

太原城市职业技术学院

信息安全实训平台、教学入侵防御系统
等设备采购项目采购合同

合同编号: 11N7572978702023401



太 原 市 建 筑 业 学 校 学 生

学 习 人 员 考 试 合 格 实 际 安 全 考 试

考 试 成 果 目 录 考 试 成 果 考 卷



太原城市职业技术学院信息安全实训平台、教学入侵防御系统 等设备采购项目采购合同

合同编号：11N7572978702023401

需方：太原城市职业技术学院

供方：山西君焱锐圣数字网络有限公司

供方在山西德融工程咨询有限公司组织的太原城市职业技术学院信息安全实训平台、教学入侵防御系统等设备采购项目项目公开招标采购中成交，经双方协商一致，签订本合同。

一、货物条款

供方向需方提供以下货物

序号	名称	品牌	型号	单价	数量	合计
1	教学实验防火墙	天融信	NGFW4000-UF	18500	4台	74000
2	教学入侵防御系统	天融信	TopIDP 3000	51000	4台	204000
3	教学实验WEB应用安全防护系统	天融信	TopWAF	42240	4台	168960
4	运维安全审计系统	天融信	TopSAG	48200	1套	48200
5	日志收集与分析系统	天融信	TA-LOG	47980	1套	47980
6	脆弱性扫描与管理系 统	天融信	TopScanner 7000	67580	1套	67580
7	教学实验上网行为管 理系统	天融信	TopACM	12650	4套	50600
8	※信息安全实训平台	天融信	TSP8001-ADS-SP800	513000	1套	513000
9	攻防对战终端	宝德	PR2710P	45860	1套	45860
10	网络安全实训工作台	森华众	定制	3890	8套	31120

11	教学控制台	森华众	定制	43470	1 套	43470
12	教学设备管理系统	噢易云	噢易 OSS 系统 V8	12490	1 套	12490
13	电子教室模块	噢易云	噢易多媒体网络教室软件 V9.0	8450	1 套	8450
14	合计					1315710

以上设备具体技术指标见合同附件，合同附件为本合同不可分割部分。

二、合同总金额：

人民币（大写）：壹佰叁拾壹万伍仟柒佰壹拾元整

（小写）：¥1315710

合同总金额包含包装、仓储、运输、装卸、安装调试、税费、保险费、供方应当提供的伴随服务/售后服务费用以及验收合格之前与质保期内备品备件发生的所有费用。此价格为合同执行不变价，不因国家政策变化而变化。

三、合同资金支付

资金支付条件及方式：需方付款前，供方应开具符合需方要求的增值税普通等额发票，否则需方有权顺延付款期限且不承担逾期付款责任。项目验收合格后，一次性付清合同全款。

履约保证金：

供方在签订合同前向需方提交合同总金额5%（不得超过合同总金额的5%）的履约保证金。验收合格之日起180日历天后，一次性足额无息返还。

四、售后服务及承诺

供方向需方承诺：

- 1、本项目所有产品质保期3年；
- 2、供方派遣技术人员进行现场设备的操作指导；
- 3、售后服务培训要求：
 - 1) 供方提供教学实验系统配套教学资料。
 - 2) 供方提供主流的网络安全技术培训，例如攻防、渗透测技术、网络安全前沿技术、等保合规、数据安全、应急响应等课程。
 - 3) 供方提供3年安全设备课程资源、网络安全攻防演练实训项目。

4) 供方免费提供两期（寒暑期）教学培训，每期历时5天，培训内容为主流的网络安全技术、例如攻防、渗透测技术、网络安全前沿技术、等保合规、数据安全、应急响应等课程。

五、交货

1. 交货期限：签订合同50日历天内完成
2. 交货地点：太原市兴华街3号

六、交验

1. 验收由需方组织进行，必要时可邀请国家认可的质量检测机构参加验收工作，需方验收供方所交的货物后要制作填写“合同履行情况验收报告”。验收结果须供需双方共同确认。

2. 交货时供方就所投产品提供生产厂家完整的随机资料，包括完整的使用手册、产品说明书等。

3. 供方所供商品包装需符合《商品包装政府采购需求标准（试行）》，快递包装需符合《快递包装政府采购需求标准（试行）》，必要时需方可要求供方提供商品包装、快递包装的检测报告。

4. 供方交付产品中的软件应无知识产权纠纷，若出现知识产权纠纷等法律问题，由供方自行承担。

5. 需方要按照谈判文件中的验收标准来进行验收，按照与履约验收挂钩的资金支付条件及时间执行。

七、需方责任

1. 及时办理付款手续。不得以机构变动、人员更替、政策调整等为由延迟付款，不得将谈判文件和合同中未规定的义务作为向供应商付款的条件。

2. 协调各系统厂商接入服务平台的沟通事宜。

3. 负责提供工作场地，协助供方办理有关事宜。

4. 对合同条款及价格负有保密义务。

八、供方责任

1. 保证所供货物均为响应文件承诺的，符合相关质量检测标准，具有该产品的软件证书。

2. 保证售后服务，严格依据响应文件及相关承诺，进行保修、维护等服务。

九、违约责任

1. 需方无正当理由逾期支付货款的，每逾期一日向供方偿付合同款总额（0.1%）的违约金，逾期付款超过（15）日，供方有权解除合同，届时需方向供方退还已收到的货物，并赔偿由此给供方造成的全部经济损失。

2. 供方所交的货物品种、型号、规格、质量、商品包装、快递包装不符合合同规定标准，需方有权拒收。同时，供方向需方支付合同款总额（1%）的违约金，如违约金不足以弥补需方损失的，还应当承担赔偿责任。

