|  |
| --- |
| 永嘉县政府采购招标文件（分散委托）项目名称：永嘉县一体化智能化公共数据平台-政务外网安全提升项目项目编号：ZGCG-20211112采 购 人：永嘉县大数据管理中心代理机构：温州市中概工程管理咨询有限公司二○二一年十一月 |

**招标文件目录**

[第一部分 投标通知(邀请)书 2](#_Toc73091433)

[第二部份 采购内容及要求 6](#_Toc73091434)

[第三部分 供应商须知 42](#_Toc73091435)

[第四部分 政府采购政策功能相关说明 58](#_Toc73091436)

[第五部分 合同格式（仅供参考） 63](#_Toc73091437)

[第六部分 投标文件格式 67](#_Toc73091440)

[一、资格文件部分格式 67](#_Toc73091441)

[二、报价文件部分格式 73](#_Toc73091446)

[三、商务技术文件部分格式 75](#_Toc73091448)

[第七部分 评标定标办法 83](#_Toc73091452)

第一部分 投标通知(邀请)书

|  |  |  |
| --- | --- | --- |
| 序号 | 内容 | 说明与要求 |
| 1 | 项目名称 | 永嘉县一体化智能化公共数据平台-政务外网安全提升项目 |
| 2 | 项目编号 | ZGCG-20211112 |
| 3 | 资金来源 | 财政性资金 |
| 4 | 采购预算 | 301.7万元,本项目最高限价270万元。 |
| 5 | 采购方式 | 公开招标 |
| 6 | 采购人 | 采 购 人：永嘉县大数据管理中心联 系 人：单先生联系方式： 0577-67236276 |
| 7 | 采购代理机构 | 采购代理机构名称：温州市中概工程管理咨询有限公司地 点：温州市永嘉县南城街道环城北路618号云碓大厦503室联 系 人：胡可可联系电话：15258683545 |
| 8 | 评标办法 | 综合评分法 |
| 9 | 采购内容 | 永嘉县一体化智能化公共数据平台-政务外网安全提升项目，具体内容见招标文件。 |
| 10 | 供应商资格要求 | 1.满足《中华人民共和国政府采购法》第二十二条规定；未被“信用中国”（www.creditchina.gov.cn)、中国政府采购网（www.ccgp.gov.cn）列入失信被执行人、重大税收违法案件当事人名单、政府采购严重违法失信行为记录名单。2.落实政府采购政策需满足的资格要求：无 3.本项目的特定资格要求：无。 |
| 11 | 是否接受联合体投标 | 不接受接受 |
| 12 | 踏勘现场 | 不组织□组织  |
| 13 | 是否允许递交备选投标方案 |  不允许□ 允许 |
| 14 | 分包 | □允许不允许 |
| 15 | 报价货币 | 人民币 |
| 16 | 报价语言 | 中文 |
| 17 | 投标文件的编制 | 供应商应先安装“政采云电子交易客户端”，并按照本采购文件和“政采云平台”的要求，通过“政采云电子交易客户端”编制并加密投标文件。 |
| 18 | 报价有效期 | 提交响应文件截止时间起90天内 |
| 19 | 签字或盖章要求 | 投标文件的相应位置应加盖：电子签章。 |
