### 附件四

**湄洲湾职业技术学院**

**采购实施计划**

|  |  |
| --- | --- |
| **项目编号：** |  |
| **项目名称：** | **信息安全技术专业教学平台与实验实训设备采购与服务** |
| **实训室名称：** | **信息安全综合实训室** |
| **申报单位：** | **信息工程系** |
| **预算金额（万元）：** | **210** |
| **项目负责人：** | **朱敏** |
| **联系电话：** | **13859880561** |
| **填报日期：** | **2023.11** |

**编制说明**

1. 申购单位负责根据采购需求书编制采购实施计划。
2. 后勤管理处负责指导申购单位填写“合同订立安排”部分内容。
3. 公共实训管理中心负责指导申购单位填写“合同管理安排”部分内容。

四、编制的采购实施计划应当符合《财政部关于印发政府采购需求管理办法的通知》（财库〔2021〕22号）要求及政府采购的相关规定。

五、斜体字部分属于提醒内容，编制时应删除。

六、对不适用的内容应删除，并调整相应序号。

## 一、合同订立安排

**（一）项目采购预算**

1.项目采购预算：（币种）贰佰壹拾万元，2100000元

2.项目最高限价：（币种）贰佰壹拾万元，2100000元

**（二）开展采购活动的时间安排**

|  |  |  |
| --- | --- | --- |
| **序号** | **事项** | **时间安排** |
|  | 政府采购意向公开 | **2024.7** |
|  | 政府采购计划申报 | **2024.7** |
|  | 办理项目备案（如有） | 无 |
|  | 编制采购/招标文件 | **2024.8** |
|  | 发布采购/招标公告 | **2024.8** |
|  | 项目评审/开标、评标 | **2024.8** |
|  | 发布成交/中标公告 | **2024.9** |
|  | 签订采购合同 | **2024.9** |

**（三）采购组织形式和委托代理安排**

1.采购组织形式

□自行采购

☑委托代理公司采购

2.委托代理安排：委托代理采购

3.采购信息发布媒体（可多选）：

☑湄洲湾职业技术学院后勤通告主页

□中国政府采购网

□福建省公共资源交易中心网站

□其他：

**（四）采购包划分与合同分包**

标包一：

标包二：

……

**（五）供应商资格条件**

1.基本要求：

满足《中华人民共和国政府采购法》第二十二条规定

2.特定资格要求：

3.落实政府采购政策的要求：政府强制采购节能产品、支持创新、绿色发展、鼓励环保产品、扶持福利企业、促进残疾人就业、促进中小企业发展、支持监狱和戒毒企业等。

**（六）采购方式**

**☑公开招标（适用法定情形）**

☑达到国家公开招标限额标准的采购项目；

□采购需求客观、明确且规格、标准统一的采购项目，如通用设备、物业管理等；

□采购需求客观、明确，且技术较复杂或者专业性较强的采购项目，如大型装备、咨询服务等。

**□竞争性磋商（符合情形）**

□政府购买服务项目；

□技术复杂或者性质特殊，不能确定详细规格或者具体要求的；

□因艺术品采购、专利、专有技术或者服务的时间、数量事先不能确定等原因不能事先计算出价格总额的；

□市场竞争不充分的科研项目，以及需要扶持的科技成果转化项目；

□按照招标投标法及其实施条例必须进行招标的工程建设项目以外的工程建设项目。

**□竞争性谈判（适用情形）**

□采购需求客观、明确，且技术较复杂或者专业性较强的采购项目，如大型装备、咨询服务等；

□不能完全确定客观指标，需由供应商提供设计方案、解决方案或者组织方案的采购项目，如首购订购、设计服务、政府和社会资本合作等。

**□单一来源（适用情形）**

□只能从唯一供应商处采购的；

□发生了不可预见的紧急情况不能从其他供应商处采购的；

□必须保证原有采购项目一致性或者服务配套的要求，需要继续从原供应商处添购，且添购资金总额不超过原合同采购金额百分之十的。

**□询价（适用情形）：**采购需求客观、明确且规格、标准统一如通用设备、物业管理等。

**□核准：**达到公开招标数额标准，因特殊情况需要采用公开招标以外采购方式，已依法获得批准。

**（七）竞争范围**

☑公开邀请

□有限邀请（随机抽取或书面推荐）

□唯一供应商采购

**（八）评审规则**

☑综合评分法*（选择此评审方法原因）*

□最低评标价法*（选择此评审方法原因）*

（附件1 评审规则）

## 二、合同管理安排

**（一）合同类型**

按照民法典第九章规定的典型合同。

☑买卖合同

□供用电、水、气、热力合同

□租赁合同

□建设工程合同

□技术合同

□委托合同

□物业服务合同

**（二）定价方式**

□固定总价

□固定单价

□成本补偿

□绩效激励

☑多种方式组合定价

**（三）合同范本**

☑设备(软件)购销合同（内贸）

□家具(实验台)制作安装购销合同

□校医院药品和试剂耗材采购合同

□进口设备购置合同

□服务合同

□建设工程合同

□设备采购及安装合同

□维修改造合同

□信息化建设银校合作项目合同

**（五）风险管控措施**

1.主要风险因素的识别

（1）国家政策变化风险

☑有□无

（2）实施环境变化风险

☑有□无

（3）重大技术变化风险

☑有□无

（4）预算项目调整风险

☑有□无

（5）质疑投诉影响采购进度风险

☑有□无

（6）采购失败风险、不按规定签订或者履行合同风险

☑有□无

（7）损害国家利益和社会公共利益的风险等

☑有□无

2.存在风险事项的处置措施（根据风险情况选择）

（1）国家政策变化风险处置措施

（2）实施环境变化风险处置措施

（3）重大技术变化风险处置措施

（4）预算项目调整风险处置措施

（5）质疑投诉影响采购进度风险处置措施

（6）采购失败风险、不按规定签订或者履行合同风险处置措施

（7）损害国家利益和社会公共利益的风险处置措施

# 附件1 评审规则

1. **评标方法：** *综合评分法。*
2. **评标标准**

（1）*投标文件满足招标文件全部实质性要求且按照评审因素的量化指标评审得分最高的供应商为中标候选人。*

（2）每个投标人的评标总得分FA＝F1×A1＋F2×A2＋F3×A3＋F4×A4（若有），其中：F1指价格项评审因素得分、F2指技术项评审因素得分、F3指商务项评审因素得分，A1指价格项评审因素所占的权重、A2指技术项评审因素所占的权重、A3指商务项评审因素所占的权重，A1+A2+A3=1、F1×A1＋F2×A2＋F3×A3=100分（满分时），F4×A4为加分项（即优先类节能产品、环境标志产品在采购活动中可享有的加分优惠）。

（3）各项评审因素的设置如下：

**①价格项（F1×A1）满分为*20.00*分。**

投标报价得分=（评标基准价／投标报价）×100。因落实政府采购政策需进行价格扣除的，以扣除后的价格计算评标基准价和投标报价。

b.价格扣除的规则如下：

|  |  |
| --- | --- |
| 评标项目 | 评标方法 |
| 小型、微型企业，监狱企业，残疾人 | **1、对小型、微型企业产品（限货物）的价格给予*XX%*的扣除。 2、对监狱企业产品（限货物）的价格给予*XX%*的扣除。 3、残疾人福利性单位提供本单位制造的货物、承担的工程或服务，或提供其他残疾人福利性单位制造的货物（不包括使用非残疾人福利性单位注册商标的货物），对相应货物、工程或服务的价格给予*XX%*的扣除。3、对于节能产品、环境标志产品的价格给予*XX%*的扣除。** |