3. 供方不能交付货物时（逾期交付货物达10天的，视为不能交付货物），供方除正常支付逾期交货违约金外，还需向需方偿付合同款总额（1%）的违约金。

4. 供方逾期交付货物时，每逾 1 日供方向需方偿付合同款总额（0.1%）的滞纳金。逾期交货超过 30 天后，需方有权决定是否继续履行合同。

5. 供方在履约中，未履行供方责任的，需方有权向供方追究责任。

6. 供方在履约中，未完全履行供方责任的，需方保留向供方追究责任的权力。

7. 因需方错告或变更到货地点而给供方造成的损失，由需方负担。

8. 因需方原因导致合同变更、中止或者终止政府采购合同的，需方应当对供方受到的损失予以赔偿或者补供，贴偿或者补偿金额：（2%）。

十、不可抗力

供需双方的任何一方由于不可抗力的原因不能履行合同时，应及时向对方通报不能履行或不能完全履行理由；在取得有关主管机关证明以后，允许延期履行、部分履行或者不履行合同，根据情况可部分或全部免于承担违约责任。

十一、争议解决

供需双方在执行合同中发生争议，应通过协商解决。如协商不成，双方均可向需方住所地有管辖权的人民法院提起诉讼。

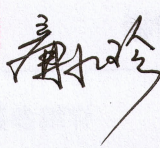
十二、合同生效及其他

1. 合同由供、需双方法定代表人或授权代表签字并加盖公章或合同专用章之日起生效。

2. 本合同一式（肆）份，双方各执（贰）份。

3. 合同执行过程中出现的未尽事宜，双方在不违背合同和谈判文件的前提下协商解决。协商结果以“纪要”形式供需双方签字盖章确认，作为合同附件，与合同具有同等效力。

需方(章): 太原城市职业技术学院

法定代表人/授权代表: 

地址: 太原市兴华街3号

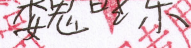
电话: 0351-5633000

开户银行: 建设银行太原市新建路支行

账号: 14001815508050012722

日期: 2023.11.23

供方(章): 山西君焱锐圣数字网络有限公司

法定代表人/授权代表: 

地址: 太原市小店区平阳路65号平阳景苑9号楼1001B一楼

电话: 0351-7673505

开户银行: 中国建设银行股份有限公司太原王村支行

账号: 14050182740800001083

日期: 2023.11.23

本合同的签署地: 太原市

附件：

产品技术指标

序号	产品名称	详细参数
1	教学实验防火墙	<p>性能规格 1U, 内存 4G, 6 个千兆电口, 防火墙吞吐 10Gbps, 并发连接 350 万; 含 3 年攻击知识库、专业版病毒知识库及应用知识库升级服务;</p> <p>功能</p> <ol style="list-style-type: none">1. 具有心跳接口物理备份及二级心跳接口功能。2. 支持基于 IPv6 的应用层检测 (FTP\TFTP)、病毒过滤、URL 过滤、ADS、IPS 检测。支持基于多元组的一体化流检测机制, 一次检查同时覆盖多个安全引擎的检查需要, 无需多个引擎多次检查。3. ★为提高链路聚合可靠性, 提供多种链路聚合负载均衡算法。4. 内置用户身份管理系统, 支持本地认证、证书认证及免认证等方式, 同时支持 RADIUS、LDAP、TACACS 等多种第三方外部认证设置。5. 检测与防御流量型 DDOS 攻击、应用型 DDOS 攻击、DOS 攻击、非法协议攻击四大类拒绝服务攻击。6. 包含 10 个终端威胁防御系统授权, 与防火墙实现主机联动准入。7. 具有资源对象、网络管理、访问控制、用户管理、带宽管理、流量控制、会话管理、应用识别、病毒防御、入侵防御、WEB 分类过滤、内容过滤、审计报表等各种功能虚拟化。8. ★支持对单条访问控制策略进行最大并发连接数限制。9. 支持黑名单功能, 可设置多个对象条件。10. 安全操作系统采用冗余设计, 出于安全性考虑, 多系统需在设备启动过程中进行选择不得在 WEB 维护界面中设置系统切换选项。11. 支持以下报警类型: 如邮件报警、声音报警、NETBIOS 报警、SNMP 报警、控制台报警。12. 随机提供 1 个同品牌的移动存储备份系统(硬件形态), 可对本系统的日志、安全日志实时加密存储、备份恢复, 即插即用, 无需配置, 满足网络安全法对日志存储时间相关要求。
2	教学入侵防御系统	<p>性能: 1U, 6 个千兆电口, 1 个扩展槽位, 整机吞吐率: 4Gbps, IPS 吞吐率 1.5Gbps; 含攻击知识库 3 年升级服务许可, 产品为专业级入侵防御系统, 非防火墙开模块或其他技术实现方式。</p> <p>功能:</p> <ol style="list-style-type: none">1. 采用在线部署方式, 能够实时检测和阻断包括溢出攻击、RPC 攻击、WebCGI 攻击、拒绝服务攻击、木马、蠕虫、系统漏洞等网络攻击行为, 可以有效的保护网络 IT 和服务资源。2. 支持攻击统计展示, 包括检测报文总数、发现攻击报文总数、以及攻击总数与检测总数百分比。3. 可以查看当前连接信息, 如当前连接正在建立, 正在握手还是已经拆除、当前连接所使用的协议、连接的源/目的地址和

