投标分项报价表

项目编号/包号：JSZC-320400-CTZB-G2026-0153

项目名称：信息安全产品配置实训室项目　　报价单位：人民币元

序号	品名	品牌商标	规格型号技术详细要求	数量	单位	投标价格	
						单价	合价
1	防火墙	奇安信网神	型号：NSG2000-DS20 1：硬件规格：标准 1U 机箱；板载 8 个千兆电口，2 个千兆光口，1 个 Console 口，1 个 USB 接口； 2：技术参数：网络层吞吐量 2G，并发连接 100 万，每秒新建连接数 2 万；80 个 IPsecVPN 并发隧道数，80 个 SSLVPN 并发用户数； 支撑教学实践内容： 3：▲失陷主机溯源：支持内置威胁情报库。支持通过本地威胁情报库进行威胁检测；支持云端威胁情报检测；支持配置 DNS 行为控制方式，实现失陷主机检测和溯源。DNS 行为支持 DNS 放行、DNS 阻断、DNSsinkhole；支持配置 DNS 行为控制方式，实现失陷主机检测和溯源；支持威胁情报库自动及手动升级。 4：具备恶意程序防范功能，支持对网络传输信息进行恶意程序检测，支持对多种恶意程序家族类型进行检测，支持对检测到的恶意程序进行阻止处理并生成审计记录。 5：应用控制：应用程序识别库：能够检测并阻断 Web 访问、在线聊天、P2P 下载、网络游戏、网络视频、网络炒股等各种网络应用。 6：▲支持以图形化界面展示网络流量情况，能按 IP 地址、时间段等条件组合对网络流量进行统计，能以报表形	6	套	59000	354000

			式输出统计结果。 7：●网络协议：支持 MPLS 流量透传；支持针对 MPLS 流量的安全审查，包括漏洞防护、反病毒、间谍软件防护、内容过滤、URL 过滤、基于终端状态访问控制等安全防护功能； 8：▲日志模板配置：支持日志模板功能，可以设置各种日志发送的哪些字段以及字段的顺序，满足日志字段定制化需求。 9：入侵防御实践：覆盖广泛的漏洞防护规则库和防间谍软件规则库，可检测木马、后门、病毒、蠕虫、僵尸网络、缓冲器溢出、XSS 跨站脚本、拒绝服务（DoS）、恶意扫描、SQL 注入、WEB 攻击、暴力破解等各种攻击行为。支持 IPS 特征库自动及手动升级。IPS 特征库包括漏洞特征及间谍软件特征。				
2	终端安全管理	奇安信网神	型号：奇安信天擎终端安全管理系统 V10.0 1：病毒-病毒防护任务支持：全盘扫描、快速扫描、强力查杀、文件专杀、隔离区恢复、断点续扫、支持自定义扫描策略；支持无文件攻击防护、文档攻击防护、横移渗透攻击防护、内存攻击防护；不少于三个杀毒引擎混合使用，提高病毒检出率，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。 2：补丁管理：常见 windows 操作系统，办公软件等应用软件的漏洞进行在线打补丁，支持隔离网离线更新补丁库、补丁文件、系统升级包等补丁管理业务需要的数据。支持按照补丁（漏洞）	6	套	500	3000

			的维度统计漏洞修复情况； 3：防火墙：支持主机防火墙功能，通过添加 IP、域名规则、支持允许/拒绝规则、支持任意流向拦截和允许，支持 TCP、UDP、TCP+UDP、ICMP、多播和组播，支持自定义端口范围、支持自定义目标 IP，支持输入 IP 范围。 4：终端管控： 单点维护、违规外联、远程协助外设管理、进程管理、违规外联、能耗管理、网络管控、服务管控、桌面加固； 远程协助：支持管理员对在线终端进行远程协助；管理员对在线终端进行远程时，支持在被控端和主控端直接进行文件传输 外设管控：对 USB 设备、存储卡、冗余硬盘、打印机、扫描仪、键盘、鼠标、红外、蓝牙、摄像头、手机/平板设备进行控制； 违规外联：支持对终端访问互联网的出口进行探测，对使用不合规出口的终端进行网络隔离 违规外联告警、告警时长统计、出口统计及互联网出口使用情况 支持外设库管理，可统计终端外接的各种设备，包括厂商和设备类型、产品、数量、PID、VID 和设备来源。 5：移动存储管理：U 盘注册、U 盘使用管理、U 盘信息查看、取消注册、密码重置、U 盘启用、U 盘停用 外出设置、内网有效期、客户端申请、移动存储策略、例外设置、自动审核 6：▲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。 7：▲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。 8：▲支持对终端节能管理，支持对长时间运行、定时关机、空闲节能、工作时间外开机等节能类型设定策略，支持仅提示、关机、注销、锁定、关闭显示器、锁定+关闭显示器、休眠和睡眠处理。并支持提示倒计时弹窗，可设置在终端取消后下一次提醒时间。				
3	行为安全管理	奇安信网神	型号：NBM200-DS60 1：硬件规格：1U 硬件，4 个千兆电接口，提供 1 个扩展插槽，1T 机械硬盘。 2：技术参数：最大并发连接数 15 万，最大新建连接数 2000/秒； 支撑教学实践主要内容如下： 3：失陷主机检测与管控、爬虫行为检测与管控、防私接、共享接入行为检测与管控、流量管理 4:▲应用数量 10000 种,移动应用 5000 种，即时消息应用 200 种，虚拟货币交易平台 40 种，论坛发帖 3000 种，代理隧道 100 种;URL 数据 2.5 亿条 5：支持策略管理、日志审计、权限分配相互独立的三权制衡管理机制;管理员和审计员的账号创建、权限变更需要审核员审批才能生效 6：▲设备在部署时支持模式选择，可设置为 Portal 模式，实现 Portal 服务器功能； 7：展示系统应用流量使用情况概览，支持自选应用标签展示，如：消耗带宽、影响工作效率、加密应用、内容外发风险应用、高风险应用和 SaaS 应用等 8：展示系统安全状态概览，如：挂马	6	套	50000	300000

