青岛工程职业学院信息安全实训室建设项目

更正公告

一、项目基本情况

原公告的采购项目编号：SDGP370200000202402001049

原公告的采购项目名称：青岛工程职业学院信息安全实训室建设项目

首次公告日期：2024-08-01

二、更正信息

更正事项：☐采购公告 ☑采购文件 ☐采购结果

更正内容：

原招标文件第四章采购需求：

（一）**原**“●网络安全综合实训平台：9.竞赛演练防作弊组件 a.具备大屏展示能力，至少具备12个展示界面，包括全局监测大屏、全局分析大屏、外部攻击（世界）大屏、外部攻击（中国）大屏、威胁情报大屏、横向攻击大屏、恶意外联（世界）大屏、恶意外联（中国）大屏、文件检测大屏、挖矿检测大屏、资产分析大屏、大屏轮播；（需提供具备 CNAS 资质的测试报告证明材料）”

现变更为：9.竞赛演练防作弊组件及其他功能 a.具备大屏展示能力，包含但不限于全局监测大屏、全局分析大屏、外部攻击大屏、威胁情报大屏、恶意外联大屏、文件检测大屏、资产分析大屏、大屏轮播。

（二）原●网络安全综合实训平台：“9.竞赛演练防作弊组件 c.内置单独分析场景模块不少于 19 个，包括：脆弱口令感知、敏感数据感知、漏洞攻击感知、风险端口感知、失陷主机感知、异常流量感知、违规互联感知、挖矿行为分析、邮件行为分析、勒索行为分析、DNS 行为分析、DDOS 行为分析、暴力破解分析、扫描探测分析、僵木蠕攻击分析、web 攻击分析、横向渗透分析、隐蔽隧道分析、VPN 通信分析；（提供防作弊组件功能截图）”。

现变更为：本项参数的设定为招标人竞赛实训使用需要，现修改为“9.竞赛演练防作弊组件 c.内置单独分析场景模块至少包括：脆弱口令感知、敏感数据感知、漏洞攻击感知、风险端口感知、失陷主机感知、异常流量感知、违规互联感知、挖矿行为分析、邮件行为分析、勒索行为分析、DNS 行为分析、DDOS 行为分析、暴力破解分析、扫描探测分析、僵木蠕攻击分析、web 攻击分析、横向渗透分析、隐蔽隧道分析、VPN 通信分析等；”。

（三）“7.WEB 应用防火墙 6.具备蜜罐检测功能，诱使攻击方对它实施攻击，从而可以对攻击行为进行捕获和阻断。具备网站

一键关停功能，客户网站异常之后可通过一键关停，把网站转为维护状态。以上两种功能提供第三方权威机构的检测报告复印件。”

现变更为：现已变更为：6.具备蜜罐检测功能，诱使攻击方对它实施攻击，从而可以对攻击行为进行捕获和阻断。具备网站关停功能，客户网站异常之后可关停，把网站转为维护状态。

（四）原“●网络安全综合实训平台：（一）培训管理系统 6.统计分析 b.★以图形化方式展示所有班级在安全管理、安全技术、竞赛培训方案的各领域的学习情况。”

现变更为：●网络安全综合实训平台：（一）培训管理系统 6.统计分析 b.以图形化、可视化方式展示所有学生、班级在实训、竞赛等领域的学习情况。

（五）原“●网络安全综合实训平台：（二）竞赛管理系统 6.实时评分模块 c.★实时监控选手提交的 flag。动态 flag 模式中如发现选手交换 flag 则取消该题成绩。”

变更为：删除“★”条款。（二）竞赛管理系统 6.实时评分模块 c.实时监控选手提交的 flag。动态 flag 应具有防作弊机制。

（六）原“3、防火墙：7.支持 TCPBBR 加速功能，通过 TCP 丢包预测，快速重传和恢复机制，提高 TCP 协议的数据传输速度，当广域网链路出现延时和丢包的情况时，可明显改变 TCP 传

输效率，提升传输速率不用在用户终端上安装任何插件和软件，即可提升链路访问速度，节省带宽资源；”

变更为：3、防火墙：7.支持 TCPBBR 加速功能，通过 TCP 丢包预测，快速重传和恢复机制，提高 TCP 协议的数据传输速度。

（七）原“4、上网行为管理 4.应用特征数不少于 7300+，移动应用不少于 2000+，规格总数 12000+；5.提供智能策略分析功能，支持策略命中分析、策略冗余分析、策略冲突检查，并可在 WEB 界面显示检测结果；支持实时和周期性对所有安全策略进行分析”

