常州机电职业技术学院工业互联网安全实训室项目合同

甲方：常州机电职业技术学院　　合同编号：XC20251044-Z

乙方：江苏首创高科信息工程技术有限公司　　签订时间：2025 年 11 月 26 日

根据常州筠诚工程咨询有限公司 2025 年 11 月 20 日进行的 JSZC-320400-CZYC-G2025-0005 号招标结果，甲、乙双方就常州机电职业技术学院工业互联网安全实训室项目，本着平等互利的原则，通过共同协商，根据《中华人民共和国政府采购法》、《中华人民共和国民法典》及有关法律法规，就相关事宜达成如下合同。

一、合同标的

序号	货物名称	型号规格	品牌	产地	数量	单位	单价（元）	金额（元）	备注
1	工业互联网安全实训控制终端	赛宁	CP5260H-S	南京	1	台	823,200.00	823,200.00	
2	工业互联网安全实训资源库管理终端	赛宁	CP5260H-P	南京	1	台	406,700.00	406,700.00	
3	工业互联网安全实训知识库管理终端	赛宁	CP5260H-T	南京	1	台	720,300.00	720,300.00	
4	高性能工作站	联想	ThinkStation P3	北京	1	台	48,000.00	48,000.00	
5	路由器	锐捷	RG-RSR20-X-28	福州	3	台	10,400.00	31,200.00	
6	接入交换机	锐捷	RG-S5310-24GT4XS-E	福州	3	台	9,400.00	28,200.00	
7	组网交换机	锐捷	RG-S5310-48GT4XS-E	福州	1	台	10,400.00	10,400.00	
合计金额 大写贰佰零陆万捌仟元；小写 2,068,000.00 元									

本合同总价款包括货物设计、制造、包装、仓储、运输装卸、保险、安装、调试及其材料及验收合格之前保管及保修期内备品备件、专用工具、伴随服务、技术图纸资料、人员培训发生的所有含税费用。本合同总价款还包含乙方应当提供的伴随服务/售后服务费用。

二、合同标的技术要求

1. 技术质量要求：（以合同附件形式附后）；

2. 下列文件是构成合同不可分割的部分，并与本合同具有同等法律效力，这些文件包括但不限于：

（1）JSZC-320400-CZYC-G2025-0005 号招标文件。

（2）乙方提交的投标文件。

（3）招标文件及相关的资料。

（4）乙方投标的其他资料及承诺。

（5）经甲、乙、双方确认的其他补充协议及相关资料。

三、交货与运输

1．货物交付：本合同货物的交货日期为收到中标通知书 30 个工作日内完成供货、安装、调试并验收合格）;具体以货物运到现场的时间为准，此日期或甲方书面通知变更后的日期为计算迟交货物违约金的依据。

2．资料交付

乙方应在交付货物的同时向甲方提供全套随机文件（含产品合格证书、使用维护说明书、验收报告书）壹套。

3．交货地点：乙方应将货物运到甲方指定的地点。货物现场交付，甲方检验无误，签署收货通知单后，货物所有权转移给甲方。

四、验收方案

乙方提供的所有货物在交接过程中都须进行严格的检验和试验。

1．出厂检验：乙方提供货物的产品合格证。

2．到货检验：货物运达目的地后，甲方通知乙方派员及验收部门赴现场共同清验交收，并形成记录材料。清验中，若发现货物由于非甲方原因（包括运输）发生任何损坏、缺陷、缺少或与合同规定的质量标准和规范不符，应做好记录，并由双方代表签字，各执一份，作为甲方向乙方提出修理、更换、索赔的依据。若乙方代表未按约定时间赴现场参加验收，甲方有权自行开箱清点检验，其检验结果和记录对双方同样有效，并作为甲方向乙方索赔的有效证据。

3.安装调试检验：货物安装调试结束后由甲方组织相关部门进行验收，并出具验收结果。若对验收结果有异议，可由双方委托权威的第三方检验机构进行检验。检验结果对双方都有约束力，检验费用由责任方负担。

4．配套服务检验：乙方必须提供货物的现场安装、启动、调试、监督等服务；提供标的物组装和一般维修所必须的工具；提供在合同规定的期限内对所提供货物实行运行监督、维修服务的前提条件是该服务并不能免除乙方在质量保证期内所承担的义务；

5．提出异议的时间和办法：如有任何货物经检验和试验不符合技术规范的要求，甲方可以拒收。乙方应更换被拒收的货物，使之符合技术规范书的要求，乙方承担由此发生的一切费用。乙方如对甲方提出的修理、更换、索赔要求有异议，应在接到甲方书面通知后 3 天内提出，并在该时间内自费派代表赴现场同甲方代表共同复验。乙方在接到甲方按本合同规定提出的索赔通知后，应尽快修理、更换或补发短缺部分，由此产生的制造、修理和运费及保险费均由乙方

