二、投标分项报价表

项目名称：河南省财政厅系统整合暨一体化信息系统升级项目安全系统升级项目

招标编号：豫财招标采购-2021-1472　　标段或包号:无

报价单位：人民币元

序号	名称	品牌	型号和规格	原产地	制造商（服务商）名称	数量	单价	总价	备注
（一）机房设备									
1	国密机房门禁系统	科松	我公司所投产品产品科松国密机房门禁系统：1、功能：科松国密门禁系统：Netking门禁管理软件共4套，配套国密门禁控制器：科松 ACM6810-LAN 共 4 套、CPU 读卡器：科松 CSG-301K 共 4 套、CPU 卡：FM1216-137 卡共 20 张、GM01 发卡器 1 套等；2、部署位置：包括一楼机房的大门、配电间各 1 套，服务器区 2 套。	中国	深圳科松技术有限公司	1	48000	48000	无
（二）财政业务外网设备									
2	高级威胁检测系统（业务外网）	网神	1、我公司所投产品网神 TSS10000-M3：为软硬一体化设备；威胁检测系统硬件：含滑轨；流量监听电口 2*GE、流量监听光口 2*10GE、存储硬盘 20TB SATA；吞吐 1Gbps；产品提供原厂三年软件升级。平台：1、威胁感知平台能够对未知威胁的恶意行为实现早期快速发现，对受害目标及攻击源头进行精准定位，最终达到对入侵途径及攻击者背景的研判与溯	中国	网神信息技术（北京）股份有限公司	1	340000	340000	无

			源； 2、实现对确定的威胁进行多种类型的响应处置，实现监测预警、威胁检测、溯源分析和响应处置一体化安全目标； 3、全包取证模块：全包取证存储系统是基于全流量进行独立存储，独立维护，独立扩容模式实现，全包存储系统基于分布式存储技术构建，底层存储使用集群，系统的分析模块可支持秒级提取海量历史流量，还原网络安全事件发生时的全部网络通讯内容，支持会话趋势展示，会话列表展示，会话协议树展示，并支持相关数据包的下载； 4、分析展示：对所有数据进行快速的处理并为检索提供支持，将存储日志与威胁情报进行碰撞以及进行日志关联性分析产生告警在屏幕上展示威胁态势。支持对告警进行深度分析，支持以告警字段进行狩猎分析及可视化展示，以攻击链的视角还原告警中的受害主机被攻击的整个过程，通过支持手机端连通的协作，实时告警提醒和处置，以及报告接收等，实现业务活动时期强大的实战化运营及快速响应； 5、威胁情报模块：威胁情报可对 APT 攻击、新型木马、特种免杀木马进行规则化描述。通过人工智能结合大数据知识以及攻击者的多个维度特征还原出攻击者的全貌，包括程序						

			形态，不同编码风格和不同攻击原理的同源木马程序，恶意服务器（C&C）等，通过全貌特征、跟踪攻击者，持续的发现未知威胁，最终确保发现的未知威胁的准确性，并生成可供系统使用的威胁情报。支持与防火墙进行联动处置高级威胁，发现威胁事件后支持对攻击 IP、恶意域名和受害资产的流量进行阻断（将策略下发给防火墙，由防火墙执行阻断）； 6、产品支持基于流量实时 IOC 匹配功能，设备具备主流的 IOC，情报总量 50+万条； 7、产品支持基于工具特征的 WEBSHELL 检测，能通过系统调用、系统配置、文件的操作来及时发现威胁；如：中国菜刀、小马上传工具、小马生成器等； 8、产品支持基于 webshell 函数的攻击检测，如文件包含漏洞、任意文件写入、任意目录读取、任意文件包含、preg_replace 代码执行等； 9、产品支持基于网络请求的语义分析检测，能够将网络请求拆分为请求头、响应头、请求体、响应体四方面详细展示请求内容，并能提升对未知威胁检测能力； 10、产品以攻击者的维度进行分析，对攻击者进行画像，画像内容包括地理位置信息、国家信息、所属组织、使用的攻击手段、攻击的所有资产。						