变更为：4、上网行为管理 4.应用特征数不少于 7000+，移动应用不少于 2000+，规格总数 12000+；5.提供智能策略分析功能，支持策略命中分析、策略冗余分析、策略冲突检查，并可显示检测结果；支持实时和周期性对所有安全策略进行分析。

（八）原“5、入侵防御设备 3.系统需具有多种防 web 扫描能力，防止攻击者通过扫描发现 Web 网站中的缺陷从而发起精确攻击，至少包括如下能力：防爬虫、防止 CGI 和漏洞扫描等，并支持阻断扫描行为和并记录日志，系统支持设置至少 4 个级别的扫描容忍度/扫描敏感度，方便安全管理者采用不同安全级别的行为控制；”

变更为：3.系统需具有多种防 web 扫描能力，精确防止通过

扫描发现 Web 网站中的漏洞，并支持阻断扫描和记录日志。

（九）原“7、WEB 应用防火墙 3.应具备 Web 恶意扫描防护的检测与防御能力，专利级别防护能力；”

变更为：7、WEB 应用防火墙 3.具备 Web 恶意扫描防护的检测与防御能力；

（十）原“10、工业威胁检测设备 5.支持对加密流量进行解密及还原：(HTTPS 证书支持 SSL3.0，TLS1.0/1.1/1.2)；支持 Modbus、S7、OPC、IEC104、IEC61850 等常用工控协议支持深度解析，审计粒度支持五元组、设备 id、类型、时间、控制点位、控制命令、控制值等；”

变更为：10、工业威胁检测设备 5.支持对加密流量进行解密及还原；支持 Modbus、IEC104 等常用工控协议的深度解析。

（十一）“8、日志审计设备 ”**增加条款**“8.支持交互式事件分析，支持多种方式查询。”

（十二）原“●网络安全综合实训平台：二、各模块技术参数要求：（一）培训管理系统：14.★能力评估：能力评估依据学员在考核、综合训练、单兵训练、学习方向等多因素的条件下，进行人员能力画像评估其安全能力的强弱项，可以根据强弱项进行发展方向的推荐和能力补足。”

现变更为：删除“★”条款。14.★能力评估：能力评估能

够依据学员在考核、学习、实训等多因素的条件下，对学员进行能力评估画像。

（十三）“●网络安全综合实训平台：（二）竞赛管理系统 c.★支持离线数据包分析功能，支持离线数据包流量信息统计分析，包括：流量大小、会话数统计、数据包统计、协议占比、TOP 主机等；支持协议元数据解析，可按照元数据字段信息进行模糊、精确检索；支持统计分析流量会话信息；支持基于情报和特征信息的回溯分析，可快速发现离线数据包中的攻击行为；”

现变更为：删除本条“★”条款。

（十四）原“●网络安全综合实训平台：12.实体设备管理 a.在场景构建过程中，支持虚实结合网络仿真技术，可外接(加入列表里的硬件设备)等实体网络设备以及用户自有实体 PC 节点。”

现变更为：12.实体设备管理 a.在场景构建过程中，支持虚实结合网络仿真技术，可外接实体设备节点。

（十五）原“2.安全意识互动体验工具箱 二、设备功能模块要求：1. ★多维度风险模拟：工具箱应能模拟恶意脚本执行、硬件插件漏洞利用、电磁干扰攻击、无线信号窃取、移动设备入侵办公网络、工业物联网络等真实网络攻击场景，以提供学员全面的网络安全风险体验。”

现变更为：删除本条“★”条款。

（十六）原“5.★与实训平台协同：工具箱应无缝对接网络安全实训平台，实现课程内容、实训操作、学习进度等信息的共享与同步。”

现变更为：5.与实训平台协同：工具箱应对接网络安全实训平台，实现课程内容、实训操作、学习进度等信息的共享与同步。

（十七）原“威胁检测设备 3.支持多数据关联展示，首页支持选择固定时间周期进行展示，包含：昨天、今天、最近 7 天、最近 15 天四个维度周期进行选择展示网内态势；展示的态势详情包含，ATT&CK 攻击矩阵对应战术，告警事件发展趋势统计，同时告警趋势应包含：高、中、低、无威胁四个等级，支持汇总曲线呈现；支持攻击、受害地址 TOP 汇总统计，并支持数据下钻；支持首页设备运行状态监控，支持监控内容至少包含：运行时间、CPU 利用率、内存利用率、磁盘利用率；支持监控接入流量，支持流量汇总呈现同时支持单接口呈现，确定网内对应区域流量趋势，保证网内流量趋势稳定；”

现变更为：威胁检测设备 3.支持多数据关联展示，支持选择按实践周期展示，展示至少包含告警事件，趋势统计等，同时告警趋势应包含：高、中、低、无威胁四个等级，支持可视化展现；支持攻击、受害地址排名汇总统计；支持设备运行状态监控；支