负担。上述索赔，甲方从付款中扣除。

6.其他（无）

五、履约保证金：

为保障合同的有效履行，签订合同前，乙方应先缴纳合同总额的 5%的履约保证金，计 103400 元,大写：拾万叁仟肆佰圆整；质保期满后 15 个工作日内退还履约保证金。（不计息）

六、付款方式：

本合同经费按以下第 2 种方式支付：

1.一次性支付，支付时间和方式。合同签订后，按验收标准验收合格后 15 个工作日内付合同总额的 100%。

2.分期支付，支付时间和方式：

（1）合同签订后 15 个工作日内甲方支付给乙方合同总额的 35 %作为预付款；

（2）余款 65% 待验收合格后 15 个工作日付清。

3.其他约定的支付方式，约定如下：_____/_____；

七、质量保证期与售后服务

1.质量保证期为自物资设备验收合格并通过试运后 三 年。

2.乙方应保证所供物资设备在安装调试合同货物时，免费派出技术人员赴甲方现场技术指导。对甲方人员进行培训，主要培训内容为：包括不限于工业互联网安全控制终端、工业互联网安全实训资源库管理终端、工业互联网安全实训知识库管理终端等，并按要求做好记录，双方签字确认。

3.质量保证期内免费更换零配件（人为损坏除外），质量保证期满后实行终身有偿维修保养。提供 7x24 响应。质保期内，发生故障时，我司在收到委托单位通知后 20 分钟内响应，一般性故障在 2 小时内解决，对严重影响系统运行的故障在 4 小时内解决，保障系统正常运行。

4.质保期结束，不能视为乙方对合同货物中存在的可能引起货物损坏的潜在缺陷所应负责任的解除。潜在缺陷指货物在制造过程中未被发现的隐患，乙方对纠正潜在缺陷应负责任，其时间应延续至质保期终止后贰年。当发现这类潜在缺陷时（经双方确认），乙方应立即予以无偿修复或更换。

5.其他承诺（无）

八、违约责任

1、乙方不履行或未按约定要求完全履行合同，甲方有权扣除履约保证金作为违约金。

2、乙方逾期交货或者甲方逾期付款,应向对方支付违约金,迟延履行违约金以逾期部分价款总额每日千分之 八 计算。任何一方逾期履行超过 十 天，应当以逾期部分价款总额 5%向

对方支付违约金，守约方有权解除合同或要求继续履行合同。

3、提供的部件不符合谈判文件的技术要求，必须按要求进行修复、拆除或重新采购；若乙方拒不按要求更正的，将对乙方处以不低于 5 倍的罚款（按不合格部件价值计算），且乙方应承担由此发生的一切费用，延误的工期不予顺延。

九、不可抗力

1. 本合同所称不可抗力，是指不能预见、不能避免并不能克服的客观情况。

2. 由于不可抗力事件，致使一方在履行其本合同项下的义务过程中遇到的障碍或延误，不能按规定的条款全部或部分履行其义务的，遇到不可抗力事件的一方（受阻方），不应视为违反本合同。