| 20 | 投标文件的形式、制作及组成 | 本项目实行在线投标响应（电子投标）。投标人须准备电子投标文件（包括“电子加密投标文件”和“备份投标文件”两类，在投标文件编制完成后同时生成）。（1）“电子加密投标文件”是指通过“政采云电子交易客户端”完成投标文件编制后生成并加密的数据电文形式的投标文件。（2）“备份投标文件”是指与“电子加密投标文件”同时生成的数据电文形式的电子文件（备份标书），其他方式编制的备份投标文件视为无效备份投标文件。以上两类投标文件均由资格文件、报价文件、商务技术文件三部分组成。 |
| 21 | 投标样品 | 不需要□需要 |
| 22 | 投标保证金 | 不需要□需要 |
| 23 | 履约担保 | 不需要需要 合同签订后成交供应商应提供合同总金额5%的履约保证金至采购人指定账户，履约保证金可以以银行或保险公司出具的保函作为履约保函。 |
| 24 | 投标文件份数 | （1）“电子加密投标文件”：在线上传递交、一份。（2）“备份投标文件”：以U盘存储，密封包装后（顺丰快递形式）在2021年12月2日16时00分前递交，一份，邮寄地址：温州市永嘉县南城街道环城北路618号云碓大厦5楼，黄曼曼收，联系电话：15858728890。 |
| 25 | 响应文件递交截止时间及开标时间 | 2021年12月3日09:30（北京时间）。 |
| 26 | 投标文件的上传和递交 | 一、“电子加密投标文件”的上传、递交：a.投标人应在投标文件递交截止时间前将“电子加密投标文件”成功上传递交至“政采云平台”，否则投标无效。b.“电子加密投标文件”成功上传递交后，供应商可自行打印投标文件接收回执。二、“备份投标文件”的密封包装、递交：a.投标人在“政采云平台”完成“电子加密投标文件”的上传递交后，还可以（建议顺丰快递形式）递交以介质（U盘）存储的 “备份投标文件”（一份）；顺丰快递形式快递至采购代理机构地址（地址详见招标采购文件，防疫期间不建议供应商本代表抵达开评标地点）；解密CA必须是上传并制作电子投标文件CA锁。b.“备份投标文件”应当密封包装，并在包装上标注投标项目名称、投标单位名称并加盖公章。没有密封包装或者逾期邮寄送达至投标地点的“备份投标文件”将不予接收。c.通过“政采云平台”成功上传递交的“电子加密投标文件”已按时解密的，“备份投标文件”自动失效。投标文件递交截止时间前，投标人仅递交了“备份投标文件”而未将“电子加密投标文件”成功上传至“政采云平台”的，投标无效。 |
| 27 | 电子加密投标文件的解密和异常情况处理 | （1）开标后，采购组织机构将向各投标人发出“电子加密投标文件”的解密通知，各投标人代表应当在接到解密通知后30分钟内自行完成“电子加密投标文件”的在线解密。（2）通过“政采云平台”成功上传递交的“电子加密投标文件”无法按时解密，投标人如按规定递交了“备份投标文件”的，以“备份投标文件”为依据（由采购组织机构按“政采云平台”操作规范将“备份投标文件”上传至“政采云平台”，上传成功后，“电子加密投标文件”自动失效），否则视为投标文件撤回。（3）投标文件递交截止时间前，投标人仅递交了“备份投标文件”而未将电子加密投标文件上传至“政采云平台”的，投标无效。 |
| 28 | 评标委员会成员的组建 | 评标委员会成员构成： 由采购人代表以及有关技术、经济等方面的专家组成，成员为5人及以上单数，其中技术、经济类专家不得少于总人数的2/3；评标专家确定方式：按相关规定从专家库中抽取。 |
| 29 | 政府采购扶持政策 | 1.本项目对符合财政扶持政策的中小企业（小型、微型）、监狱企业、残疾人福利性单位给予价格优惠扶持，价格优惠扶持见《评分办法》。2.满足财政部 工业和信息化部关于印发《政府采购促进中小企业发展管理办法》的通知（财库〔2020〕46号）的规定的中小企业可享受优惠扶持。3.满足关于政府采购支持监狱企业发展有关问题的通知（财库[2014]68号）的规定的供应商可享受优惠扶持。4.满足关于促进残疾人就业政府采购政策的通知（财库[2017]141号）的规定的供应商可享受优惠扶持。5.对节能、环保产品优先采购。 |
