				3.教师创建课程时可引用系统课程库中的课程/实验小节，可将系统课程库中的课程、实验小节重新排列组合使用。教师可编辑所引用的课程并另存为自己的课程，对原课程不影响； 4.支持新建课程内容，课程资源类型包括但不限于理论、单机、仿真、虚实四种类型。新建课程可设置建议课时、章节、关联知识点，课程内容需包括基本信息、操作手册、实验拓扑、视频、课件、工具资料等信息，实验手册支持Markdown格式编写，支持分步式实验手册设计，每一步可关联实验结果，并自动验证实验的完成条件，通过系统自动判定实验完成度实现闯关模式的实验方式； 5.系统可联网的情况下，支持以云仓库的方式对课程进行管理，支持通过云仓库在线下载、更新已购课程包中的课程资源，可查看已授权课程、可更新课程、未授权课程。云端课程在线下载、在线更新时以任务管理器方式后台运行； 6.实验操作虚拟机与操作手册分屏展示，左侧展示虚拟机，右侧展示实验配套的手册、视频、随堂练习等内容。支持拓扑内不同虚拟机之间快速切换访问，并显示当前虚拟机的登录用户名和密码； 7.为保证系统算力资源的高效应用以保障实训的并发数，需支持算力资源的自动回收，每个实验具有相应建议实验时长的倒计时，到期后自动收回资源，学生可根据实验情况手动申请延时，临近结束系统需给予是否延时的提醒； 8.结束实验时可选择是否保存实验进度，保存实验进度可使学生下次启动实验时在原进度基础上继续实验。每人可保存进度的实验数量两个，超过可保存的实验个数可手动选择覆盖哪一个实验；可一键开启/关闭拓扑中所有虚拟机，也可在拓扑中针对单个虚拟机进行启动/关闭/重置操作； 9.支持自定义实验网络拓扑，创建实验环境时可以拖拽形式组建实验拓扑，可配置拓扑中各虚拟机的CPU、内存、网口数量等参数，支持快速复制粘贴整个拓扑或单个虚拟机； 10.支持拓扑图的导出、居中显示、放大显示、全屏显示等功能。系统可计算分析拓扑所需算力资源，并根据当前系统资源总量自动计算出当前实验可支撑的并发人数； 11.系统拓扑可以场景化的机架视图形式展示，以提高实验操作的物理体验，			

				直观展示设备面板及网络连接情况； 12. 支持 WEB 文件上传，教师可将所需文件从本地电脑通过 web 页面中的上传功能直接上传至虚拟机中，在实验环境下支持本地电脑中的中文本复制至 web 虚拟机桌面； 13. 支持虚实结合功能，可将虚拟机和真实物理设备同时加入到同一个网络拓扑中进行实验，支持包含防火墙、IPS、漏扫、WAF 等多种安全硬件设备。			
3	信息安全实训系统-网络安全实训系统-教学方案模块	奇安信	CSE-EDU-TPM	规格： 1. 支持教师根据教学需要自定义教学方案，可继承系统内已有方案，也可导入 excel 格式的课程规划表以创建全新的教学方案。系统需以时序图的形式展示每学期的课程安排及课程间的关联关系，支持自定义调整时序图中的课程顺序及关联连接。支持方案内课程的授课课时统计，通过对每门课程的要求课时、规划课时、授课课时的统计对比，直观展示各班级的各课程授课进度； 2. 支持案例式的项目综合实训模式，综合实训的课程安排可按每周的周期循环形式排课，支持学生按照工作团队的形式分组参与实训，每组启动一套实训拓扑环境共同完成同一个项目； 3. 支持对项目综合实训的基本信息、项目流程、网络拓扑进行设置，项目流程默认包括项目启动、任务分工、项目规划、阶段审核、项目实施、项目测试、项目验收阶段，可根据每个项目的运行阶段添加、删除相关流程，可设计每个流程环节中的具体工作内容及任务； 4. 项目实训过程中默认支持断点保存功能，可自动保存实训内容，并支持实训过程中对项目网络拓扑的编辑修改，如重新规划网络架构、增加新设备资源、更新设备改连接线等。	38050	1	38050
4	信息安全实训系统-网络安全实训系统-考试测评模块	奇安信	CSE-EDU-EXM	规格： 1. 教师可创建考试测评试卷，创建完的试卷可选择开启是否公开，公开属性下所有教师可使用并编辑该试卷，私有属性下试卷只能被创建者查看并使用； 2. 支持添加、删除和筛选试卷，包含基于知识点或分类两种选题方式，可通过智能或手动两种方式组卷。可指定各类型题目数量、分数以快速组建考试试卷。可预览当前试卷中的建议课时、题目数量、分数、难易度、所需工具、涵盖知识点等信息；	37000	1	37000

				3.支持考试测评的题库管理功能，支持单选题、多选题、填空题、单机题、仿真题、CTF 题、简答题等多种题型，初始化内置单选题及多选题 1000 道。可按照测试题所涉及知识点进行分类，支持按照题目难易度、题目类型进行筛选。支持选择题的批量导入功能，可在线下载批量导入模板。教师可创建新的测试题，可修改和查看题目分类、题干、难易度、关联知识点、参考答案等内容； 4.支持自定义管理所添加的物理硬件设备，可修改设备资产的设备名称、设备类型、设备图标、设备面板、设备描述等信息。可设置设备的串口端口及网络端口的对应端口号，支持网络端口的增、删、改； 5.系统支持串口通信，可通过系统对物理真实设备的前后台双向控制管理，既可以通过系统跳转到物理设备的 web 页面完成参数的配置，也可通过系统中的虚拟机控制台进行底层操作配置； 6.可通过知识库的知识脉络实现对基础教学内容、项目实训、技能测评等多方面教学内容的关联查询，方便教师根据课程知识点进行相关教学内容的安排及学生根据相关知识点进行补充、发散学习； 7.支持对系统镜像、虚拟设备、真实物理设备、平台级图形设备等虚拟组件的管理，虚拟设备涵盖网络设备、基础服务器、应用服务器、个人终端等多种类型； 8.支持虚拟组建的增、删、改、查，虚拟设备的创建支持上传和安装两种方式，支持对虚拟设备的设备名称、设备类型、设备图标、设备描述等信息的修改； 9.支持在线启动和查看虚拟设备，启动时可动态设置 CPU 数量及内存大小。可快速克隆虚拟设备，并支持增量和完整两种克隆方式，可查看引用该虚拟设备的相关课程。可查看物理设备被占用的相关课程学习小组等详情； 10.内置 80 个安全工具，支持工具的增、删、改、查，可在线下载工具到本地。			
5	信息安全实训系统-网络安全实训系统-教学管理模块	奇安信	CSE-EDU-JXM	规格： 1.支持按照课表教学、学生自学两种教学模式，教师可设置学生的自学时间段，并可选择开启周期性循环自学模式。可统一设定一个班级所有升学的自学模式，也可选择部分学生设置自学模式；	38000	1	38000