（三）财政业务专网设备								
3	高级威胁检测系统平台（部署在业务专网）	网神	我公司所投产品为软硬一体化设备网神TSS10000-A58、网神TSS10000-S56，与高级威胁检测系统平台（部署在业务外网）品牌一致。 一、采集探针： 1、性能：吞吐 8Gbps； 2、硬件：流量监听电口 2*GE；流量监听光口 2*10GE；冗余电源；存储硬盘 4TB SATA； 3、功能：威胁感知平台能够对未知威胁的恶意行为实现早期快速发现，对受害目标及攻击源头进行精准定位，最终达到对入侵途径及攻击者背景的研判与溯源；实现对确定的威胁进行多种类型的响应处置，实现监测预警、威胁检测、溯源分析和响应处置一体化安全目标；全包取证存储系统是基于全流量进行独立存储，独立维护，独立扩容模式实现，全包存储系统基于分布式存储技术构建，底层存储使用集群，系统的分析模块可支持秒级提取海量历史流量，还原网络安全事件发生时的全部网络通讯内容，支持会话趋势展示，会话列表展示，会话协议树展示，并支持相关数据包的下载；产品支持基于流量实时 IOC 匹配功能，设备具备主流的 IOC，情报总量 50 万条；产品支持基于工具特征的 WEBSHELL 检测，能通过系统调用、系统配置、文件的操作来及时发现威胁；如：中国菜	中国	网神信息技术（北京）股份有限公司	1	750000	750000	无

			刀、小马上传工具、小马生成器等；产品支持基于webshell函数的攻击检测，如文件包含漏洞、任意文件写入、任意目录读取、任意文件包含、preg_replace代码执行等；产品支持基于网络请求的语义分析检测，能够将网络请求拆分后从请求头、响应头、请求体、响应体四方面详细展示请求内容，并能提升对未知威胁检测能力； 4、服务：产品支持三年硬件质保、三年软件升级。 二、分析展示： 1、硬件：含滑轨一台。管理电口4*GE；接口4*USB；冗余电源；存储硬盘960GB SSD+12*4TB SATA； 2、功能：对所有数据进行快速的处理并为检索提供支持，将存储日志与威胁情报进行碰撞以及进行日志关联性分析产生告警在屏幕上展示威胁态势。支持对告警进行深度分析，支持以告警字段进行狩猎分析及可视化展示，以攻击链的视角还原告警中的受害主机被攻击的整个过程，通过支持与终端进行的协作，实时告警提醒和处置，以及报告接收等，实现强大的实战化运营及快速响应；威胁情报模块：威胁情报可对APT攻击、新型木马、特种免杀木马进行规则化描述。通过人工智能结合大数据知识以及攻击者的多个维度特征还原出攻击者的全貌，包括程序形态，不同编码风						

			格和不同攻击原理的同源木马程序，恶意服务器（C&C）等，通过全貌特征‘跟踪’攻击者，持续的发现未知威胁，最终确保发现的未知威胁的准确性，并生成了可供系统使用的威胁情报。产品支持与防火墙进行联动处置高级威胁，发现威胁事件后支持对攻击 IP、恶意域名和受害资产的流量进行阻断（将策略下发给防火墙，由防火墙执行阻断）；产品以攻击者的维度进行分析，对攻击者进行画像，画像内容包括地理位置信息、国家信息、所属组织、使用的攻击手段、攻击的所有资产。						
4	网络全流量安全分析取证系统（部署在业务专网）	科来	我公司所投产品科来 TSAS3014ST、科来 BFCS3AF： 一、总体描述： 1、我公司所投产品具有国内自主知识产权，对网络通讯数据进行 7*24 小时的捕获、存储、挖掘及专家分析，从而提供对任何时间点的通讯数据进行回溯分析能力，通过对网络元数据提取和行为建模，发现未知网络威胁，具备多维的数据分析及深度挖掘能力，针对特种木马攻击，渗透，窃密等行为进行精确定位； 2、还原网络安全事件发生时的全部网络通讯内容，实现数据包级的数据取证和责任判定。 二、网络全流量安全分析系统： 1、我公司所投产品为软硬	中国	成都科来网络技术有限公司	1	730000	730000	无

			一体化设备，系统存储容量 8TB，外接存储为 48TB，外接储存与分析设备为同一品牌，采用 RAID5，采集端口：2 个千兆光口+2 个千兆电口（含多模光模块），数据捕获能力 3000Mbps； 2、系统部署：系统基于 C/S 架构，提供专用客户端软件，能够通过自身控制台界面对设备采集的数据进行精细化分析，真实还原安全事件的发生过程，对各种异常网络行为进行精准的定性和数据取证；同时对捕获到的所有通讯数据包进行长期存储。（已提供产品界面截图，已加盖原厂公章）； 3、协议识别：能够识别 1500 种协议识别和 10000 种网络应用； 4、行为建模：支持用户自定义根据分析、提取和统计 13 类元数据日志提取，元数据提取字段个数 200 种。通过元数据提取，对各种网络异常行为进行描述，建立异常行为模型感知网络会话异常行为。（已提供产品界面截图，已加盖原厂公章）； 5、安全分析：（1）及时发现潜在未知网络威胁，针对特种木马攻击，渗透，窃密等行为进行精确定位，通过事件关联分析对安全事件影响进行有效评估。（2）通过内置情报特征库、自定义特征库及行为模型，对木马心跳通讯、可疑文件传输、主动外联、境外通讯、异常 DNS、高危						

