投标分项报价表（分包号：包 1）

序号	产品名称	品牌	规格	技术参数	产地	单位	数量	单价	总价
1	互联网出口防火墙（核心产品）	山石网科	SG-6000-P2227	≥1U 设备，双电源;配置不少于 6 个千兆电口+2 个万兆接口(包含光模块)，支持光口、电口以及存储接口扩展板;默认支持下一代防火墙访问控制、入侵防御、网络防病毒、上网行为及 URL 分类管理、流控和 IPSecVPN 模块;质保期 3 年内免费维修；可选配硬盘。含 IPS 特征库、防病毒特征库、应用识别及 URL 分类库三年升级服务。 ▲防火墙整机吞吐率(bps)≥10G，配置防病毒、防入侵、僵尸网络防御功能，支持配置≥200 个 ZTNA 零信任访问并发用户数。最大并发连接数≥220 万，每秒新建连接数≥13 万。提供产品彩页并盖原厂公章证明 支持源 NAT/目的 NAT 规则冗余检测，检查规则被覆盖情况，排除由于 NAT 规则覆盖导致有些 NAT 规则无法被命中的问题；检测可显示出冗余的规则 ID，覆盖此 SNAT/DNAT 规则的 ID，支持详情查看，并可直接对冗余策略执行删除、禁用操作，优化系统运行效率 支持出站负载均衡功能，能够自动探测多出口，选择最快的出口转发；支持基于多出口的 DNS 代理功能，可根据配置实现对不同外网线路的 DNS 服务器地址管理；支持入站 SmartDNS,能自动判断访问者的 IP 地址并解析出对应的 IP 地址,提升网站访问速度；支持服务器负载均衡功能，提供加权轮询、加权最小连接数、加权散列等多种负载均衡方式；支持 web 界面实时显示所有服务器的状态和当前连接数 支持线路过载保护功能,当某条外网线路拥塞时，自动将其流量切换到其他链路；系统对各出口的流量带宽进行实时监测，当自身接口的流量带宽超过配置的阈值时，新建会话的流量将不再从这个接口转发。当此接口的流量带宽回落到正常值以下时，新建会话的流量再恢复从这个接口转发 支持 LLDP 链路发现协议,通过物理接口定期与直连设备发送、接收组播报文，建立邻居关系，以供网络管理系统查询、分析当前网络的二层拓扑结构以及拓扑结构中存在的问题； ▲提供策略助手功能，可根据流量自学习，支持策略学习结果的源目地址合并，支持自动生成服务对象，并自动生成安全策略（提供产品功能截	苏州	台	2	129510	259020

				图并加盖原厂公章） 支持基于国家/地区维度进行流量控制等安全策略，支持垃圾策略清理，支持聚合策略以及策略导出 ▲提供策略命中分析功能，支持在 WEB 页面显示策略创建时间、首次命中时间、最近一次命中时间和最近未命中天数，便于管理员识别策略是否有效，便于进行策略优化调整，提供配置界面截图并加盖原厂公章； 支持基于源 MAC、目的 MAC 地址的二层访问控制策略，支持正向、反向和双向流量匹配，支持通过和丢弃动作，提供配置界面截图并加盖公章； 具备基于状态、精准的高性能攻击检测和防御，支持针对 HTTP、SMTP、IMAP、POP3、VOIP、NETBIOS 等 20 余种协议和应用的攻击检测和防御 具备 16000 种以上入侵防御攻击特征库规则列表，至少支持基于协议类型、操作系统、攻击类型、流行程度、严重程度、特征 ID 等方式的查询（提供产品界面截图加盖原厂公章有效） 具备 100 万种以上病毒特征库规则，支持基于安全策略和安全域启用防病毒功能；病毒扫描协议支持病毒处理动作，支持填充魔术数、重置连接、警告、只记录日志等处理方式（提供产品界面截图加盖原厂公章有效） 具备僵尸网络防护功能，含僵尸网络 C&C 恶意域名库和恶意 IP 地址库，可以离线和在线更新（提供产品界面截图并加盖原厂公章有效） 支持阻断访问恶意域名的 DNS 解析请求 支持丰富高可靠的 VPN 特性，具备 IPSec VPN、SSL VPN、L2TP VPN 和 GRE 等 VPN 技术； 支持 L2TP VPN，支持 LNS 和 LAC 功能 支持 SSL VPN 双因素认证，支持短信口令认证、令牌口令认证、邮件口令认证、证书口令认证等方式。 支持对登录 SSL VPN 的用户端系统进行端点安全检查 支持 SSL VPN 资源列表发布，可以通过点击链接直接访问内部资源。 具备应用识别特征库，特征库数量不少于 5900 种； 支持国内外主流云盘、云应用的识别，包括百度网盘、360 云盘、腾讯微云、华为云盘、新浪微盘、iCloud 等，防止通过云应用泄露敏感数据； 支持流量配额功能，可以对用户/用户组每天或者					