**②技术项（F2×A2）满分为70.00分。**

|  |  |  |
| --- | --- | --- |
| 评标项目 | 评标分值 | 评标方法描述 |
| 投标技术响应情况 | 46.00 | 根据技术要求中的各项要求的响应情况，由评委进行评分。 ①技术和服务要求中标注“★”号的若有负偏离以无效投标处理；②带“▲”号的参数为重要参数，每负偏离一项扣3分； ③其他非“★”“▲”号的参数的为普通技术参数，每负偏离一项扣1分，直至此项分值扣完为止，正偏离不加分。注：要求提供佐证材料证明必须提供，材料提供不全或者未提供者，视为负偏离。 |
| 现场演示 | 21.00 | 针对（教学竞赛靶场平台）以下7项演示内容进行演示，完全满足技术参数要求的得 21分。  1.场景创建时支持以图形化拖拽的方式绘制场景拓扑，拓扑元素包含虚拟终端、虚拟网络设备、虚拟安全设备，虚拟网络设备至少包含虚拟交换机、虚拟路由器，虚拟安全设备至少包含数据库审计、日志审计、APT攻击预警、主机安全、Web应用防火墙、堡垒机等，同时支持对拓扑中元素的属性进行配置；以上内容需全部现场演示，符合要求的得3分，未提供演示或演示不符合要求的不得分。  2.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；以上内容需全部现场演示，符合要求的得3分，未提供演示或演示不符合要求的不得分。  3.动态试卷支持以规则的形式保存试卷，当考试使用时，每个人进入考试都会根据动态试卷规则生成全新试卷；试卷规则支持依据题目类型、标签、难度等维度进行配置，每条规则支持设置对应题目的数量和分数，每张试卷支持配置多条规则，根据规则进行组卷；以上内容需全部现场演示，符合要求的得3分，未提供演示或演示不符合要求的不得分。  4.支持混合竞赛模式，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。赛制支持夺旗赛、定向渗透赛、攻防对抗赛、领地争夺赛、理论赛五种类型。以上内容需全部现场演示，符合要求的得3分，未提供演示或演示不符合要求的不得分。  5.提供不少于5个APT及其他攻击事件应急研究场景，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；以上内容需全部现场演示，符合要求的得3分，未提供演示或演示不符合要求的不得分。  6.提供APT组织场景演示，APT组织场景要求2层及以上的网络拓扑结构，至少具备5个有效靶标，场景中至少涵盖Tomcat相关漏洞、Docker逃逸相关漏洞、Gitlab相关漏洞及其他重点漏洞，场景中总计涵盖不少于10种攻防手段，需包含目录扫描、漏洞利用、Docker逃逸、内网穿透、内网横向渗透、密码破解、浏览器密码获取等手段，场景包含域环境及相关攻防手段；以上内容需全部现场演示，符合要求的得3分，未提供演示或演示不符合要求的不得分。  7.提供不少于10个行业应用案例研究场景，场景至少应当包括APT攻防场景、钓鱼网站场景、2个及不同类型电信诈骗网站信息收集等场景（每个场景不少于6个步骤）；以上内容需全部现场演示，符合要求的得3分，未提供演示或演示不符合要求的不得分。 |
| 项目实施方案 | 3.00 | 根据投标人的组织计划、进度安排方案进行评价,方案详细完整、合理可行的得3分，方案较详细具体，虽有缺漏，但不怎么影响项目预期效果的得2分，存在缺漏，但基本满足项目实施需要的得1分，其他不得分。 |

**③商务项（F3×A3）满分为*10.00*分。**

|  |  |  |
| --- | --- | --- |
| 评标项目 | 评标分值 | 评标方法描述 |
| **综合实力1** | **3.00** | **为了保障本次产品成熟度，要求投标人或所投产品制造商具备以下资质：**  **（1）CMMI能力成熟度模型集成五级资质；**  **（2）公安部认可的信息安全等级保护检查工具箱研发单位；**  **（3）中国信息安全测评中心授予的《国家信息安全测评信息安全服务资质证书（安全工程类三级）》；**  **以上资质全部满足得3分，每提供一个得1分，需提供相关证明材料并加盖投标人公章。** |
| **综合实力2** | **3.00** | **为了保障本次产品成熟度，要求投标人或所投产品制造商为标准起草单位之一：**  **（1）《信息安全技术 WEB应用安全扫描产品安全技术要求》（GA/T 1107-2013）；**  **（2）《信息安全技术 网络型流量控制产品安全技术要求》（GA/T 1454-2018）；**  **（3）《信息安全技术 WEB应用安全检测系统安全技术要求和测试评价方法》（GB/T 37931-2019）。**  **每参与一份标准起草单位之一的得1分，全部满分得3分，提供相关证明材料并加盖投标人公章。** |
| **综合实力3** | **2.00** | **为了保障本次产品成熟度，要求投标人或所投产品制造商为：**  **（1）CNVD国家信息安全漏洞共享平台支撑单位(技术组）；**  **（2）CNVD2022年度漏洞信息报送贡献单位；**  **（3）CNVD2022年度原创漏洞发现突出贡献单位；**  **（4）CNVD2022年度最具价值漏洞报送单位；**  **以上四项同时满足得2分，每满足一项得0.5分，需提供相关证明材料并加盖投标人公章。** |
| **履约能力** | **1.00** | **为保障项目的顺利实施，投标人需配备专业的技术服务人员，每提供1名具有PMP证书的专业技术服务人员，得0.5分，最高得1分； (提供PMP证书复印件，并提供投标人近6个月内任一个月为其缴纳的社保证明) 不提供不得分。** |
| **售后服务方案** | **1.00** | **投标人提供售后服务方案，售后服务方案中有详细的在产品发生不同类型故障后的到达现场时间、解决故障时间、补救措施等方面的措施或方案，同时具有明确的承诺且符合实际需求，提供详细的售后服务方案及售后服务承诺等。售后服务方案充实详细、有质量保证承诺，具体可行得1分；售后服务方案基本可行得0.5分；售后服务方案欠缺或不提供售后服务方案不得分，满分1分。** |

