四、投标分项报价表

项目编号/包号：常采公[2022]0134 号/分包 2　项目名称：常州市自然资源和规划局 GPU 服务器等算力支撑系统、边界安全等防护系统项目　报价单位：人民币元

序号	分项名称	品牌商标	规格型号	技术参数	数量	单位	投标价格	
							单价	合价
1	全网流量威胁感知分析系统（安全态势分析平台）	深信服	SIP-1000-B400	国产化品牌 ☆内存≥96G，硬盘≥8*4T，产品提供不少于 4 个千兆电口，产品采用标准 2U 架构，配备冗余电源， ☆支持不同安全视角展示 16 个独立的大屏展示功能，包括全网安全态势感知大屏、分支安全态势、安全事件态势、通报预警态势、资产态势大屏等，同时能满足多种场景的监控，比如日常运维、护网场景（需提供产品功能截图证明） ☆支持 700 种以上安全设备、网络设备、DHCP 服务器、蜜罐、中间件等设备日志接入，支持 syslog、winlogbeat、jdbc、wmi、webservice、ftp、snmp trap 等接入方式（需提供产品功能截图证明） ☆支持自定义分支管理权限，分支管理员具备独立的管理页面，只能管理和查看所属分支的业务和终端资产的安全信息且具备完整的功能展示（需提供产品功能截图证明） ☆支持通过主动发送微量包的扫描方式探测潜在的服务器（影子资产）以及学习服务器的基础信息，资产指纹信息包括资产类型、端口、操作系统、mac 地址、主机名等（需提供产品功能截图证明） ☆支持资产多级分支管理，最多可至 15 级分支，支持资产全生命周期自动管理，包括资产自动发现、多级资产、资产入库审核、资产离线风险识别、资产退库、资产数据更新，责任人管理机制等（提供产品功能截图证明） 密码检测技术基于人工智能学习技术（无监督自我学习）提取登陆成功的特征，通过人工智能技术对响应体内容和登录跳转路径进行持续学习训练登录成功特征，包括响应体内容、响应体关键字、响应体、响应体长度	1	台	298500	298500

				☆具备基于AI的webshell通信流量检测，可检出加密（如冰蝎）的通信流量。具备650+webshell规则检测，且覆盖 webshell 整个攻击阶段检测，包括webshell上传点探测、webshell上传下载、webshell通信（提供产品功能截图证明）				
				支持资产属性重新识别，当发现资产数据不准确时，可清空该资产属性，如主机名、备注、操作系统、标签、地理位置、硬件信息、应用软件信息、账号信息、责任人信息、端口信息等，重新发起识别后，平台会自动补齐资产属性，可批量操作				
				具备元数据行为分析引擎：httpflow、dnsflow、adflow、icmpflow、maillflow 等，通过异常行为分析，结合各类机器学习算法完成未知威胁检测。包括：内网穿透、代理、远控、隧道、反弹shell等事后检测场景				
				☆支持挖矿专项检测页面，具备挖矿攻击事前、事中和事后全链路的检测分析能力，综合运用威胁情报、IPS特征规则和行为关联分析技术，如检测发现文件传输（上传下载）阶段的异常，对挖矿早期的准备动作即告警（提供产品功能截图证明）				
				☆支持文件、邮件、勒索、挖矿相关安全事件专项页面展示，且所有专项告警支持直接进行联动处置，联动处置支持自动调用内置处置策略模板，也支持自动化编排的自定义处置流程策略（提供产品功能截图证明）				
				支持平台内置的静态文件检测引擎、AI 智能引擎、未知威胁查杀引擎、webshell 检测引擎，利用 LSA, Auto Encoder, LogicRegression, SVM, 随机森林，XGBoost 等多种机器学习算法组合进行综合研判。支持采用 AI 技术针对无文件落地的恶意脚本进行检测				
				支持可快速生成月度、季度、年度 PPT 报表，包含网络安全整体解读、网络安全风险详情、告警及事件响应盘点等，帮助用户高效汇报，体现安全工作价值				
				☆支持利用人工智能画像技术进行资产的行为分析，对这些对象进行持续的学习和行为画像构建，以基线画				