				每月的流量配额进行限制和控制；当用户流量达到流量配额规则模板限定的日配额或者月配额时，系统将阻断该用户的流量，提供用户配额监控了解已使用流量信息； 为满足日常巡检及自动化运维操作和故障调试，产品必须支持全功能命令行的 CLI 配置、查看及 DEBUG 操作（提供产品界面截图加盖原厂公章有效） 支持 2 个系统软件并存，并支持系统软件切换，支持 10 个配置文件并存，并支持配置备份与恢复； 支持通过 RESTAPI 接口进行防火墙状态监控、配置管理等，支持对策略、对象、网络、系统的配置，设备交付时须提供完整 API 电子手册； 提供 WEB 界面故障分析服务，当某个业务不通时，可根据设备对数据包的处理流程自动分析出故障点，便于管理员参考排查故障，提升运维效率。 提供中华人民共和国工业和信息化部颁发的《电信设备进网许可证》； ▲为更全面的发现网络僵木蠕攻击，提高网络安全防护，出口设备要求加入微软安全响应中心发起的 MAPP 计划，作为该计划成员，可在微软发布每月安全公告之前获得微软产品的详细漏洞信息，为用户提供更及时的安全防护。提供最新微软第三方证明或微软网站截图和网站查询链接 需要满足新北区卫生数据中心网络安全防护及监管要求，免费提供接入数据中心网络安全监管平台。（提供承诺函加盖投标人公章）					
2	内网防火墙	山石网科	SG-6000-P2227	≥1U 设备，双电源;配置不少于 6 个千兆电口+2 个万兆接口(包含光模块)，支持光口、电口以及存储接口扩展板;默认支持下一代防火墙访问控制、入侵防御、网络防病毒、上网行为及 URL 分类管理、流控和 IPSecVPN 模块;质保期 3 年内免费维修；可选配硬盘。含 IPS 特征库、防病毒特征库、应用识别及 URL 分类库三年升级服务。 防火墙整机吞吐率(bps)≥10G，配置防病毒、防入侵、僵尸网络防御功能，支持配置≥200 个 ZTNA 零信任访问并发用户数。最大并发连接数≥220 万，每秒新建连接数≥13 万。 支持源 NAT/目的 NAT 规则冗余检测，检查规则被覆盖情况，排除由于 NAT 规则覆盖导致有些 NAT 规则无法被命中的问题；检测可显示出冗余的规则 ID，覆盖此 SNAT/DNAT 规则的 ID，支持详情查看，并可直接对冗余策略执行删除、禁用操作，	苏州	台	2	119006	238012