3. 不可抗力事件终止或被排除后，受阻方应继续履行本合同，并应立即通知另一方。受阻方可以延长履行义务的时间，延长期应相当于不可抗力事件实际造成延误的时间。

十、合同纠纷处理

因履行本合同发生争议，由双方协商解决，解决不成则提交常州仲裁委员会仲裁。

十一、生效

本合同自双方签字盖章之日起生效。见证方对甲方通过见证方平台采购本合同标的的事实进行见证，本合同的履行与见证方无关。

十二、合同份数

本合同一式伍份。甲方叁份、乙方贰份。

甲方：常州机电职业技术学院

单位名称（章）：

单位地址：常州市武进区鸣新中路 26 号

法定代表人：

委托代理人：

项目负责人：

开户银行：农行邱墅支行

账　　号：10-605701040004030

税　　号：123200004660069658

电　　话：

乙方：江苏首创高科信息工程技术有限公司

单位名称（章）：

单位地址：常州市新北区府琛商务广场 1 幢乙单元 910 室

法定代表人：

委托代理人：

开户银行：中国建设银行常州惠民支行

帐号：32001629701052501072

税号：913204117437317018

电　话：0519-85160051

附件一

一、主要设备参数要求

序号	货物名称	技术指标要求
1	工业互联网安全实训控制终端	一、硬件规格 1. ★CPU：海光 x86 架构 2*5380 及以上 2. ★内存：≥DDR4 3200MHz REG 2R 32GB*4 3. 硬盘：SAS 硬盘：1.8TB 2.5 英寸 10K RPM 12Gb 硬盘×6 SSD：1.92TB 2.5 英寸 SATA 6Gb/s 企业级 SSD 480GB 2.5 英寸 SATA 6Gb/s 企业级固态硬盘×2 4. 网络：2*GE 口+2*10GE 口 5. 电源模块：550W 电源模块*2 150cm 10A AC 国标电源线*2 滑轨 二、软件功能 1. ▲平台支持对常见的操作系统进行虚拟化仿真，包括：Linux、Windows、Unix、MacOS 等，提供截图证明。 2. 平台支持模拟多种类型虚拟设备，包括路由器、交换机、防火墙、IPS 等。 3. 支持对虚拟链路的详细特性进行设置，特性包括链路的带宽、延迟和丢包率等。 4. 支持通过 Web 控制台接入到虚拟机、容器以及实体设备，支持的接入协议包括：rdp、ssh、telnet、vnc、串口等。 5. 支持通过 TCP/IP 协议接入实体设备，实体设备可与虚拟靶标共同组网。 6. ▲平台支持 SNMP 配置功能，配置项包含：版本选择、读取团体字、ip 等信息；支持采集实装设备信息，包括 CPU/内存/硬盘使用率、网络接口流量大小等。提供截图证明。 7. 支持对实装接入设备进行监控，包括实装设备的 CPU、内存、硬盘使用情况、接口流量、引用状态。 8. ▲支持虚拟机、容器、 dynamips、仿真节点、实装混合组网。提供第三方检测机构出具的具有 CMA 或 CNAS 标志的检测报告或认证证书复印件。 9. 拓扑编辑器支持背景定制、拖拽添加设备、交互缩放与全屏展示，还包含快捷键操作、区域块绘制与嵌套拖动，以及个性化设置如显示工具、链路端口名称、简易连线模式和提示最大节点数。 10. ▲支持对拓扑中的元素进行自定义操作，自定义操作包含设置区域的填充颜色、填充图片、旋转角度、边框颜色、边框宽度、边框圆角、边框线形、边框是否动效、文本颜色、文本大小、文本粗细、文本偏移、文本旋转角度。要求现场演示该功能。 11. ▲支持配置拓扑中连线的基础属性，支持配置连线类型包括直线、曲线、折线，支持连线交叉时自动跳线。支持设置连线填充颜色、连线宽度、连线是否动效、链路文本大小、链路文本粗细、标签块颜色、标签块圆角。提供截图证明。 12. 内置仿真交换机支持配置设备信息，以仿真真实交换设备的光口和电口排布展示各个网口的占用情况，支持设置仿真交换机的地址段、网关地址、DNS 信息、是否开启 DHCP 等网络信息。 13. 支持对场景拓扑中虚拟链路特性进行设置，包括：链路的上行带宽、下