				像的形式检测异于基线的异常行为作为入口点，结合以降维、聚类、决策树为主的计算处理模型发现异常用户/资产行为。共含有 19 种异常行为学习模型；并支持用户对人工智能画像基线进行自定义调整，优化模型（提供产品功能截图证明）				
				☆支持云端与本地威胁情报共享，实时收集同步攻击者 IP，并详细展示情报列表，包括 IOC、区域、来源、更新时间、剩余封锁时间、状态、操作等，并可对本地威胁情报及云端威胁情报联动本项目中互联网防火墙实现自动封锁（提供产品功能截图证明）				
				☆所投产品具有公安部《计算机信息系统专用产品销售许可证》，需提供相关证明材料				
				☆三年软硬件质保升级服务，提供售后服务承诺函。				
				质保期内需配合用户方提供平台优化、部署及运维服务。				
2	全网流量威胁感知分析系统（流量采集设备）	启明星辰	天阗 NT3000-CSW	国产化品牌	1	台	214300	214300
				标准 2U 机架设备，双电源，专用硬件平台和安全操作系统				
				☆设备标配 1 个 RJ-45 Console 口，6 个 10/100/1000 Base-T 接口，4 个 SFP 接口（不含模块），2 个 USB 口.二个扩展插槽.				
				最大并发连接数不低于 200W				
				每秒新建连接数不低于 4W				
				物理存储容量 2TB				
				☆采用 Venusense 多核并行操作系统架构或 LODP 系统架构或 ANIMAS 系统架构；非传统多线程、ASIC 等架构方式（需提供产品功能截图证明）				
				☆系统需具备分布式部署能力，可以支持一个管理中心管理多台检测引擎的部署方式，方便攻击告警信息在统一平台展示 系统需具备多级部署能力，可以支持管理中心设备级联部署，方便大型多级网络的统一管理和分析（提供截图证明）				
				系统需具备全面的攻击检测能力，可检测常见的 Web 攻击、缓冲溢出攻击、安全漏洞攻击、安全扫描攻击、拒绝服务攻击、木马后门攻击、蠕虫				

				病毒攻击、穷举探测攻击、CGI 攻击等				
				系统需具备全面的 Web 应用类攻击检测能力，能够检测各种 SQL 注入攻击、XSS 跨站攻击、Webshell 上传、命令注入、目录遍历、命令执行等攻击行为				
				☆系统提供的攻击特征不应少于 6500 条有效最新攻击规则（提供截图证明）				
				☆支持自定义规则，可结合用户业务进行深度检测，自定义内容包括源 IP、源端口、目的 IP、目的端口、协议、事件威胁等级、主机状态、事件类型、攻击阶段、攻击结果、攻击手段；支持关联规则分析，进行双向检测规则编写，兼容业界主流 snort 规则（需提供界面截图）；				
				系统需具备提取攻击信息的能力，告警信息应包括攻击的事件名称、事件风险级别、事件安全类型、事件攻击类型、攻击者 ip、受害 ip、源端口、目的端口、攻击发生的时间、攻击发送次数、事件解决方案等信息				
				☆系统需支持统计近 24 小时木马病毒、端口扫描、拒绝服务等攻击的数量，并支持下钻查看具体攻击事件内容，支持统计近 24 小时攻击事件的 TOP5，支持统计近 24 小时高危事件、中危事件、低危事件的网络威胁趋势图（提供截图证明）				
				☆系统需具备事件威胁的实时事件展示能力，可以将引擎检测到的攻击在威胁展示界面进行实时显示，显示内容需全面丰富，包括：事件名称、事件风险级别、攻击 ip、受害 ip、事件攻击类型、事件安全类型、事件发生时间等，并支持配置实时事件展示页面自动刷新时间，方便运维展示（提供截图证明）				
				系统需具备自动发现用户网络资产的能力，可自动上报网络中的存活资产，并支持获取内网资产的暴露面信息和资产指纹信息，				
				系统需具备未知（非法）资产入网发现的能力，可以及时发现违规入网的 IP 地址，防止内网资产乱接乱用				
				系统需具备自动发现内部资产与互联网设备互联的能力，并能准确显示				