				优化系统运行效率 支持出站负载均衡功能，能够自动探测多出口，选择最快的出口转发；支持基于多出口的 DNS 代理功能，可根据配置实现对不同外网线路的 DNS 服务器地址管理；支持入站 SmartDNS,能自动判断访问者的 IP 地址并解析出对应的 IP 地址,提升网站访问速度；支持服务器负载均衡功能，提供加权轮询、加权最小连接数、加权散列等多种负载均衡方式；支持 web 界面实时显示所有服务器的状态和当前连接数 支持线路过载保护功能,当某条外网线路拥塞时，自动将其流量切换到其他链路；系统对各出口的流量带宽进行实时监测，当自身接口的流量带宽超过配置的阈值时，新建会话的流量将不再从这个接口转发。当此接口的流量带宽回落到正常值以下时，新建会话的流量再恢复从这个接口转发 支持 LLDP 链路发现协议,通过物理接口定期与直连设备发送、接收组播报文，建立邻居关系，以供网络管理系统查询、分析当前网络的二层拓扑结构以及拓扑结构中存在的问题； 提供策略助手功能，可根据流量自学习，支持策略学习结果的源目地址合并，支持自动生成服务对象，并自动生成安全策略 支持基于国家/地区维度进行流量控制等安全策略，支持垃圾策略清理，支持聚合策略以及策略导出 提供策略命中分析功能，支持在 WEB 页面显示策略创建时间、首次命中时间、最近一次命中时间和最近未命中天数，便于管理员识别策略是否有效，便于进行策略优化调整； 支持基于源 MAC、目的 MAC 地址的二层访问控制策略，支持正向、反向和双向流量匹配，支持通过和丢弃动作； 具备基于状态、精准的高性能攻击检测和防御，支持针对 HTTP、SMTP、IMAP、POP3、VOIP、NETBIOS 等 20 余种协议和应用的攻击检测和防御 具备 16000 种以上入侵防御攻击特征库规则列表，至少支持基于协议类型、操作系统、攻击类型、流行程度、严重程度、特征 ID 等方式的查询 具备 100 万种以上病毒特征库规则，支持基于安全策略和安全域启用防病毒功能；病毒扫描协议支持病毒处理动作，支持填充魔术数、重置连接、警告、只记录日志等处理方式 具备僵尸网络防护功能，含僵尸网络 C&C 恶意域					

				名库和恶意 IP 地址库，可以离线和在线更新 支持阻断访问恶意域名的 DNS 解析请求 支持丰富高可靠的 VPN 特性，具备 IPSec VPN、SSL VPN、L2TP VPN 和 GRE 等 VPN 技术； 支持 L2TP VPN，支持 LNS 和 LAC 功能 支持 SSL VPN 双因素认证，支持短信口令认证、令牌口令认证、邮件口令认证、证书口令认证等方式。 支持对登录 SSL VPN 的用户端系统进行端点安全检查 支持 SSL VPN 资源列表发布，可以通过点击链接直接访问内部资源。 具备应用识别特征库，特征库数量不少于 5900 种； 支持国内外主流云盘、云应用的识别，包括百度网盘、360 云盘、腾讯微云、华为云盘、新浪微盘、iCloud 等，防止通过云应用泄露敏感数据； 支持流量配额功能，可以对用户/用户组每天或者每月的流量配额进行限制和控制；当用户流量达到流量配额规则模板限定的日配额或者月配额时，系统将阻断该用户的流量，提供用户配额监控了解已使用流量信息； 为满足日常巡检及自动化运维操作和故障调试，产品必须支持全功能命令行的 CLI 配置、查看及 DEBUG 操作 支持 2 个系统软件并存，并支持系统软件切换，支持 10 个配置文件并存，并支持配置备份与恢复； 支持通过 RESTAPI 接口进行防火墙状态监控、配置管理等，支持对策略、对象、网络、系统的配置，设备交付时须提供完整 API 电子手册； 提供 WEB 界面故障分析服务，当某个业务不通时，可根据设备对数据包的处理流程自动分析出故障点，便于管理员参考排查故障，提升运维效率。 提供中华人民共和国工业和信息化部颁发的《电信设备进网许可证》； ▲为保障日常使用的稳定性，必须通过国家电子计算机质量监督检验中心或同等权威第三方检测机构的浪涌（冲击）抗扰度（4KV）测试项目，提供有关机构出具的含 CMA 检测报告复印件并加盖公章 需要满足新北区卫生数据中心网络安全防护及监管要求，免费提供接入数据中心网络安全监管平台。（提供承诺函加盖投标人公章）					