		行带宽等。 14. ▲支持自定义场景拓扑中节点的 3D 节点模型，并能够将自定义模型应用到态势展示中。提供截图证明。 15. ▲场景中的终端节点支持配置网卡数量、CPU 核数、内存大小、磁盘大小、使用的镜像快照、虚拟 USB 设备及实装 USB 设备的挂载。要求现场演示该功能。 16. ▲支持自定义镜像，格式包括：Qcow2、VMDK、VDI。提供第三方检测机构出具的具有 CMA 或 CNAS 标志的检测报告或认证证书复印件。 17. 支持对靶标进行快照操作，支持展示快照路径关系，支持合并快照。 18. 支持对虚拟靶标资源进行管理，靶标的属性包括名称、logo、设备类型、操作系统、占用资源大小、接入方式等。 19. ▲平台支持对虚拟 USB 靶标进行管理；支持虚拟 USB 设备和其它设备一起构建虚拟网络结构；支持启动和停止 USB 设备。提供截图证明。 20. 支持流量包、流量脚本两种流量定义方式，其中流量脚本支持 Python、Shell 等语言，流量脚本支持自定义脚本参数。 21. 导入流量包后支持自动分析流量包中的有效协议，并支持选择指定协议重组流量包。 22. 支持流量集合功能，可将背景流量与攻击流量进行组合管理。 23. 支持对场景内的操作系统、应用系统、安全软件进行数据采集。 24. ▲支持采集文件变更事件，包括监控文件大小变更、权限变更、所有者变更、最后修改日期变更、校验和变更、目录新增文件、目录删除文件、目录文件变更等。提供截图证明。 25. ▲支持采集注册表变更事件，包括监控包括 size 变更、mtime 变更、inode 变更、md5 变更、sha1 变更、sha256 变更等。提供截图证明。 26. 支持采集并展示虚拟资源中的虚拟内核大小及使用率、虚拟内存大小及使用率、硬盘大小及使用率、服务状态、节点状态。 27. 支持对平台中的场景实例进行监控，支持通过场景状态筛选并展示场景实例。支持关闭场景实例及清除场景实例数据。 28. ▲支持按照承载业务服务的物理节点进行筛选并展示，展示内容包括业务服务名称、服务状态、运行时长，并支持一键重启。提供截图证明。 29. 支持对截屏及录屏资源进行管理，支持通过用户、组织和场景名称对资源进行过滤。 30. ▲支持硬件设备资源监控，支持显示 CPU 使用率、内存使用率等硬件设备资源使用情况。提供第三方检测机构出具的具有 CMA 或 CNAS 标志的检测报告或认证证书复印件。 31. ▲支持根据训练场景 2D 拓扑编排自动转换为 3D 网络拓扑，转换元素包含各类型节点、区域及链路，支持 3D 拓扑界面展示攻击手法、攻击动态、攻击流量、攻击端口等信息。要求现场演示该功能。 32. 课时支持理论课、实验课两种形式。理论课包含课程讲义、视频、附件、课后练习；实验课包含实验指导、视频、附件、实验场景、课后练习； 33. 支持课时单/双屏切换功能，双屏模式下能够同时展示课件和实操场景，便于用户做实验时随时查看实验指导； 34. ▲实验课时支持实验报告功能，学员可在线提交实验报告，实验报告支持保存草稿与提交两种形式；支持在远程虚拟机桌面中进行截图，能够将截图自动放入实验报告中；提供截图证明；

		35. ▲讲义和实验指导支持在线展示 doc/docx 格式文档，在线文档支持区分大小写查找并显示页数，点击查找结果能够跳转至关联页面，关联页面中对查找的关键字进行标记展示，支持按照显示比例进行缩放功能，缩放比例包括 50%、75%、100%、150%、200%、页面宽度、整页选项，提供截图证明； 36. ▲讲义和实验指导支持使用 ppt/pptx 格式在线展示。展示需支持如下能力：文档中的动画效果无损展示，动画效果包括但不限于飞入、擦除等，支持文档快捷键功能，支持的快捷键包括但不限于前后页切换等，要求现场演示该功能； 37. ▲讲义和实验指导支持视频播放，支持的播放模式包括当前页播放、画中画播放等，支持文档中音频播放，音频格式包括但不限于 MP3、M4A 等，支持文档中的视频和音频按照倍数进行播放，提供截图证明； 38. ▲支持视频学习进度追踪，自动设置、自定义两种检查点设置方式，并通过智能分析技术实现对课程学习进程的精准追踪与评估，提供截图证明； 39. 支持个人中心信息展示功能，包含用户基本信息、岗位信息、公告信息，个人启动的场景、虚拟机、容器、实装设备等资源占用统计； 40. 支持查看我的日历，日历可查看个人课程、训练和比赛任务安排； 41. 支持常驻显示活动场景功能，在前台所有页面均可直接展示当前活动场景数量，并支持点击弹窗查看详情，点击场景可快速跳转到场景所在页面； 42. 我的职业展示当前职业的岗位职责、知识点、技能点，当前岗位下的课程学习路径及课程学习完成度，当前岗位下的任务训练路径及训练完成度； 43. 支持岗位评估功能，展示当前岗位下知识体系清单、岗位课程学习进度、技能体系清单、技能训练记录，以及综合的岗位匹配度； 44. 支持网安人才培养 3D 态势展示，统计优秀组织排名、复合人才排名、个人岗位复合度排名； 45. 支持单兵训练，团队训练两种训练模式； 46. 单兵训练场景包含训练说明，任务列表，训练记录；训练说明详细展示基本信息和前置技能，任务列表以矩阵形式实时显示提交状态，训练记录包含提交时间、时长、完成情况和得分。 47. 学员可提交训练任务，实时查看题解，实时判定任务，查看进度和得分；训练过程中支持查看训练资料、任务矩阵，并可以多虚拟环境无缝切换操作。 48. 管理员可进行单兵训练的基础信息编排、拓扑编排、任务编排， 学员可自主启动/删除训练场景；支持训练场景测试； 49. 支持统计个人、组织单兵训练得分排名；支持统计各参训人员完成训练次数、提交任务数、任务正确率、任务得分、综合排名； 50. ▲支持根据训练类别和难度筛选训练列表，同时能够展示每项训练所对应的技能。支持根据训练关联的攻击手段匹配 ATT&CK 或 Engage 模型，并展示该训练在不同阶段所对应的技能数量，便于学员根据自己的需求筛选训练。要求现场演示该功能。 51. 团队训练支持提供训练模板，教员可编排拓扑、人员、任务，并设定难度、时长、目标和前置技能。支持模板授权、角色分配、任务模板导入