		<p>端口号、该连接是否应用源 NAT/目的 NAT 策略、该连接建立过程中源地址发送的数据报文个数、目的地址发送的数据报文的个数等信息。</p> <p>4. ★具有攻击报文取证功能,检测到攻击事件后将原始报文完整记录下来,作为电子证据。</p> <p>5. 支持自定义规则,并且自定义规则库可以导入导出。</p> <p>6. 支持对设备接口流量的阈值进行设置及报警。</p> <p>7. 系统支持 DNS 异常包及 DNS Flood 攻击防御;系统支持 DHCP 异常包及 DHCP Flood 攻击防御;系统支持 CC 攻击防御,且能够对 Web 服务器上的指定 URI 页面进行防护设置;系统支持 DDoS 机器人自学习功能,学习时间可设置。</p> <p>8. 系统能够根据数据内容而非端口智能识别包括 P2P、即时通讯、电子商务、股票交易、网络游戏、网络电视、移动应用等在内的多种应用。</p> <p>9. 支持对应用协议的连接数和流量的报警信息进行展示,红色表示有报警,绿色表示没报警。</p> <p>10. 支持查看任意接口接受和发送报文字节大小分布图。</p> <p>11. ★支持查看近 24 小时、一周、一个月内历史系统性能件事情况、连接数变化情况及新建会话速率情况。</p> <p>12. 支持登陆界面图形验证码功能,防止管理员账号被暴力破解。</p> <p>13. ★支持提供同品牌的无线入侵检测探针,支持无线自动扫描分组;支持检测并抑制干扰 AP、流氓 AP;支持黑白名单、开放区域;支持动态黑名单功能;支持 AP 名称、MAC、位置、状态等扫描发现;支持扫描周期、扫描时长参数调整。</p> <p>14. 随机提供 1 个同品牌的移动存储备份系统(硬件形态),可对本系统的日志、安全日志实时加密存储、备份恢复,即插即用,无需配置,满足网络安全法对日志存储时间相关要求。</p>
3	教学实验WEB应用安全防护系统	<p>性能: 1U 机箱,千兆电口 6 个(支持 1 对 Bypass),单电源;网络层吞吐 6.5G,并发连接 500W;含 3 年特征库升级服务。 产品为专业性 WEB 应用防火墙硬件设备,而非下一代防火墙、UTM 类设备集成的 WEB 防护功能。</p> <p>功能:</p> <p>1. 支持虚拟线无论任何网络环境可强制数据从一个接口转发到另一个接口。</p> <p>2. 代理模式下支持 HTTPS 流量解析,支持 SSL 卸载功能。</p> <p>3. 能识别和阻断 SQL 注入攻击, Cookie 注入攻击,命令注入攻击;应能识别和阻断跨站脚本(XSS)攻击。</p> <p>4. ★支持扫描防护:通过人机识别方式,进行恶意扫描智能检测;支持扫描防护阈值设置和扫描 IP 的阻断周期设置。</p> <p>5. 支持虚拟补丁功能,支持导入 appscan、w3af 等第三方扫描器的扫描结果生成 WAF 的规则,对此类网站漏洞直接防护。</p> <p>6. 支持基线学习,可以自动学习用户 http 正常流量阈值模型,并给出推荐阈值配置项。</p> <p>7. 支持 WEB 缓存, URL 重写, HTTP 压缩等应用交付功能。</p> <p>8. Web 界面直观查看 WAF 扩展卡、接口、USB 口、管理口、HA 口及业务口的运行状态;可以实时查看设备并发连接数、每秒事务数及 HTTP 应用层吞吐率等数据并以可视化的方式展示。</p> <p>9. ★支持日志敏感信息脱敏,记录日志时将敏感数据替换为某个特定字符。</p>

		<p>10. 支持账号策略自定义，支持定义允许最大登录失败次数、密码错误账号锁定时间、最大在线管理员数、对其他非法在线管理员强制下线、防管理员账号暴力破解。</p>
4	运维安全审计系统	<p>功能</p> <ol style="list-style-type: none"> 1. 支持集中化账号管理、高强度认证加固、细粒度授权控制和多形式审计记录，使内部人员和第三方人员的操作处于可管、可控、可见、可审的状态下，规范运维的操作步骤，避免误操作和非授权操作带来的隐患，有效保障组织机构的服务器、虚拟机、网络设备、安全设备、数据库、业务系统等资产的安全运行和数据的安全使用。 2. 支持组定义类型（用户、资源、综合）便于管理和快速查找。 3. 完整的用户帐号生命周期管理，实现帐号的创建、维护、修改、删除的集中管理；自定义用户类型，基于针对用户类型进行用户地址策略。 4. 主帐号支持从 AD 域内抽取，方便快捷建立主账号。 5. 用户有效期定义，针对临时用户或者短期用户可以建立有效期用户，过期后自动注销。 6. 支持资源从账号的管理，系统具有各种资源类型驱动器能够将资源上的账号进行自动抽取、推送及属性的变更等。 7. 定期检查平台存储的设备账号密码与设备实际密码是否匹配，以便进校验密码一致性，提高设备的安全性避免密码混乱无法登陆现象发生。 8. 资源授权模式基于岗位授权，岗位上绑定资源账号，这样授权可迁移、授权粒度更细；并可针对岗位设置相关安全策略。 9. 自身提供证书认证服务，也可与第三方 CA、动态令牌、生物识别、短信认证等方式进行结合。支持组合认证，提高访问的安全性。 10. ★平台在网络设备的认证协议上不仅支持 RADIUS 和 TACACS+协议，而且产品系统自身可以作为 RADIUS 和 TACACS 服务器。 11. 支持网络设备的脚本自动化执行，脚本编辑可以支持文本框方式和交互方式。 12. 支持对 RDP 实时会话的锁定和解锁，并可以在锁定解锁时发送即时通讯消息。发现危险操作可立即进行锁定操作。 13. ★审计日志可以采用 syslog 形式分类外发，可以分为系统类日志，内部审计日志，行为审计日志，违规命令日志，违规登录日志等。 14. 支持授权审批功能，即针对不属于自己岗位的资源，需要临时运维操作进行临时申请审批，申请中包含需要临时登录的资源，账号，登录时间范围等信息。 15. 随机提供 1 个同品牌的移动存储备份系统（硬件形态），可对运维安全审计系统的日志、安全日志实时加密存储、备份恢复，即插即用，无需配置，满足网络安全法对日志存储时间相关要求。 16. 运维工具箱： <ol style="list-style-type: none"> 一、硬件： <ol style="list-style-type: none"> 1、桌面型设备，支持透明网桥模式、路由模式、NAT 模式、旁路分析模式、混合模式等多种模式部署，具备管理接口*1，千兆电接口*3，USB 2.0*2；单直流电源； 二、软件： <ol style="list-style-type: none"> 1、★关联运维分析功能：可根据设置条件将不同应用、流量