			网站访问、钓鱼网站访问、恶意软件下载、病毒传播、失陷主机事件和爬虫行为； 9：流量管控：支持基于连接数进行流量管理，可以每个人的并发/新建连接数量进行控制 10：可审计、控制 Oracle,MySql,SqlServer,PostgreSQL 等数据库的访问与操作，包括添加、删除、修改、查询等 11：可对用户设置流量限额策略，针对超出限额的部分可以设置阻塞或限速 12：支持 web 本地认证、微信认证、短信认证、二维码认证等，并支持多种认证方式组合的混合认证。 13：▲可对 HTTP/FTP/IMAP/SMTP/POP3/SCP/SFTP 传输的文件进行与云端杀毒平台联动识别病毒，并可通过威胁情报大数据平台识别失陷主机。 14：●支持 FTP/SFTP/SCP 文件上传管理，可根据文件大小、文件名、扩展名、传输方向、内容关键字进行审计过滤；支持对帐号、命令的审计与过滤。				
4	漏洞扫描	奇安信网神	型号：S1200-W010 1:硬件规格：便携式漏洞扫描系统，64G 硬盘，6 个千兆电口，2 个 USB 口，1 个 Console 口，单电源。 2:技术参数:Web 扫描域名 100 个,Web 扫描任务并发数 1 个域名。系统扫描 IP 地址 1024 个，支持扫描 A 类、B 类、C 类地址，系统扫描支持 30 个 IP 地址并行扫描。 支撑教学实践主要内容如下： 3：系统应能提供 4 大独立扫描模块，包含系统扫描、Web 扫描、数据库扫描、	6	套	80000	480000

			弱口令扫描的全面扫描能力，每个模块具备各自的配置项，可灵活修改每个模块的配置参数以满足不同场景下的扫描需求； 4：系统应支持针对指定 IP 段，同时一键下发系统扫描、Web 扫描、弱口令扫描任务，其中 Web 扫描能够自动发现该网段内的在线网站并开展扫描；弱口令扫描能自动发现该网段 IP 开放服务并自动开展弱口令扫描 5：▲系统应支持检测的系统漏洞覆盖 CVE、CVSS、CNNVD、CNCVE、Bugtraq 多种漏洞标准。 6：系统应支持导出同时包含系统扫描、Web 扫描、弱口令扫描结果的报表，可以统一分析网站漏洞、网站所在主机漏洞以及主机弱口令 7：自动探测实践-系统应支持自动探测指定网段中的 Web 站点，并可一键转为 Web 资产或一键下发 Web 扫描任务 8：系统应支持至少三种漏洞验证方式如浏览器验证、注入验证、通用验证。 9：▲系统应支持 Web 登录扫描，系统应支持 Cookie 认证、Form 认证、Basic 认证、NTLM 认证、Session 认证、Digest 认证、上传网站证书，确保 Web 登录成功。 10：●系统应支持中间件弱口令检测功能，包含但不限于：Tomcat、WebLogic、JBoss、WebSphere、GlassFish、ActiveMQ、phpMyAdmin				
5	入侵检测与防护	奇	型号： P2000-DG20P 1：硬件规格：标准 1U 机箱，单电源，4TB 硬盘；8 个千兆电口（支持 3 组 bypass），4 个千兆光口，2 个扩展插槽。 2：技术参数：网络层吞吐量 4G，IPS	6	套	60000	360000