				2.支持以日历表的形式呈现教学课程表，可按年/月/周的形式查看或设置课表，可通过课程表点击每节课查看教学任务详情； 3.支持教学任务的下发，任务类型包括课程、实验、考试、项目，教师可根据不同任务类型安排授课方式、任务时长，可面向班级进行常规授课，也可面向部分学生进行定向授课。课程/实验可设置单人/分组的实验形式。项目排课时可按照课表进行详细规划，可设置小组数量及每组人数； 4.支持排课过程中进行资源动态分配，教师排课时可以根据上课人数、实验所需资源自动分配硬件资源，若资源不足，系统可自动提醒教师切换成分组的实验形式，并可根据资源情况自动计算设置小组数量； 5.教师可对当前课程学习模式进行个性化设置，系统提供标准和自定义扩展两种学习模式，标准模式默认开启操作手册、参考视频、随堂练习、网络拓扑等学习资源，扩展模式可自定义开启/隐藏以上资源； 6.支持在线查看当前课堂学生出勤情况，实验课程中教师可远程进入学生虚拟机在线观察学生的实验操作情况； 7.支持学生在线提交实验报告，可在线下载实验报告模板，实验报告支持重复提交； 8.可针对教学任务进行课后的教学管理，包括查看每节课中的出勤情况、考试测评的成绩分析、项目实训的完成情况及得分等，可在线下载查阅学生上传的实验报告并在线打分。可按时间、班级、课程类型查询相关教学事务并以表格形式导出该事务的相关数据； 9.系统具备教学数据分析功能，提供教师教学数据的统计分析，可对教学的课时安排及完成情况、全年课时分布、基础教学成绩、考试测评成绩、项目实训成绩的分析及图形化展示，可按班级查询教学的数据分析结果。提供对学生学习数据的统计分析，可对学习的总学时、出勤情况、排名趋势、技能方向、积分排名进行图形化展示。			
6	信息安全实训系统-网络安全实训系统-系统管理模块	奇安信	CSE-EDU-SMM	规格： 1.包含教师、学生、管理员三种角色，可对用户头像、姓名、密码等信息进行管理维护，需支持批量导入、导出学生账号并可在线下载导入的模板。支持单独/批量禁用账号，支持对专业、班级信息的管理和维护。可在线查看实时教师、学生在线人数；	38000	1	38000

				2. 支持对系统的内存、硬盘、CPU 等资源的使用情况进行图形化展示，支持对教学课表的上课时间、教学时长等进行全局设置； 3. 支持以 web 界面及 SSH 两种形式进行远程运维及调试，并可记录运维时间、运维人员及运维内容等运维日志 4. 系统联网的情况下，可远程更新升级系统版本及功能。			
7	信息安全实训系统-网络安全实训系统用户授权	奇安信	CSE-EDU-FL-5	规格： 提供 5 个并发用户的授权。	33050	8	264400
8	课程资源包-系统安全课程资源包	奇安信	CSE-Course-J CVM-SS	规格： 1. 通过该课程资源包中所含课程的学习，可使学生掌握计算机信息系统安全的基本概念、基本理论与基本技术。强调底层性和系统性，使学生掌握分析和解决计算机信息系统安全实际问题的基本能力； 2. 包含 400 个 Linux 操作系统安全、恶意代码分析实践、逆向工程技术实战、日志分析基础、Kali Linux、软件安全、容灾与备份、数字取证、信息隐藏与数字水印、移动安全、安卓应用安全、二进制漏洞分析与利用、计算机病毒、安全评估等相关理论或实验教学内容。每个实验均须有对应知识点的实验环境及详细的实验指导手册，学生可自主地通过实验指导手册完成实验的操作练习，每个理论课程均需有连贯的理论讲解视频。	180000	1	180000
9	课程资源包-网络安全攻防技术实战课程资源包	奇安信	CSE-Course-J CVM-GFSZ	规格： 1. 课程从实际信息系统渗透技术要点出发，重点介绍渗透测试过程涉及到的理论知识和攻击技术，通过学习渗透测试全流程所需的知识和技术要点，掌握渗透的过程、信息收集的手段、网络协议漏洞的利用、口令的爆破利用、常见系统及软件的渗透、以及渗透后的权限维持、后渗透和痕迹清除等内容； 2. 课程按照渗透测试工程师岗位对职业能力和职业素质的要求通过完整的工作内容所需要的知识框架来组织教学内容，宏观上采用模块化结构构建课程内容体系，即将课程主要知识点分 9 个教学情境，理论和实践内容相结合，以实践能力考核为主的课程评价方法，切实提高学生的职业能力和就业竞争力。使学生通过本课程的学习，可从事网络安全工程、网络设备安全维护、网络安全服务、网络渗透测试、网络威胁排除等基础工作，具有解决网络安	395800	1	395800