		<p>方向、源目的 IP/IP 段、终端类型等流量镜像至指定网络接口，与第三方审计设备联动，便于用户做精细化、个性化的数据分析；</p> <p>2、★支持缓存牵引，可以根据策略将视频或大流量下载用户牵引到指定的缓存，提升用户体验并节省带宽；</p> <p>3、支持网络故障定位功能，对网络中各种应用的时延进行检测，各种协议时延要求包括客户时延、服务时延、应用时延等；（我公司提供视频演示）</p> <p>4、支持网络优化控制功能，可根据源 IP、目标 IP、访问域名、所在线路等组合条件实现对域名访问的 QPS 速率做总量控制和单 IP 控制以及 DNS QPS 策略前后趋势图，可以显示一天，一周和一月趋势；（我公司提供视频演示）</p> <p>5、支持 IPv6 相关日志运维分析和故障定位；</p> <p>6、支持将数据库表结构开放，以方便后期对接其他数据分析系统；</p> <p>7、★支持创建包转发策略，策略内容包括：策略标识、策略备注、源接口、用户组、VLAN、TTL、源地址、源端口、外网端口、传输协议、应用协议、DSCP、执行动作（包转发、IWANSR）、下一跳；（我公司提供视频演示）</p>
5	日志收集与分析系统	<p>功能</p> <p>1. 支持单级部署；支持代理分布式部署采集日志。</p> <p>2. 数据存储能力：压缩加密存储，压缩比 10:1；日志存储 10000 条/M。</p> <p>3. 支持对日志流量非常大但是日志重要程度低的 syslog 类型日志源进行限制接收速率，降低对系统资源的占用，保障重要日志的收集，支持限制速率设置为 1000 条/秒、3000 条/秒和 5000 条/秒等。</p> <p>4. 支持安全设备、网络设备、中间件、服务器、数据库、操作系统、业务系统等日志对象的日志数据采集。</p> <p>5. 支持日志转发给第三方系统平台，支持设置多个日志转发 IP 地址，支持转发格式化日志或仅转发原始日志。</p> <p>6. 支持存储空间图像化、动态监控，超过阈值进行告警。支持从存储空间、存储时间多维度进行动态监控。</p> <p>7. ★支持根据设备重要程度设置独立设置每个被采集源的数据存储时间为 1 个月、3 个月、6 个月和永久保存等参数。</p> <p>8. 系统支持智能报表创建，每添加一个日志源，系统自动分析日志源类型进行相应报表创建，无需人工干预，报表和资产一一对应。</p> <p>9. ★支持为不同类型日志设置不同的查询条件和显示条件。</p> <p>10. 支持主动、被动相结合的数据采集方式；支持支持多种方式进行数据采集；支持通过 Agent 采集日志数据。</p> <p>11. 支持自定义统计报表报告，支持 PDF、Word、Execl、Html 等方式导出报表，支持实时报表、计划报表。</p> <p>12. 支持数据投屏展示，以动态的形式展示数据流向轨迹，包括 SYN 源目的、SSDP 源目的、NTP 源目的、MSDS 源目的、热点应用、未知协议组、DNS 用户、新增域名访问、资产数，用户数、域名数、连接趋势、热点资产、热点用户、热点应用、热点域名、资产时延。</p> <p>13. ★支持会话日志，会话日志包含设备编号、接口、访问时间、源地址、目标地址、NAT 地址、账号信息、域名、协议类型、七层协议名称、流量、运营商、地理位置等多个元素；同</p>