# 技术参数

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **序号** | **名称** | **技术参数及功能要求** | **数量** | **单位** | **备注** |
| 1 | 教学竞赛靶场物理机 | 1.硬件外形：2U标准机架式设备；  2.电源：1+1冗余电源；  3.CPU：≥2\*16核 64线程  4.内存：≥256G  5.硬盘容量：≥4T\*4，可用空间不小于7T  6.固态盘：≥960G SSD\*2  7.Raid卡：≥4GB SAS 12Gb 8口RAID卡  8.电口：≥千兆网口 \*4  9.光口：≥万兆光口\*2（带多模光模块）  10.安装：带滑轨  ★11. 用于运行教学竞赛靶场的资源，需满足教学竞赛靶场平台并发量需求。 | 6 | 台 |  |
| 2 | 交换机 | 1. ≥24+4口交换机：  2. ≥24个10/100/1000Base-T以太网端口；  3. ≥4个千兆光；  4. 传输速率≥51Mpps/126Mpps | 4 | 台 |  |
| 3 | 运维审计与风险控制系统 | 1.硬件规格：1U 性能：标配资产数(个) ≥100；并发字符连接最大数≥100个,并发图形连接最大数≥20个；网口≥6\*GE电口 其他自带接口≥2\*USB接口，1\*RJ45串口 磁盘≥1T 电源（标配）：单电源  2.支持按部门组织架构（至少5个层级的部门）管理用户数据、资产数据、授权数据、审计数据；  3.支持手机APP动态口令认证方式登录堡垒机，且新用户首次登录后需强制绑定APP动态口令；  4.基于不同的用户设置不同的双因子认证模式，如user1用动态令牌、user2用USBkey、user3手机APP动态口令认证；  5.可以设置用户密码的长度、复杂度、相关度，其中相关度可以设置密码与用户名的关系，可以选择是否检查历史密码。并可支持密码过期前告警；  6.支持自动收集设备IP、运维协议、端口号、账号、密码、与用户的权限关系，甚至可自动完成授权；  7.支持对主机联通性、账号有效性进行周期性检测。并可设置是否开启检测连通性、有效性功能；  8.支持使用本地的WinSCP/FlashFXP/SecureFX等客户端工具登录堡垒机访问SFTP/FTP设备；  9.支持批量登录字符设备功能：能自动生成SecurCRT/XShell工具的批量登录文件，实现在工具中批量自动登录多台设备；  10.支持审计主流数据库（如DB2、Oracle、MySQL、SQL Server）运维中的SQL语句，可进行关键信息定位查询。 | 2 | 台 |  |
| 4 | Web应用防火墙 | 1.标准1U机架式，CPU≥4核\*1，内存≥8G，硬盘≥2T\*1，电源：单电源，网络接口：千兆电口≥4个（支持2对电口BYPASS），管理接口：千兆电口≥1个，Console串口≥1个，USB接口≥2个；HTTP应用层吞吐量≥500Mbps,HTTP最大新建数≥4000个,HTTP最大并发数≥30000个；  2.支持透明串接和旁路反向代理下的HTTPS业务的安全防护；  3.支持自动发现网络环境中存在的Web业务系统，记录服务器的IP、Port、域名等信息；  4.支持HTTPS站点SSL算法自动探测功能。探测时可以设置指定站点及端口，可以显示探测结果；  5.支持对HTTP请求关键字段进行合规性的检测（包括Host字段、User-Agent、Content-type字段等）；  6.支持对HTTP头部各字段内容长度进行限制并可以自定义调整限制大小，包括参数名长度、参数值长度、HTTP请求头部长度、URL长度、Cookie长度、User-Agent长度、Content-type长度、Host长度等；  7.内置身份证、银行卡、手机号、社保号等个人敏感信息数据，对服务器返回的敏感个人信息数据通过星号进行隐藏，并支持用户自定义敏感词；  8.支持客户端安全防护，插入特殊的HTTP报头以保护客户端免受某些攻击包括但不限于增加以下安全报头：X-Frame-Options（用于防护客户端免受Clickjacking攻击）、X-Content-Type-Options（以防止浏览器将文件解释为内容类型声明以外的其他内容）、X-XSS-Protect（用于当检测到XSS攻击时，指示浏览器停止加载页面）、Content-Security-Policy（用于降低浏览器上的XSS风险和数据注入攻击）  （须提供带有国家认可的检验检测机构出具的检测报告CMA标识或CNAS标识或ilac-MRA标识，及  盖有检测专用章的检验（检测报告）佐证，同时为确保功能成熟稳定，检测时间必须在该项目发标前。）；  9.支持设定机器学习的周期，域名信息，可信任的客户端IP，不可信的客户端IP以及不学习的URL信息；  10.支持根据细粒度条件对CC攻击进行检测和防护；匹配条件由URL参数、请求头部字段、目的IP、请求方法、地理位置组成；测量指标由请求速率、请求集中度、请求离散度组成；客户端检测对象由IP、IP+URL、IP+User\_Agent等参数组成；支持从请求头字段获取真实源IP地址；（须提供带有国家认可的检验检测机构出具的检测报告CMA标识或CNAS标识或ilac-MRA标识，及盖有检测专用章的检验（检测报告）佐证，同时为确保功能成熟稳定，检测时间必须在该项目发标前。）；  11.根据产生的安全日志进行智能分析，提高人工分析效率，减小规则误判概率。 | 2 | 台 |  |
| 5 | 安全网关 | 1.1U机架式，CPU≥4核，内存≥4GB，电源规格：单电源。网络接口：千兆电口≥8个(含1组电口Bypass），千兆光口≥4个，不带光模块，整机吞吐≥1Gbps,最大并发数≥50万,最大新建数≥2万/秒；  2.支持基于时间段的SNAT、DNAT规则；SNAT转换地址池支持黑洞路由，支持SNAT的源端口不转换模式；DNAT-双向NAT模式支持基于地址池的源转换方式，DNAT的健康探测支持的协议TCP和ICMP；NAT66支持前缀转换方式；  3.系统预定义超过11000条主流攻击规则，包含对应IPS规则的级别、防护对象、操作系统、CVE编号等详细信息；（须提供带有国家认可的检验检测机构出具的检测报告CMA标识或CNAS标识或ilac-MRA标识，及盖有检测专用章的检验（检测报告）佐证，同时为确保功能成熟稳定，检测时间必须在该项目发标前。）；  4.支持独立的Web防护模块，系统定义超过4500条WAF规则防护功能，支持常规HTTP漏洞、SQL注入、组件、CMS、WebShell和XSS等类型的Web防护；支持HTTP协议的URL、Method、Referer、User-Agent、Cookie、URL-args等字段的等于、不等于、包含、不包含、正则等多种匹配方式的访问控制；  5.支持HTTP、FTP、POP3、SMTP、IMAP协议的110多种预定义文件类型过滤，支持上传下载的方向选择；并支持自定义文件类型过滤；  6.安全模式支持智能模式和普通模式。在普通模式下，安全引擎处理网络报文遇到资源不足时会将报文直接丢弃，会影响网络转发；在智能模式下，安全引擎将尽可能的处理网络报文，但不影响网络转发；  7.支持基于源IP地址、目的IP地址、端口、协议的黑名单配置，支持自定义黑名单生效时间；   1. 支持SSL加密流量解密功能，支持HTTPS、SMTPS、POPS、IMAPS协议加密的流量解密，支持HTTPS流量按域名分类做流量解密。并支持上层内容安全功能查杀和访问控制，如入侵防御，内容过滤等；   9.提供对控制策略、上网认证策略、带宽策略、策略路由、源NAT等策略的策略分析，可分析并展示问题策略数量以及所占百分比、问题策略详情、策略宽松度分布情况，简化运维工作； | 2 | 台 |  |
| 6 | 主机安全及管理系统 | 1.纯软件产品，建议部署要求：CPU核数≥4核、内存≥8GB、可用磁盘空间≥500GB；  2.支持对CPU、内存、磁盘读写、网络上下行流量达到配置阈值时告警。支持对CPU、内存达到一定阈值时客户端进行熔断；  3.支持对本机的扩展行为（信息收集、权限提升）进行监测，防止提权行为和信息泄露；  4.对失陷后主机远控持久化行为进行检测（反弹Shell、远程控制），可阻断远控；  5.对内网的恶意攻击行为进行识别（漏洞利用、横向移动），可阻断恶意探测行为；  6.支持防端口扫描，锁定恶意的端口扫描，并记录告警；  7.违规外联支持黑、白名单双模式，白名单模式可配置是否允许访问特定的网站和地址；黑名单模式可自定义恶意IP，支持黑名单告警和阻断；  8.内核级防火墙（业务间流量东西向隔离）功能，包括IP、端口、协议、流向等细粒度权限控制；  9.支持登录防护，包括以系统账号为粒度的异常登录防护、支持五个任意维度(任意地理位置，任意IP，任意域名，任意计算机名，任意时间)的系统登录访问策略设置；  10.管理中心可作为补丁服务器，支持管理中心可上网和不可上网2种情况。提供离线补丁下载器，按需智能获取内网所需补丁；  11.支持扫描的漏洞类型包括但不限于操作系统漏洞（Windows、Linux等）、数据库漏洞（MySQL等）、Web容器漏洞（Tomcat、Apache、Ngnix等）、其他组件漏洞。 | 2 | 台 |  |