				全防护问题和初步渗透测试的能力； 3.课程通过高度仿真的教、学、做一体化的场景化教学，按照信息收集、漏洞发现和利用、Web 渗透测试、权限提升、权限维持、内网渗透代理、内网常见攻击、后渗透、痕迹清除、日志清除的攻击流程进行教学。			
10	防火墙课程资源包+纯虚化实验产品-智慧防火墙系统	奇安信	NSG-VM100-S-LAB-A-QW	规格： 1.IPSec 隧道数 1000； 2.并发连接数 180 万； 3.SSL VPN 并发用户数 1000； 4.支持路由、透明、交换以及混合模式接入，满足复杂应用环境的接入需求。支持旁路模式； 5.支持 VTEP（VxLan Tunnel EndPoint）模式接入 VxLAN 网络，并可作为 VXLAN 二层、三层网关实现 VxLan 网络与传统以太网的相同子网内、跨子网间互联互通； 6.支持通过绑定 VLAN、VNI（VXLAN Network Identifier）、远程 VTEP，手动管理 VxLan 网络；支持 MAC、VNI、VTEP 静态绑定； 7.支持 MPLS 流量透传，支持 MTU≥9000byte 的巨型帧 Jumbo Frame； 8.支持静态路由、策略路由。策略路由支持用户自定义其优先级；必须支持静态和动态多播路由，动态多播路由必须支持 PIM-SM（稀疏模式）； 9.支持基于策略的路由负载，支持根据应用和服务进行智能选路，支持源地址目的地址哈希、源地址哈希、轮询、时延负载、备份、随机、流量均衡、源地址轮询、目的地址哈希、最优链路带宽负载、最优链路带宽备份、跳数负载等 12 种路由负载均衡方式； 10.支持 ISP 路由负载均衡，最大可支持 4 条链路负载，支持自定义负载权重，支持基于优先级的 ISP 路由链路备份； 11.支持全面的 NAT 转换配置，包括一对一，一对多，多对一的源、目的地址转换。支持在会话的源、目的地址同为 IPv4 地址时，可将目的地址转换至指定服务器地址； 12.支持在源地址转换过程中，对 SNAT（源地址转换）使用的地址池利用率进行监控，并在地址池利用率超过阈值时，通过 SNMP Trap、邮件等方式告警； 13.支持 IPv4 的 DNS 代理功能，即从指定的入接口或源 ISP 接收到的 DNS 解	19250	1	19250

				析请求； 14.支持出站的DNS代理功能，支持在不更改内网终端设备DNS服务器地址设置的情况下，将DNS解析请求发送至指定的DNS服务器，并代理原DNS服务器返回解析结果； 15.支持DNS64功能；支持IPv6入站的DNS代理功能，即从指定的入接口或源ISP接收到的DNS解析请求，设备可根据自定义的IP、域名对应关系，代理DNS服务器返回查询结果； 16.支持针对IPv6流量通过HTTP、HTTPS实现Web认证，用户身份信息可存储在本地或Active Directory\Radius\TACACS+\POP3等第三方服务器；通过HTTPS实现Web认证必须支持使用本地CA颁发的证书同时使用证书验证客户端身份； 17.支持将物理防火墙资源，如会话数、安全策略数、源NAT数、目的NAT数，日志存储数量以保留值及最大值的形式自动分配； 18.支持在虚系统内独立配置漏洞防护、间谍软件防护、URL过滤、文件过滤、内容过滤、邮件过滤、行为管控等安全功能。并可支持对本虚系统内产生的日志进行独立审计； 19.支持基于源安全域、目的安全域、源用户、源地址、源地区、目的地址、目的地区、服务、应用、隧道、时间、VLAN等多种方式进行访问控制，并支持地理区域对象的导入以及重复策略的检查； 20.支持应用识别，应用特征库包含的应用数量（非应用协议的规则总数）大于200种，可深度识别每种应用的属性，为每种应用提供预定义的风险系数，并将应用基于类型、使用场景、数据传输、风险等级等特征分类； 21.必须支持基于用户的访问控制，可与LDAP/Radius/证书/Active Directory/TACACS+/POP3等用户认证系统联动； 22.支持对应用的文件传输行为进行上传、下载、双向的文件类型过滤，应用至少包含即时通讯、常用协议、文件共享、论坛、博客、网页邮件五种分类； 23.支持上传、下载、双向的文件内容过滤；内容过滤支持手工及文件批量导入两种方式进行敏感信息定义；内容过滤至少支持html、doc、docx、xls、xlsx、ppt、pptx、chm、7z等30种常见文件类型；文件类型识别基于文件特征而非扩展名，更改文件扩展名后仍可有效识别；			