		<p>时采用 1:1 的日志输出；</p> <p>14. 对网络中各种应用的时延进行检测，各种协议时延要求包括客户时延、服务时延、应用时延等。</p>
6	脆弱性扫描与管理系统	<p>功能</p> <ol style="list-style-type: none"> 1. 采用经过系统加固的专有操作系统。 2. 支持 IPv4/IPv6 双协议栈地址场景漏洞扫描。 3. 支持资产自动发现功能，支持利用历史扫描过程中所发现的在线主机信息，来添加资产。 4. 产品漏洞库涵盖目前的安全漏洞和攻击特征，漏洞库具备 CVE、CNNVD、CNCVE、CNVD、BUGTRAQ 编号。 5. ★产品扫描信息包括主机信息、用户信息、服务信息、漏洞信息等内容。 6. ★支持主机存活探测，探测方式支持 ARP、ICMP ping、TCP ping 及 UDP ping 等类型。 7. 支持每台主机最大并发检测数设置，支持单个任务并发扫描数设置。” 8. 支持资产设备漏洞查询，支持根据节点名称、设备名称、设备 IP、设备管理员、设备操作系统、风险等级、漏洞名称、端口号、检测时间段等查看设备漏洞情况，并保存导出。 9. ★为确保报表安全，支持导出报表加密功能。
7	教学实验上网行为管理系统	<p>功能</p> <ol style="list-style-type: none"> 1. 支持将多个以太网物理端口捆绑成一条逻辑端口(即将多个端口捆绑成一个逻辑的端口以增加带宽，同时增加链路备份)支持基于 mac、轮循、主备、哈希、广播、802.3ad、发送自适应、双向自适应等等多种负载方式。 2. 支持 l2tp、gre vpn、pptp、ipsec。 3. 支持 DNS 链路健康检查算法；支持 ICMP 链路健康检查算法；支持 TCP 链路健康检查算法；支持自定义的链路健康检查算法； 4. 支持管理员通过 Radius 认证后才能登录设备。 5. 提供图形化排障及抓包工具，便于管理员排查策略错误等故障； 6. 能够实时展现每个接口接收发送流量、字节数、包个数以及错误、丢弃、帧冲突个数。 7. 支持基于策略方向、源地址、目的地址、服务、生效时间的安全策略。
8	※信息安全实训平台	<p>本实训平台包含攻防对抗平台-管理模块、攻防对抗平台-考试模块、攻防对抗平台-学习模块、域内核心转发平台（1 台）、域内转发平台（4 台）、域间转发平台（1 台）、KVM 切换器（1 台）以及集成服务等组成。</p> <p>实训平台硬件参数及性能： 设备形态：2U 机架式结构；管理接口：3*100/1000Base_T，2*USB 接口；处理器：双路 XEON 4210R*2（双路十核 20 线程）；内存：DDR4 32G*4 内存，硬盘：3 * 480G SSD + 5* 2T HDD 存储；RAID 卡：4GB SAS 8 口（断电保护）；电源双通道冗余电源；并发访问数量：单台设备并发访问数 200；并发虚拟机数量 50；支持集群部署。</p> <p>攻防对抗平台-管理模块：</p> <ol style="list-style-type: none"> 1. 支持使用用户账户名和邮箱两种方式登录； 2. 管理后台可以监控平台中虚拟机模板的总数、已开启虚拟机实例总数、总用户数与在线用户数、正在进行的比赛数等。

	<p>以及监控各节点硬件资源的使用情况，包括内存使用率、CPU使用率、硬盘使用率、剩余可用内存、每分钟系统负载等数据；</p> <ol style="list-style-type: none"> 3. 支持课程统计，其中包括：理论题数量、机试题数量、实验数量、课件数、漏洞数、知识点数、工具集数； 4. 支持人员管理，其中包括：用户创建/导入、用户删除、用户禁用与启用、用户权限分配等，支持团队管理，其中包括：团队创建、团队删除、团队成员添加与删除等； 5. 支持分权管理，支持超级管理员、教师、资料管理员、虚拟机管理员等角色，且超级管理员可创建角色，并根据实际需要为角色赋予相应权限； 6. 支持通过团队管理进行批量的分级管理，并可通过有效时间进行账号回收； 7. 支持对虚拟机管理，其中包括：导入虚拟机模板、开启虚拟机实例、关闭虚拟机实例、删除虚拟机模板，支持学员操作机管理等功能； 8. 平台提供的虚拟机支持通过 Web、Windows 远程桌面、Linux SSH 方式访问； 9. 支持实验管理，其中包括：实验添加、实验删除、实验编辑等，实验文档类型支持 PDF、html、markdown 等； 10. 支持对工具库进行管理，其中包括：对现有工具的编辑与上传工具到平台扩充工具库； 11. 支持对课件进行管理，其中包括：创建课件类别、对现有课件进行编辑修改、上传课件，课件类型支持 pdf、markdown、html、mp4 等； 12. 管理员可进行笔试题库管理、机试题库管理、知识点管理等功能； 13. 支持 CTF 管理，可对 CTF 题目的类型、标签、难度进行管理； 14. 支持上传虚拟机模板用于部署实验或竞赛考题； 15. 支持上传在研究中发现的新漏洞，不断完善漏洞库； 16. 支持查看所有学生错题记录； 17. 支持创建职业体系，规划学习路径； 18. 支持创建综合闯关训练，并能够查看学员闯关情况； 19. 支持创建经典赛事，让学员体验真实大赛的考题内容； 20. 直播、录播教学课堂管理，可管理学生学习课程权限，设置课程表、课程章节、课件下载、资料下载、课程实验、学员满意度调查内容； 21. 支持数据备份与恢复； 22. 支持实例类型编辑，可根据虚拟机类型配置资源，包括 CPU 核心数、内存大小、硬盘大小等； 23. 可对已有的实验环境或考题环境进行在线编辑，在线完成实验环境或考题环境的搭建与修改，修改完成之后可一键保存为模板，快速的完成实验或考题环境的搭建； 24. 提供系统公告功能，向所有学员发布课程学习计划调整或其他公告内容； 25. 学生学习情况管理：教师或管理员可查看学员的在线时长、累计积分，已学习知识点、课件、漏洞库、工具等数据； <p>攻防对抗平台-考试模块：</p> <ol style="list-style-type: none"> 1. 支持理论竞赛和实操竞赛； 2. 理论考核支持单选、多选、判断； 3. 理论考题 2000 道，支持题库自动生成，支持添加或批量导
--	--