| 30 | 供应商信用查询 | 1、投标供应商信用信息查询的查询渠道：“信用中国”([www.creditchina.gov.cn](http://www.creditchina.gov.cn))；“中国政府采购网”（http://www.ccgp.gov.cn/）；2、投标供应商信用信息查询截止时点：招标公告发布之日至投标截止时间前；3、投标供应商信用信息查询记录和证据留存的具体方式：网页截图打印；4、信用信息的使用规则：对列入失信被执行人、重大税收违法案件当事人名单、政府采购严重违法失信行为记录名单及其他不符合《中华人民共和国政府采购法》第二十二条规定条件的供应商，其投标做无效投标处理。5、▲关于“信用中国”(www.creditchina.gov.cn) 信用记录网页截图相关说明：①若供应商查询页面“行政处罚”栏显示有行政处罚事项，须将所有行政处罚事项在“信用中国”网页上列出的明细一并打印，并附说明，是否属于“经营活动中的重大违法记录”。②若供应商在“信用中国”无数据，亦须将搜索结果页面打印，并附说明。③未按照以上①-②条要求提供“信用中国”查询结果记录的，将按照资格审查不通过处理。 |
| 31 | 合同备案 | 1、中标供应商须在发出中标通知书之日起30日历天内与采购人签订合同。2、中标供应商与采购人签订合同后，2日历天内将合同原件交温州市中概工程管理咨询有限公司备案。合同原件扫描件电子版发给温州市中概工程管理咨询有限公司：邮箱：1437567478 @qq.com；3、本项目政府采购合同按规定在浙江政府采购网（http://www.zjzfcg.gov.cn）予以公告。 |
| 32 | 合同履约管理 | 合同签订后，采购人依法加强对合同履约进行管理，并在成交供应商服务、项目验收等重要关节，如实填写《合同验收报告》，并及时向同级财政部门报告验收过程中遇到的问题。 |
| 33 | 免则声明 | 1、供应商自行承担投标过程中产生的费用。无论何种因素导致采购项目延期开标、废标（流标）、供应商未成交、项目终止采购的，采购人与代理机构均不承担供应商投标费用。2、供应商在投标、合同履行过程中必须做好安全保障工作，不因项目实施而危及自身及第三方人员、财产安全。若发生任何安全事故，由成交供应商自行承担一切责任并赔偿损失。 |
| 34 | 解释权 | 构成本招标文件的各个组成文件应互为解释，互为说明；如有不明确或不一致，构成合同文件组成内容的，以合同文件约定内容为准，且以专用合同条款约定的合同文件优先顺序解释；仅适用于采购阶段的约定，按采购公告、供应商须知、评标办法、响应文件格式的先后顺序解释；同一文件中就同一事项的约定不一致的，以逻辑顺序在后者为准；同一文件不同版本之间有不一致的，以形成时间在后者为准。按本款前述约定仍不能形成结论的，由采购人负责解释。 |
| 35 | 招标代理服务费 | 本次项目招标代理服务费按固定金额34000元收取。采购人不负责任何招标代理服务费用。招标代理服务费由中标人支付，请报价人在报价时予以考虑。招标代理服务费汇入以下帐户：开户银行：中国建设银行永嘉广场支行开户名称：温州市中概工程管理咨询有限公司开户帐号：33050162766300000011招标代理服务费须在领取《中标通知书》前付清。 |