		安信网神	吞吐 1G，并发连接 200 万。 支撑教学实践主要内容如下： 3：产品支持路由、旁路、交换以及混合模式接入； 4：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 3000 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、数据传输、风险等级等特征分类 5：▲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、微博七种分类； 6：支持基于主机或威胁情报视图，统计网络中存在失陷主机或者风险主机数量以及对应的风险等级，至少可查看遭遇风险的时间、威胁类别、情报来源、威胁简介、失陷主机 IP、用户名、资产等信息 7：能够对 HTTP/FTP/POP3/SMTP/IMAP/SMB/IPTUX 七种协议进行病毒查杀；本地病毒库规模大于 3000 万，支持样本留存和上传。所投产品必须支持病毒样本上传和页面消息推送功能 8：▲支持基于源 MAC、SSLAMAC、源地址、VLAN、前缀、跳数等条件进行 RA 管控。能够基于 M 标记、O 标记进行置位和不置位检测管控。 9：支持分析识别流量中包括的具体协议类型，包括：ICMP、HTTP、FTP、SNMP、TELNET、SMTP、POP3、IMAP、NFS、SMB、NETBIOS 等，并能对 ICMP、HTTP、FTP、SNMP、TELNET、SMTP、POP3、IMAP、NFS、SMB、NETBIOS 流量进行统计；能够对 IPv6 基础协议（ICMPv6）进行识				

			别和统计。 10：●支持灵活的细粒度引流策略，可基于源安全域、目的安全域、源用户、源地址、目的地址、服务、VLAN、服务链、流量方向（内网到外网/外网到内网）的引流策略，并详细记录日志。 11：支持威胁大屏威胁展示，至少包含：威胁严重性、威胁事件趋势、威胁类型等；且能够基于中国地图、世界地图和在线实时地图的具体攻击路径展示效果 12：▲支持与本方案中配置的桌面杀毒或终端管理软件联动，实现基于终端健康状态的访问控制；并支持阻断“高风险”的终端和未安装杀毒的终端的网络活动 13：支持基于源安全域、目的安全域、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				
6	WAF技术与应用	奇安信网神	型号：WAF3300-DG10M 1：硬件规格：标准1U机箱，256G SSD+4TB机械硬盘，双电源，8个千兆电口（3组bypass）+4个千兆光口，2个扩展卡插槽 2：技术参数：HTTP吞吐量700Mbps，HTTP新建连接数3500/秒，HTTP并发连接数15万。 3：在旁路镜像阻断模式下，可配置多组阻断以及镜像口，对检测到的攻击进行旁路阻断，并可指定对端设备MAC地址 4：▲学习轻量级蜜罐防御功能，提供伪造的后台管理系统页面，主动诱使黑客进行攻击，记录攻击行为	6	套	70000	420000

			5：调试入侵防护功能，并提供入侵防护特征库，特征库需要提供 20 种类型并提供 10000 条入侵检测特征库 6：学习攻击态势大屏实时展示功能，可通过产品自带的实时态势监测模块进行攻击态势地图展示，包含对源地址、源地域、目标资产、安全防护攻击类型、攻击趋势、HTTP 并发请求及实时事件的动画统计； 7：应急管理功能学习：支持移动端对资产的一键断网功能，提供网站一键下线以及批量下线的应急措施 8：▲支持智能封禁，通过对网站发起的攻击次数、危害级别两个维度进行算法分析与识别，进行智能封禁，并自定义攻击者封禁时间。 9：▲支持移动端管理功能，不需要安装 APP 和第三方插件，通过手机浏览器即可管理设备，并可查看设备 CPU、内存使用情况，支持移动端对资产的一键断网功能，提供网站一键下线以及批量下线的应急措施。 10：支持防暴力破解功能，可支持频率阈值，动态令牌以及频率阈值+动态令牌等三种方式实现暴力破解防护 11：支持检测并清洗的攻击类型：IP 攻击，TCP 攻击，UDP 攻击，ICMP 攻击，DNS 攻击，HTTP 攻击等 20 多种 DDoS 攻击类型 12：支持虚拟补丁功能，支持导入 Appscan 和 SecVSS 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 13：具备 WEB 应用访问控制功能，支持对 HTTP 传输内容的关键字、HTTP 请求方式（GET、POST、PUT、HEAD 等）、HTTP 请求文件类型、HTTP 协议头中各字段长度（general-header、				