			特种木马以及僵尸网络检测分析； 6、流量解析：（1）多维数据分析和提取，可提取17个维度的数据统计，流量统计指标50个。（2）对TCP会话中的详细应用数据传输过程进行深入分析，能够区分每一个TCP和请求和响应，能够图形化的显示TCP会话中的数据交互传输过程，能够图形化显示数据传输中的时间间隔。（3）针对TCP/UDP会话的流重组功能，将会话中的数据流重组显示，支持数据流解压显示； 7、数据挖掘：（1）数据分析的时间精度为纳秒级，且支持分钟、小时、天等多种时间窗口对流量数据进行检索、挖掘、提取。（2）多层次数据钻取，5个层次的数据钻取分析，并且支持第五层原始数据的流还原可视或可提取。（3）以十六进制和ASCII码方式展现数据包内容，展现tcp会话建立连接三次握手及关闭连接的交易时序图，数据流还原传输文件的内容、还原图片、证书、常见文档等； 8、回溯分析：支持通过原始数据包对任意时间流量进行完整回溯，定位安全事件时间、源IP、目的IP、事件起因、事件经过以及事件造成的影响；支持对第三方安全设备告警日志安全事件回溯，通过IP等信息检索方式提取安全事件所涉及的流量数据包。（已提供产品界面截图，						

			已加盖原厂公章）； 9、数据取证：通过原始数据包对任意时间进行完整回溯，定位安全事件时间、源 IP、目的 IP、事件起因、事件经过以及事件造成的影响；支持对第三方安全设备告警日志安全事件回溯，通过 IP 等信息检索方式提取安全事件所涉及的流量数据包。（已提供产品界面截图，已加盖原厂公章）； 10、产品具备公安部监制的计算机信息系统安全专用产品销售许可证和检验报告； 11、产品具备软件著作权证书； 12、产品具备中国信息安全认证中心颁发的网络关键设备和网络安全专用产品安全认证证书。 三、大数据追踪取证系统： 1、配置：2U 标准服务器，管理接口：2 个电口+2 个光口，系统存储容量 16TB，支持 RAID5； 2、威胁可视：支持安全态势展示，包括实时攻击情况，全球攻击源分布，攻击关联和威胁类型分布； 3、数据存储：支持中心自定义保存任意 IP 的历史流量以 pcap 格式存储到中心，并支持 500Mb 的数据包文件； 4、威胁分析：支持 IP 画像展示攻击影响面、通联关系、威胁情报信息，对警报日志进行自定义的多维度统计分析，支持警报日志列表分析、笛卡尔分析、维度分析、数据透视						

			分析；支持攻击者和被攻击者的载荷传输时间统计，精度达到微秒级，支持ASCII,EBCDIC,GBK,UTF-8等5种编码切换展示攻击载荷；支持NAT网络环境下，纵深部署的多节点自动关联真实攻击源IP（已提供产品界面截图，已加盖原厂公章）； 5、威胁情报分析：支持新增情报自动回查历史通讯数据，支持用户自定义威胁情报； 6、支持网络日志关联原始数据包分析，保存网络日志数据透析条件，便于反复利用； 7、第三方警报日志关联分析：支持防火墙、IDS、IPS等安全设备告警日志关联数据包，用于攻击研判，取证；支持自动关联保存第三方安全设备警报日志相关数据包； 8、数据包分析：支持web在线解码原始数据包分析；支持中文数据包分析工具解码数据进行分析； 9、网络流量基线：支持网络流量机器学习，能够自动学习建立网络正常运行基线，并能对异常指标进行标记；基线数据类型括但不限于：流量总字节数、入网流量、出网流量、总包数、入网包数、出网包数、ARP包数、icmp包数、小于64字节数据包数量、tcp总数据包数，tcpsyn数据包数、tcpsynack数据包数、tcprst数据包数、tcp重传数据包数、新建会						