第二部份 采购内容及要求

**一、项目背景**

政府数字化转型是政府主动适应数字化时代背景，对施政理念、方式、流程、手段、工具等进行全局性、系统性、根本性重塑，通过数据共享促进业务协同，实现政府治理体系和治理能力现代化。推进政府数字化转型，建设数字政府，是贯彻落实网络强国、数字中国、智慧社会的关键抓手；是深化“最多跑一次”改革、推进政府职能转变，构建政府有为、市场有效、企业有利、百姓受益体制机制不断创新的必然要求；是强谋划、强执行，提升服务质量、行政效率和政府公信力，建设以人民为中心的服务型政府，推动高质量发展的重要举措。

**二、建设内容**

一体化智能安全建设以实战化安全运营为主旨，以资产为核心，基于大数据架构自主构建的面向政企客户的可信任、全场景的安全管理平台。一体化智能安全建设通过统一全网流量和异构日志数据，融合威胁情报进行实时分析、智能决策，实现资产管理、漏洞管理的全周期管控，实现威胁事件调查分析溯源和取证响应等闭环处置，辅助安全编排和异常行为分析帮助客户落地布局安全中心，为安全运营（管理、分析、响应）提供有效支撑，实现全域安全态势感知和协同指挥，促进企业安全防护良性生态体系的建立。

**1、****全网全域全方位监测管理**

提供多方式资产测绘（日志&流量&终端式被动发现、情报&评估探针式主动发现）进行暴露面梳理，发现资产死角，建立安全资产台账，配合资产基线和资产稽核消除资产管理中的信息孤岛，结合资产感知和资产画像实现资产分级分层监测与管控，保障IT资产的完整性和安全性。

**2、动态纵深防御检测分析**

基于大数据技术统一汇聚各类安全检测、识别、审计、防护策略、身份、认证等数据，结合终端EDR、蜜罐诱捕等技术，辅助威胁情报等数据基于独创的威胁分析建模引擎、异常行为分析引擎、安全治理分析引擎进行深度威胁关联分析，实现已知、未知和灰度行为的检测与分析，如失陷主机、网络病毒、违规外联、APT事件和勒索病毒等威胁事件的精准检测，借助ATT&CK攻击战术升级提供图谱化攻击路径展示，提高网络安全检测精准度和智能化能力。

**3、****安全合规风险持续评估**

提供覆盖系统漏洞、网站漏洞、配置基线、弱口令、渗透测试、等保配置检查等综合脆弱性管理，帮助企业安全运营人员实现自动化等保合规与风险持续评估的同时，配合自主原创的“优先化”模型算法和漏洞威胁闭环管理框架辅助漏洞管理运营与量化分析，帮助企业安全管理者快速了解企业物理环境、通信网络、制度、人员和建设管理的等保合规情况。

**4、****精准指挥联防协同防护**

基于攻防实践积累的高可信威胁分析算法和模型，有效提升分析结果准确性，根据高频攻击场景与平台全要素关联分析进行攻击路径推理和预测；并通过SOAR技术手段提供多种安全分析场景的威胁事件进行调查取证和联动响应，快速且聚焦的实现网络侧、终端侧进行阻断，亦可将封堵指令同步三方设备进行阻断和抑制，帮助用户实现分钟级事件响应闭环，并结合内外部情报信息和多种通报预警方式（钉钉、微信、短信和邮件等）及时通告安全信息实现企业侧的联防联控，协同指挥。

**5、****态势感知多层数据可视**

基于可视化技术从不同安全运营与分析角度对网络安全态势呈现，提供综合态势、环境感知态势、威胁分析态势、脆弱性态势、运营响应态势和日志审计态势帮助高层随时了解最新的安全趋势和风险状态，通过安全治理指标量化展示帮助高层管理者掌握企业全网安全状况。通过威胁、漏洞和资产运维监控维度帮助中层落地管理体系。

**6、****完善的敏感数据识别分析能力**

一体化智能化安全建设通过对接敏感数据梳理与评估系统敏感数据发现与风险评估系统、数据防泄漏系统数据防泄漏，提供对于敏感数据、敏感文件的自动识别功能。同时平台内置了运营商等多个行业的数据资产分类分级策略模板，并支持自定义创建行业分类分级模板。支持自动下发相关分类分级策略至敏感数据发现与风险评估系统、数据防泄漏进行自动扫描。一体化智能化安全建设基于数据、文件识别结果进行数据资产分类分级呈现，并结合自研敏感度评估算法对数据资产以数据表、文件存储目录为单位，对数据资产整体进行敏感度打分。