		和阶段管理；提供流量矩阵展示、一键控制，以及战场通信（点对点、团队群聊、历史记录查看）。 52. 支持学员能力得分与训练得分的综合评分，教员可设定权重并添加评语，以雷达图展示技能评分。训练详情页可查看报告，包含多种统计和排名，支持 PDF 导出。 53. ▲支持 3D 态势复盘功能，能够通过动作类型、事件类型筛选复盘数据，其中动作类型包含攻击、防御、阻断、归属，事件类型包含任务导调事件、流量采集事件、手动导调事件、主机采集事件。提供截图证明。 54. ▲回放录屏支持单屏及多屏模式，多屏模式下支持打开一个主屏及 3 个副屏同时播放虚拟机录制的视频文件，主屏幕回放过程中支持播放/暂停以及全屏播放功能。提供截图证明。 55. ▲支持动态新增、删除、配置仿真任务，仿真任务配置包括但不限于：延时、抖动、IPG、时长、流量发生速率、流量发生模式（均匀分布、随机分布、二项分布、指数分布、高斯分布）、TCP 配置（MSS、UGR、ACK、PSH、RST、SYN、FIN、源端口、目的端口）、IPv4 配置(TTL、TOS/DSCP、源 IP、目的 IP)等。提供截图证明。 56. 管理员可进行团队训练的基础信息编排、拓扑编排、任务编排， 学员可自主启动/删除训练场景；支持训练场景测试。 57. ▲支持训练监控，支持在已创建训练的指挥大屏页面，显示导调控制、任务裁决、探针采集、流量分析、屏幕监控等信息。提供第三方检测机构出具的具有 CMA 或 CNAS 标志的检测报告或认证证书复印件。 58. 支持按个人、组织进行团队训练得分排名；统计各参训人员训练次数、提交任务数、任务正确率、任务得分、综合排名。
2	工业互联网安全实训资源库管理终端	一、硬件规格 1. ★CPU：海光 x86 架构 2*5380 及以上 2. ★内存：≥DDR4 3200MHz REG 2R 32GB*4 3. ★硬盘≥1.92T 2.5 英寸 SATA 6Gb R SSD 4. 网络：板载双口千兆 RJ45 网卡（1Gbps） 5. 电源模块：550W 电源模块*2 6. 硬盘背板（04 背板型号） 二、软件功能 1. 提供工业控制基础、工业控制系统安全、工控政策标准解读、工控安全攻防、工控安全技术、工控系统网络安全、工业网络基础、工业安全管理体系、工控网络安全意识等课程资源，包括理论课、实验课所需的配套文档及母本资源。 2. 支持理论基础、夺旗练习两类练习方式。 3. 理论题库≥3000 个，覆盖移动安全、接入安全、主机安全、网络安全、办公安全、应用安全、数据库安全、云安全、密码学、法律法规、安全防护、安全运维、工控安全等网络安全理论知识。 4. 夺旗 CTF 题目数量≥280 个，覆盖密码学 Crypto、逆向 Re、二进制漏洞挖掘与利用 Pwn、杂项 Misc、移动 Mobile、Web、工控安全等，并提供全套解题思路。
3	工业互联网安全实训	一、硬件规格 1. ★CPU：海光 x86 架构 2*5380 及以上 2. ★内存：≥DDR4 3200MHz REG 2R 32GB*4

