供或提供不符合要求的，视为无效。

（2）演示视频要求：上表中标注“★”号的为需要演示内容（共 5 处），演示视频须将所有演示条款按顺序整合编辑成 1 个视频文件，命名为“（供应商公司名称）-演示视频”，格式为 mp4 等常见格式，视频中需有对应的讲解或文字说明，未按要求提供完整视频的，视为不满足该技术条款并按照规定扣除相应的技术分。不按要求制作、模糊不清或现场视频无法打开导致的风险供应商自行承担。其他要求演示要求详见采购文件第四章。

注 3：

（1）核心产品：上表中标注“▲”号的为核心产品；核心产品提供相同品牌产品且通过资格审查、符合性审查的不同供应商参加同一合同项下投标的，按一家供应商计算，评审后得分最高的同品牌供应商获得成交人推荐资格；评审得分相同的，报价得分最高的获得成交人推荐资格，其他同品牌供应商不作为成交候选人。

（2）表中标注“*”号的为重要技术参数，其他为基础技术参数，供应商须在投标文件中对技术参数偏离情况进行说明。

三、供货要求

1.免费服务期：项目正式验收后不低于 3 年。服务期内成交供应商提供免费网络远程/上门服务和 7×24 小时电话服务，服务内容包括但不限于软件系统和数据资源的维护、优化、

升级、服务响应、使用培训非模块级的功能需求变更、部署结构变化等服务。

服务响应时间要求：成交供应商在接到采购人服务要求时，2 小时内响应，4 小时内网络远程或现场处理问题，24 小时内需解决问题并修复问题时间段内的系统或数据延误。

2.服务期内成交供应商对所提供软件系统提供 7×24 小时的安全运维监测和告警服务，并提供专业的解决方案建议。

3.成交供应商对于本项目中存在的 Bug、缺陷、安全风险隐患等，在服务期内外均提供持续的修补和消除服务。

4.成交供应商根据采购人所有业务系统的需求和运作规律,有针对性地制定项目系统平台的运维和服务保障方案，建立完善的服务体系。

5.成交供应商在服务过程中提供完善的文档记录，包括故障处理报告、健康巡检月度报告、服务年度报告等。

6.成交供应商提供故障分级响应机制,按照服务计划和质量保证承诺向采购人提供优质的技术支持服务。

7.成交供应商提供服务期外的有偿服务，所提供服务与服务期内服务相同，并承担同样的责任与义务，服务期后只收维修成本费，不收工时费。

8.成交供应商提供不少于 1 名驻场人员且在校园内驻场服务时间不少于 2 年,需负责本次招标项目的系统维护与硬件设施维修。系统维护主要包含网络安全实训子系统、靶场子系统、竞赛子系统的故障处理；硬件设施如有问题不能及时修复，需要 48 小时内提供备用机器保障教学的稳定进行。

9.本项目为交钥匙工程；成交供应商报价包含设备耗材及安装调试等所有费用。

10.成交供应商保证提供给采购人的软件，采购人可永久使用，确保采购人具备项目完整知识产权，确保项目资源无版权纠纷且不侵犯任何第三方知识产权。

四、验收要求

1.货物安装、调试完成后，供应商应主动以书面形式向采购人提出初步验收申请，双方共同清点检查并签署验收意见。采购人如果发现数量不足或有质量、技术等不符合合同规定的问题，采购人有权拒收。供应商应负责按照采购人的要求采取补足、更换或退货等补救措施，按照采购人要求限期整改并重新提交验收申请，且由供应商承担由此发生的一切损失和费用。

2．初步验收合格，在货物正常运行满 15 个工作日后，由项目建设单位向

学校国有资产管理处提出正式验收申请，由校级验收小组对项目进行最终运行效果验收，验收合格的，由国有资产管理处出具正式的《验收报告》证明材料，学校验收通过后，才能支付剩余合同款项。