			话数量、并发会话数量；（已提供产品界面截图，已加盖原厂公章）。 10、威胁扩线：支持对探针全流量数据进行特征回查，支持域名、IP 通联关系可视化统计和挖掘；支持对探针进行数据包级的流间行为历史数据回溯分析。						
5	远程安全评估系统（部署在业务专网）	天融信	我公司所投产品天融信脆弱性扫描与管理系统 TopScanner 7000 V3：1、规格性能：1U 标准机架式设备，含交流单电源模块；1 个 RJ45 串口，1 个 GE 管理口，配置 4 个 10M/100M/1000M 自适应以太网电口扫描口，4 个千兆 SFP 插槽（不含光纤接口模块），1 个接口扩展槽，硬盘容量 1TB，最大并发扫描 60 个主机，最大扫描速度 1000ip/h，标准配置提供 1 路授权扫描端口； 2、授权扫描无限地址或域名； 3、支持检测的漏洞数量 21 万条，兼容 CVE、CNCVE、CNNVD、CNVD、Bugtraq 等主流标准； 4、提供符合安全等级保护配置检查规范 2.0 进行安全配置合规分析，提供符合通用配置检查规范进行安全配置合规分析，安全配置检查模块类型包括：windows、solaris、Linux、AIX、HP-UX 操作系统；Oracle、Sybase、MySQL、DB2、SQL Server、informix 数据库；Tomcat、Apache、WebLogic、WebSphere、Jboss、IIS、Nginx、Resin、	中国	北京天融信网络安全技术有限公司	1	490000	490000	无

			BIND、Exchange、Domino 中间件；Juniper、Cisco、Huawei、ZTE、H3C 路由器；Juniper SRX、Juniper Netstreen、Huawei、Pix、H3C、Fortigate、Dptech、Hillstone、Nsfocus 防火墙；Cisco、Huawei、ZTE、H3C 交换机；Dptech、H3C、Topsec、Nsfocus 网络入侵检测系统；Dptech、H3C、Topsec、Nsfocus 网络入侵防护系统；Dptech、H3C、Topsec、Nsfocus WEB 应用防火墙等； 5、漏洞验证模块：提供针对扫描的部分系统漏洞进行取证性质的验证；通过漏洞扫描、漏洞告警、漏洞管理、漏洞跟踪处理、统计分析以及资产设备管理对漏洞进行管理控制；有利于跟踪和追溯系统设备的安全风险，并且能够有效的评估整个网络系统的安全状况，识别出网络薄弱环节；具备单独口令猜测扫描任务，支持多种口令猜测方式，包括利用 SMB、TELNET、FTP、SSH、POP3、TOMCAT、SQL SERVER、MYSQL、ORACLE、SYBASE、DB2、SNMP 等协议进行口令猜测，允许外挂用户提供的用户名字典、密码字典和用户名密码组合字典；提供高级漏洞模板过滤器，支持将符合筛选条件的漏洞自动加入到自定义漏洞模板中，及后续插件升级包中的漏洞也可以自动加入到模板中；容器镜像扫描模块：提供容器镜像扫描功能，能够针对容						

			器镜像进行漏洞检测和分析。提供安全配置检查功能：能够针对容器镜像配置进行检测，提供针对容器镜像的安全配置检测和分析； 6、系统提供 HTTP/RPC 接口支持，方便与第三方产品联动； 7、服务：我公司提供三年漏洞库升级服务。						
6	WEB 漏洞验证专用扫描器（部署在业务专网）	绿盟	我公司所投产品绿盟 WEB 应用漏洞扫描系统 V6.0（WVSS NX3-S）：1、规格性能：1U 标准机架式设备，含交流单电源模块；1 个 GE 管理口，配置 4 个 10M/100M/1000M 自适应以太网电口扫描口，4 个千兆 SFP 插槽（不含光纤接口模块），1 个接口扩展槽，页面处理能力 20 万页/天，标准配置提供 1 路授权扫描端口；授权扫描无限地址或域名。 2、部署方式：支持分布式部署，多台设备的集群管理，支持多任务负载均衡，单任务 URL 级别的负载均衡方式。 3、检测范围：漏洞知识库漏洞信息 2400 条，漏洞知识库与 CVE、CNCVE、CNNVD、CNVD、CVSS 等主流标准兼容；支持 Cookie 注入、XSS 检测、Cookie 有效性检测，支持网页挂马检测；支持隐藏字段检测；支持跨站脚本攻击检测，检测出 20 种基于 GET 请求、POST 请求的跨站攻击方法及变种； 4、检测能力：对 Web 应用提供专业的漏洞、挂马检	中国	北京神州绿盟科技有限公司	1	210000	210000	无