3	杀毒软件	火绒	终端安全管理系统V2.0	1.标准网络版管理中心 1 套。系统服务端软件，提供防病毒策略管理、下发任务、病毒告警分析、报表等功能，可管理 win 系列客户端、Linux 系列客户端，可安装在 Windows2008R2 及以上操作系统、Win7sp1、Win10 或 centos7.0、Redhat7.0 及以上操作系统。 2.管理中心集成可视化威胁数据概览、终端统一运维管控、漏洞修复、资产管理、级联部署、中心管理、威胁日志报表、邮件预警等八大模块功能，有效针对全网终端安全进行管理与防护。 1. 终端支持 Windows Server 2003 SP1 及以上版本 / Windows XP(SP3)/ Windows Vista / Windows 7 及以上版本 2.终端基于虚拟沙盒环境与通用脱壳技术实现对病毒的有效识别，将病毒防御、系统防御、网络防御和访问控制四大模块深度协作运行，构建主动防御入侵系统，为全网终端保驾护航 要求支持终端发现可以通过扫描发现需要安装但没有安装终端的计算机，以免出现漏管漏控的情况； 要求支持备用中心查看和审批，支持通过本地安装的配置工具申请成为主中心的备用中心，主中心审批通过后，显示备用中心的相关信息； 控制中心支持负载均衡功能，可对主中心配置单个或多个负载中心，终端可根据主中心资源占用情况自动连接到负载中心； 支持终端事件邮件告警规则，当选择的指定分组或终端发生异常、离线、升级失败、网络攻击、病毒威胁、系统防护和访问控制等事件时，向管理者发送自定义信息的邮件通知； 管理后台支持开启登录地址限制，可通过添加 IP 地址的方式，对登录的 IP 进行限制； 要求支持第三方软件调用 API 接口，包括调用漏洞修复信息查看、下发查杀任务、查看、创建、修改和删除分组信息、查询终端详情、终端资产信息、调用接口修改终端名称等； 要求中心可统计全网操作系统版本信息、安装时间、激活状态且具有操作系统占比可视化数据图；可统计全网终端硬件信息包括 CPU、内存、硬盘、硬盘序列号、硬盘 ID、网卡、显卡、主板、主机序列号、显示器且支持硬件清单导出、支持全网终端硬件、软件变更历史记录包括变更时间等其他信息； 要求具有反病毒底层技术，反病毒引擎为本地反	北京	套	100	105	10500

				病毒引擎，不依赖云（联网时的病毒查杀能力与断网时的病毒查杀能力一致）具有轻量级的病毒库，却有较强的病毒查杀能力； 要求支持勒索病毒诱捕，可在根目录生成 txt、pem、sql、xlsx、mdb、jpg、rtf、xls、doc、docx 等格式的诱捕文件，当出现勒索行为，对其进行捕获并进行隔离； 要求支持外设申请功能，管理员可审批终端用户的外设使用申请，支持设备截止时间设置，并支持信任设备列表和审批记录筛选搜索； 要求具有终端动态口令验证功能，当终端用户登录计算机时都将弹出动态口令安全认证窗口，若用户设置了计算机密码，该弹窗将在用户输入正确的账户密码后弹出用户需再次输入正确的动态口令才可登入计算机且可设置应用范围：远程登录时启用或本地登录时启用； 要求支持导出安全分析报告，对当前中心进行安全状况分析并生成分析报告，可按照最近 7 天、最近 30 天、最近一年等时间范围生成报告，也可自定义时间范围生成报告，安全报告支持邮件订阅功能，可给管理员配置订阅功能；					
4	态势感知	奇安信	TY-TSS10000-S80-PA	至少 4*GE 电口，4TB SATA 企业级硬盘，单电源。包含基础系统软件一套，需要包含网页漏洞利用检测、webshell 上传检测、网络攻击检测、威胁情报检测功能，支持提供离线 pcap 包导入检测、基础旁路阻断和基础 SSL 解密功能，至少支持 600M 吞吐量。 内置基本软件包，系统包含文件还原、威胁情报检测、规则检测、Web 攻击检测、Webshell 攻击检测、网络攻击检测、异常流量检测、失陷主机检测、弱口令检测、暴力猜解检测、Flood 攻击检测、情报查询、态势感知大屏、挖矿专项；平台框架、场景分析、资产梳理、脆弱性分析、联动响应、态势大屏等模块，还包括首页、节点管理，知识库、系统自身管理。提供 3 年的产品升级服务，包括平台知识库(包括流量策略库)的手动和自动升级服务。 支持 IPv4 和 IPv6 网络环境下的部署，接口支持 IPv4、IPv6 配置，支持对 IPv4 路由监控和对 IPv6 路由监控，可同时对 IPv4 和 IPv6 网络流量分析检测。 ▲支持手动批量导入 PCAP 包对离线流量采集，单次总大小支持 1 个 G；支持通过配置 FTP 方式批量导入 PCAP 包对离线流量采集；记录 PCAP 包导	北京	台	1	272000	272000