**7、****全面的数据资产安全防护能力**

一体化智能化安全建设支持通过WebService等形式，统一管控网络数据防泄漏、数据库防火墙，支持基于数据资产分类分级结果和数据资产访问策略，智能向防护设备下发相关防护策略，同时支持当检测到数据安全事件时，支持一键拦截攻击者。

**8、****先进的数据安全风险监控能力**

一体化智能化安全建设通过采集网络数据防泄漏、数据库审计、全流量探针相关流量日志，结合关键数据系统日志进行综合分析，利用平台自身集成大数据分析引擎和分析引擎，已接口为维度，自动构建涉敏接口发现、敏感数据流流转极限模型，并支持基于构建生成的数据访问继续，自动甄别数据访问异常行为，对非法爬虫、数据泄漏事件进行及时发现和告警，灵活的数据安全持续运营能力。一体化智能化安全建设支持对接数据脱敏设备日志，基于脱敏后数据集采样，并结合脱敏效果评估算法。帮助用户有效评估数据脱敏效果，避免因脱敏配置不当导致的敏感数据异常泄漏。

一体化数据安全监测平台还提供综合的数据安全运营报告与数据资产稽核功能。

帮助客户从数据资产盘点、数据平台漏洞管理、数据安全风险事件等多个维度有效了解组织数据安全全貌。及时制定挑战数据安全策略，落实数据安全责任到人，并基于安全性与合规性对相关责任人进行有效定期稽核。

**9、政务外网安全提升**

为了确保政务外网的安全，采用IPS入侵防御系统+终端安全防护+未知威胁防护系统（APT）+上网行为管理+日志审计+WAF+漏洞扫描+堡垒机+数据库审计+终端安全防护等组成的安全防护方案，全部安全防护能力配合一体化智能安全运营平台，实现政务网的网络安全与数据安全一体化防护（其中上网行为管理设备已有）。针对前面分析的情况，此次需要注入新的安全能力来保障系统的高可靠性、高可用性，为当前系统安全增添核心能力，提升其可靠性、安全性。

三、**采购清单**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **产品名称** | **数量** | **单位** | **详细内容** | **核心设备** |
| 下一代防火墙（服务器区） | 2 | 套 | 服务器区边界防护（含集成调试） | 是 |
| 下一代防火墙（边界） | 2 | 套 | 政务网边界防护（含集成调试） | 是 |
| APT | 1 | 套 | 集合行为分析、虚拟执行、多维关联分析、机器学习等技术，对威胁进行追踪与定位实现对APT攻击的全生命周期的检测分析与预警，帮助用户全面、直观掌握网络安全风险状况。（含集成调试） | 否 |
| 多功能探针 | 1 | 套 | 多功能探针支持对僵尸网络行为、木马控制行为、蠕虫活动行为、勒索病毒行为、移动端木马控制行为等多种僵尸主机行为检测。对被检测到的僵尸主机异常行为多功能探针支持对异常行为报文取证、事件记录，事件记录包括攻。（含集成调试） | 否 |
| 态势感知 | 1 | 套 | 系统支持威胁情报接入，告警流程化处置及安全设备集中管控，有效提高整体网络安全风险识别分析和监测预警处置能力。实现及时处置安全事件，进而提升整理网络安全态势感知能力。（含集成调试） | 是 |
| 安全资源池(含漏洞扫描组件、数据库审计组件、日志审计组件、堡垒机组件) | 1 | 套 | 利用安全功能虚拟化技术将多种安全设备虚拟化，以虚拟机的形式运行于一台安全设备，同时利用SDN技术实现安全服务链的动态编排，能够满足云上虚拟网络边界防护，提供安全能力动态弹性扩展、为不同的业务提供差异化的、按需的安全防护能力。（含集成调试） | 否 |
| 自适应安全防护 | 300 | 套 | 通过资产清点、风险发现、入侵防御、病毒查杀、网络微隔离等功能实现持续监控和分析，帮助客户精准感知安全威胁，发现入侵事件，提供快速的响应能力，提升主机安全防护水平。（含集成调试） | 否 |