				互联的方向，能够区分是内部服务器向外发起连接还是外部设备向用户内部服务器发起的连接				
				☆系统需具备可视化展示各业务系统资产分组互联关系的能力，支持查看资产分组内的互联情况和资产分组之间的互联情况，方便分析人员分析（提供截图证明）				
				系统需具备应用层协议解析能力，支持解析 HTTP 协议 URL 数据、DNS 协议域名数据等应用层数据信息；				
				☆支持内置网络主机异常行为特征算法（非数据包特征），通过主机的互联行为可以主动发现内网具有一定威胁的异常主机，包括中招蠕虫主机、网络扫描主机等（提供截图证明）				
				系统需具备检测策略管理能力，支持检测策略规则可以按照协议类型、攻击类型、安全类型、影响系统、影响设备等多个维度进行展示，方便运维人员按照不同的业务场景创建检测策略集				
				系统需具备用户管理能力，支持三权分立原则，系统具有用户管理员、审计管理员、配置管理员，支持创建不同的配置管理员，并赋予不同的授权角色，控制管理员的配置权限				
				基于网络全流量分析技术，对网络所有数据进行安全分析。通过对网络链路全流量采集、全数据分析，对网络异常行为有敏锐的感知能力，具备多维数据索引能力，能够对网络攻击进行定位与取证： ☆支持通过页面，对告警前后存储报文数量进行配置，最多支持存储和下载告警前 50 个和后 50 个数据包（需提供界面截图）；				
				系统需具备多种数据报表类型，每种报表类型的数据统计方式应从不同的维度进行分析，方便不同层次的技术人员进行数据汇总。				
				系统需具备数据交叉统计能力，支持按照事件名称、源地址、目的地址等多个维度对事件进行交叉统计分析，帮助分析人员快速定位攻击				
				☆三年软硬件质保升级服务，提供售后服务承诺函。				
				☆需与省厅态势感知平台无缝对接，并通过相关接口上报数据，提供接口				

				测试报告截图。				
				质保期内需配合用户方提供平台优化、部署及运维服务。				
3	内联防火墙	深信服	AF-1000-B1510	信创产品 ☆网络层吞吐量≥6G，应用层吞吐量≥2G，并发连接数≥180 万，每秒新建连接数≥6 万，内存≥4G，产品配备≥14 个千兆电口+4 个千兆光口 支持路由、透明、虚拟网线、旁路镜像等多种部署方式，适应复杂使用环境的接入要求 支持静态路由、策略路由和多播路由，支持 RIP、OSPF、BGP 等动态路由协议 支持 IPSec VPN 智能选路功能，根据线路质量和应用实现自动链路切换 ☆支持僵尸主机检测功能，产品预定义特征库超过 128 万种，可识别主机的异常外联行为（需提供产品功能截图证明） ☆支持预定义漏洞特征数量超过 10800 种，支持在产品漏洞特征库中以漏洞名称、漏洞 ID、漏洞 CVE 标识、危险等级和漏洞描述等条件快速查询特定漏洞特征信息，支持用户自定义 IPS 规则（需提供产品功能截图证明） 支持对 SMTP、HTTP、FTP、SMB、POP3、HTTPS、IMAP 等协议进行病毒防御 ☆支持勒索病毒检测与防御功能(需提供产品功能截图证明和第三方检测报告) 支持基于 IMAP、FTP、RDP、VNC、SSH、TELNET、ORACLE、MYSQL、MSSQL 等应用协议进行深度检测与防护 ☆支持策略生命周期管理功能，支持对安全策略修改的时间、原因、变更类型进行统一管理，便于策略的运维与管理（需提供产品功能截图证明） ☆所投产品具备计算机信息系统安全专用产品销售许可证，提供相关证明材料 ☆三年原厂硬件质保和软件升级服务，三年入侵防御规则库和防病毒规则库升级。 质保期内需配合用户方提供设备优化、部署及运维服务。	1	台	145000	145000
4	外网边界安	深信服	AF-100	信创产品	1	台	145400	145400

	全网关		0-B1810	☆网络层吞吐量≥12G，应用层吞吐量≥4.4G，并发连接数≥200 万，每秒新建连接数≥8 万，内存≥8G，产品配备≥6 个千兆电口+2 个千兆光口+2 个万兆光口				
				支持路由、透明、虚拟网线、旁路镜像等多种部署方式，适应复杂使用环境的接入要求				
				支持静态路由、策略路由和多播路由，支持 RIP、OSPF、BGP 等动态路由协议				
				☆支持 IPSec VPN 智能选路功能，根据线路质量和应用实现自动链路切换（需提供产品功能截图证明）				
				☆支持僵尸主机检测功能，产品预定义特征库超过 128 万种，可识别主机的异常外联行为（需提供产品功能截图证明）				
				☆支持预定义漏洞特征数量超过 10800 种，支持在产品漏洞特征库中以漏洞名称、漏洞 ID、漏洞 CVE 标识、危险等级和漏洞描述等条件快速查询特定漏洞特征信息，支持用户自定义 IPS 规则（需提供产品功能截图证明）				
				支持对 SMTP、HTTP、FTP、SMB、POP3、HTTPS、IMAP 等协议进行病毒防御				
				☆支持勒索病毒检测与防御功能(需提供产品功能截图证明和第三方检测报告)				
				支持基于 IMAP、FTP、RDP、VNC、SSH、TELNET、ORACLE、MYSQL、MSSQL 等应用协议进行深度检测与防护				
				☆支持策略生命周期管理功能，支持对安全策略修改的时间、原因、变更类型进行统一管理，便于策略的运维与管理（需提供产品功能截图证明）				
				☆所投产品具备计算机信息系统安全专用产品销售许可证，提供相关证明材料				
				☆三年原厂硬件质保和软件升级服务，三年入侵防御规则库和蜜罐规则库升级				
				质保期内需配合用户方提供设备优化、部署及运维服务。				
5	多功能安全审计设备（核心产	启明星辰	天玥 0SM-4500-S	信创产品，启明星辰/思福迪/深信服	1	台	133400	133400
				☆采用专用硬件平台和安全操作系统，具备液晶屏，采用 Venusense 多				