				24.支持基于不同安全区域防御 SYN Flood、UDP Flood、ICMP Flood、IP Flood、DNS Flood、HTTP Flood 攻击，并支持警告、丢弃、普通防护、增强防护、授权服务器防护等多种防护措施； 25.能够对 HTTP/FTP/POP3/SMTP/IMAP/SMB 六种协议进行病毒查杀； 26.支持漏洞防护功能，同时将漏洞防护特征库分类，至少包括缓冲区溢出、跨站脚本、拒绝服务、恶意扫描、SQL 注入、WEB 攻击等六种分类；漏洞防护支持日志、阻断、放行、重置等执行动作，可批量设置针对某一分类或全部攻击签名的执行动作；支持基于 FTP、HTTP、IMAP、OTHER_APP、POP3、SMB、SMTP 等应用协议的漏洞防护； 27.支持自定义 TCP、UDP、HTTP 协议的漏洞特征，漏洞特征可通过多个字段以文本或正则表达式的形式进行有序和无序匹配，并可自定义漏洞的源、目的端口范围；同时可标识自定义漏洞的 CVE 编号或 CNNVD 编号； 28.支持 L2TP、支持 L2TP over IPSec、支持 PPTP ，并支持本地认证以及 LDAP/Radius/证书/Active Directory/TACACS+/POP3 等第三方用户认证系统。			
11	防火墙课程资源包+纯虚化实验产品-智慧防火墙系统全功能模块升级服务许可	奇安信	NSG-VM-LAB-A-SWB-1Y-QW	规格： 提供 1 年智慧防火墙系统全功能模块升级服务（APP/URL/AV/IPS/IOC）。	5500	2	11000
12	防火墙课程资源包+纯虚化实验产品-智慧防火墙课程资源包	奇安信	CSE-Course-JCCP-VM-NGFW	规格： 1.以纯虚化实验产品-智慧防火墙系统为教学基准，提供 10 个实验任务可覆盖 30 课时的实验教学，采用循序渐进的模式，学生通过任务制模式阶段性对防火墙安全产品的功能和技术进行应用，主要涉及“三大模块，十个场景”，三大模块包括防火墙初始化配置、防火墙网络功能部署和防火墙安全功能应用，其中防火墙初始化配置模块涉及防火墙基本配置场景，涵盖知识点包括防火墙部署方式、初始化配置、安全域等相关内容，解决用户对于防火墙在出厂零配置状态下需要进行的初始化配置操作等相关问题；防火墙网络功能部署模块涉及路由通信、透明部署、网关多出口与流量管理、DNS 域名解析、目的 NAT 映射共 5 个实验场景，涵盖知识点包括三层路由模式、二层透明网	101000	1	101000

				桥模式、DHCP 服务、地址转换、QoS、DNS 透明代理等内容，解决防火墙在信息系统网络边界出口关键位置需要发挥的网络通信功能和访问控制能力；防火墙安全功能应用模块涉及安全防护、访问控制、安全认证与审计和 SSL VPN 搭建共 4 个实验场景，涵盖知识点包括安全配置文件（行为管控、关键字过滤、内容过滤、文件过滤、邮件过滤、URL 过滤）、安全认证、攻击防御（恶意扫描防御、流量型攻击防御、应用层 Flood 攻击防御）等相关内容，解决企业网络内部应用管理、敏感信息管控、网络安全威胁等安全风险，实现提高企业信息系统安全性的目的； 2. 本课程通过高度仿真的教、学、做一体化的场景化教学，培养学生学习企业网最典型的边界安全设备--防火墙的相关知识、技术，使学生掌握企业网络安全域的划分、防火墙的网络部署、防火墙的策略配置、防火墙安全防护与运维等操作技术。该课程在实验操作部分中提供了丰富的知识点内容补充，可以加强学生对于防火墙技术的理解和应用。学生通过对防火墙设备的配置操作，积累解决实际问题的工作经验，学习深入的专业理论知识，培养和提高学生的安全能力和综合素质； 3. 智慧防火墙课程资源包 包含课程大纲、教学 ppt、实验指导书、实训实验等丰富的教学及实操资源，可满足高校一个学期的理论和实验教学需求。 以硬件防火墙设备为教学基准，主要介绍防火墙的基本知识、结构、配置方法。通过本课程能够学习智慧防火墙部署运维。			
13	终端安全课程资源包+纯虚化实验产品-终端安全课程资源包	奇安信	CSE-Course-JCCP-ENDPOINTSEC	规格： 1. 以纯虚化实验产品-终端安全管理系统为教学基准，提供 11 个实验任务可覆盖 26 课时实验教学，围绕终端部署、资产管理、统一安全基线、病毒与补丁管理、统一软件发布，通过 WindowsPC 终端，Windows Server 终端、Linux Server 终端进行逐一管理需求验证实验，最后通过使用辅助分析工具对操作系统的进程、服务、注册表、启动项等进行排查和管理实验，掌握对操作系统的常用处置方法。以终端管理工作需求为目标，从终端管理软件部署开始到逐步开展终端管理策略为主线，由浅入深。终端部署→资产管理→安全基线→病毒与补丁管理→统一软件管理→辅助分析工具； 2. 通过该课程的学习，使学生学习理解终端安全管理的概念和工作范畴，理解并掌握终端安全管理相关的技术手段和实施方法，理解并掌握终端安全事	95000	1	95000

				件处置与响应相关的技术手段和实施方法。学生通过对终端安全管理系统软件进行配置实践操作，提高学生实际动手能力，积累解决终端安全实际问题的工作经验并学习深入的专业理论知识，提高学生解决问题能力和综合素质； 3. 终端安全课程资源包 包含课程大纲、教学 ppt、实验指导书、试题库、实训实验等丰富的教学及实操资源，可满足高校一个学期的理论和实验教学需求。 以终端安全管理为教学基准，主要介绍终端安全的基本知识、结构、配置方法。通过本课程能够学习终端安全管理产品的部署运维。			
14	终端安全课程资源包+纯虚化实验产品-终端安全管理系统	奇安信	TXZB-LAB-A-JXZB-03	规格： 1.支持根据分组、计算机名称、IP 地址、操作系统、在线状态等条件的组合筛选出符合条件的终端进行管理； 2.支持与 NTP 时间服务器同步，可设置同步时间间隔，使终端时间保持和时间服务器相同； 3.支持单个页面展示终端部署统计、终端在线统计、终端安全趋势、病毒查杀趋势、安全更新和重要补丁安装趋势等信息，均可通过图形化展示； 4.支持对单个客户端进行维护，终端视角查看终端基本信息，包括计算机名、型号、IP、MAC 地址、工作组、域信息、本次开机时间、上次关机时间、应用功能、在线状态； 5.支持通过高级筛选方式对终端概况进行筛选查看指定范围终端实时统计数据，支持“与或”组合筛选； 6.支持自动分组，按 IP 地址、CPU 数量、操作系统类型、操作系统版本等参数进行自动动态调整分组； 7.管理控制中心当登录账号输入密码错误次数超过锁定阈值后账号将被锁定，且可设置锁定时间，该时间内账号登录请求不被接受。同时应支持双因子认证登录方式，提高安全性； 8.客户端主程序、病毒库版本支持按分组和多批次进行灰度更新，保持在低风险中完成终端能力更新。支持设置不同终端类型设置和每批次观察时长。当检测到新版本将从第一批次重新观察； 9.支持在线更新病毒库、补丁库、威胁情报等数据，并且支持“按月、按周、按天、按小时”灵活设置更新时间； 10.支持文件下载分级缓存，支持下载文件限速和日志上传限速，可设置带宽	320	1	320