			request-header、response-header 等）、HTTP 上传文件类型、HTTP 请求频率、HTTP 返回的响应内容、HTTPS 流量解密等进行控制。				
7	机柜	大唐安普	型号：B3 1： 标准机架，24U；外形尺寸 600mm（宽）×600mm（深）×1200mm（高）；前后网孔门带锁，侧板可拆，上下设走线孔； 2：主立柱板厚 1.5mm，门板/侧板 1.0mm，SPCC 冷轧钢板；静电喷塑，整机静态承重 500kg； 3：配置 4 根带 U 标方孔立柱；标配承重托盘、顶部风扇;机柜 PDU 数量 2 个。	6	台	3000	18000
8	信安产品运维配置虚拟仿真平台	奇安信网神	型号：奇安信网神网络安全综合演练系统 V7.0（CSE-ZHYL） 1：●支持虚拟设备的增、删、改、查功能，支持创建 KVM、容器两种类型的虚拟设备，可设置设备权限为公开还是私有，私有设备仅创建人可用，虚拟设备的创建支持上传镜像和安装 ISO 两种方式，支持对虚拟设备的名称、分类、图标、描述等基础信息设置，支持配置网卡名称、网卡数量、CPU、RAM、登录账号信息，KVM 类型设备支持网卡驱动、硬盘驱动、是否 UEFI 启动等信息配置，容器支持启动命令自定义配置；支持引用溯源，查看设备资源被哪些业务资源所引用； 2：支持商用虚拟化安全设备的管理，包括虚拟化防火墙、上网行为管理、漏洞扫描、入侵检测、Web 应用防火墙等虚拟化安全设备； 3：支持自定义实验网络拓扑，拖拽虚拟设备、物理设备、漏洞靶标至画布区快速搭建实验拓扑，拓扑编辑时设备图标即拖即用，无需配置关联镜像，可自定义修改虚拟机设备的 CPU、内	1	套	275000	275000

			存、网卡数量、网卡驱动、硬盘驱动等参数； 4：支持网络设备模拟，模拟数字路由器和数字交换机，可通过页面简单配置完成网络调试，启动数字网络设备不占用算力资源； 5：支持空节点图标辅助搭建网络拓扑，既丰富拓扑展示效果，又不占用算力资源，支持文本框节点，在拓扑中自定义文本描述； 6：▲支持设备连线，支持设备分组划分区域展示，支持拓扑图导出、居中显示、放大缩小显示，支持输入设备名称查询并将设备居中选中显示；支持统计拓扑所需算力资源，计算最大并发套数；支持复制整个拓扑或单个虚拟机到其他拓扑中粘贴实现快速搭建拓扑； 7：▲支持一键启动/关闭拓扑设备，也支持单个设备启动/关闭，设备关闭时显示灰色图标，设备启动后变为蓝色图标；支持编辑后的虚拟机另存为私有虚拟设备模板；支持设置每个拓扑节点在学员端的展示和操作权限，权限包括是否显示节点，是否能操作，是否能启动； 8：▲支持拓扑设备 IP 地址管理，支持 web 页面及虚拟机内部两种 IP 地址及分配操作，在 web 页面配置虚拟机及容器的 IP、掩码、网关信息，虚拟机内只需设置为自动获取 IP；虚拟机内配置静态 IP 信息，系统自动监测并同步显示在 web 页面； 9：●支持设备 VNC、RDP、SSH 几种连接访问模式，支持向虚拟机内粘贴文本和导入文件，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 RDP/SSH 模式下				

			虚拟机文件管理树形展示虚拟机内的文件列表，并支持将文件下载至本地电脑；支持标签页形式在多个设备控制台之间快速切换； 10：支持资源自动回收机制，以保证系统有限算力资源下的高并发需求，拓扑启动虚拟化资源后出现资源回收的倒计时，到期后自动收回资源，支持用户手动延时。 11：●支持系统状态检测，检测集群中每台服务器 CPU\VCPU\内存\磁盘的使用情况，检测关键服务的运行状态，包括但不限于虚拟化服务、探针服务、存储服务等； 12：支持性能管理，展示各任务对系统性能的占用情况，统计来源模块、任务名称、占用人员、占用 VCPU、占用内容等信息，并提供批量关闭及销毁功能用于资源释放； 13：●支持能力模型编排，每个能力模型支持自定义一到五级的能力等级，配置模型各等级对需要掌握能力点的要求程度，如熟悉、掌握和精通，支持按照能力要求模块设置权重，权重支持自动平均分配和手动配置两种模式。				
合计							2210000
本采购包中提供的符合本国产品标准的产品成本之和占该采购包提供的全部产品成本之和的比例为 85 %。							

注：1. 本表应按包分别填写。

2. 如果不提供分项报价将视为没有实质性响应招标文件。

3. 本表行数可以按照项目分项情况增加。

4. 上述各项的详细规格、技术参数如表格中填写不下的，可以逐项另页描述。

5. 本采购包中含有多种产品时，供应商未填写本采购包中提供的符合本国产品标准的产品成本之和占该采购包提供的全部产品成本之和的比例数值的，或比例数值未达到 80%的，将不享受本国产品价格评审优惠。

投标人名称（加盖公章）：北京信沃智数科技有限公司

日期：2026 年 11 月 25 日