| 7 | APT攻击预警平台 | 1.1U标准机架式设备,电源：单电源 内存：8G 硬盘容量≥2T\*1 接口数量≥6个 接口类型：千兆RJ45网口≥2(管理口≥2)、千兆RJ45网口≥4，整机吞吐量≥500Mbps；  2.支持旁路部署和分布式部署，对探测器可以添加、删除，显示探测器版本、状态和IP，管理中心可实现告警统一管理；可自定义管理中心和探测器之间的数据传输速率、时间、发送目录等参数；  3.管理中心支持自动同步版本、策略及排错平台升级包到探测器设备；  4.支持IPv4和IPv6网络环境下的部署，可同时对IPv4和IPv6网络流量分析检测；  5.支持风险数据包保存功能，以帮助用户还原攻击过程，进行取证和关联分析；并支持系统内置Wireshark组件预览风险数据包；  6.导航：支持大屏展示网络攻击态势，包括攻击地图、紧急事件数/总数、恶意文件数/扫描总数、风险趋势（高、中、低风险）、流量分析（吞吐量、HTTP流量、DNS流量）、高危风险类别排名、攻击源区域排名、紧急事件/高危事件，并支持全球地图、中国地图切换展示；  7.支持检测Web攻击、恶意文件攻击、远程控制、Web后门访问、行为分析、非法数据、DGA域名请求、SMB远程溢出攻击、弱口令、拒绝服务攻击、隧道通信、暴力破解、挖矿、恶意工具利用、扫描行为、漏洞利用、邮件社工攻击、ARP欺骗、密码明文形式传输等；  8.支持文件白名单、发件人邮箱白名单、发件人域名白名单、黑域名白名单、黑IP白名单、域名白名单、客户端IP白名单、服务端IP白名单、WEB特征风险白名单、IDS规则白名单的配置；  9.支持自定义HTTP登录行为的用户名获取来源，支持状态码和返回内容的自定义配置以判定登录状态；  10.可显示文件运行过程中企图访问的IP、域名，以及域名及对应的IP；  11.支持沙箱逃逸检测，当恶意文件进行逃逸尝试，在沙箱报告中进行体现；  12.支持一键登录排错平台，对系统进行深度配置和排错，支持一键检测故障、配置核对、表分区检查、表检测、信息收集等功能。 | 2 | 台 |  |
| 8 | 综合日志审计平台 | 1.标准1U硬件；CPU≥4核4线程/2.0GHZ 2MB，内存≥8G ，硬盘≥2T\*1 ，电源：单电源，网口≥6个千兆工作管理口(1管理口+1HA口+4审计口) , ≥1个console口；  2.采用解决方案包上传对产品进行功能扩展，无需要代码开发；  3.支持Kafka日志接收转发、大数据安全域同步、APT沙箱报告转发等大数据联调功能；  4.支持手动或按周期自动备份系统配置，可随时对系统资产等配置进行还原操作，且自动备份周期与备份包个数可配；支持系统配置备份自动备份至远程服务器；  5.支持常见的虚拟机环境日志收集，包括Xen、VMWare、Hyper-V等；  6.内置5000+解析规则，支持对收集的5000+设备类型日志进行解析（标准化、归一化），解析维度多达200+，解析规则可以根据客户要求定制扩展；  7.支持美观易用的思维导图模式的解析规则界面自定义；  **▲**8.三维关联分析；支持通过资产、安全知识库、弱点库三个维度分析事件是否存在威胁，并形成关联事件；（须提供带有国家认可的检验检测机构出具的检测报告CMA标识或CNAS标识或ilac-MRA标识，及盖有检测专用章的检验（检测报告）佐证，同时为确保功能成熟稳定，检测时间必须在该项目发标前。）  9.支持日志备份自动传送到远程服务器；  10.支持亿级的日志里根据做任意的关键字及其它的检索条件，在秒级里返回查询结果；  **▲**11.通过在目标主机上安装Agent程序，支持监测目标主机的CPU利用率、内存使用率、磁盘使用率、磁盘使用情况、流量等信息；（须提供带有国家认可的检验检测机构出具的检测报告CMA标识或CNAS标识或ilac-MRA标识，及盖有检测专用章的检验（检测报告）佐证，同时为确保功能成熟稳定，检测时间必须在该项目发标前。）  12.资产拓扑支持按照实际的用户环境进行编辑发布并可以和资产进行绑定，拓扑可以显示资产采集的事件数量被采集资产的状态等信息；择同步日志范围，按需转发数据。（须提供带有国家认可的检验检测机构出具的检测报告CMA标识或CNAS标识或ilac-MRA标识，及盖有检测专用章的检验（检测报告）佐证，同时为确保功能成熟稳定，检测时间必须在该项目发标前。） | 2 | 台 |  |
| 9 | 数据库审计与风险控制系统 | 1.1U机架式；CPU≥4核4线程\*1；内存≥8GB；硬盘≥2TB\*1；内置单电源； ≥2个千兆电口管理口；≥6个千兆业务电口；整机吞吐≥1Gbps,双向审计数据库流量≥50Mbps,峰值SQL事务处理能力≥4000条/秒,数据库实例数≥2个；  2.支持和ES平台对接，将审计日志和告警日志存储在ES系统中，并支持通过页面查询日志；  3.支持在审计页面配置审计代理的CPU亲和性、最大CPU使用率、最大内存使用率、CPU使用率阈值、内存使用率阈值、流量接收端口、抓包过滤串；  4.支持在审计页面批量安装、卸载、重新安装审计代理。  5.支持MongoDB、Hbase、Hive、Impala、Elastic Search、HDFS、Canssandra、Greenplum、LibrA、GraphBase、Cache等数据库审计；  6.支持超长SQL语句（最长4M）审计；  7.内置安全特征库不少于900条，如SQL注入、缓冲区溢出等；  8.支持内置安全规则单独升级；（须提供带有国家认可的检验检测机构出具的检测报告CMA标识或CNAS标识或ilac-MRA标识，及盖有检测专用章的检验（检测报告）佐证，同时为确保功能成熟稳定，检测时间必须在该项目发标前。）  9.支持信任规则，信任规则至少支持18个匹配条件；  10.支持在审计日志中一键添加过滤规则，支持在告警规则中一键添加信任规则和规则白名单；  11.支持管理中心和审计节点手工同步配置信息。 | 2 | 台 |  |
| 10 | 机柜 | 机柜大小600\*600\*800，15U | 2 | 台 |  |
| 11 | 安全运维管理平台 | 一、主要参数  1.硬件外形：2U标准机架式设备；  2.电源：1+1冗余电源；  3.CPU：≥2\*10核 20线程  4.内存：≥128G  5.硬盘容量：≥4T\*4，可用空间不小于7T  6.固态盘：≥960G SSD\*2  7.Raid卡：≥2GB SAS 12Gb 8口RAID卡  8.电口：≥千兆网口 \*4  9.光口：≥万兆光口\*2（带多模光模块）  10.安装：带滑轨  ★11.提供多种真实的组网环境，支持学生进行真实的网络环境搭建、设备连线实操、运维实操等实验内容，需满足教学竞赛靶场平台并发量需求；  12.提供统一的管理平台，对接入设备进行统一管理；  13.提供多种不同行业方向的企业级虚拟化场景，帮助学员掌握对企业网络进行安全设备部署、策略配置调优以及安全检测的能力。  二、智慧融合控制台参数  （1）主板采用工业级高速多核嵌入式CPU，嵌入式融合控制操作系统；  （2）智慧安全融合管理台电源部分：固定220V 10A防脱落智能强电输出插座口≥8路，旁路输出插座≥1路，每路插座接口为新国标五孔插口，每路可扩展独立的无线控制开关，集成电源时序功能。可对每路输出的用电做分析；整机输出功率≥3.5KW，防雷防浪涌。  （3）设备主机已集成智慧电能管理系统，支持电流、电压、功率以及温度的条件限定，实现设备对用电的过流、过压、过载、过温的实时保护，可实时本机查询各端口用电实时数据，实现所有输出线路的用电安全智能化管理。（须提供带有国家认可的检验检测机构出具的检测报告CMA标识或CNAS标识或ilac-MRA标识，及盖有检测专用章的检验（检测报告）佐证，同时为确保功能成熟稳定，检测时间必须在该项目发标前。）  ▲（4）设备集成网络物联部分要求：≥8个10/100/1000M以太网RJ45网络接口、1个SFP插槽、1路独立RJ45（用于485通讯）、1路USB3.0接口（提供该设备以上端口实物照片），可外接空调红外控制模块。可外接温度、湿度的采集模块，可外接智能插座红外遥控器控制；（提供带有国家认可的检验检测机构出具的检测报告CMA标识或CNAS标识或ilac-MRA标识，及盖有检测专用章的检验（检测报告）佐证）  （5）可自定义每路输出电路端口的名称，自动统计、查询和控制各种用电多媒体设备的使用状况及状态。  （6）设备支持TCP/IP集中或远程云平台管理，可以通过手机APP终端或微信进行远程管理和控制输出设备的使用，通过云端智慧安全控制管理平台无缝对接，包括设备的每路电源输出开关控制、用电情况等。  ▲（7）设备带有≥1.5寸LCD或OLED显示屏，屏幕监视工作状态，可显示工作状态，对设备工作情况及负载情况进行精确判断，包括功率、电压、电流、温湿度等状态作出显示。（须提供带有国家认可的检验检测机构出具的检测报告CMA标识或CNAS标识或ilac-MRA标识，及盖有检测专用章的检验（检测报告）佐证，同时为确保功能成熟稳定，检测时间必须在该项目发标前。）  （8）以上技术规格所描述的端口固定集成要求：最新国标电源输出5孔插座口≥9个、千兆RJ45网络接口≥8个、SFP插槽≥1个、USB3.0接口≥1个、RJ45类型的485接口≥1个、RJ45管理口≥1个、1个≥1.5寸的OLED显示屏等须全部集成固定在此设备上，设备为标准19英寸1U机架式安装，大小尺寸≤440MM\*270MM\*45MM。同时上面所提到的每项指标功能要求必须逐条对应满足。 | 1 | 套 |  |
| 12 | Vxlan交换机 | 1.虚实结合交换机，带VXLAN功能；  2.24个10/100/1000BASE-T以太网端口,≥4个万兆SFP+,单子卡槽位,含1个150W交流电源,可拔插双电源，带VXLAN功能。 | 1 | 台 |  |
| 13 | 核心交换机 | 1.24+4口交换机：  2.24个10/100/1000Base-T以太网端口；  3.4个千兆光；  4.传输速率≥51Mpps/126Mpps | 1 | 台 |  |