				最大流量和限速时间，避免过多占用网络带宽，影响业务办公； 11.支持终端用户和管理员是一套账号管理系统，简化账号管理复杂度，一个账号解决所有身份认证，既可以用于终端登录，也可以用于管理中心； 12.支持自定义告警规则，例如系统一段时间内病毒和未知文件超过一定数量后会通过邮件发送给收件人查阅； 13.支持终端密码保护功能，支持终端“防退出”密码保护、“防卸载”密码保护。支持设置自我保护功能，可有效防止客户端进程被恶意终止、注入，提高客户端进程、数据、配置的安全性； 14.病毒防护日志包含：病毒查杀日志、查杀任务日志、攻击防护日志、系统防护日志、按分组、按终端、按时间； 15.病毒报表支持病毒查杀趋势、扫描触发方式趋势、发现病毒趋势、终端感染趋势、病毒类型统计、病毒处理结果统计、病毒触发方式统计、趋势图表、按分组、按终端、按病毒名称； 16.支持手动导入、导出黑白名单，添加黑白名单。支持通过文件导入添加黑白名单； 17.支持信任区设置，病毒扫描或实时防护时不扫描目录或文件； 18.病毒扫描支持扫描所有文件和仅扫描程序及文档文件设置，支持对压缩包文件设置最大扫描层数和大小，当发现压缩包内存在病毒时，还需继续扫描压缩包内其他文件； 19.支持对终端当扫描到感染型病毒、顽固木马时，自动进入深度调查模式，可设置禁止终端用户管理路径或文件白名单、禁止终端用户管理扩展名白名单、扫描时不允许终端用户暂停或停止扫描任务； 20.支持扫描资源占用设置，可设置不限制、均衡型、低资源三种模式； 21.支持对进程防护、注册表防护、驱动防护、U盘安全防护、邮件防护、下载防护、IM防护、局域网文件防护、网页安全防护、勒索软件防护； 22.支持自动阻止远程登录行为，防护黑客远程爆破和拦截恶意的远程登录； 23.支持网络入侵拦截对流入本机的网络包数据和行为进行检测，根据策略在网络层拦截漏洞攻击、黑客入侵等威胁； 24.支持僵尸网络攻击防护，对流出本机的网络包数据和行为进行检测，根据策略在网络层拦截后门攻击、C2连接等威胁；			

				25.支持防护对流出本机的网络包数据和行为进行检测，根据策略在网络层拦截后门攻击、C2 连接等威胁； 26.支持 ARP 攻击防护根据策略检测和拦截局域网中的 ARP 欺骗攻击行为； 27.客户端弹窗支持免打扰模式和智能模式，使用免打扰模式可以对不能弹窗的终端设备中避免弹窗。使用智能模式是智能调整弹窗，对已知的病毒自动处理，对未知的病毒提示处理； 28.支持三个杀毒引擎混合使用，提高病毒检出率； 29.支持针对 Windows XP 系统可带来安全隐患的设计机制进行加固性修复，支持远程漏洞攻击防护、本地钓鱼攻击防护和浏览器漏洞攻击防护； 30.支持针对 Windows 7 系统可带来安全隐患的设计机制进行加固性修复，支持远程漏洞攻击防护、本地钓鱼攻击防护和浏览器漏洞攻击防护； 支持对 Windows 操作系统、IE、.NET Framework、Office、Adobe Flash Player、Adobe Acrobat 和 Adobe Acrobat Reader DC、硬件驱动更新等软件进行补丁修复； 31.支持按补丁类型和级别修复，补丁级别需包括：安全更新、重要补丁、功能补丁、可选补丁； 32.支持开启自动修复漏洞，包括开机时修复，并支持随机延迟执行、间隔修复和按时间段修复，可设置延迟时间、间隔修复时间和修复时间段； 33.支持影响到编辑 Office 文档时提醒，可取消此次修复任务； 34.允许终端用户手动修复漏洞，如果发现“修复内容”中设置的需要修复的漏洞和功能缺陷没有修复成功则提醒终端用户修复； 35.支持对停服系统补丁管理，支持统计即将停服的操作系统，显示操作系统、版本类型、系统位数、停服日期、终端数和升级建议，可直接下发策略进行升级； 36.支持按照补丁的维度统计补丁安装情况，包括补丁号、系统类型、补丁类型、补丁级别、补丁名称、补丁描述、发布日期、发布状态等。 37.支持系统状态基线核查，应包括：是否安装关键和重要系统补丁、是否安装防病毒软件、工作组命名检查、是否加入域、计算机命名检查、系统备份还原点检查、系统重要目录对 Everyone 或 Guests 来宾账户开放检查、空口令检查、操作系统是否开启 Hardware DEP Available 保护检查、系统隐藏用			

