## 采购项目商务和技术要求

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 需求名称 | 技术参数和需求内容 | 备注 |
| （**此项为实质性响应，不允许负偏离**） | 基本要求 | 1、提供安全能力提升平台一套，软硬件一体交付，包含教学管理、培训学习、综合实训、攻防演练及平台资源库等功能，可以进行网络安全培训学习、动手操作实训、培训考核、攻防演练等； 2、为医院提供至少10名医院人员的安全培训。 |  |
| **\***硬件配置要求 | 1、硬件服务器集群部署，服务器数目不少于2台，保证CUP使用率不大于70%； 2、提供交换机1台。 |  |
| **\***产品资格 | 所投产品（系统）具有中华人民共和国国家版权局颁发的计算机软件著作权登记证书；须提供相关证明材料并加盖原厂商公章 |  |
| 1 | 技术力量 | 投标单位需提供培训讲师对平台的使用进行现场培训，并提供以下人员三个月投标单位社保证明并加盖原厂公章：  **·**1.投标单位培训讲师支撑过省级技能选拔赛，提供证明材料复印件并加盖投标单位公章  **·**2.投标单位培训讲师支撑参与过省级以上职业技能竞赛命题工作，提供获得荣誉证书或荣誉称号等，提供证明材料复印件并加盖投标单位公章 为确保项目能够顺利交付，要求投标单位具备如下能力：  **·**3.投标单位具有中国信息安全测评中心颁发的信息安全服务安全开发类二级以上证书； 提供相关证明材料并加盖投标单位公章  **·**4.投标单位具有中国信息安全测评中心颁发的国家信息安全测评信息安全服务资质证书（安全工程类二级以上）；提供相关证明材料并加盖投标单位公章  **·**5投标单位获得近三年CNNVD优秀技术支撑单位证书或获得CNNVD漏洞信息共享合作单位证书；提供相关证明材料并加盖投标单位公章 |  |
| 2 | 2.1服务器配置 | 单台服务器配置如下： 2U机架式服务器，带导轨  操作系统：正版操作系统，支持linux操作系统； 配套软件：安装主流数据库操作系统；  电源：≥2个\*800W，冗余满配； CPU:≥2颗，每颗主频≥2.4G,每颗≥16核； 内存≥256GB，单条≥32G，内存槽≥8条； 硬盘：固态盘≥2块，每块容量≥960G；机械硬盘≥4块，每块容量≥4T，转速≥7200rpm. 接口数量：千兆电口≥4个,万兆光口≥2个（带多模光模块） 其他：固态硬盘支持RAID1，实际可用不小于800G，机械硬盘支持RAID10，实际可用不小于7T。 |  |
| 2.2交换机配置 | 交换机硬件规格要求： ≥24个10/100/1000Base-T以太网端口； ≥4个千兆光口； 交换机硬件性能： 传输速率≥51Mpps/126Mpps |  |
| 2.3基础云管理技术要求 | 1.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； 2.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； |  |
| 2.4实训教学 | 1.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； 2.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； 3.平台支持管理学习路径，内置常用学习路径，支持教员自行添加与组建新的学习路径；学习路径支持分阶段管理，同时每个阶段可以按顺序设置多门学习课程； **·**4.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；支持查看所有状态的班级学习情况，学习情况包含待批改作业、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，支持各班培训组织效果的对比； |  |
|
| 2.5考试考核 | 1.每个学员进行考试时会根据规则生成全新试卷，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； 2.考试支持防作弊模式：模式包括选手看到的题目答案顺序随机打乱；或者每个选手拿到的题目都不一样； 3.平台支持理论考试功能，支持固定时间段统一考试；支持在设定的时间段内，考生可任意时间进入并根据固定考试时长进行考试；支持开放型考试，学生随时进入考试根据考试时长进行考试； |  |
| 2.6实训教学资源 | 1.网络安全教学课时数不少于1500课时，每个课时不少于20分钟，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； 2.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，支持日志的批量导出、检索和周期性清理； 3.资源库包含镜像库、工具库、漏洞库、知识库、场景库；支持资源的增加删除、批量管理； 4.镜像数量不少于600个，镜像类型应包含Windows、Linux两种类别，可以根据镜像类型进行筛选； **·**5.工具库支持用户自定义创建工具，工具类型可以支持虚拟机型及下载型；工具数量不少于500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等类别，工具不得捆绑具有木马后门、病毒程序； **·**6.漏洞库支持漏洞的管理与创建，创建时支持关联漏洞利用方法、修复方案、复现环境、测试工具等内容，支持通过漏洞状态、漏洞来源、漏洞等级、漏洞名称、漏洞编号等信息检索漏洞； |  |