| 14 | 网络安全等级保护检查工具箱 | 一、产品简介  1.网络安全等级保护检查工具箱是信息系统运营单位开展等级测评工作的一体化专用设备，具有规范检查、工具调用、结果展示等功能。集成定制有专门的安全检查工具，为信息系统运营单位提供了专业检查知识和检查方法，并实现对获取数据的关联分析、统计比对、处理流转等功能，提高等级保护合规检查工作的标准化、规范化和专业化水平。  2.处理器：≥英特尔® 酷睿I7系列；  3.内存：≥16GB；  4.硬盘容量：≥256GSSD+1T机械硬盘；  5.屏幕规格：≥14英寸。  二、产品功能  1.等级保护检查工具箱  （1）检查任务  1）检查可支持大数据安全检查任务类型。持按照大数据安全扩展要求相关指标进行安全检查，支持生成大数据安全检查报告；  2）检查可支持物联网安全检查任务类型。支持按照物联网安全扩展要求相关指标进行安全检查，支持生成物联网安全检查报告；  3）检查可支持移动互联网安全检查任务类型。支持按照移动互联安全扩展要求相关指标进行安全检查，支持生成移动互联安全检查报告；  4）检查内容：支持系统定级情况、岗位设置情况、安全审计情况等检查内容。  5）检查要点：支持检查对象检查内容具体检查指标项进行检查；  6）检查结果录入类型：单项判定：支持判定未检查、不适用、符合、不符合、部分符合；  7）针对每个检查要点应提供相应的检查方法，检查结果判定依据等相关检查知识，以便引导进行现场检查；  8）支持对检查过程中具体检查对象（例如：主机、网络设备等）进行调整功能，要求可以选择已有的检查对象或录入新的检查对象；  9）支持手动填写测评概述，概述内容包括测评目的、测评依据、测评过程，支持手动填写整体测评结果汇总、总体评价等。  （2）数据汇总  1）支持一键导入功能，将检查工具集检测结果自动导入到工具箱；  2）支持手动导入工具检查结果到工具箱及关联任务检查对象。  （3）报表中心  1）支持测评方案的自动生成；  2）导出的检查结果应按照指定的接口规范导出；  3）支持自动生成不同类型检查任务的检查报告，检查报告应包含不符合项的风险描述信息和安全评分；  4）知识库内容应包含检查指标的检查方法、检查结果判定依据和不符合项的风险提示；  5）知识库可以依据网络安全的标准和分析模型，对检查工具的检查结果进行自动分析，给出相应的检查结果记录。  （4）知识库升级维护  1）知识库内容必须覆盖所有检查指标；  2）知识库内容应包含检查指标的检查方法、检查结果判定依据和不符合项的风险提示；  3）知识库可以依据网络安全的标准和分析模型，对检查工具的检查结果进行自动分析，给出相应的检查结果记录。  （5）风险提示  所有检查工具启动时，默认都会进行风险提示，支持通过配置是否下次启用风险提示。  2.系统管理  （1）自定义模板及知识库  1）支持测评模板的自定义，支持新增、删除检查项；支持引用自定义知识库的内容作为检查结果的描述；  2）支持对用户账户进行管理，支持管理员、审计员角色账户增加、口令修改，支持对账户新增、修改、删除；  3）支持对用户账户进行管理，支持管理员、审计员角色账户增加、口令修改，内置角色默认权限。  （2）用户管理  1）支持对用户账户进行管理，支持管理员、审计员角色账户增加、口令修改，支持对账户新增、修改、删除；  2）支持对用户账户进行管理，支持管理员、审计员角色账户增加、口令修改，内置角色默认权限。  3.离线安全检查工具集  （1）Windows病毒木马检查工具  1）支持检查系统中的木马程序、Rootkit、间谍程序等；检查流氓软件、蠕虫病毒、其它恶意程序等；支持快速扫描、全盘扫描、自定义目录扫描；  2）运行环境支持Windows XP及以上Windows系列操作系统和服务器操作系统、UOS等操作系统类型。  4.在线检查工具集  （1）Linux主机安全配置检查工具  1）安全审计检测，支持检查是否对登录进行日志记录，检查是否配置su命令使用情况记录，检查是否记录用户对设备的操作；  2）恶意代码防范检测，支持检查是否安装chkrootkit进行系统监测；  3）访问控制检测，支持检查是否删除了潜在危险文件和与设备运行、维护等工作无关的账号；是否存在空口令账号；检查是否使用PAM认证模块禁止wheel组之外的用户su为root；是否修改SNMP默认团体字；是否设置除root之外UID为0的用户；是否限制FTP用户登录后能访问的目录；  4）入侵防范检测，支持检查是否关闭不必要的服务和端口、数据包转发功能（适用于不做路由功能的系统）、IP伪装和绑定多IP功能；检查是否安装系统补丁。  （2）数据库安全检查工具  1）信创数据库检测，支持国产信创数据库类型，包括达梦、人大金仓、瀚高、优炫、南大通用、神通等；  2）数据库扫描支持的检测类型大于10种，至少包括弱口令、执行权限过大、访问控制漏洞、提权漏洞、缓冲区溢出漏洞、缺省配置、访问权限绕过、PL-SQL注入、危险程序、安全信息查看等；  3）数据库扫描的漏洞库数量大于3000条，提供详细的漏洞描述和对应的解决方案描述；漏洞知识库与CVE、CNNVD等国际、国内漏洞库标准兼容。  （3）网站安全检测工具  1）产品提供Web应用漏洞扫描功能，支持对Discuz、大汉CMS、PHPCMS、DEDECMS、ECSHOP、WordPress、eWebEditor、FCKeditor、Struts2等国内外常见第三方组件进行扫描；  2）检查对象支持，支持WEB 2.0，支持各类JavaScript脚本解析；  3）动态页面检测，支持JSP、PHP、ASP、.NET等类型动态页面；  4）支持前后端分离的网站类型扫描；  5）支持常见Web漏洞类型的扫描，包括SQL注入、跨站脚本、命令执行、命令注入、代码注入、弱口令、目录遍历、URL跳转、文件包含、反序列化漏洞、文件上传、CSRF跨站请求伪造、信息泄露等。支持OWASP TOP10等主流安全漏洞；  6）漏洞特征库大于12000条，漏洞评分支持CVSS3.0标准；  7）提供当前域、整个域、当前页、子路径四种不同的选择；可设定强制检测的URL地址；  8）支持将漏洞以紧急、高危、中危、低危、信息进行危害程度的分类，并且可根据用户需要自定义漏洞等级；  9）支持识别国内外主流Web应用防火墙品牌；  10）支持获取整个网站目录结构，并能导出所爬行到的URL。  （4）新一代系统漏洞检测工具  1）厂商漏洞特征库大于250000条，漏洞知识库与CVE、CNNVD、Bugtraq、CNCVE、CNVD等国际、国内漏洞库标准兼容；  2）扫描结果在产品界面中支持查看目标应用返回的软件版本，可以方便与漏洞描述对比进行漏洞验证。 | 1 | 套 |  |
| 15 | 86寸一体机 | 一、整机硬件部分：  1.整机采用一体设计，外部无任何可见内部功能模块连接线。边角采用弧形设计，表面无尖锐边缘或凸起。整机屏幕采用≥86英寸液晶显示器。整机采用超高清LED液晶显示屏，显示比例16:9，分辨率3840×2160。  2. 嵌入式系统版本不低于Android13，内存≥2GB，存储空间≥8GB。采用红外触控技术，支持Windows系统中进行40点或以上触控，支持在Android系统中进行40点或以上触控。  3.从内部Android通道切换到内部PC通道后，触摸框在1s内达到可触控状态。  4.从内部PC通道切换到外部通道后，触摸框在3s内达到可触控状态。前置USB接口支持Android系统、Windows系统读取外接移动存储设备。整机能感应并自动调节屏幕亮度来达到在不同光照环境下的不同亮度显示效果，此功能可自行开启或关闭。  5.整机内置2.2声道扬声器，位于设备上边框，顶置朝前发声，前朝向10W高音扬声器2个，上朝向20W中低音扬声器2个，额定总功率60W。整机内置非独立外扩展的8阵列麦克风，拾音角度≥180°，可用于对教室环境音频进行采集，拾音距离≥12m，（须提供带有国家认可的检验检测机构出具的检测报告CMA标识或CNAS标识或ilac-MRA标识，及盖有检测专用章的检验（检测报告）佐证，同时为确保功能成熟稳定，检测时间必须在该项目发标前。）  6.支持标准、听力、观影和AI空间感知音效模式，AI空间感知音效模式可通过内置麦克风采集教室物理环境声音，自动生成符合当前教室物理环境的频段、音量、音效。  7.整机色域覆盖率（NTSC）≥72%。整机背光系统支持DC调光方式，多级亮度调节，支持白颜色背景下最暗亮度≤100nit，用于提升显示对比度。整机支持色彩空间可选，包含标准模式和sRGB模式，在sRGB模式下可做到高色准△E≤1  ▲8.支持标准、多媒体和节能三种图像模式调节。整机系统支持手势上滑调出人工智能画质调节模式（AI-PQ），在安卓通道下可根据屏幕内容自动调节画质参数，当屏幕出现人物、建筑、夜景等元素时，自动调整对比度、饱和度、锐利度、色调色相值、高光/阴影，（须提供带有国家认可的检验检测机构出具的检测报告CMA标识或CNAS标识或ilac-MRA标识，及盖有检测专用章的检验（检测报告）佐证，同时为确保功能成熟稳定，检测时间必须在该项目发标前。）  9.整机全通道支持纸质护眼模式，可实现画面纹理的实时调整；支持纸质纹理：牛皮纸、素描纸、宣纸、水彩纸、水纹纸；支持透明度调节；支持色温调节。纸质护眼模式下，显示画面各像素点灰度不规则，减少背景干扰。  10.三合一电源按键，同一电源物理按键完成Android系统和Windows系统的开机、节能熄屏、关机操作；关机状态下按按键开机；开机状态下按按键实现节能熄屏/唤醒，长按按键实现关机。整机具备至少6个前置按键，可实现开关机、调出中控菜单、音量+/-、护眼、录屏操作。  11.整机支持5个自定义前置按键，“设置”、“音量-”，“音量+”，“录屏”，“护眼”按键，可通过自定义设置实现前置面板功能按键一键启用任一全局小工具（批注、截屏、计时、降半屏、放大镜、倒数日、日历）、快捷开关（节能模式、纸质护眼模式、经典护眼模式、自动亮度模式）、课堂智能反馈。  