持监控接入流量，支持显示流量汇总和单接口流量；

（十八）原”★演示分值设定≥5 分的项目，如投标人未提供演示或提供演示但最终得分低于演示分值 50%（含）的，按无效投标处理”。

现变更为：本条删除。

（十九）原“5.竞赛管理系统（1 套）：赛前管理:用户可通过赛前管理模块组建一场竞赛，并可设定竞赛的名称、logo、参赛队、赛题等信息。赛中管理:管理员可以对正在进行的竞赛进行管理。管理员可以通过赛中管理模块发布公告、管理竞赛虚拟机状态。赛后管理:管理员可以对已经完成的竞赛进行管理。管理员可以通过赛后管理模块浏览竞赛最终排名。提供 200 道 CTF 题目，题目类型包含：安全入门、数据隐写、取证分析、逆向分析、编程技术、Web 安全、密码学等。提供 20 道 AWD 题目，题目知识点涉及：代码审计、漏洞利用、漏洞修补、SQL 注入、文件遍历、爆破、溢出、后门的发现、利用、隐蔽等。提供不少于 5 套综合渗透靶机，每套不少于 2 台靶机，模拟真实网络环境的网站或应用场景，难度分别是容易、中等、较难，知识点涉及近两年国内网典型的系统与应用层面漏洞。提供 20000 道理论题目，包含安全管理、安全技术两个方向的知识点。”

变更为：5.竞赛管理系统（1 套）：赛前管理:用户可通过赛

前管理模块组建一场竞赛，并可设定竞赛的名称、logo、参赛队、赛题等信息。赛中管理:管理员可以对正在进行的竞赛进行管理。管理员可以通过赛中管理模块发布公告、管理竞赛虚拟机状态。赛后管理:管理员可以对已经完成的竞赛进行管理。管理员可以通过赛后管理模块浏览竞赛最终排名。提供不少于 200 道 CTF 题目，题目类型包含：安全入门、数据隐写、取证分析、逆向分析、编程技术、Web 安全、密码学等。提供不少于 20 道 AWD 题目，题目知识点涉及：代码审计、漏洞利用、漏洞修补、SQL 注入、文件遍历、爆破、溢出、后门的发现、利用、隐蔽等。提供不少于 5 套综合渗透靶机，每套不少于 2 台靶机，模拟真实网络环境的网站或应用场景，难度分别是容易、中等、较难，知识点涉及近两年国内网典型的系统与应用层面漏洞。提供不少于 20000 道理论题目，包含安全管理、安全技术两个方向的知识点。

(二十)原“11.漏洞库管理 b.漏洞库中整合近年来的 CVE 漏洞，不少于 10W 个 POC，附带 poc，教员或管理员亦可通过页面上传其它漏洞，打造漏洞学习平台。”

现变更为：11.漏洞库管理 b.漏洞库中整合近年来 CVE 漏洞，不少于 10 万个 POC，教员或管理员亦可通过页面上传其它漏洞，打造漏洞学习平台。

（二十一）“3、防火墙”增加条款“为保证竞赛演练溯源功

能，需支持 payload 信息数据回溯功能。”

（二十二）“3、防火墙”增加条款“需具备 SDWAN 双边加速、链路复制等功能。”

评分标准现变更为：

评分项目		分数	评分标准
商务部分	投标报价	30	评标基准价 C=所有有效标书投标报价(或最终价格)中的最低投标报价。最终报价： 1、对于小型和微型企业制造的货物(服务)，给予小型和微型企业包括相互之间组成的联合体的产品 10% 的价格扣除，扣除后的价格为最终报价 2、大中型企业和其他自然人、法人或者其他组织与小型、微型企业组成的联合体，联合体协议中约定，小微企业的协议合同金额占比 30% 以上的，给予 0%的价格扣除，扣除后的价格为最终报价 报价得分 = 评标基准价÷（投标报价或者最终价格）×满分

	质保期	4	质保期在满足招标文件的基础上，每增加1年加2分，该项最多得4分(以商务响应表为准)。
	节能、环保	5	产品具有市场监管总局确定的认证机构出具的、处于有效期之内的节能产品、环境标志产品认证证书。加分计算方法是：“节能、环保产品”优采加分：加分=5×[所投“节能环保产品”（政府强制采购节能产品除外）中的产品价格在投标报价中所占比例],总计最高加5分。若所投产品同时具有节能产品认证证书和环境标志产品认证证书的，则应当优先于只具有一种认证证书的进行优采加分，不能重复加分。 开标时，须同时提供市场监管总局关于发布参与实施政府采购节能产品、环境标志产品认证机构名录的公告（附认证机构名录）和市场监管总局确定的节能产品、环境标志产品认证机构出具的、处于有效期之内的节能产品、环境标志产品认证证书电子文档，否则不得