	知识库管理终端	3. ★硬盘≥1.92T 2.5英寸 SATA 6Gb R SSD 4. 网络：板载双口千兆RJ45网卡（1Gbps） 5. 电源模块：550W电源模块*2 6. 硬盘背板（04背板型号） 二、软件功能 1. 提供不少于250个靶标镜像，包括：操作系统靶标，应用系统靶标，网络设备靶标，安全设备靶标，工控设备靶标。 2. ▲工控设备靶标（施耐德、西门子、罗克韦尔、菲尼克斯、三菱、倍福等至少6家PLC仿真能力）提供针此类型靶标的系统功能截图证明； 3. ▲具备Wincc、iFix、Intouch、Kingview、KingSCADA、Vijeo Citect、ForceControl、FCPower、RealInfo、MCGS等至少10种组态软件的仿真镜像资源，模拟操作员站节点,提供针此类型靶标的系统功能截图证明； 4. ▲具备TIA Portal、STEP7、UnityPro、SoMachine、Studio5000、CCW、PME、TwinCAT等至少8种编程软件的仿真镜像资源，模拟工程师站节点，提供针此类型靶标的系统功能截图证明； 5. ▲具备InoTouch Editor、McgsPro、HT8001CN、NaTouch、NaView、DopSoft、FvDesigner等至少7种HMI编程软件的仿真镜像资源，模拟HMI编程组态节点，提供针此类型靶标的系统功能截图证明； 6. ▲具备KEPServer数据采集仿真镜像资源，构建典型的OPCServer节点，提供针此类型靶标的系统功能截图证明。 7. ▲提供不少于6个工控安全场景，模式覆盖单兵训练、团队训练，包含且不限于风力发电、水力发电、火力发电、石油管网、智能制造、轨道交通等纯虚拟化工业控制系统业务场景，配备全套场景说明、网络拓扑、训练任务、场景流量、数据探针、训练手册等。提供各场景功能截图证明； 8. 提供10种数据采集探针，至少包含信息类、日志类、事件类等。 9. 系统提供自研背景流量和攻击流量库，至少包含基础网络流量、应用软件流量、WEB攻击、远程溢出攻击、DDOS等多种类型的流量和攻击方式，数量不低于100个。支持自定义修改。 10. 提供不少于500个攻防工具；支持用户搜索、查看和下载工具；工具类型包括：权限维持、加密解密、漏洞利用、隐写取证、信息探测、逆向分析、网络扫描、漏洞管理、WAF、渗透测试、漏洞扫描、漏洞检测等；支持按照平台进行分类，包括Windows、Linux、Mac、Android等；支持按照授权分类进行查询。 11. 提供350000+漏洞信息条目；提供常用漏洞的展示、详情查看、下载使用的功能；漏洞数据来自CVE、CNNVD等漏洞库信息；支持按照分类、编号等对漏洞进行查询；支持重置功能。 12. 提供40000+EXP/POC条目；提供可用漏洞Exploit的展示、详情查看、下载使用的功能；支持已验证、有应用等维度进行搜索；支持按照内容、作者、标题、CVE等不同维度进行查询；支持重置功能；EXP库支持DOS、Local、Papers、Remote、Shellcode、WebApps等多种类型的EXP。 13. 提供Google hacker数据库，数量不低于4000个；支持按照关键字、作者等方式查询，支持重置。
4	高性能工作站	1. ★CPU：I9-14900K处理器及以上，主频≥3.2Ghz 2. ★内存：≥128G

		3. ★硬盘≥2TB M.2 NVME SSD+2*4TB 企业级 SATA 硬盘 4. ★显卡：RTX5090 及以上 5. 显示器≥27 英寸 4K 144Hz，分辨率：3840*2160，响应时间：1ms
5	路由器	一、性能规格 1.★支持固化三层千兆光口数量≥2，三层千兆电口数量≥4，二层千兆以太电口数≥24 个，转发性能≥3Mpps 2.支持冗余电源模块（非 RPS 电源），支持万兆以太接口卡 3.可用扩展模块插槽≥4 个（非 SFP 模块插槽），可扩展 TDD/FDD LTE 全制式 4G 模块，E1/CE1 模块、同步/异步串口模块、国密局加密模块等 4.可扩展模块可以热插拔，配置 USB 接口≥1，SD 卡接口≥1 5.为便于设备管理，要求路由器面板提供多功能复原键 ，便于紧急情况的设备状态恢复 二、功能要求 1.支持并实配支持 L2TP、IPSec VPN、GRE VPN、DMVPN 功能，如需购买软件或 License 才能支持该功能特性，则要求必须配置相应软件或 License。 2.支持静态路由、RIPv1/v2、OSPF、BGP4 等路由协议 3.支持 IGMP、PIM-SM、PIM-DM、DVMRP 等组播协议 4.支持流量分析功能，支持状态防火墙功能 5.支持并内置 MPLS VPN、IPv6 等组网功能 6.支持 web 管理界面、TR-069 网管协议、SNMP v1/v2c/v3 网管协议 三、配置要求 1.配置 1 个 2 端口端口模块和 1 根串口线缆
6	接入交换机	一、性能规格 1.★交换容量交换容量≥672Gbps ，转发性能≥156Mpps，固化 10/100/1000M 以太网端口≥24，固化 10G/1G SFP+光接口≥4 个 2.整机采用绿色环保设计，非 POE 最大功耗≤40W 3.要求所投产品端口浪涌抗扰度≥10KV（即具备 10KV 的防雷能力） 二、功能要求 1.支持静态路由、RIP/RIPng、OSPFv2/OSPFv3 等三层路由协议 2.支持虚拟路由器冗余协议（VRRP），有效保障网络稳定 3.要求所投设备支持 1 对 1、1 对多、多对 1 和基于流的镜像；且支持 RSPAN 和 ERSPAN 4.支持虚拟路由器冗余协议（VRRP），有效保障网络稳定 5.支持专门针对 CPU 保护机制功能，可将送 CPU 的报文，如 ARP 报文的速率进行限制，使 CPU 的使用率降低到 15%以内，保障 CPU 的安全 6.支持专门基础网络保护机制功能，支持多种类型的防护，如 ARP 防护，当 ARP 速率超过攻击水线，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 7.支持虚拟化功能，可将多台物理设备虚拟化为一台逻辑设备统一管理 三、配置要求 1.配置 1 个 70W 交流电源模块
7	组网交换机	1.★接口：48 个 10/100/1000Base-T 以太网端口，4 个万兆 SFP+ 2.电源：交流或直流供电，支持冗余电源 3.背板带宽：598Gbps/5.98Tbps 4.包转发率：252Mpps