			测和分析功能，提供 Web 漏洞验证功能，支持手动、自动的 Web 漏洞验证操作；通过获取网站的指纹信息，根据所述网站的指纹信息确定网站对应的漏洞库，然后对网站进行漏洞检测；有效提升漏洞扫描的准确率；支持基于 basic、NTLM、Cookie 等认证方式的 Web 应用系统安全扫描；支持基于 HTTPS 应用系统的扫描；产品支持自定义扫描连接与自定义排除连接，支持预设 Cookie 和登录预录制检测；支持 HTTP 和 SOCKS 代理扫描，支持自定义 User-Agent 设置；支持动态和静态结合的交互式检测；支持探测网站前是否有防护产品，如 WAF 设备； 5、漏洞分析与管理：仪表盘功能，直观展示最近 10 天整体风险等级、扫描站点列表、危险站点 TOP10 等内容；产品具有漏洞验证功能，直观展示漏洞验证过程信息，验证漏洞真实存在； 6、服务：提供三年漏洞验证功能的规则包升级。						
7	入侵防御（部署在业务专网）	绿盟	我公司所投产品绿盟网络入侵防护系统 NX3（千兆）V5.6（NIPSNX3-HD2200）： 1、硬件：具备 BYPASS 功能的 10/100/1000Base-T 接口 4 个，网络接口扩展槽位 1 个。含嵌入式集中管理中心软件一套，最大整机吞吐量 5G，最大并发连接数 300 万；IPS 吞吐量 1G； 2、操作系统：操作系统为	中国	北京神州绿盟科技有限公司	1	42000	42000	无

			通用安全平台，具备高效、智能、安全、健壮、易扩展等特点； 3、入侵防御功能：系统可检测的入侵防御事件库事件数量 4000 条，系统支持事件响应模版，能够批量修改事件响应动作，包括：事件级别、事件启用开关、动作、日志合并方式、日志开关、抓包取证。系统支持多种防 web 扫描能力，包括爬虫、CGI 和漏洞扫描等，并支持设置 5 个不同级别的扫描容忍度/扫描敏感度。系统支持弱口令检测功能，支持 8 种网络协议并支持 7 种弱口令检测元素，文字说明支持的网络协议和定义弱口令的检测元素。系统支持 SQL 注入、XSS 攻击检测能力，并支持提供白名单定义功能，能够精确到检测测字段、属性和名称。并支持 10 类和 70 个配置项目； 4、恶意代码检测功能：系统应提供扩展静态恶意代码（APT）检测引擎，针对 http、ftp、SMTP 等协议中包含的未知恶意文件进行检测；系统支持与动态恶意代码（APT）检测系统联动功能，通过联动功能可将恶意样本发送到动态 APT 引擎进行深度检测，并将检测结果生成攻击特征样品进行动态拦截；系统支持可扩展未知 C&C 通道（隐蔽通道）检测功能，能够提供 C&C 通道的危险级别、连接建立时间、连接持续时间、控制端 IP 地址和端口、受控端 IP 地址						

			和端口等 C&C 通道信息，系统除具备可扩展的本地恶意代码检测功能外，还应具备云查杀、云检测等防御机制； 5、其他：提供三年入侵防御特征库升级授权；						
8	日志审计（部署在业务专网）	绿盟	我公司所投产品绿盟日志审计系统 V2.0（LASNX3-L6000）：1、规格性能：2U 标准机架式设备，含交流双电源模块，专用硬件平台和安全操作系统；2 个 GE 管理口，配置 4 个 10/100/1000M 电口（2 路 Bypass），内置存储：3*12TB 硬盘做 RAID5，单台设备平均日志处理性能：10000EPS，支持扩展外置采集器；授权接入 750 个日志源，日志存储时间 180 天； 2、监测范围：管理范围包括但不限于网络安全设备、网络设备、数据库、中间件、操作系统、应用系统等； 3、系统部署：系统支持 IPv4、IPv6 环境下部署；系统支持 NAT 场景的日志采集。 4、数据采集：系统支持配置外置采集器，外置采集器数据应提供加密压缩传输，以确保数据安全以及传输效率；系统支持的数据采集方式包括但不限于 SYSLOG、RSYSLOG、SNMP Trap、FTP、ODBC、JDBC、Netflow、WMI、二进制数据、专用 Agent 等方式采集日志；支持获取待识别的会话数据包，将二级网段 IP 地址相同的会话数据	中国	北京神州绿盟科技有限公司	1	350000	350000	无

			包划分为一类分类数据包，将包含相同域名的分类数据包合并为目标数据包，然后获取待查找的应用关键词，并确定与应用关键词对应的目标域名，最后将目标数据包中包含目标域名的会话数据包作为待分析会话数据包。 5、日志管理：系统应能实现海量日志数据的采集并保存原始日志数据；系统能够对异构日志格式进行统一化处理并保存统一化处理后的日志数据；系统支持范式化日志多级提取，支持正则、KV、格式串等多种灵活的提取方式；系统支持 IPv4、IPv6 日志数据的采集、范式化、分析、展示；系统支持日志源监控能力，包括采集器维度及资产维度的监控，资产维度支持展示资产详细信息；日志转发：系统应提供日志转发功能，应支持日志转发多个目标地址，可实现原始日志、范式化日志的转发，且不丢失原始日志源 IP 信息。 6、日志存储扩展：系统支持以 NFS 网络共享存储扩展的方式进行日志存储扩展。 7、统计与报表：系统支持自定义报表目录、LOGO 等。						
9	数据库库内容保密检查系统（部	世平	2、产品配置：网口：	中国	杭州世平信息科技有限公司	1	340000	340000	无