				户检查、关键进程是否运行或禁止检查、禁止开放端口检查； 38.访问控制应包括：Guest 账户状态、将本地账户使用空白密码限制为仅控制台登录、允许 Windows 自动连接到建议的开放式热点或与联系人共享的网络以及提供付费服务的热点、允许用户使用远程桌面服务、管理员账户状态、允许 ICMP 重定向覆盖 OSPF 生成的路由、检查是否关闭了默认共享、不显示上次登录、清除虚拟内存页面文件、重命名管理员账户、提示用户在密码过期之前更改密码、操作系统 UAC 用户账户控制是否开启至指定级别、设置活动但空闲的远程桌面服务会话的时间限制、TCP/IP 筛选； 39.支持对网卡进行防护，支持阻止终端修改 IP 地址、使用动态 IP 地址、热点创建和 IPV6 地址使用等，可自定义提示内容和生效时间； 40.支持在指定应用区域或全屏展示自定义水印信息，包括当前日期、用户名、当前时间、IP 地址、MAC、操作系统账号、计算机名、使用人、手机尾号和资产责任人等。			
15	终端安全课程资源包+纯虚化实验产品-WindowsServer 功能授权	奇安信	TXZB-LAB-A-WINSER-03	规格： 支持终端安全管理系统 WindowsServer 客户端防病毒、补丁管理功能。	890	8	7120
16	终端安全课程资源包+纯虚化实验产品-WindowsPC 功能授权	奇安信	TXZB-LAB-A-WINPC-03	规格： 支持终端安全管理系统 WindowsPC 客户端的防病毒、基线核查、文件审计、补丁管理、终端数据防泄漏、终端管控、软件管理、停服系统加固、安全水印功能授权功能。	650	8	5200
17	终端安全课程资源包+纯虚化实验产品-Linux 功能授权	奇安信	TXZB-LAB-A-Linux-03	规格： 支持终端安全管理系统 Linux 端的防病毒。	1210	8	9680
18	终端安全课程资源包+纯虚	奇安信	TXZB-LAB-A-WINSER-SZSQ-0	规格： 支持终端安全管理系统 WindowsServer 客户端防病毒、补丁管理功能授权—	780	16	12480

	化实验产品-WindowsServer更新服务		3	年更新服务。			
19	终端安全课程资源包+纯虚化实验产品-WindowsPC更新服务	奇安信	TXZB-LAB-A-WINPC-SZSQ-03	规格： 支持终端安全管理系统 WindowsPC 客户端的防病毒、基线核查、文件审计、补丁管理、终端数据防泄漏、终端管控、软件管理、停服系统加固、安全水印功能授权一年更新服务。	510	16	8160
20	终端安全课程资源包+纯虚化实验产品-Linux 更新服务	奇安信	TXZB-LAB-A-Linux-SZSQ-03	规格： 支持终端安全管理系统 Linux 端的防病毒功能授权一年更新服务。	1090	16	17440
21	项目实训类课程-学历教育-企业网等保测评课程资源包	奇安信	CSE-Course-XMCP-DBCP	规格： 1. 课程以等保测评项目背景为基础，从实际信息系统等级测评要点出发，学习中小型企业网络安全等级保护项目工作开展流程，掌握定级、备案、建设整改、等级测评、监督维护环节中所涉及的工作活动开展和注意事项； 2. 需使学生理解和掌握针对信息系统中的身份鉴别、访问控制、安全审计、入侵防范、恶意代码防范等安全控制点相关的详细测评测评项和测评方法，按照网络安全等级保护工程师岗位对职业能力和职业素质的要求通过完整的工作内容所需要的知识框架来组织教学内容； 3. 系统中提供的课程资源需包含但指导手册、实验拓扑两类，实验拓扑 18 个网络节点，可在线一键开启拓扑环境。指导手册详细介绍了课程任务所依托的业务场景及所涉及的知识点，并详细介绍了实验原理和逐步的操作步骤以便教师备课和学生自学。	160000	1	160000
22	堡垒机-堡垒机软件基础包	奇安信	C6000-BH-C-SY-LAB-A-01	规格： 1. 提供堡垒机的虚拟机安装包，用户额外准备虚拟化环境部署。核心功能：包含账号管理、监控、审计功能。支持 SSH、RDP、VNC 协议资产连接，客户端无需安装代理； 2. 支持 LDAP 认证及用户组同步；	135000	1	135000

				3.通过 Ansible 实现批量命令执行与文件上传/下载; 4.支持管理 MySQL、Oracle、SQL Server 等数据库，配置参数包括数据库 IP、端口、数据库类型、用户名、密码等; 5.可管理路由器、交换机等网络设备，需配置设备的 IP、SNMP 共同体字符串等参数以实现设备信息采集和管理; 6.可根据业务、部门等维度对资产进行分组管理，便于权限分配和资产查找。每个资产分组可设置组名、描述等信息; 7.可将用户或用户组与资产或资产组进行关联，授予用户访问特定资产的权限，可配置读、写、执行等不同权限级别; 8.可针对特定用户或用户组，设置允许或禁止执行的命令列表，细粒度控制用户在资产上的操作权限; 9.可设置用户对资产的访问时间段，如仅允许在工作日的工作时间内访问; 10.可配置允许用户登录 JumpServer 或访问资产的 IP 地址范围，增强访问安全性。			
23	一体化云终端	和信创天	VECTX-H548	规格： 1. 该终端包括 1 个教师端和 40 套学生端以及配套的键盘鼠标及 23.8 寸的终端显示装置，支持 1980*1020，一 VGA，一个 HDMI; 2.教师机要求： CPU：物理核心 8 核; 内存：16G DDR4; 硬盘：512G SSD; 接口：6 个 USB 接口，一个 VGA,一个 HDMI; 网口：1 个千兆。 2.学生机要求： CPU：物理核心 8 核; 内存：8G DDR4; 硬盘：256G SSD; 接口：6 个 USB 接口，一个 VGA,一个 HDMI; 网口：1 个千兆。	249200	1	249200
24	云桌面系统	和信创	NGD5-PMC	规格：	189000	1	189000