二、功能要求

2.1 系统功能性要求

系统整体验收包括工业互联网安全控制终端、工业互联网安全实训资源库管理终端、工业互联网安全实训知识库管理终端、高性能工作站、组网交换机各一台，路由器和接入交换机各三台。

2.1.1 工业互联网安全实训控制终端

（1）课程训练

课程页面可分为课程过滤、学习内容，学习内容部分展示了当前匹配到的所有课程，课程过滤功能可帮助用户快速定位到需要学习的课程。

课程搜索：可通过页面方向、难度选项卡过滤课程，提供多条件组合过滤功能；也能通过右侧搜索框键输入课程名或关键字搜索，支持不完全匹配；

学习内容：展示当前匹配到的所有课程，每个课程下方显示了该课程包含的课时数和预计学习时间；

留言功能：课程支持留言功能，学员可以进行评论留言，并可以对他人留言进行回复；

笔记功能：课程支持笔记功能，学员可以记录笔记，笔记支持附件上传；

实验报告功能：实验课时支持实验报告功能，学员可以针对实验课时提交实验报告，讲师在后台可以查看和批阅学生的实验报告，另外实验报告可进行拖拽放置在页面任意位置。

（2）攻防实训

练习模块包含理论题、实操题两个子功能模块

理论题：包含不同方向的网络安全理论知识，题目样式为单选、多选、判断、填空、简答类型。可以通过自由练习或者组卷的方式进行练习，适用于对相关理论知识的练习和考察。

实操题：以操作题为主，有动态答题环境和静态答题环境，需用户接入标靶，最终将得到的 flag 答案填入，获得分值。

（3）个人中心

个人中心信息包括：岗位简介/岗位评估、我的职业、我的日程、能力评估、我的资源、公告信息以及课程训练等。

资源统计：统计该用户的场景数、虚拟机数量、容器数量、Dynamips 数量和实装设备数量；

岗位选择：根据用户需求选择不同职业岗位，并变更当前岗位；

岗位评估：针对已选择的岗位，可以对岗位进行评估，展示用户的基本信息包含姓名、组织、岗位职责匹配度、岗位角色和岗位角色描述。同时展示岗位职责清单：包括岗位职责、知识点和技能点，以及知识体系清单和岗位课程学习记录；

我的职业：包括当前职业中所包含的岗位职责、知识点、技能点以及课程学习、技能训练等信息；

我的日程：日程规划可以查看用户的课程表等信息，展示学员近期的课程安排；

能力评估：根据 NICE/RTKS 人才评价体系评估，展示个人技能六维图；

课程训练：课程训练包括我的提问、我的回复、我的笔记、我的收藏，学习统计和我的学习任务。学习统计包含岗位学习进度和学习总览。

（4）单兵训练

为用户提供信息安全作战的个人技能训练功能，用户可以自由的进行单人作战训练。训练场景包含训练说明，任务列表，训练记录，训练说明详细展示基本信息和前置技能，任务列表以矩阵形式实时显示提交状态，训练记录包含提交时间、时长、完成情况和得

分。

（5）团队训练

团队训练模块主要为用户提供系统性团队训练。提供训练模板，教员可编排拓扑、人员、任务，并设定难度、时长、目标和前置技能。支持模板授权、角色分配、任务模板导入和阶段管理。管理员可进行团队训练的基础信息编排、拓扑编排、任务编排， 学员可自主启动/删除训练场景。支持按个人、组织进行团队训练得分排名；统计各参训人员训练次数、提交任务数、任务正确率、任务得分、综合排名。