	署在业务专网）		4*10/100/1000Base-T，可扩展 2*SFP；存储：1Tb SSD；电源：单交流电源，100G/天（包含压缩文件、图片和文件指纹识别）150G/天（不包含压缩文件、图片和文件指纹识别），1500 万条/时（普通表 80%与二进制表 20%混合模式），2500 万条/时（纯字符、数字字段）； 系统功能： 1、支持国外主流数据类型的保密检查：MySQL、MariaDB、Sqlserver、PostgreSQL、SQLite、Oracle、Sybase、DB2、Informix、Microsoft Access 等；（提供系统截图，已加盖原厂公章） 2、支持国内主流数据类型的保密检查：达梦、人大金仓、神通、神舟 OSCAR、南大通用、瀚高、虚谷、优炫、高斯、Tidb、TinkerPop 数据库等；（提供系统截图，已加盖原厂公章） 3、支持非关系型数据库检查：Redis、HBase、MongoDB 等；支持基于 Linux 搭建服务器的检查，通过 SSH 协议的方式进行数据采集；支持基于 Windows 搭建服务器的检查，例如门户、OA 等系统内容的检查，通过 SMB/FTP 协议的方式进行数据采集； 4、支持 OFD、Ceb、Cebx 等国产化数据格式的内容识别检查；（提供系统截图，已加盖原厂公章） 5、可扩展配置国产化终端保密检查模块：绿色终端						

			分布式保密检查，无需安装，一键部署。可扩展 1000 个终端许可。（提供系统截图，已加盖原厂公章） 6、其他：能够提供国家保密技术测评中心的测评报告，已加盖原厂公章。						
10	服务器端 SSL 证书	华测	我公司所投产品华测服务器端 SSL 证书：1、功能：应用系统数据传输时需要使用 SSL 协议，SSL 是为网络通信提供安全及数据完整性的一种安全协议；客户端访问服务器应用系统时，通过服务器颁发导入的 SSL VPN 证书可实现客户端访问身份认证和数据加密传输功能，可保证网络通信的安全和数据的完整性； 2、算法：SSL 证书支持 SM1、SM2、SM3、SM4 等国密算法； 3、服务：三年授权服务。	中国	华测电子认证有限责任公司	1	33600	33600	无
11	安全国密浏览器	海泰	我公司所投产品 SHM1602-G 安全浏览器密码模块：1、适配国产化 CPU 架构，能够适配国产化终端（适配 ARM 架构） 2、功能：高性能安全浏览器密码模块，支持国产密码算法；支持我国网络自主信任体系，支持我国关于密码的相关规范。基于 SM2、SM3、SM4 算法及系列国家密码标准，实现 SM2 算法 SSL 链接功能；支持国产算法证书，并原生支持国内各大 CA 根证书及相应证书链；提供对 USBKEY 等多种形态身份认证设备、使用环境及相关控件的管理，打造安全省心的业务使用环境，保障重要业务系统的安全可	中国	北京海泰方圆科技股份有限公司	50	148	7400	无

			靠。 3、浏览器内核及优化组件、浏览器界面 UI、密码算法/SSL 协议逻辑运算模块、智能密码钥匙接入模块、插件和证书管控模块、安全策略模块。支持 SM2、SM3、SM4 算法，与 Web 服务器之间建立安全通道，保证 Web 网页访问的安全性。采用 SM2(ECC)_SM4_SM3 算法组合时，在 SSL 隧道下，吞吐率 80Mbps 4、提供浏览器密码模块《商用密码产品认证证书》，（提供复印件已加盖原厂公章）						
12	智能密码钥匙	海泰	我公司所投产品 SJK1110-G 智能密码钥匙： 1、适配国产化 CPU 架构，能够适配国产化终端（适配 ARM 架构） 2、功能：支持 SM1、SM2、SM3 算法，具有身份认证、加/解密、签名/验签等功能；SM1 加/解密速率 1.65Mbps/1.65Mbps；SM2 密钥对生成速率 21.33 对/秒；加/解密速率 60.00Kbps/189.00Kbps；签名速率 103.26 次/秒；验签速率 59.24 次/秒；SM3 运算速率 3.[illegible]Mbps。 3、提供智能密码钥匙《商用密码产品认证证书》，（提供复印件已加盖原厂公章）	中国	北京海泰方圆科技股份有限公司	6000	28	168000	无
13	数据库语句安全审查（部	云和恩墨	我公司所投产品云和恩墨 SQL 质量管控平台[简称：Enmo-SQM]：软硬一体化设备：能够自动抓取数据库开发与运行环境中的对象设计与 SQL 信息，并依据	中国	云和恩墨（北京）信息技术	1	338000	338000	无