**四、采购内容及要求**

**4.1下一代防火墙(服务器区)**

|  |  |  |
| --- | --- | --- |
| **指标** | **指标项** | **详细要求** |
| ★**基本要求** | 系统结构 | 产品由专用的硬件平台、安全操作系统及功能软件构成。设备采用自主知识产权的专用安全操作系统，采用多核多平台并行处理特性（提供证明材料）；为使保证安全产品做到安全自主可控，要求为国产品牌。为保证系统软件设计全面性、保密性、完整性，要求招标产品系统遵从行业标准和政府法规，产品符合 CNITSEC-SP-01 测评准则，提供第三方权威证明材料。 |
| 操作系统 | 安全操作系统采用冗余设计，出于安全性考虑，多系统需在设备启动过程中进行选择不得在WEB维护界面中设置系统切换选项。 |
| 为保障产品运行的安全及稳定性，要求产品设计、开发、生产及售后服务符合TL9000-H-S-V相关标准要求；提供第三方权威证明材料。 |
| 性能要求 | 2U,4个SFP插槽2个SFP+插槽和6个10/100/1000BASE-T(100m，RJ45),2个扩展槽位,防火墙吞吐40G，并发连接1000万，每秒新建连接30万，默认包含应用识别功能；可扩展IPSEC VPN、SSL VPN、三权分立模块；支持扩展IPS入侵防御、WAF、URL过滤及AV防病毒功能；要求支持芯片硬件加速技术，实现硬件资源充分利用，保障设备处理效率，提供第三方证明材料 |
| 安全功能模块 | 配置入侵防御功能模块，WEB应用防护功能模块及默认包含3年规则库升级授权； |
| **集成技术支持** | 工作模式 | 支持路由、交换、虚拟线、Listening、混合工作模式；  |
| 路由交换 | 支持RIP、OSPF、BGP4、QinQ、PIM-SM、PIM-DM； |
| 支持策略路由，支持根据入接口、源/目的IP地址、协议、用户、应用、选路算法、探测等多种条件设置策略路由；  |
| 链路聚合 | 支持手动和LACP链路聚合，可根据源/目的MAC、源/目的IP、源/目的端口、五元组、端口轮询等条件提供不少于10种链路负载算法。 |
| IP/MAC绑定 | 支持IP/MAC绑定，支持跨三层绑定，支持IP/MAC绑定表导入导出，以便对IP/MAC绑定关系进行批量操作；  |
| 地址转换 | 支持多种地址转换，支持源/目的NAT、双向NAT、NoNAT转换方式；支持源IP转换同一性；支持端口块地址转换和EIM地址转换 |
| DNS Doctoring | 支持DNS Doctoring功能，能够将来自内部网络的域名解析请求定向到真实内网资源，提高访问效率，同时支持通过配置多条 DNS Doctoring，实现内网资源服务器的负载均衡（提供截图）； |
| 媒体业务接入 | ★支持H.323、SIP等媒体协议,符合GB/T 28181-2016《安全防范视频监控联网系统信息传输、交换、控制技术要求》及TC/OP(XZ)2B-185-2017相关技术要求，提供权威测试报告； |
| 访问控制 | ★支持一体化安全策略配置，可以通过一条策略实现五元组、源MAC、源地区、目的地区、域名、应用、服务、时间、长连接、并发会话、WEB认证、IPS、AV、URL过滤、高级威胁防护、WAF、邮件安全、数据过滤、文件过滤、僵木蠕防御、审计、防代理、APT等功能配置,简化用户管理；（提供截图） |
| 提供策略分析功能，支持策略命中分析、策略冗余分析、策略冲突检查、策略包含分析，可在WEB界面显示检测结果；（提供截图） |