12.整机无需外接无线网卡，在Android和Windows系统下可实现Wi-Fi无线上网连接、AP无线热点发射和BT蓝牙连接功能。Wi-Fi和AP热点工作距离≥12m。整机支持蓝牙Bluetooth 5.4标准，固件版本号HCI13.0/LMP13.0。  13.整机内置传屏接收模块，整机不需要连接任何附加设备，可实现外部电脑、手机等设备的音视频信号实时传输到整机上；当使用外部电脑传屏时，支持触摸回传，在屏幕上部显示传屏工具栏，可以进行触摸回传控制、勿扰模式、暂停投屏功能；开启勿扰模式时，不允许其他人再进行传屏；投屏时可以选择过滤特定应用窗口，如邮件应用等窗口。  14.整机内置双WiFi6无线网卡（不接受外接），在Android和Windows系统下，可实现Wi-Fi无线上网连接、AP无线热点发射。整机内置双WiFi6无线网卡（不接受外接），在Android下支持无线设备同时连接数量≥32个，在Windows系统下支持无线设备同时连接≥8个。  15.整机上边框内置非独立式摄像头，采用一体化集成设计，摄像头数量≥4个。整机上边框内置非独立式广角高清摄像头，视场角≥142度且水平视场角≥121度，支持输出4:3、16:9比例的图片和视频；整机上边框内置非独式广角摄像头和智能拼接摄像头， 均支持 3D 降噪算法和数字宽动态范围成像WDR 技术，支持输出 MJPG、 H.264 视频格式。  16.整机上边框内置非独立式摄像头，视场角≥141度且水平视场角≥139度，可拍摄≥1600万像素的照片，支持输出8192×2048分辨率的照片和视频，支持画面畸变矫正功能 。  17.整机触控书写功能集成预测算法，在书写速度≥50cm/s，支持笔迹距离笔的距离小于20mm。整机支持提笔书写，在Windows系统下可实现无需点击任意功能入口，当检测到红外笔笔尖接触屏幕时，自动进入书写模式。整机触摸支持动态压力感应，支持无任何电子功能的普通书写笔在整机上书写或点压时，整机能感应压力变化，书写或点压过程笔迹呈现不同粗细。  18.支持将自定义图片、动画设置为开机画面。type-C 支持最大充电功率15W。无PC状态下，嵌入式系统内置互动白板支持十笔书写及手掌擦除（手掌擦除面积根据手掌与屏幕的接触面大小自动调整），白板书写内容可以PDF、IWB和SVG格式导出。支持10种以上平面图形工具。支持8种以上立体图形工具。  19.整机内置触摸中控菜单，在整机全信号源通道下通过手势在屏幕上调取该触摸菜单；支持信号源通道切换、护眼、声音调节功能；支持切换智能息屏、经典护眼模式、纸质护眼模式、自动亮度模式；并可支持调节音量、亮度，支持自动亮度模式，支持点击静音按钮静音。  20.整机具备智能手势识别功能，在整机全信号源通道下均可识别五指上、下、左、右方向手势，五指画 O、画~、左右晃动、缩/放方向手势滑动并调用相应功能。支持将各手势滑动方向自定义设置为无操作、熄屏、批注、桌面、半屏模式，  21.整机支持同一品牌的视频展台通过 USB 等方式连接，支持一键打开/关闭展台软件；在任意通道下均可实时查看视频展台连接状态，当设备连接/断开连接时，提供实时反馈提示；同时支持读取视频展台设备型号，对应显示设备实物图片。  22.整机支持同一品牌智能笔，通过BLE（蓝牙低能耗技术）、USB Dongle（通用串口总线接收器）等方式连接，当整机和智能笔均支持BLE功能时，支持指定区域内智能笔自动发现、自动连接，并支持读取智能笔型号。  23.整机Windows通道支持文件传输应用，支持多人同时将手机文件传输到整机上；当手机端登录账号与整机一致时，接收文件不需要二次确认，当手机端登录账号与整机不一致时，且距离连接成功或上次传输超过3分钟，则接收文件需要二次确认。整机Windows通道支持文件传输应用，支持通过扫码、wifi直联、超声三种方式与手机进行握手连接，实现文件传输功能。  24.整机设备自带地震预警软件。支持在地震预警页面中获取位置，可以手动进行位置校准。支持在地震预警页面中选择提醒阈值。支持在地震预警界面中开启和关闭地震预警服务。  电脑模块  1.搭载Intel 酷睿系列≥i5 CPU  2.内存：≥8GB DDR4笔记本内存或以上配置。  3.硬盘：≥256GB或以上SSD固态硬盘。  4.采用按压式卡扣，无需工具就可快速拆卸电脑模块。  5.具有标准 PC 防盗锁孔，确保电脑模块安全防盗。和整机的连接采用万兆级接口，传输速率≥10Gbps。  交互式白板软件：  1.备授课一体化，具有备课模式及授课模式，支持老师个人账号注册登录使用，也可通过USB key进行身份快速识别登录。支持课件云存储，无需使用U盘等存储设备，老师只需联网登录即可获取云课件。  2.支持点对点分享云课件，用户可在软件中直接将课件发送给其它用户，同时也可以在软件中直接接收并打开其它用户分享的课件；同时支持链接分享课件，接收方打开链接后可直接输入账号获取课件。  3.支持用户在软件中打开pptx格式文件，且用户可在软件中自由编辑原文件中的图片、文字、表格等元素，并支持修改原文件中的动画。方便老师利用软件互动功能在原有PPT基础上修改课件。  4.高级图形：支持对话框、五角星、大括号、旗子等特殊图形绘制，同时支持自定义绘制复杂的任意多边形及曲边图形。 | 2 | 台 |  |
| 16 | 教学竞赛靶场平台 | 1.平台提供物理机管理，支持手动添加和关联多台物理机设备资源；  2.平台支持多台主机资源的集群管理，同时支持集群的横向扩容，并能通过弹性云计算方法自动轮询调度虚拟主机；  3.平台支持容器和KVM两个类型的集群管理，其中KVM支持至少三种以上的集群类型；平台提供网段管理，支持配置多IP地址段，用以自动分配创建的实例化资产；  4.平台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容器类型；  5.虚拟终端类型包含包含windows、linux两种类别，其中涵盖但不限于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；  6.虚拟网络设备类型包含交换机、路由器、防火墙等网络和网络安全设备；  7.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；  8.物理接入设备类型包含计算终端、路由器、交换机、安全防护设备等；  9.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；  10.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，支持通过单一设备接入与网络接入等方式实现实体设备的接入；能够根据接入方式提供网络选项配置，支持L2接入与L3接入，L2模式接入不限制实体设备本身使用的VLAN，L3模式支持NAT接入和路由器接入等形式；  11.支持展示实体设备被引用场景拓扑，实体设备接入场景采用独占的形式，即限制单台实体设备同一时刻只能被同一套场景所引用；  12.平台支持以图形化拖拽的方式绘制场景拓扑，拓扑编辑支持根据网元类型筛选拓扑元素，网元类型包括路由器、交换机、虚拟机、docker、安全设备、物理设备等，并支持通过名称检索的方式搜索具体拓扑元素拖拽使用，同时支持对拓扑中元素的属性以及链路的属性进行配置；  13.平台支持将绘制的场景拓扑保存为模板，并支持通过加载多个模板进行组合连线的方式构建新的拓扑场景；  14.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、内存、硬盘等资源的使用情况；agent节点监控，即在不依赖网络的情况下，能够获取节点内的进程、端口、文件等情况；  15.支持物理机监控，包括CPU型号、操作系统、运行时间、CPU、内存、存储使用情况、网卡信息、实时流量、丢包率、收发包统计、端口开放情况、运行的进程的信息等数据的监控；能够对关键性指标设置阈值，并进行实时监测，当设备关键性指标超出阈值后设备会发出告警；  16.支持拓扑场景全流量采集的能力；  17.平台用户管理可以为用户分配多个角色，并支持对用户信息进行禁用、启用、修改密码等操作；  18.平台支持用户账号注册功能，支持注册申请教员、学员等角色账号，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；  19.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；  20.平台支持查看平台整体资源占用和分配情况，包括CPU、内存、硬盘、虚拟机、路由、交换机等；  21.平台支持查看单物理机硬盘、内存、CPU的使用情况；  22.平台支持查看平台日志吞吐量的相关数据情况；  23.平台支持对实例进行管理，包含虚拟机、Docker容器等类型；可以对实例进行一键回收、关机、重启、回收、快照的创建、恢复、重置等独立操作与统一化管理，同时支持查看实例的IP地址和开放的端口号，支持通过浏览器的方式操作虚拟终端；  24.平台支持实例资源创建时的相关配置，支持自定义配置实例回收时间和个数以实现实例资源合理调度分配；提供实例端口映射导出能力，可批量导出正在运行的实例环境端口映射信息；  25.平台支持对端口映射进行管理，包括配置端口映射的入口IP、端口的最小与最大值、开启与关闭；  26.平台支持实例日志管理功能，能够审查实例资源的调度使用情况，展示信息包含实例资源的名称、类型、来源、操作人、操作时间、操作、操作结果等，支持日志的批量导出、检索和周期性清理；  27.平台支持日志审计功能，支持记录和查看平台用户的操作日志信息，同时支持日志检索以及批量导出；  28.