	署在业务专网）		既定的审核规则分析，找出对象设计与 SQL 中的潜在问题，给出专业改进建议。SQM 可在应用开发、测试、上线、生产不同阶段对 SQL 进行质量管控，前置性地保障应用稳定、高效运行。支持 Oracle 数据库、达梦等国产数据库。能够检测原 Oracle 数据库迁移到国产数据库数据库上的语法兼容性；在应用改造的测试阶段发现 SQL 的规范和性能问题，避免线上故障。通过连库审核、Jenkins、openAPI 等功能，可以监控生产数据库上 SQL 的运行，对性能较差的 SQL 进行优化，提升生产环境的稳定性。性能：SQL 审核速度 400 条/秒；采集模块微服务化，多源数据库并行审核；单日单库审核 SQL 日志量 1.5G。		有限公司				
14	云安全资源池升级（部署在业务专网）	深信服	我公司所投产品深信服云安全管理平台 CSSP、深信服 SdSec-1000-C606：原云安全服务软件平台组件升级：原有安全资源池平台含有 3 套虚拟化安全组件，本次对原有 3 套软件版行升级，以确保软件能够起到正常安全防护的功能。本次升级针对原安全资源池内的防火墙、Web 防火墙，上网行为管理、VPN、数据库审计、堡垒机、日志审计、终端安全 EDR、应用交付、网页防串改等组件进行版本和规则库的升级。升级服务年限：1 年。云安全服务软件平台组件扩容： 1、本次扩容新增 1 套具备	中国	深信服科技股份有限公司	1	661000	661000	无

			公安三所颁发的《云计算产品信息安全认证证书》-SaaS 增强级的云安全服务软件平台（提供原厂证明材料，已加盖原厂公章）：包含云安全服务平台底层超融合软件，可以达成对底层虚拟资源的灵活调用以及对安全组件的灵活分配。平台还需包含租户管理、安全架构、系统管理等功能模块。 2、支持分布式部署多套安全资源池的集中运维，在主节点上可集中查看分支节点的资源利用率（包括CPU、内存、磁盘利用率），并对授权池服务到期，网络故障以及主机资源不足的节点进行集中告警，支持在主节点上直接管理分支节点；支持对云安全服务平台中的集群资源环境一键检测，对硬件健康、平台底层的虚拟化的运行状态和配置，进行多个维度进行检查，提供快速定位问题功能，确保系统最佳状态；平台支持同步主流云管（如华为）的租户信息，自动完成租户创建；与云平台松耦合，便于适应多厂商云平台，不能在云平台内部以虚拟机的方式安装安全产品，不能采用网络设备硬件一虚多的方式，降低扩展性；支持基于同一套安全防护组件来防护多云上的用户业务，为用户提供跨云一致的安全体验；本次扩容需要新增20套云安全服务平台组件，包含防火墙、Web防火墙，上网行为管理、						

			VPN、数据库审计、堡垒机、日志审计、终端安全 EDR、应用交付、网页防串改等类型安全组件。新增安全组件可根据云平台系统业务和系统安全级别的变化，进行灵活的安全组件转换、调整、组合，以便可以满足不同业务系统的个性化安全需求。 3、平台能够提供虚拟下一代防火墙、虚拟上网行为管理、虚拟 SSL VPN、虚拟负载均衡、虚拟数据库审计、虚拟运维安全管理、虚拟日志审计、虚拟云镜脆弱性扫描、终端安全检测与响应、虚拟 IPS、虚拟 WAF、网页防篡改等独立的安全组件，还能够集成第三方生态产品以扩充平台安全能力。（提供产品界面截图，并加盖厂商公章）。 4、支持在系统界面上以滑尺方式动态分配安全组件的性能规格，同时支持已分配组件规格的动态变更和授权回收，回收后的授权可以分配给其他用户和其他类型的安全组件使用；支持关键安全组件双机功能，保障安全组件高可用。 5、VPN、下一代防火墙、数据库审计等安全组件和底层资源池部分的（计算虚拟化、存储虚拟化、网络虚拟化）应为同一厂商品牌提供，以保障平台的扩展性和兼容性。（提供上述产品原厂商软件著作权证明，已加盖原厂公章）。						