				分。
技术部分	响应情况	基本分	5	基本分为5分，实质性条款有1条不满足的为无效投标。
		负偏离	0	非实质性条款每出现一条负偏离扣除基础分1分，扣完基础分为止。
	现场演示		8	供应商进行不超过5分钟的现场演示，并对实训平台的能力模型、能力评估、多种实体设备接入和快速构建虚实网络拓扑功能主要功能进行现场演示。 根据投标人提供的材料详实情况、系统演示进行综合评审。满足技术要求，与招标人实际情况贴合紧密，适配性强，保障性强得8分；技术演示内容存在细微瑕疵，但整体符合招标人实际情况，适配性、保障性较强得4分；与技术要求存在偏差，与招标人实际情况存在差距，适配性、保障性一般得2分；未准备相关内容不得分。投标人于本项目后期交付成果的功能、内容不得低于本次演示质量。 注：演示形式为现场演示，须采用真

			实软件系统进行功能性演示,如采用 PPT、动画、视频等其他方式演示则不予认定。
	产品保障	4	为保障信息系统建设能力,具备国家信息安全测评信息安全服务资质(安全工程类三级及以上）得 2 分，具备国家信息安全测评信息安全服务资质(安全工程类三级）（不含三级）以下得 1 分，没有不得分，须提供证明材料的原件扫描件。 为保证教学实训贴合真实网络环境，本项目内的防火墙、入侵防御设备、威胁检测设备等设备能够进行联动，提供证明材料得 2 分，不提供不得分。
	项目实施方案	10	项目实施方案包括整体实施方案、供货方案、进度安排、安装调试方案。满分 10 分。 整体实施方案内容全面、措施得当得 4 分，方案内容相对全面、措施相对得当得 2 分，方案内容不全面、措施不得当不得分。 供货方案内容全面、措施得当得2分，

			方案内容相对全面、措施相对得当得1分，方案内容不全面、措施不得当不得分。 进度安排得当得2分，进度安排相对得当得1分，进度安排不得当不得分。 安装调试方案内容全面、措施得当得2分，方案内容相对全面、措施相对得当得 1 分，方案内容不全面、措施不得当不得分。
	应急组织措施	10	根据投标人针对本项目特点提出的应急保障体系、保障措施以及具体方案等进行评价：应急保障措施合理得当、应急响应迅速、应急保障全面的得10分。应急保障措施相对合理、应急响应较为迅速、应急保障较为全面的得6分。应急保障措施一般、应急响应一般、应急保障一般的得 2分。没有此项内容的不得分。
	培训方案	12	投标人提供的培训计划和培训方案（培训对象、培训时长、培训内容、培训人员、培训系统分类等）内容安排详实明确，流程清晰合理，且能够提供多人次的

			企业级信息安全高级认证培训，得12分；培训内容简单，流程基本合理，能提供多人次企业级信息安全高级认证培训的，得6分；培训内容粗略，流程简单，无法提供多人次企业级信息安全高级认证培训得3分，培训内容、培训流程不符合项目使用得1分。投标人未提供本项内容的，不得分。
	售后服务	12	技术人员配置、服务响应时间完善，得3分，技术人员配置简单、服务响应时间不完善得1分。（提供常驻地行政部门出具的社保证明原件电子扫描件或社保网站打印的社保证明原件电子扫描件，未提供或者提供不全的不得分）； 有详细的售后服务方案、质量保证期内产品维护措施，得9分，售后服务方案、质量保证期内产品维护措施基本完整得5分，售后服务方案、质量保证期内产品维护措施不完整且不符合项目实际情况得1分。

原开标时间:2024/8/22 9:30:00 变更后时间:2024-09-04 09:30:00,原开标室:三楼 8 号开标室(312 室)变更后开标室:三楼 3 号开标室(304 室)

FYQ 已重新上传，其他内容不变，投标人应持续密切关注本项目公告页面，更正公告一经发出，视为投标人已收到。

本公告作为招标文件的组成部分之一，与招标文件或招标公告不一致的部分以本公告为准。

三、其他补充事宜

无

四、凡对本次公告内容提出询问，请按以下方式联系

1.采购人名称: 青岛工程职业学院　地址：山东省青岛市城阳区上马街道龙翔路中段

联系方式：0532-58266682

2.代理机构名称：青岛青招招标有限公司　地址：青岛市崂山区深圳路 163 号 1109 室

联系方式：0532-88913680

3.项目联系人：　代玉芬　联系方式：0532-88913680