| 网络接入 | 支持RADVD、ND、RIPng、OSPFv3、BGP4+，支持IPv6静态、动态组播路由；（提供截图） |
| 支持NAT64、NAT46、NAT66地址转换，支持6to4隧道、ISATAP隧道；（提供截图） |
| 访问控制 | ★支持IPv6安全控制策略设置，能针对IPv6的目的/源地址、目的/源服务端口、区域、服务、时间、扩展头属性等条件进行安全访问规则的设置（提供截图）； |
| 支持IPv6域名控制，支持对多级域名进行控制，域名对象支持通配符； |
| 安全防护 | 支持对IPv6报文进行病毒防御、入侵防御、URL过滤、抗DDOS、WAF防护、僵木蠕、流量控制、连接限制、文件过滤、数据过滤等；（提供截图） |
| 资源虚拟化 | 支持在一台物理设备上划分出128个相互独立的虚拟系统（提供截图） |
| 功能虚拟化 | 支持配置文件、系统服务、路由、链路聚合、安全策略、NAT策略、带宽管理、认证策略、IPV6功能、URL过滤、病毒过滤、WAF、僵木蠕、高级威胁防护、内容过滤、邮件安全、审计、报表、防代理等安全功能虚拟化；  |
| 负载均衡 | 支持用户服务器的负载均衡，保证用户关键服务的有效性； |
| 防火墙在链路高数据量情况下，可以实现防火墙网络地址转换动态负载均衡，提供第三方权威证明文件； |
| 为保证产品功能健壮性，要求产品研发厂商通过软件成熟度CMMI5认证，提供第三方权威证明文件。 |
| 操作系统 | 可在发生系统故障时，实现系统自动修复。提供第三方权威证明文件； |
| 入侵防御 | 支持独立的入侵防护规则特征库，特征总数在5500条以上（提供截图），能对常见漏洞进行安全防护，兼容国家信息安全漏洞库（提供权威资质证明）； |
| ★厂商需具备强大的漏洞和攻防研究能力，为CNNVD一级支撑单位和CNVD技术组成员（提供证明材料），能够确保每周至少更新1次攻击特征库； |
| DDOS防御 | 支持针对IP、ICMP、TCP、UDP、DNS、HTTP、HTTPS、SIP、NTP等协议进行DDOS防护；支持预定义和自定义策略模板；（提供截图） |
| 支持TCP DDOS防护，采用阀值检查、源/目的限流、源认证、会话检查等方式综合进行SYN FLOOD、SYN-ACK FLOOD、FIN FLOOD、RST FLOOD、FRAG FLOOD、连接耗尽等攻击防护；（提供截图） |
| 支持NTP DDOS防护，采用阀值检查、源/目的限流、源认证等方式综合进行NTP REQUEST FLOOD、NTP REPLY FLOOD攻击防护；（提供截图） |
| 支持SIP DDOS防护，采用阀值检查、源/目的限流、源认证方式进行SIP FLOOD攻击防护；（提供截图） |
| 支持HTTPS DDOS防护，采用阀值检查、源/目的限流方式进行HTTPS FLOOD攻击防护；（提供截图） |
| URL过滤 | 支持超过80类、1000万的URL地址分类库，用户可对搜索引擎、微博、网购、求职、婚恋、娱乐、恶意网站、赌博、色情、反动、暴力、迷信等网站进行全面管控； |
| 支持自定义URL分类和地址，支持URL黑/白名单，支持自定义阻断页面； |
| 内容过滤 | 内置内容过滤功能，支持基于http、ftp、telnet、smtp、pop3协议的内容过滤策略，可对FTP上传/下载的文件名进行过滤，同时支持过滤FTP信令：上传文件、下载文件、删除文件、重命名文件、创建目录、删除目录、列出目录等，邮件过滤支持对发件人、收件人、主题、内容、附件等进行过滤；（提供截图） |