				入记录及检测状态。（提供截图证明并加盖投标人公章） 支持流量过滤策略，通过 ip、ip 段、端口、协议等进行流量过滤，过滤语法支持 and、or、not 等多条件过滤语句。支持通过配置 BPF 语法条件进行流量过滤。（提供截图证明并加盖投标人公章） ▲支持配置外发 tcp、udp 流量日志中上下行负载的长度，最大支持 10K。（提供截图证明并加盖投标人公章） 支持常见协议识别并还原网络流量，用于取证分析、威胁发现，支持：http、dns、dhcp、smtp、pop3、imap、webmail、db2、oracle、mysql、mssql-db、sybase、smb、ftp、snmp、telnet、nfs、icmp、ssl、ssh、redis、ldap、radius、kerberos、netbios、modbus、ntp、ipv6 等。 支持 WebMail、SMTP、POP3、IMAP 邮件行为解析，生成流量日志。 ☆支持识别 FTP、SMB、Oracle、MySQL、MSSQL 、PostgreSQL、SSH、POP3、IMAP、SMTP、redis、CouchDB、Membase、Mongo DB 等登录行为； 支持 VLAN 、VXLAN 的网络流量的解析检测。云场景下，支持 GENEVE 协议双层隧道封装流量的解析检测。 支持自定义协议和端口，满足特殊场景下的流量抓取。支持非标端口下的常规协议自动识别、解析和威胁检测功能。（提供截图证明） 支持对 HTTP、FTP_DATA、SMB、SMTP、POP3、WEBMAIL、IMAP、TFTP、QQ、NFS 等类型协议的流量进行文件还原。（提供截图证明） 支持配置网络日志外发的标准模式、精简模式、自定义模式，支持自定义配置 19 种网络日志的外发字段。（提供截图证明） ▲ 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 500+万条。（提供截图证明并加盖投标人公章） 系统默认内置 13000+条检测规则，支持检测 WEB 攻击、Webshell 攻击、网络攻击、后门程序、僵木蠕检测、C2 外连、恶意通信、SMB 远程溢出攻击、文件上传、弱口令、暴力猜解、挖矿、黑客工具、明文密码传输、漏洞利用、ARP 欺骗、恶意扫描等风险。 支持检测模式的标准模式、精简模式、自定义模式的切换，支持自定义检测深度，支持 DNS 隧道					