		<p>入笔试题库；</p> <ol style="list-style-type: none"> 4. 理论竞赛支持根据设定的比赛开始时间进行比赛倒计时或根据选手进入比赛的时间进行比赛倒计时，理论竞赛，自动对未答题目进行标记。手动交卷时，如果存在未答题目，系统将会给出提示信息； 5. 实操竞赛支持机试实操 CTF、风险评估、应急响应、闯关等形式，支持个人赛和团队赛。； 6. 支持在同一场竞赛中添加多种竞赛模式，分数累加。； 7. 实操考题数量如下要求：机试实操考题 CTF10 套、风险评估考题 5 套、应急响应考题 2 套； 8. 支持题库管理（题库编辑、题库导入导出）、考试管理、考试人员管理、考试暂停等功能； 9. 支持竞赛倒计时功能； 10. 支持自动评分并进行实时排名； 11. 支持竞赛观摩，竞赛实时排名、得分展示等功能； 12. 支持成绩报表导出，导出数据包含“竞赛名称”、“选手名”、“得分”、“答对题目”、“答错题目”等条目； 13. 竞赛人员能够实时查看个人排名、得分情况、系统公告、比赛时间等相关比赛信息。 14. 支持经典竞赛，包含近几年各类竞赛真题，经典竞赛数量 4 场。 <p>攻防对抗平台-学习模块：</p> <ol style="list-style-type: none"> 1. 平台提供多种类型操作系统模板，管理员也可上传虚拟机模板至平台，扩充教学实训资源； 2. 覆盖 Windows 系统安全、Linux 系统安全、MySQL 数据库、SQLserver 数据库、Oracle 数据库等 20 类主要课程实验模块，实操环境标配 600 个； 3. 每个实验包含具体的实验目的，实验环境描述，实验详细步骤等介绍说明； 4. 平台提供 CTF 类教学和考试内容，覆盖 Web 安全（SQL 注入、XSS 跨站、文件上传、文件包含、代码审计）、Mobile 移动安全（apk 逆向分析）、取证分析（内存取证、数据恢复、日志分析）、逆向分析、密码学、PWN 等； 5. 包含安全运维、渗透测试、网络攻防、移动安全、安全开发、应急响应取证、代码审计等视频课件，课件数量 400； 6. 包含网络安全法、安全保密意识、信息安全管理、人员安全管理、第三方安全、拍照泄密防范、邮寄与快递安全、打印传真与复印安全、工作站电脑安全、桌面安全、移动媒介使用、信息资产保护、办公环境安全、物理访问安全、金融诈骗防范、网络钓鱼防范、电话诈骗防范、社会工程学防范、恶意代码防范、信息安全事件、个人信息保护、信息清除与销毁、数据备份与恢复、机密信息保护、公司信息披露、社交网络安全、公共场所安全、远程工作安全、差旅信息安全、移动设备安全、密码安全、无线安全、即时消息安全、浏览器及上网安全、文档安全、邮件安全、网络会议安全、网络法规遵循、信息安全职责、网络使用准则、常规安全知识等视频课件和互动课件，课件数量 300； 7. 包含中间件、数据库、CMS 等漏洞库分析库，漏洞分析库数量 200； 8. 提供仿真互联网系统漏洞靶机供教学实训使用，靶机数量 200；
--	--	--

	<p>9. 包含抓包工具、注入工具、嗅探工具、漏洞利用、提权工具、暴力破解、扫描工具、PE 工具、应急响应、数据恢复、后门检测、移动安全、信息隐写、文件分析、编程开发等工具使用教程和下载模块，工具数量 100；</p> <p>10. 支持闯关训练、自由组合训练、错题集中训练；</p> <p>11. 自由组合练习与错题回收训练支持查看正确答案和答题解析思路；</p> <p>12. 支持在线直播、录播课程，学员需仅批准后方可学习课程，可设置课程表、课程章节、课件下载、资料下载、课程实验、学员满意度调查，平台提供在线讨论、笔记、作业上传功能；</p> <p>13. 平台提供学员个人在线虚拟终端，供学员学习或实操；</p> <p>14. 支持用户自主设计网络拓扑，用户可以通过简单的拖放操作在网络拓扑编辑器的工作区中快速、方便的配置起自己的仿真网络，也可以对网络中网络设备的属性进行设置。用户还可以建立新的组件或修改已有组件，并支持保存为拓扑模板。拓扑制作过程中支持靶机、安全设备、路由器、交换机等设备进行拖拽式组建自定义拓扑；</p> <p>15. 支持排行挑战，学员可进行 CTF 的题目挑战并可在 CTF 排行榜中看到对应排行信息；</p> <p>16. CTF 挑战支持题目的搜索和筛选，题目筛选条件包括题目类型、题目标签、题目难度以及答题的状态，状态分为未挑战、挑战中和已挑战，类型、标签、难度后台可自定义；</p> <p>17. CTF 挑战支持随机挑战功能，学员可根据筛选的条件进行筛选后题目随机一题进行答题；</p> <p>18. CTF 挑战在答对题目后，支持挑战消息实时更新展示；</p> <p>19. 支持 CTF 挑战战力图鉴，为用户提供各个类型 CTF 题目答题数量的雷达统计图；</p> <p>20. 支持多种 CTF 排行，包括积分榜、挑战榜、爆肝榜，分别用于对用户答题得到的积分、解题数以及今日解题数进行排行；</p> <p>21. 可提供持续的课件升级；</p> <p>22. 支持学员进入下一实验时自动关闭上一实验所使用的虚拟机资源，避免资源浪费；</p> <p>23. 域内核心转发模块 1 个：48 个 10/100/1000M 自适应电口，4 个 1G/10G SFP+光口，1 个业务扩展槽，内置固化双风扇，2 个模块化电源插槽，含电源模块；</p> <p>24. 域内转发模块 4 个：24 个 10/100/1000M 自适应电口，4 个 1G/10G SFP+光口，固化交流电源和风扇；</p> <p>25. 域间转发模块 1 个：包括 28 个 GE 口，其中 4GE WAN 口（2 电+2 光电复用）、24GE LAN 口；1 个 Console/AUX 口，1 个 USB 口，1 个 SD 卡插槽，1 个精灵键，4 个 HSIC 模块插槽，固化 1 个 AC 电源；</p> <p>26. KVM 切换器 1 个：LED KVM 整合 LED 屏、超薄键盘、触摸鼠标板，集成在 1U 高度单元内，抽屉式安装方式，彻底解决空间不足的问题。采用高品质 A 级 17" TFT LED（无亮点），内置切换器可直接管理 8 台服务器；支持 1 本地用户和 1 远程用户在全球任何地方同时操作不同服务器，支持本地通道和数字通道之间的资源相互共享。多用户单控制端设置，提供 1 位管理员用户和最多 4 位普通用户，管理员可分别授权普通用户的用户名密码以及对服务器的操作、查看甚至屏蔽权限。所有传输数据皆以 SSL 256 位 安全加密，SSL 证书管理；</p>
--	---