		天		1. 云桌面系统，采用云计算超融合系统架构，多副本的分布式存储机制，支持 VDI、VOI、IDV 三种云桌面架构于一体，通过统一管理方式，为用户提供了虚拟磁盘管理、软件分发、系统还原、个人安全磁盘、远程控制、外设访问控制、客户端截屏、灰度更新、ARP 防护、软件白名单等功能，可支持 GPU 直通与 GPU 虚拟化，实现桌面管理统一化、数据存储集中化、运维服务简单化，为用户提供按需扩展、按需融合、按需选用的全场景企业级云桌面。为保障用户后期终端云管控系统的业务扩展及统一管理，系统应采用 mysql 或者 Oracle 大型数据库，一台服务器支持 500 台终端同时流畅运行 AutoCAD、3DMax、视频制作、图像处理等大型软件及医学影像大文件调用，保障用户良好的并发使用体验。 2.采用新一代虚拟仿真技术，终端本地硬盘无需安装操作系统，通过 PXE 网络部署和引导，启动虚拟桌面方式运行操作系统及应用，简化部署维护工作。 3.服务端和管理端均支持跨平台，既可以在 windows 服务器上部署，也可以在 linux 服务器上部署。 4.支持离线超管功能，可以直接在客户机终端上开启镜像模版并进行修改，并支持在广域网线路上将修改的镜像模版文件自动上传到服务器上。 5.满足个性化设置迁移，客户端系统重启后还原，可自动清除系统进程和服务中的木马病毒，但会保留用户自定义的用户名和密码、桌面壁纸等个性化配置不会还原。 6.为便捷用户管理维护，允许同时开启多个超级管理权限并对多个操作系统镜像进行更新升级或者软件安装，提高管理效率；当网络环境不佳，支持在终端启用离线超级管理员模式，进行后台上传更新，降低对服务器及网络的资源占用，保障更新维护照常运行。可针对特定用户需求，将服务端指定目录下的文件穿透到策略中设置的客户端相应的虚拟磁盘中，实现服务端文件实时分发到客户端的目的，简化管理维护。 7.支持虚拟桌面模板功能，可使用快速克隆部署方式，部署单个虚拟桌面时			

				间不超过 10 秒。 8. 支持 GPU 虚拟化，可指定虚拟桌面启用 GPU，分配显卡资源，满足 3D 应用类设计需求。 9. 支持管理员恢复误删除的桌面或彻底删除云桌面，可针对特定桌面提供 CPU、内存等资源保障和实时看护；并支持桌面信息导出功能，包括虚拟机名称、虚拟机规格、分组信息、所属用户等信息。 10. 系统可以支持对用户上网行为的审计功能，能够记录终端计算机上网的 URL 痕迹；支持终端计算机按时间段进行自动截屏。 11. 为保证内网环境的安全性，系统应支持 ARP 防护功能，避免因为 ARP 病毒导致网络瘫痪，并支持流量控制功能，该功能必须是基于驱动层而不是应用层来实现客户机的流量控制，能够按照内网/外网/上传/下载/流量大小等多种条件进行规则判断，能够防止蠕虫病毒产生的大流量数据包发送。 12. 支持对终端本地的硬盘保护；可对本地硬盘各分区进行还原保护。 13. 支持灵活的数据保护策略，可按时间段设置数据保护模式，如不保护、完全禁用、只读或只写，并支持本地 USB 过滤，除指定列表中 USB 设备外，其他 USB 设备可以被过滤和禁止。 14. 镜像融合：可支持 VOI、VDI、IDV 不同架构的桌面资源共用同一个镜像，支持 WEB 管理端制作及修改镜像模板，例如在 web 管理端修改 VDI 的镜像模板，VOI、IDV 镜像数据也随之更新，方便用户统一运维。 14. 数据融合：可针对 VOI、VDI、IDV 三种架构的桌面分配同一网络数据盘，用户登录不同桌面资源时，均可访问到自己的存储数据，并无需二次登录认证，高度保障用户数据的统一性。 15. 管理融合：云桌面系统应具备先进的前瞻性，可支持前后端混合计算，同时支持后端计算模式 VDI，可实现移动办公，支持前端智能计算模式 VOI，可用于网络突发故障的环境下仍提供稳定高计算性能服务，并可 100%利旧终端已有计算及存储性能、无损耗，以及前端虚拟计算模式 IDV，解决跨硬件平台的操作系统部署。 16. 该系统搭载环境为：CPU：物理核心 4 核，主频 3.5GHz；内存：32G DDR4；系统盘：240G SSD 2.5 寸企业级；数据盘：2TB HDD 3.5 寸企业级。			

25	云桌面系统授权	和信创天	NGD5-E-1000	规格： License 授权，按用户使用数量授权	1280	41	52480
26	教学管理系统	奇安信	VETMS	规格： 1.软件支持三种以上语言环境支持，至少包含中文简体、中文繁体、英文语言包，满足不同操作系统语言环境的教学需求。 2.软件授权支持班级授权和校级授权，可以从本地读取授权，也可以从授权服务器或集中授权服务器读取授权，软件激活支持有互联网环境的在线激活和无互联网环境的离线激活方式。 3.软件整体具有但不限于教学、互动、管理、测评四大软件功能模块，界面直观，简洁友好，操作便利，有在线使用帮助，符合使用习惯。 4.学生端与教师端的连接方式三种方式，可以选择老师登录、自动登录、IP地址段登录；支持多频道教学，支持多达 30 个以上频道的划分，一个教师可对单个班级或多个班级同时上课；多个教师可同时对多个班级进行不同内容的教学，互不影响干扰。 5.广播教学：可将教师机屏幕和教师讲话实时广播给单一、部分或全体学生，可选择全屏或窗口方式。窗口模式下或教师机与学生机分辨率不同情况下，学生机可以以不同的窗口方式接收广播，此时学生可跟着教师操作，边看边练。教师教学时可调用屏幕笔工具，突出显示项目、添加注释，添加批注等，并可以进行屏幕录制。支持教师机连接两个显示器，可在广播时选择将任意一个显示器的内容广播到学生机。 6.屏幕广播速度增强：支持 Direct3D，能支持三维设计软件的广播教学，比如：Cool3D，AutoCAD，Pro-Engineer，3DMAX 等，屏幕广播时支持多种画面质量的调节，根据网络的不同选择最好的效果进行教学。 7.学生演示：教师可选定一台学生机作为示范，由此学生代替教师进行示范教学在学生示范演示过程中，老师可接管学生键鼠操作，并能够进行屏幕快照，也可将示范操作进行屏幕录制，便于老师对学生的示范进行后期的点评讲解。 8.网络影院：采用流媒体技术，流畅无延时，支持几乎所有常见的媒体音视频格式， Windows Media 文件，VCD 文件，DVD 文件，Real 文件，AVI 文件，MP3 等主流文件格式；为保障使用体验良好，可依据网络及电脑配置情况，选	281500	1	281500