（6）平台基础功能

包括仪表盘、统计分析、课程管理、题库管理、综合训练、资源管理、靶标管理、拓扑管理、流量管理、探针管理、任务方法、职业框架、系统管理、系统运维等模块。

2.1.2 工业互联网安全实训资源库管理终端

1. 提供工业控制基础、工业控制系统安全、工控政策标准解读、工控安全攻防、工控安全技术、工控系统网络安全、工业网络基础、工业安全管理体系、工控网络安全意识等课程资源，包括理论课、实验课所需的配套文档及母本资源。
2. 支持理论基础、夺旗练习两类练习方式。
3. 理论题库≥3000 个，覆盖移动安全、接入安全、主机安全、网络安全、办公安全、应用安全、数据库安全、云安全、密码学、法律法规、安全防护、安全运维、工控安全等网络安全理论知识。
4. 夺旗 CTF 题目数量≥280 个，覆盖密码学 Crypto、逆向 Re、二进制漏洞挖掘与利用 Pwn、杂项 Misc、移动 Mobile、Web、工控安全等，并提供全套解题思路。

2.1.3 工业互联网安全实训知识库管理终端

1. 提供不少于 250 个靶标镜像，包括：操作系统靶标，应用系统靶标，网络设备靶标，安全设备靶标，工控设备靶标。
2. 工控设备靶标（施耐德、西门子、罗克韦尔、菲尼克斯、三菱、倍福等至少 6 家 PLC 仿真能力）。
3. 具备 Wincc、iFix、Intouch、Kingview、KingSCADA、Vijeo Citect、ForceControl、FCPower、RealInfo、MCGS 等至少 10 种组态软件的仿真镜像资源，模拟操作员站节点。
4. 具备 TIA Portal、STEP7、UnityPro、SoMachine、Studio5000、CCW、PME、TwinCAT 等至少 8 种编程软件的仿真镜像资源，模拟工程师站节点。
5. 具备 InoTouch Editor、McgsPro、HT8001CN、NaTouch、NaView、DopSoft、FvDesigner 等至少 7 种 HMI 编程软件的仿真镜像资源，模拟 HMI 编程组态节点。
6. 具备 KEPServer 数据采集仿真镜像资源，构建典型的 OPCServer 节点。
7. 提供不少于 6 个工控安全场景，模式覆盖单兵训练、团队训练，包含且不限于风力发电、水力发电、火力发电、石油管网、智能制造、轨道交通等纯虚拟化工业控制系统业务场景，配备全套场景说明、网络拓扑、训练任务、场景流量、数据探针、训练手册等。
8. 提供 10 种数据采集探针，至少包含信息类、日志类、事件类等。
9. 系统提供自研背景流量和攻击流量库，至少包含基础网络流量、应用软件流量、WEB 攻击、远程溢出攻击、DDOS 等多种类型的流量和攻击方式，数量不低于 100 个。支持自定义修改。
10. 提供不少于 500 个攻防工具；支持用户搜索、查看和下载工具；工具类型包括：权限维持、加密解密、漏洞利用、隐写取证、信息探测、逆向分析、网络扫描、漏洞管理、WAF、渗透测试、漏洞扫描、漏洞检测等；支持按照平台进行分类，包括 Windows、Linux、Mac、Android 等；支持按照授权分类进行查询。

11. 提供 350000+漏洞信息条目；提供常用漏洞的展示、详情查看、下载使用的功能；漏洞数据来自 CVE、CNNVD 等漏洞库信息；支持按照分类、编号等对漏洞进行查询；支持重置功能。
12. 提供 40000+EXP/POC 条目；提供可用漏洞 Exploit 的展示、详情查看、下载使用的功能；支持已验证、有应用等维度进行搜索；支持按照内容、作者、标题、CVE 等不同维度进行查询；支持重置功能；EXP 库支持 DOS、Local、Papers、Remote、Shellcode、WebApps 等多种类型的 EXP。
13. 提供 Google hacker 数据库，数量不低于 4000 个；支持按照关键字、作者等方式查询，支持重置。

2.2 系统非功能性要求

要求：系统需采用 B/S 架构和云原生部署（K8S 管理容器化应用），实现前后端分离和微服务扩展。为保证用户体验，系统支持并发访问 50 用户。系统兼容主流浏览器（Chrome、Edge 等），确保在不同浏览器内核下功能展示和操作流畅性一致。服务器端保证在不同操作系统下的稳定性和兼容性，支持部署和运行。