		集成服务:我公司完成各个软硬件系统的相关的综合布线并完成室内空间隔断, 具体施工要求以甲方的现场需求为准。
9	攻防对战终端	<p>硬件:</p> <ol style="list-style-type: none"> 1. 标准 2U 高度, 机架式安装并配置导轨; 2. 处理器: 配置两颗可扩展处理器, 主频 2.2GHz, 每颗处理器 10 核心 20 线程 3. 内存: 128G DDR4 内存, 配置 16 个内存插槽; 4. 存储: 配置 2 块 480GB SSD 企业级硬盘和 5 块 2TB SATA 企业级硬盘. 5. 配置非集成 2G RAID 卡 (含超级电容), 支持 RAID 0\1\5\6\10\50 等; 6. 网络控制器: 配置双口千兆网卡, 具有负载均衡、链路汇聚及冗余特性, 可有效减少网络延迟; 支持 1 个 100M IPMI 专用远程管理网口, 可实现 KVM OVER IP 带外管理; 7. 配置一块双口千兆网卡和一块双口万兆网卡 (含模块) 8. 电源: 配置 1+1 冗余电源; 9. 安全模块: 可选配嵌入式生物指纹识别, 开机密码保护, 提高服务器管理安全性保护级别服务。
10	网络安全实训工作台	<p>产品生产工艺先进, 质量达到国家技术标准, 通过相关检测认证, 经久耐用, 以保护用户的投资和使用。采用环保板材, 加厚环保板材, 纹理清晰、防刮耐磨, 承重力强, 稳固耐用。</p> <ol style="list-style-type: none"> 1. 每套实训台包括 (实训台 1 组+椅子 6 把); 2. 规格: 六角桌边长 850-1000mm, 高度 760mm; 3. 外观要求: 台面厚度 25MM, 主架采用 20*40*1.2 的钢管焊接, 两侧用网孔挡板包围, 款式为六边形结构设计; 4. 靠背椅: 要求网布面, 海绵坐垫, 无扶手靠背椅; <p>优选板材, 采用防火板材, 安全环保 加厚钢架, 坚固安全耐用 承重力强, 安全稳固耐用, 强力承重 脚垫设计, 耐磨防滑, 延长使用寿命 安全油漆精巧设计, 贴心设计, 学习舒心</p>
11	教学控制台	<p>产品生产工艺先进, 质量达到国家技术标准, 通过相关检测认证, 经久耐用, 以保护用户的投资和使用。采用环保板材, 加厚环保板材, 纹理清晰、防刮耐磨, 承重力强, 稳固耐用。</p> <ol style="list-style-type: none"> 1. 教师工作台 1 个, 规格: 1400*700*760, 台面厚度 25MM, 材质: 生态颗粒板座椅 1 把, 靠背椅: 网布面, 海绵坐垫, 带扶手靠背椅。 2. 教学展示终端 3 台: 尺寸 86 英寸, 支持红外 20 点触摸感应方式, 触摸方式: 手指、笔, 或其他任何非透明物体, 免驱动操作, 即插即用。表面硬度 7H。 采用 LED 背光源。屏前玻璃厚度 4mm 确保抗撞击性能。圆弧角设计, 玻璃无任何边角直接外露。 前置接口: USB3.0*3 个, TYPEC*1 个, 支持双系统共享前置 USB 接口, 无需区分。 支持自定义设置开机显示通道, 包括 OPS、Android、HDMI 等通道。 为方便老师操作, 整机具有前置实体按键 (为减少误操作拒绝采用触摸按键), 数量 8 个, 功能包括主页、设置、电源、锁屏、触摸锁定、录屏、音量等。为便于操作, 前置按键均须具有清晰简体中文标识, 有效避免教学误操作。