				择 VCD、DVD、720p、1080p 不同大小的码流播放，且可设定缓冲区大小，确保视频播放清晰和流畅均衡；可以选择一个或多个视频文件进行播放，在播放过程中可以进行切换全屏与窗口。 9.视频直播：通过 USB 摄像头将教师的画面实时广播到学生机，达到更形象的教学 D 效果，具有引导客户选择视频设，备的提示画面，以便客户快速完成摄像头设备的设置。 10.监控：教师机可以监视单一、部分、全体学生机的屏幕，教师机每屏可监视多达 36 个学生屏幕，可以控制教师机监控的同屏幕窗口数量、屏幕与屏幕间的切换速度。可手动或自动循环监视。监看时，老师可对单一学生进行键鼠的独立或共享控制，并可监看到具有典范的学生，分享屏幕，给其他学生进行演示。 11.远程命令：可以进行远程开机、关机、重启等操作，支持远程打开网页、远程启动程序和远程关闭所有学生正在执行的应用程序；并可远程设置学生桌面主题、桌面背景、屏幕保护方案、学生的频道号和音量、学生的卸载密码，是否启用进程保护，断线锁屏，热键退出等。 12.分组讨论：教师可以创建多个小组进行讨论活动，并可任意选择分组加入讨论活动。同组师生支持多种方式进行交流，包括文字，表情，图片等。 13.分组教学：教师分派组长执行指定的功能，组长代替教师；进行小，组教学，小组不需要再临时创建，可以直接使用既有分组信息，教师可以监控每个分组的教学过程，以了解分组教学的进度。 14.调查：教师可随时发起调查，将课堂教学知识点分解出题，让全体学生参与，将调查结果以答案柱状图进行分析，了解学习对各知识点的掌握情况。调查也可用于班级选举，学生评优，老师教学水平的评价等。 15.文件管理：允许教师将教师机不同盘符中的目录或文件一起发送至生机的某目录下。目录不存在自动新建此目录；盘符不存在或路径非法不允许分发；文件已存在选择自动覆盖或保留原始文件。并且学生可以把做好的作业直接提交到教师机，方便教师批改作业要收取的麻烦。通过特殊设置，学生提交作业时必需经过教师审批通过后才可提交，教师可以选择接收和拒绝学生提交的文件。支持拖拽添加文件，并且教师可以限制学生提交文件的数目和大小。			

				16.语音教学：将教师机麦克风的声音广播给学生，教学过程中，可以请任何一位已登录的学生发言，其他学生和教师收听该学生发言。教师可以选择任意一名已登录学生与其进行双向语音交谈，除教师和此学生外，其他学生不会受到干扰，可以动态切换对讲对象。 17.软件提供四种显示视图，支持监控视图、报告视图、策略视图、文件提交视图；监控视图页面提供客户端画面监控缩略图，并支持缩略图多级放大缩小。 18.分组管理：教师可以新建，删除，重命名分组，添加和删除分组中的成员，设置小组长。分组信息随班级模型永久保存，下次上课可以直接使用保存的分组。 19.报告视图：老师能详细了解整个计算机教室内，各学生姓名、IP 地址、系统类型、网络利用率、电池电量等信息。 20.终端管理：支持对 U 盘限制、网页限制、程序限制等功能；教师可以获取学生端计算机的名称、登录名和其它常用信息，并可以列出学生端的应用程序、进程和进程 ID，教师还可以远程终止学生端的进程。 21.黑屏肃静：教师可以对单一、部分、全体学生执行黑屏肃静来禁止其进行任何操作，达到专心听课目的，教师可自定义黑屏的内容与图片。 22.班级管理：班级模型中有单独的管理界面，实现对班级模型的统一管理，并能够导入、导出，调用不同网络教室中的班级模型。班级模型中可以显示学生机桌面的缩图。缩图显示大小也可自由设定。 23.签到：提供学生名单管理工具，为软件和考试模块提供实名验证。提供点名功能，支持保留学生多次登录记录、考勤统计、签到信息的导出与对比。 24.自动锁屏：独有的断线保护自动锁屏技术，通过网卡的是否激活来锁定屏幕，避免学生拔掉网线违反纪律。 25.防杀进程：为安全起见，学生端程序运行后，防止学生通过任务管理器结束学生端程序进程来逃脱教师控制。 26.请求帮助：学生端遇到问题可请求帮助，教师端可远程遥控帮助学生解决问题。			
27	服务器机柜	图腾	G3.6024	规格： 1、网络服务器机柜，	3600	1	3600

				2、机柜尺寸：42u 标准 19 英寸，高*深*宽 2000mm*1000mm*600mm； 3、整体加厚钢板，钢板厚度 1.2mm，网眼门。			
28	防静电地板	彬雯	定制	规格： 1、全钢硬质钢板结构，内部填充优良发泡水泥； 2、贴面选用瓷砖;加大加深底槽； 3、加强四周边载荷。 4、防静电地板采用上下 2 层，优良冷轧钢板厚度上 0.5mm，下 0.4mm，集中载荷≥250Kg。	375	192	72000
	合计（元）：叁佰贰拾陆万伍仟壹佰捌拾元整						3265180.00