资源库包含镜像库、工具库、漏洞库、知识库、场景库，具有统一管理界面；支持资源的上下线、批量管理、横向扩展，所有资源支持标签化管理；  29.资源库支持以平台、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；  30.场景创建时支持以图形化拖拽的方式绘制场景拓扑，拓扑元素包含虚拟终端、虚拟网络设备、虚拟安全设备，虚拟网络设备至少包含虚拟交换机、虚拟路由器，虚拟安全设备至少包含数据库审计、日志审计、APT攻击预警、主机安全、Web应用防火墙、堡垒机等，同时支持对拓扑中元素的属性进行配置；  31.课程支持管理三级标签，每个课程可以拥有多个标签，平台能够按照标签进行课程的分类和筛选，同时课程支持按照难易程度进行划分和筛选；  32.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；  33.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；  34.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；  35.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；  36.支持课程目录导航，快速进行章节的切换，导航中显示章节的课时数和个人学习进度，同时当课程拥有多个课程资源时，支持课程资源的快速切换；  37.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；  38.培训支持以图形化的方式展示班级中学员考试、作业成绩的分布情况；支持查看全部、进行中、已结束等状态的班级学习情况，学习情况包含班级数量、待批改作业、待批改试卷、培训平均完成率、作业平均提交率、考试平均完成率、平均学习课时、平均学习时长、考试成绩分布、作业成绩分布等数据信息，并支持各班培训组织效果的对比；  39.动态试卷支持以规则的形式保存试卷，当考试使用时，每个人进入考试都会根据动态试卷规则生成全新试卷；试卷规则支持依据题目类型、标签、难度等维度进行配置，每条规则支持设置对应题目的数量和分数，每张试卷支持配置多条规则，根据规则进行组卷；  40.考试支持花卷和动态试卷两种防作弊模式：花卷模式是指选手看到的题目答案顺序随机打乱；动态试卷模式是指每个选手拿到的题目都不一样；  41.平台支持考试统计功能，支持对考试总人数、完成人数、缺席人数、作弊人数等数据进行统计，并支持以图表的形式展示成绩分布情况以及试题正确率排行榜；  42.创建安全研究时，支持设置难度等级以及关联安全场景；支持用户针对自定义安全场景开展安全研究工作，提交研究成果；研究成果支持上传附件或关联平台漏洞作为相应成果，附件类型支持word、pdf、mp4等格式，可设置针对指定用户开放；  43.支持混合竞赛模式，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。赛制支持夺旗赛、定向渗透赛、攻防对抗赛、领地争夺赛、理论赛五种类型。  ★44.需满足100个学生同时在线进行学习，支持虚拟安全设备在线做拓扑搭建实验；满足50个学生分组进行企业综合场景搭建实验。  45.精品课程包  （1）网络安全教学课程不少于40门，课时数不少于1500课时，课程体系应覆盖信息安全基础、应用安全、数据安全、安全编程、安全运维、安全工具及攻防竞赛等知识领域，涵盖网络安全、系统安全、安全意识、等级保护、保密培训、安全协议、密码学、渗透测试、代码审计、移动安全、二进制安全、物联网安全、云计算安全、电子取证、数据存储安全、工控安全、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、CTF夺旗赛等知识点；  （2）恶意代码分析课程须包括：恶意软件基础知识、病毒木马检测（手动）、恶意代码分析实战；实验包括：Word宏病毒实验、手工木马检测、脚本病毒编写实验、MPEG2网马实验、木马攻击实验、脚本及恶意网页病毒、病毒防范-文件的扩展名、PE型病毒实验、VBS病毒实验、COM病毒实验、实验工具文件格式猜测、使用OD分析恶意软件反向shell等内容，至少满足25课时；  （3）安卓攻防实训课程须包括：移动APP安全概述、基础篇、工具篇、调试篇、加固篇、实战篇、通信篇、安全测试篇；实验包括：使用Androguard静态分析Android程序、使用IDA pro动态分析Android程序、使用method profiling动态分析Android程序、使用GDB server调试Android进程、使用Androguard静态分析Android程序、使用GDB server调试Android进程、smali插桩、注册机开发、使用AntiLVL对Google Play Licence方式的破解、针对Android授权KEY方式的破解、程序签名与发布、短信欺诈漏洞、短信拦截、Android图像化口令破解（3#3破解）、CVE-2011-2825（任意地址读漏洞实验）、CVE-2012-2871（任意地址写漏洞实验）、移动智能终端PIN码破解、BroadcastAnyWhere（Google Bug 17356824）Android漏洞、Activity劫持、Activity组件安全检测、Service组件安全检测、BroadcastReceiver组件安全检测、ContentProvider组件安全检测、Android应用通信过程漏洞检测等学习内容，至少满足25课时；  （4）渗透测试实战演练实验须包括：74cms程序、BEESCMS程序、Linux、Tomcat、GhostScript 、metinfo、Discuz、ECShop、FCKeditor、FengCms、Getboo、HDWiki、IIS6、Mono、Mutillidae、PHPMyWind、PHPok、SDCMS、Webgoat.Net、YunGouCMS、appcms、cacti、dvwa、espcms、flask、iwebSNS、jdcms、php168、phpwind、speedcms、tipask、酷维（Kuwei）、Apache、Bluecms、DirCMS、Easytalk、ElasticSearch、PhpMoAdmin、Simple-Log、ThinkSNS、ecmall、jishigou、qibocms、天生创想CRM系统、学生成绩查询分析系统、方维O2O系统、睿思网络学习系统等经典CMS渗透测试实战实验，至少满足140课时；  （5）应用密码学课程内容须包括：密码学概述、古典密码体制、对称密码体制、密码学数学基础、公钥密码体制、Hash函数和消息认证、希尔密码破解、认识LSFR及序列密码、RC4实验、DES实验、AES实验、3DES实验、IDEA实验、SMS4实验、大数运算、素性测试、模幂、原根、求逆、RSA密码实验、Hash基础、MD5实验、MD5破解、SHA算法、SHA256算法、SHA224算法、HMAC算法、RSA签名算法、ELGamal签名算法、ECC签名算法，至少满足40课时；  （6）Web渗透测试实战指南课程内容须包括：渗透测试基础、信息收集、漏洞扫描工具、文件上传漏洞、任意文件下载/读取漏洞、文件包含漏洞、跨站脚本攻击漏洞、跨站请求伪造漏洞、SQL注入漏洞、服务器端请求伪造漏洞、高级渗透测试技术、网络安全技能扩展、综合实战；实验包括：BurpSuite本地安装、BurpSuite抓包配置、BurpSuite抓取HTTPS报文配置、本地Kali实验环境搭建、信息收集实战、Nmap工具使用、AWVS本地安装、AWVS发起简单的扫描、AppScan本地安装、AppScan扫描、Nessus本地安装、Nessus使用、上传漏洞JavaScript校验绕过、跨站请求伪造漏洞、万能密码、MySQL注入实验、Brute force Web认证、Tomcat弱口令、越权漏洞挖掘与利用、XerCMS越权漏洞挖掘与利用、脏牛 Dirty COW(CVE-2016-5195)、Ubuntu 16.04 本地提权(CVE-2017-16995)、Web应用渗透测试 PHPStudy后门实战、Linux主机渗透测试 从Struts2到Getshell提权、Web应用渗透测试 YXCMS实战，至少满足50课时；  （7）JAVA代码审计综合实训实验须包括：代码审计安装与基本操作、命令与执行注入、XSS反射型漏洞实验、XSS存储型漏洞与本地包含与远程包含实验、SQL注入与CSRF跨站请求伪造实验、JAVA权限控制漏洞、JAVA代码审计之业务逻辑问题、JAVA代码审计之服务器安全配置、JAVA代码审计杂项、JAVA代码审计实战、JAVA代码审计综合实验，至少满足15课时；  （8）网络安全协议分析实验须包括：协议工具介绍、网络层协议分析、传输层协议分析、IPSec 协议分析、SSL 协议分析、电子邮件协议分析、HTTP及其安全性、DNS与DHCP协议分析、针对WEB攻击的协议分析、针对DDOS攻击的流量分析、综合实验，至少满足15课时；  （9）CTF入门指南课程内容须包括：CTF 基本概念以及技巧介绍、CTF Web安全 考点以及实战演练、CTF 密码学 考点以及实战演练、CTF 杂项 考点及实战演练、CTF 逆向 考点及实战演练、CTF 二进制安全考点及实战演练、CTF Web 攻防赛思路与技巧，至少满足100课时；  （10）微课堂之信息安全意识课程内容为短视频形式，内容须包括：常规安全知识、网络使用准则、信息安全职责、网络法规遵循、网络会议安全、邮件安全、即时消息、文档安全、浏览器及上网安全、无线网络安全、远程工作安全、公共场所安全、博客信息安全、社交网络安全、公司信息披露、机密信息保护、数据备份及恢复、信息清除与销毁、个人信息保护、客户信息安全、信息安全事件、知识产权意识、软件安装使用、恶意代码防范、社工工程学防范、电话诈骗、网络钓鱼防范、金融诈骗防范、桌面安全、工作站电脑安全、打印、传真与复印安全、邮寄与快递、拍照泄密防范、第三方安全、人员安全管理、信息安全管理、安全保密意识、信息安全文艺、信息安全互动测试，至少满足250课时；  （11）内网渗透课程内容须包括：常见内网穿透手段与工具介绍与使用、常见C2工具介绍与使用、内网主机信息收集、Windows域内提权的几种方式、Windows域内横向扩展、后渗透持久化技术，至少满足10课时；  （12）网络安全应急响应课程内容须包括应急响应介绍、信息搜集、入侵排查方向、流量分析、应急响应常见处置案例、应急响应工具介绍、安全事件安全加固、服务器身份验证加固、内存分析-volatility的使用、镜像分析-autopsy的使用、网络安全应急响应报告，至少满足35课时；  **▲**（13）网络安全攻防技术课程至少满足64课时，配套课件须包括信息收集技术、安全漏洞检测与利用、Windows操作系统的安全加固、SQL注入的原理及利用、XSS注入的原理与利用、WEBshell与文件上传漏洞、OWASP与常见WEB安全漏洞、WEB漏洞扫描与渗透测试、常见安全产品简介等不少于9个；配套实验手册须包括信息收集技术实验手册、安全漏洞的检测与利用实验手册、Windows操作系统的安全加固实验手册、SQL注入的原理与利用实验手册、XSS注入的原理与利用实验手册、WEBshell与文件上传漏洞实验手册、OWASP TOP10与常见漏洞实验手册、WEB漏洞扫描与渗透测试实验手册等不少于8个；配套视频资源须包括信息收集基本思路、Nmap端口扫描器的使用、安全漏洞的基本概念、安全加固基本思路、WEB应用安全概述、HTTP协议基础、HTML语言基础、服务端脚本基础、数据库与SQL基础、Burp暴力破解、SQL注入漏洞的利用、OWASP Top10与常见漏洞讲解等不少于12个。（提供这门课程主要内容演示视频，视频体现内容包括但不限于12个配套视频片段的资源名称、主要内容、可看到每个配套视频时长不少于30分钟，演示视频时长不超过5分钟。）  **▲**（14）网络空间安全导论课程至少满足56课时，配套课件须包括信息安全概述、物理安全、身份认证、访问控制、网络威胁、网络防御、内容安全、信息安全管理等不少于8个；配套实验手册须包括DNS服务期及CA证书实验手册、域控与组策略实验手册、ARP欺骗实验手册等不少于3个；配套视频资源须包括信息安全概述、密码学基础、物理安全、身份认证、网络安全协议、内容安全、信息安全管理等不少于7个。（提供这门课程主要内容演示视频，视频体现内容包括但不限于7个配套视频片段的资源名称、主要内容、可看到每个配套视频时长不少于30分钟，演示视频时长不超过5分钟。）  （15）提供安全运维管理实训课程实训任务书须包括关于防火墙类开源项目的学习研究、关于资产管理类开源项目的学习研究、关于堡垒机开源项目的学习研究、关于HIDS项目的学习研究、关于NIDS项目的学习研究、关于蜜罐的学习研究等不少于6个。  46.经典赛题包  （1）平台内置理论赛题、夺旗赛题、定向渗透赛题、攻防对抗赛题、领地争夺赛题等题目类型，题目至少包含Web安全、Crypto密码学、Reverse逆向工程、Misc安全杂项、Pwn溢出等五大方向；  （2）平台内置理论赛题数量不少于3500道；  （3）平台内置夺旗赛题数量不少于350道；  （4）题库应涵盖如下所有知识技能大纲：  1）Web安全：HTTP请求伪造、HTTP来源头伪造、HTTP返回头分析、HTTP返回内容分析、HTTP请求UA头伪造、SQL基本注入、SQL无回显盲注、SQL二次注入、SQL WAF绕过注入、SQL宽字节注入、SQL报错注入、SQL文件操作、SQL比较盲注、SQL有回显注入、PHP代码执行、PHP弱类型特性、PHP反序列化、PHP文件包含、备份泄露、文件泄露、网站信息泄露、文件上传基础利用、文件上传条件竞争、数据校验绕过、Python模板注入、Python沙箱逃逸、有回显XXE、个人信息搜集、常规暴力破解、反射型XSS、WAF绕过XSS、CSRF基本利用。  2）Crypto密码学：指定规则的简单代换密码、流密码、RSA、数字签名、Costas阵列、凯撒密码、ASCII移位、栅栏密码、猪圈密码、背包密码、Paillier加密、DSA已知k攻击k、DSA共享攻击、AES加密CBCECB、电脑键盘QWE加密、dvorak键盘加密、仿射密码词频分析、维吉尼亚密码、Playfair密码、四方密码、LCG A、B、M以及N0已知等。  3）Reverse逆向工程：Java逆向、Python逆向、JS逆向、Native逆向、C#逆向、GO逆向、迷宫加解密、矩阵解密、BlowFish加解密、SHA加解密、MD5异或、Base64、rot位移、RC4、AES、自定义加密、方程组、RSA、固件解包、Win32消息处理、Win32资源处理、TLS反调试、ptrace反调试、调试器检测、STARTUPINFO信息检测、二叉树、vector。  4）Misc安全杂项：内存取证、安全事件分析、U盘取证、磁盘取证、Web流量分析、蓝牙流量分析、网络协议流量分析、加密流量分析、图片隐写、文件修复文件检测、压缩包爆破、压缩包伪加密、压缩包明文攻击、压缩包CRC32碰撞、压缩包暴力破解、压缩包注释查看、数据及编解码转换。  5）Pwn溢出：栈漏洞利用ret2shellcode、栈漏洞利用canary绕过、栈漏洞利用ret2libc、栈漏洞利用BROP、栈漏洞利用ret2text、栈漏洞利用stack pivoting、整数溢出符号位溢出、整数溢出进位溢出、堆漏洞利用Fastbin Attack、堆漏洞利用Double Free、堆漏洞利用off by one、堆漏洞利用UAF、堆漏洞利用Tcache Attack、堆漏洞利用off by null、堆漏洞利用House of Rabbit。  47.教学竞赛信息资源包  （1）镜像数量不少于600个，镜像类型应包含Windows、Linux两种类别，其中涵盖但不限于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；  （2）工具数量不少于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；  （3）漏洞数量应不少于80000个，带复现环境CVE漏洞不少于200个；  （4）安全知识类型包含信息安全基础、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2000多课时的课程与实验资源；课件具有PPT、PDF、视频等多媒体课件、CTF实验课件、实验指导手册等类型；实验课程提供课程实验介绍、详细实验指导书、实验环境靶机、实验工具等内容；  （5）理论题库数量不少于3500道。  48.扩展课程包1  扩展课程包1课程不少于60门，课时数不少于500课时，包含Linux操作系统综合实训、密码学与应用、PKI、攻防对抗实训、DDOS详解、安全攻防基础、网络嗅探、HTTP协议、HTTP与TLS协议分析、Wireshark工具使用、当前网络安全形势、信息安全产品检验标准、安全报告、JavaWeb应用安全开发与测试、业务逻辑漏洞、Java反序列化远程代码执行、Struts2漏洞、自动化渗透测试技术、渗透测试基础讲解、信息收集综合实训、安卓综合实训、逆向工程基础、云计算与安全、大数据安全技术、数据库安全基础、数据库安全实践、容灾备份、数字水印、安全测试工具实战指南、安全代码编写、软件安全开发生命周期（SDL）、软件源代码安全检测、网站渗透与加固、OPSEC安全加固指南、服务器渗透与加固、应用系统安全、服务器运维、防火墙原理与技术、数据隐私与取证、数据库取证基础、网络设备取证基础、攻防关联取证分析、日志审计工具、操作系统取证基础、应用程序取证基础等课程，课程包含PDF、视频等多媒体课件及实验环境、实验指导手册等资源。  49.拓展课程包2  拓展课程包2课程不少于 40 门，课时数不少于 400 课时，包含但不限网络安全等级保护、数据安全与实践、渗透测试技术、操作系统安全、软件安全，课程包含PDF、视频等多媒体课件及实验环境、实验指导手册等资源。 | 1 | 套 |  |
| 17 | 运维靶场课程及实训资源 | 包含网络安全基础概念、计算环境安全基础、网络协议与安全、恶意代码原理与防治、网络安全防护技术、Web应用漏洞剖析、渗透测试、漏洞扫描等课程，共66课时。包含边界防护、WEB应用安全、安全运维、数据安全、终端安全等课程，共34课时。包含日志分析、流量分析和安全设备告警分析等课程，共22课时。包含企业基础网络安全防护能力建设实训、企业网络安全防护体系优化实训、企业威胁监测实训等课程，共9课时。为保证教学效果，运维靶场需支持与教学竞赛靶场保持联动，平台互通。 | 1 | 套 |  |
| 18 | 维保服务 | 1.提供3年免费升级维护；  2.维保期内，提供每年更新50个带环境的漏洞，其余资源实时更新；  3.提供安装调试后7天内本地操作培训；  4.提供7\*24小时支持热线；  5.本地应急响应时间≤2小时。 | 1 | 套 |  |
| 19 | 专业课程体系重构服务 | 实训室建设完成后，协助学校完成信息安全技术应用方向对应产业全链职业课程体系的设计和建设，产教融合实现课程体系与岗位标准一致，开展“课岗对接、课证融合”实践教学。 |  |
| 20 | 项目实践服务 | 实训室建设完成后，提供国家级重大活动网络安全安保实习机会，在合同期内每年名额不低于4个。 |  |