| 2.7竞赛演练管理 | 1.支持对整场比赛相关情况进行查看，包括竞赛情况、实际参赛人员情况、赛题情况、竞赛靶机状态、竞赛阶段相关信息，支持提供快速入口进入相关信息的配置界面； 2.竞赛支持混合模式，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，赛制支持夺旗赛、漏洞渗透赛、攻防对抗赛、权限争夺赛、理论赛五种类型； |  |
| 2.8竞赛赛题管理 | 1.夺旗赛题创建时，配置的答题类型支持配置FLAG关联内容，支持配置多种类型靶机，支持关联场景版本及镜像环境，支持配置靶机类型为共享或独占，共享类型靶机支持配置负载能力； 2.攻防对抗演练支持设置初始分值和每轮时长；支持设置是否对选手开放重置靶机功能；支持设置靶机重置保护时间；支持开启靶机重置扣分模式，该模式下支持配置最大重置次数及超出次数后的扣分分值。 3.漏洞防渗透演练支持对题目的基本信息进行配置，并支持对题目内关卡的基本信息进行配置，同支持显示或隐藏关卡，展示关卡相关信息。 **·**4.权限争夺演练支持设置是否开启选手自有靶机以及自由靶机的用户名与密码，并支持设置初始保护时间。 |  |
| 2.9场景演练管理 | 1.平台支持以图形化拖拽的方式绘制场景拓扑，拓扑可编辑的设备种类包括路由器 、交换机、虚拟机、docker、安全设备、物理设备等，支持通过名称检索的方式搜索具体设备拖拽使用，支持属性配置； 2.场景库支持通过新建和已有版本复制的方式创建新的场景版本；场景支持拓扑预览功能； 3.支持查看场景拓扑，并支持安全场景的构建、回收、重新创建、快照的生成与恢复； |  |
| 2.10实训演练场景资源 | 1.攻防对抗实训须包括：无线网络破解、DDoS攻击检测及防御实现、冰河木马实验、破解MySQL\_root密码等； **·**2.数据安全实训须包括：数据存储方式和存储介质、数据加密方式、数据恢复实验、数据传输安全实验、oracle网络相关安全设置、防火墙设置、密码恢复工具的使用、oracle安全杂项配置、oracle TNS监听器安全oracle数据库审计、oracle用户与权限管理、oracle应用系统安全实践、数据库漏洞利用与拖库、数据库安全扫描、综合实验、SQL Server身份认证、SQL Server权限管理、SQL Server安全加固、MySQL管理维护、MySQL的数据库实践、MySQL数据备份与恢复等； 3.web安全综合实训须包括：HTTP漏洞扫描、HTTP安全测试、典型安全通信协议的配置使用(Apache）、WEB服务器部署工具的使用、IIS的安全设置、IIS架构动态网论坛系统、使用工具清除IIS日志、Web服务安全配置实验、一句话木马测试分析、ARP欺骗攻击防御、局域网ARP攻击、Shadow database scanner扫描数据库、CA和CCA的使用、Sksockserver结合sockcap实现代理跳板、cain在windows下的应用等； **·**4.渗透场景须包括：用户提权、正反向代理应用、勒索病毒应急响应实践、数据泄露应急响应实践等； |  |
| 2.11节点仿真管理 | 1.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； 2.虚拟终端类型包含windows、linux两种类别，其中涵盖windows10、windows server 2008、windows server 2012、windows server 2016、centos、ubuntu、Debain8、Kali等操作系统类型； 3.虚拟终端类型包含国产化操作系统，包括统信系统、麒麟系统； 4.虚拟网络设备类型包含交换机、路由器、防火墙等； |  |
| 2.12平台并发人数要求 | ≥30人 |  |
| **商务要求（不接受负偏离）** | | | |
| 3 | 附加验收条件 | 通过系统全流程运行测试，运行检测时间≥1个月。 |  |
| 4 | 认证培训服务 | 为医院提供至少10名医院人员参加cisp培训及考核。  考核类型可从如下六类中选取：中国信息安全测评中心（CISP）认证培训：（1）注册信息安全专业人员认证CISP(CISE/CISO)；（2）工业控制系统安全工程师(CISP-ICSSE)；（3）大数据安全分析师(CISP-BDSA)；（4）云安全工程师(CISP-CSE)；（5）注册信息安全专业人员渗透测试工程师(CISP-PTE)；（6）注册渗透测试专家(CISP-PTS)； | **提供承诺函** |
| 5 | 交货时间 | 签订合同后90日内。 |  |
| 6 | 交货地点 | 北京市海淀区 |  |
| 7 | 付款条件 | 设备到货部署完成后付款70%，验收后付25%，验收之后满一年付5% |  |
| 8 | 售后服务 | 提供3年免费升级维保，维保开始时间从验收之日起。 维保期内，提供每年免费更新至少50道赛题。 提供安装调试后本地操作培训，次数根据甲方需求来定。  提供24小时支持热线。 本地应急响应时间≤2小时。 |  |