		<p>支持前置物理按键和虚拟按键启动录屏功能，Windows 下所有操作过程均可录制。</p> <p>安卓主页面提供 7 个应用程序，安卓主页面具备信号源预览窗口，支持 OPS，HDMI 等信号源预览。</p> <p>支持屏体双侧快捷功能键，在任意通道下支持左右侧边悬浮球工具栏功能，侧边工具栏 8 个菜单工具，具有中文标识，包含的选项有主页、设置、音量、窗口下移、亮度、批注、多任务窗口切换、信号源切换等；操作便捷，功能丰富，满足教学应用需求。</p> <p>在任意信号源通道下（包括安卓、Windows、HDMI、VGA、TV、YpbPr 信号源）五指按压屏幕，可实现屏幕背光的关闭和开启。</p>
12	教学设备管理系统	<p>噢易机房 OSS 系统是一套围绕计算机实验教学而设计的支撑系统。它根据计算机中心管理老师们共同认可的标准而设计，能让机房管理摆脱日常琐碎而重复的工作，降低机房管理的维护成本，提高了机房运行的稳定性，让机房的管理效率得到了有效的提升。将机房打造成标准化示范型计算机实验室。</p> <p>本次配置 50 个授权客户端。</p> <p>保护还原。</p> <p>支持多种操作系统。</p> <p>支持 GPT 分区结构，完美支持 64T 容量硬盘。</p> <p>支持双硬盘同传和保护，同时可以保护和同传两块硬盘数据。</p> <p>支持 SATA、m. 2、MSSATA、PCI-E 和 m. 2 (NVME) 等接口的 HDD、SHDD 和 SSD 硬盘，</p> <p>支持多种保护模式，如保护模式、开放模式和考试模式。</p> <p>支持多种恢复频率，如手动恢复、自动恢复、定时恢复（如每隔 1 天、最多为 30 天）。</p> <p>网络同传：</p> <p>同传部署时，接收端电脑无需安装同传模块，即可通过网络引导进入同传进行批量部署。</p> <p>同时支持 1000 台电脑智能同传。</p> <p>IP 分配，支持自动批量分配的 IP、DNS、网关等参数。单台计算机 IP 参数自动记录，再次同传后无需重新设定。</p> <p>支持“断点续传”，同传过程接收端电脑网线掉线或以外终端，只需重新排除故障，连线后即可从断点处继续传输。</p> <p>支持“断电续传”，同传过程突然掉电，来电后同传可从断点处继续传输。</p> <p>支持自动连线，即任意一台计算机启动同传发送功能，其他计算机开机自动连线进入同传。</p> <p>千兆网络环境下同传速度可达 4G-6G/分。</p> <p>支持本地硬盘对拷复制，一次可以同时复制三块硬盘。</p> <p>本机系统部署时，如果有多个系统一致，无需逐个系统安装，可通过系统克隆直接复制多个系统。</p> <p>网络管理：</p> <p>设备锁定，支持统一锁定学生端的屏幕、USB 端口、键盘、鼠标、光驱等设备。</p> <p>远程开关机，同传和网络控制工具支持远程开机、关机、重启等功能。</p> <p>远程查看，支持教师端可远程监看学生端的屏幕操作，支持“全屏幕”和“多窗口同时监看”两种监看模式。</p> <p>计划任务，教师端可设定各种计划任务，在任意时间点或周期性的对所有学生端执行各种命令。如：远程还原/远程保存/</p>

		<p>远程开机……等指令。</p> <p>文件分发传输，支持教师端将指定的文件夹或文件，发送到学生端电脑中任意位置并进行安装。</p> <p>远程命令，支持教师端可对学生端下达远程命令，以运行或关闭学生端上的各种应用程序。</p>
13	电子教室模块	<p>通过基于标准网络架构的“多媒体教学管理系统”，教师不仅可以通过网络进行授课，答疑，还可以为学生进行可视化讲解，演示各学科的应用软件系统；而且学生可以向老师提问，让老师帮助学生解答。这些均是通过计算机和网络技术来实现，老师和学生不必离开自己的座位。同时教师还可以通过多媒体教室进行其它与课堂相关的管理。本系统为学生提供丰富生动教学素材，达到寓教于乐效果。并对集中化的机房进行统一的管理和维护，在教学过程中提供强有力的运维支持。保障了教学效果不打折扣。</p> <p>本产品是基于 TCP/IP 的网络应用系统。它利用一套软件，在计算机教室中，把影视、图形、图像、声音、动画以及文字等各种多媒体信息及控制实时动态地引入教学过程，是一种专用电脑网络的平台，是利用计算机技术、网络技术、多媒体技术进行现代化教学活动的一个系统。</p> <p>广播教学，支持教师机在上课时演示共享软件操作给所有学生机，即广播本地屏幕到所有学生机。</p> <p>学生演示，支持教师机指定某些学生在学生机演示操作，共享给其他学生进行演示。</p> <p>电子点名，支持教师机通过电子点名获取班级出勤情况，同时支持预置班级名册，没有点学生姓名一目了然。</p> <p>分组模型，支持针对不同的上课班级，进行学生图标的位置排列及别名的命名，存为该班级的模型，等后续老师上课时，直接加载该班级模型即可实现快速教学。</p> <p>语音广播，支持广播教师端麦克风的的声音给共享给学生机，以实现实时的语音教学。</p> <p>批量频道，支持远程批量修改学生端的频道数。</p> <p>网页广播，支持教师机批量发送指定网页地址到学生端，学生端收到后自动打开该网页。</p> <p>程序限制，教师端可通过黑白名单控制学生端程序使用或禁用。</p> <p>上网限制，教师端可以通过黑白名单来控制学生浏览的网页。</p> <p>断网锁屏，支持学生端断线（网线拔出、IP 异常等情况）时会自动锁定学生端电脑的屏幕。</p> <p>支持学生举手，学生有问题时可以通过软件向老师发送请求。</p> <p>支持作业提交，学生在学生端将完成的作业，提交到老师指定位置；支持所有在线学生同时提交作业。</p> <p>支持消息互动，教师端和学生可以互相点对点发送消息进行沟通。</p>