				检测、CS 流量检测、MSF 检测、暗网流量检测等十几种机器学习模型的自定义配置。（提供截图证明） 支持检测针对 WEB 应用的攻击，如 SQL 注入、XSS、代码执行、系统配置等注入型攻击。 支持跨站请求伪造 CSRF 攻击检测。 支持其他类型的 WEB 攻击，如目录遍历、弱口令、权限绕过、命令执行、文件读写、信息泄漏、文件包含、文件写入攻击、挖矿等检测。 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（提供截图证明） 支持基于 webshell 函数的攻击检测，如任意文件上传、任意函数执行后门、任意文件写入、任意文件包含、任意目录读取、命令执行后门、preg_replace 代码执行等。（提供截图证明） 支持多种攻击检测，能更全面的从流量中发现威胁，如：SQL 注入、XSS、信息泄露、间谍软件、协议异常、网络欺骗、黑市工具、代码执行、挖矿等。 ☆支持非 TCP 完整流、畸形包检测、数据包完整性检测、IP 碎片攻击检测、编码绕过检测、高级逃逸 AET 检测等防逃逸检测能力。 支持根据威胁情报、检测规则、用户配置数据，来检测失陷主机通信活动行为。 支持自定义弱口令字典，支持 HTTP、HTTPS、SMB、Telnet、FTP、POP3、SMTP、IMAP 等协议的自定义弱口令检测。 支持自定义弱口令规则，支持正则表达式方式自定义弱口令强度、复杂度规则。支持配置多条弱口令检测的正则表达式（提供截图证明）。 ☆支持 HTTP、SMB、FTP、IMAP、POP3、SMTP、MSSql、Mysql、Oracle、Sip 、Redis 、Ldap 、Nntp 、SSH、Telnet、Sybase 、VNC、RADMIN、RDP 等协议暴力破解检测，能识别出尝试登录次数、账户信息、爆破成功与否的攻击状态。 支持 ACK Flood、SYN Flood、UDP Flood 和 Ping Flood；支持应用层 Flood 攻击检测，包括 DNS Flood 和 HTTP Flood。 支持与云端威胁情报中心联动，可对受害 IP、攻击 IP、IOC/规则 ID、文件 MD5 进行一键搜索，查看基本信息、开源情报、相关样本、可视化分析、域名解析、注册信息、关联域名、数字证书等；					

				（提供截图证明） 支持威胁告警的相关 pcap 数据留存，支持本地下载及外发。 ▲态势感知大屏，包含外部威胁态势感知、威胁事件态势、资产风险态势、访问态势和脆弱性态势五个部分，用于将发现的威胁在大屏上进行展示，使得结果更加直观地展示。（提供截图证明并加盖投标人公章） 支持门罗币、莱特币、以太坊、比特币、斯特币、渡鸦币、云储币等二十余种币种的检测，区分挖矿行为阶段：恶意代码传输、远控通信、连接矿池、登录矿池、获取挖矿任务、提交挖矿份额。（提供截图证明） 支持机器学习检测引擎，能够提供高级病毒检测能力 支持虚拟执行外链，能够检测样本有无外链行为 支持云查杀引擎，云端样本库大规模覆盖文件，快速返回判定结果，节省分析资源（提供截图证明） 支持自定义生成周期、报表格式、报表模版，报表发送对象 默认提供多种报表模版（支持用户自定义模版），模版包括告警、受害资产、日志、威胁分析等 ▲ 支持基于 IP 地址的旁路阻断，能够在实时镜像的流量中发现恶意 IP 并实现实时阻断。（提供截图证明并加盖投标人公章） 支持基于 URL 的旁路阻断，并能将 URL 请求进行重定向。（提供截图证明） 为了更好发挥态势感知对于未知威胁以及 ODAY 攻击防范能力；需提供免费接入新北区数据中心网络安全监管平台。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），检测到网络中存在异常行为或潜在威胁时，如某个 IP 地址频繁尝试进行未授权访问、特定端口接收到大量恶意流量等，它会立即触发联动机制，将相关信息和威胁情报传递给防火墙系统。（提供承诺函并加盖投标人公章）					