	品）			核并行操作系统架构或 LODP 系统架构或 ANIMAS 系统架构；非传统多线程、ASIC 等架构方式（需提供产品功能截图证明）				
				☆设备标配 6 个千兆电口 2 个万兆光口 2 个千兆光口，具有 2 个扩展插槽，此次包含 50 个被管资源数授权.				
				字符协议≧600 个				
				图形协议≧200 个				
				物理存储容量 4TB				
				物理旁路，逻辑串联模式，无需镜像、无需改造现有网络结构 ☆可分布式部署：支持添加一台或多台协议代理服务器，分担审计中心性能压力（需提供产品功能截图证明））。				
				字符协议：SSHv1、SSHv2、TELNET、RLOGIN				
				☆数据库协议：支持 Oracle、MS SQL Server、IBM DB2、Sybase、IBM Informix Dynamic Server、MySQL、PostgreSQL 等数据库类型（需提供产品功能截图证明）。				
				☆支持通过应用发布进行协议扩展第三方客户端；支持通过应用发布进行协议审计，记录命令详情，包括字符协议和数据库协议等，审计回放支持协议回放和图形回放（需提供产品功能截图证明）。				
				☆oracle，postgresql，sybase，mysql，sqlserver 数据库下行返回行数和 oracle 数据库变量绑定（需提供产品功能截图证明）。				
				WEB 页面支持 IE（8-11 版本）、Firefox 浏览器				
				支持 TELNET、SSH 协议使用 SecureCRT 工具批量登录目标资源。				
				基本认证：本地账号+密码认证；USB-KEY 强认证模式；其它认证支持 AD/RADIUS/LDAP。				
				从账号密码代填登录，使用人员不必知道服务器帐号及密码。				
				从账号密码自行输入，使用人员也可以选择自行输入服务器账号密码。				
				按用户、目标设备、系统帐号、命令集和生效时间等内容或按访问授权策略设定安全事件规则；支持指令黑白名单				
				针对 SSH、Telnet、Rlogin、FTP/SF				

				TP、数据库操作进行记录及审计；记录会话时间、命令执行时间、会话协议、服务端 IP、服务器端口、客户端 IP、客户端端口、操作命令、返回信息、运维用户帐号、审批用户帐号、资源账号等信息。				
				针对 RDP、VNC 等图形终端操作的连接情况进行记录及审计；记录会话时间、命令执行时间、会话协议、服务端 IP、服务器端口、客户端 IP、客户端端口、运维用户帐号、资源账号等信息				
				☆会话协议回放空闲时间过滤，应用发布图像操作回放支持操作空闲过滤（可设置无操作多长时间开始过滤）（需提供产品功能截图证明）。				
				审计查询关键字和结果显示支持多种编码(UTF-8,Big5,EUC-JP,EUC-KR,GB2312,GB18030,ISO-8859-2,KOI9-R,KS_C_5601_1987,Shift_JIS,Window-874)，由用户自主选择。				
				☆支持通过增加 Portal 服务器、Dataserver 服务器将系统升级到核心信息管控系统；核心信息管控系统支持运维工具集中发布，支持编辑工具集中发布（需提供产品功能截图证明）。				
				☆支持通过国产化运维客户端登录（银河麒麟 V10、统信 UOS20、凝思 42）（需提供产品功能截图证明）				
				产品具备《计算机信息系统安全专用产品销售许可证》 运维安全管理产品（增强级）				
				☆三年软硬件质保升级服务，提供售后服务承诺函。				
				质保期内需配合用户方提供平台优化、部署及运维服务。				
合　　计							936600 元	

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. 上述各项的服务内容如表格中填写不下的，可以逐项另页描述。

投标人名称（加盖公章）：中电鸿信信息科技有限公司

日期：2022 年 8 月 18 日