			6、负载均衡组件支持主动探测方式与被动观测方式结合使用的服务器健康检查手段，以便适应各种复杂应用交互流程，保障业务系统的高可用性；微隔离：支持将服务器划分业务组，并且配置业务的应用角色，支持基于业务域的应用角色访问控制的配置，支持基于业务域的应用角色访问策略的显示，支持根据 IP 和端口访问控制的配置。 7、为保障防火墙对未知威胁防护的安全能力，所投防火墙组件的生产厂商具备中国信息安全测评中心、公安部信息安全产品检测中心、中国软件评测中心之中任意一家机构出具关于“未知威胁检测”的测试报告复印件，已加盖原厂公章。 8、为保障终端安全检测与响应的威胁检测能力，构建轻量级、智能化、响应快的终端安全系统，需提供赛可达实验室产品测试报告复印件，已加盖原厂公章。 9、本次扩容新增 1 套云安全运营中心：包含云安全平台运营中心平台，能够提供平台和租户的事件管理、报表管理和安全大屏等模块，以便能够实现统一监测和收集各租户的安全事件，实现安全风险统一管理和闭环处置；支持展示模式和排障模式两种形态的安全架构页面，方便运维人员在全局展示和故障排查之间快速切换。						

			10、支持基于单租户视角的安全运营中心，能够统一监测和收集各安全组件的日志，从业务系统维度实现安全风险统一管理，并且能够通过大屏进行投放，实现租户安全集中可视化。（提供产品界面截图） 11、支持基于云平台整体视角的安全运营中心，能够统一监测和收集各租户的安全事件，从租户维度实现安全风险统一管理，并且能够通过大屏进行投放，展示安全资源池的运营情况，及租户的安全建设情况。（提供产品界面截图，并加盖厂商公章） 12、本次扩容需要新增 1 套云安全日志中心：需要包含云安全平台日志中心平台，能够实现对平台中的安全日志、管理日志、运维日志、攻击日志和风险日志等进行留存和审计，满足合规。 13、支持以月、周为单位定期生成租户的 PDF 安全报表，包括业务的风险情况，及运维人员的服务情况，提升租户的服务感知。（提供界面截图和安全报表示例并加盖厂商公章） 14、对安全事件重新定级。能根据统一的安全策略，按照安全设备识别名、事件类别、事件级别等所有可能的条件及各种条件的组合对事件严重级别进行重定义；系统既可以完全收集采集对象上的日志信息，也支持在安全事件收集引擎上设置过滤条件，						

			可过滤出无关安全事件，满足根据实际业务需求减少采集对象发送到核心服务器的安全事件数，从而减少对网络带宽和数据库存储空间地占用；此次新增的云安全服务软件平台需要和原有云安全服务软件平台无缝对接，原有云安全组件可以在新增的云安全服务平台上运行，且可实现统一纳管管理。 15、云安全服务硬件平台扩容：此次新增的云安全服务硬件平台性能可以承载原有和本次新扩容的安全组件。硬件平台扩容：配 2 台，单台性能：CPU：2 颗 GOLD 6226R 2.90GHz（16C）;内存:8*32GB DDR4 2666；系统盘：1*240GB SATA SSD，缓存盘：1*480GB，数据盘：2*4TB，标配盘位数：12；电源：白金，冗余电源；接口：6 千兆电口+6 万兆光口;含：1 个授权销售 key；4 个服务器万兆光模块;3 年产品质保。						
（四）安全服务									
15	安全风险及运维管理服务	定制	我公司所投产品山谷服务：1、根据自身安全现状，梳理运营工作，开展的安全运营体系，结合组织架构、信息化程度建立等安全运营体系；根据“一个中心，三重防护”的安全防护设计理念，构建一个安全管理中心的安全运营管理服务。开展联动处置、威胁预警功能，通过与其他安全产品进行联动对接，实现安全威胁及时有效的处置；开展资产发现、	中山谷网安科技股份有限公司		1	62000	62000	无

			资产管理、脆弱性管理、资产风险评估等功能，实现对全网资产探查、资产变化情况有效掌控；对展平台中报表的数据分析，高质量的报表内容能够有效协助运营人员进行决策分析，可按照时间和空间维度持续的反映出当前网络所存在的安全问题。 2、服务：提供 12 个月 1 人的 5*8 小时驻场运行安全维护服务。						
总价：小写：4570000.00 元　大写：肆佰伍拾柒万元整									

投标人：山谷网安科技股份有限公司（企业电子签章）

法定代表人或负责人或委托代理人：_____（个人电子签章）

日　　期：2021 年 12 月 16 日

注：1. 货物名称的排列顺序应与招标文件中提供的货物名称排列顺序一致。

2. 上述货物中的报价应包含招标文件中规定的全部内容。

3. 上述各项的详细分项报价及用于本项目的备品备件、专用工具、伴随的技术服务等其他内容，投标人如果认为需要写明，可另页描述。

4. 如果开标一览表（报价表）内容与本表内容和合计金额不一致的，以开标一览表（报价表）内容为准。