5	日志审计	金电网安	V2.0-S30D	▲系统基于经过加固的安全操作平台，为主机提供深度防御；（提供相关证明并加盖投标人公章）≥1U 标准机架式，双电源，6 个千兆电口 2 个千兆光口，1 个扩展槽位，2 个 USB 接口，硬盘容量:32Gminisata+4T SATA，支持≥30 个审计对象授权，提供三年质保及维保服务； 支持在线自定义标准化策略，支持主流设备日志接入，支持类型不低于 1200 种日志的接入和范式化处理；包括不限于以下设备安全设备：启明 WAF 防火墙、绿盟 IDS、华为防火墙、Juniper 防火墙、天融信防火墙等；操作系统：Linux、Windows、Window server、Uinx 等操作系统、数据库：Oracle、MySQL、SQLServer 等、应用系统：如 Apache、Tomcat、IIS、weblogic 等；网络设备：主流的路由器、交换机、负载均衡等网络设备等，如 Cisco、华为、juniper 等（提供功能截图并加盖投标人公章） 可以添加、修改、删除资产对资产的基本属性进行维护资产可以增加自定义属性；可对网络中的设备 IP 进行资产发现，通过资产发现自动识别设备的 IP、系统类型等属性信息 系统支持对 IP 对象的自动发现功能对自动发现的设备可以转资产或删除。（提供功能截图并加盖投标人公章） ▲为了挖掘不同类型、来源于不同设备或系统的日志或安全事件之间可能存在的关联关系，系统提供了 GUI 方式的关联规则设置功能，关联的类型包括基于规则和基于统计的，支持基于因果式的状态关联分析。（提供功能截图并加盖投标人公章） 支持显示审计事件分类统计列表，根据审计策略名称、审计事件类型、被审计人员、目标设备地址四个维度展现（提供功能截图并加盖投标人公章） 支持定义部门和人员的对应关系，支持定义人员与账号的对应关系（提供功能截图并加盖投标人公章） 系统从不同设备或系统中所获得的各类日志、事件中抽取相关片段准确和完整地映射至安全事件的标准字段，日志清洗后的标准化字段粒度至少达到 90 个字段 系统可以完全收集采集对象上的日志信息，也可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	上海	台	1	11500	11500

				对象发送到核心服务器的安全事件数，减少对网络带宽和数据库存储空间地占用。 ▲系统需具有归并技术，安全事件收集代理会在一段时间内比较收到的安全事件，如果安全事件相同，则只需存储一条安全事件，该安全事件应包括安全事件详情及该安全事件发生的次数，这样可以减少安全事件通信量（提供功能截图并加盖投标人公章） 系统提供全文检索功能。能对系统内的对象提供全文检索功能，对于海量数据的检索可限定检索时间段（主要针对安全事件）。全文检索提供一个输入栏，需要置顶，在任何页面都能够看到。（提供功能截图并加盖投标人公章） 日志查询支持普通查询和更加精确的专家模式查询，根据页面的指导提示，通过组合查询表达式完成精确查询。 ▲支持 IP 全球地理位置库，能够在世界地图、中国地图实时攻击日志的定位源和目的的地理位置信息（提供功能截图并加盖投标人公章） 支持根据三权分立的原则和要求进行职、权分离，对系统本身进行分角色定义 支持网站管理配置，系统自动发现域名并监控域名的访问及攻击情况；在传统的访问和攻击监控的基础上；支持网站告警监控，访问状态码分布、访问量统计、被访问资源 top10、客户端系统和浏览器分布、请求方式及平均响应时间等。（提供功能截图并加盖投标人公章） ▲1.支持自定义仪表板，客户可以选择对应的微件，组成想要关注的仪表展现内容（提供功能截图并加盖投标人公章） 2.支持大屏态势展示，应包括总览、实时攻击态势、用户行为日志、可自定义。（提供功能截图并加盖投标人公章） 支持对接三未信安、得安、格尔等主流加密设备，实现对原始日志做国密算法的完整性校验。（提供功能截图并加盖投标人公章） 要求提供产品生产厂家出具质保承诺书原件并加盖投标人公章					
6	服务器	H3C	R4930 G5	2*CPU(2.5GHz/16 核)，4*64G，2*480G SSD，，2*4T HDD，4 口千兆，2*双口万兆（含 4 个多模模块）双电源，虚拟化管理系统标准版	杭州	台	3	99806	299418

7	风评	国产	优质	针对机房网络环境提供风险评估报告；给出相应的安全隐患和脆弱性报告，以及安全性整改建议；用户对系统安全性状况和整体安全状况有全面具体的了解；针对报告对存在的安全隐患给出解决方案。	国产	项	1	50000	50000
8	系统集成	国产	优质	系统集成；技术服务；针对网络设备提供完善的部署解决方案；完成设备的安装部署及后续技术支持工作；	国产	项	1	89000	89000
投标总报价（人民币：元）									1368450

交付期：合同签订之日 90 天内完成并运营上线，信息系统建设完成初验后试运行 2 个月，信息系统维保期 2 年 。