| Web攻击防护 | 配置独立的WAF引擎，WAF防护特征总数在1300条以上，可对常见Web攻击进行防护；  |
| 高级威胁防护 | 内置高级威胁防护，可对DGA、隐蔽信道、恶意加密流量进行检测，支持监控高级威胁检测数据，并进行可视化展示； |
| 支持与APT联动，获取APT监测设备上的威胁检测结果，实现协同防护；（提供截图） |
| 内置行为分析功能，对新建连接数、并发连接数、流量等数据进行统计分析，建立业务行为基线，对异常行为进行告警；支持行为分析监控展示，可展示不同行为分析策略的实时数据和基线数据趋势； |
| 邮件安全 | 内置邮件安全防护功能，支持邮件过滤、邮箱防暴力破解、邮件泛洪攻击防护、邮件黑、白名单检测；（提供截图） |
| 资产管理 | 支持资产管理，可查看资产详情、安全防护策略，并对资产进行分组和防护优化； |
| 智能防护 | 支持对网络资产进行一键检查，获取网络中资产信息、分析资产安全状态，一键完成风险资产安全防护； |
| 漏扫联动 | 支持与漏扫联动，获取漏扫资产信息，提供资产脆弱等级、安全评分等信息，并可对资产设置安全防护策略；（提供截图） |
| EDR联动 | 支持与EDR联动，获取EDR资产信息，提供资产IP、资产状态、安全状态、资产详情等信息，并可对资产按照安全状态、资产类别、操作系统等分类进行统计；支持监督网络中主机安装EDR客户端；（提供截图） |
| DLP联动 | 支持与DLP产品联动，获取DLP设备检测到的具有威胁的五元组信息，防火墙进行动态阻断；（提供截图） |
| 数据库审计联动 | 支持与数据库审计产品联动，获取数据库审计设备检测到的具有威胁的五元组信息，防火墙进行动态阻断；（提供截图） |
| ★**资质与服务要求** | 产品资质 | 信息安全产品自主原创证明； |
| 防火墙密码检测证书； |
| 信息安全产品分级评估（EAL4+）； |
| 国家信息安全漏洞库兼容性资质； |
| 所投厂商具备云安全成熟度模型CS-CMMI 5认证，提供证书复印件 |
| 投标产品应该是被广泛应用的成熟产品，在国内市场具有较高的市场份额，近3年市场占有率排名不应低于前3名。须提供知名第三方机构（如IDC）出具的市场占有率排名有效证明材料。 |
| 服务 | 原厂商五年硬件保修，因该设备是我单位重要等保安全设备，中标后七天内，我单位有权利要求中标公司提供样机对所投产品功能逐一验证，如果发现有不满足要求，将有权追究相关代理商和厂商虚假应标的责任。 |

**4.2下一代防火墙（边界）**

|  |  |  |
| --- | --- | --- |
| **指标** | **指标项** | **详细要求** |
| ★**基本要求** | 系统结构 | 产品由专用的硬件平台、安全操作系统及功能软件构成。设备采用自主知识产权的专用安全操作系统，采用多核多平台并行处理特性（提供证明材料）；为使保证安全产品做到安全自主可控，要求为国产品牌。为保证系统软件设计全面性、保密性、完整性，要求招标产品系统遵从行业标准和政府法规，产品符合 CNITSEC-SP-01 测评准则，提供第三方权威证明材料。 |
| 操作系统 | 安全操作系统采用冗余设计，出于安全性考虑，多系统需在设备启动过程中进行选择不得在WEB维护界面中设置系统切换选项。 |
| 为保障产品运行的安全及稳定性，要求产品设计、开发、生产及售后服务符合TL9000-H-S-V相关标准要求；提供第三方权威证明材料。 |
| 性能要求 | 2U,6个千兆电口，2个SFP插槽,双电源,2个扩展槽位,防火墙吞吐20G，并发连接500万，每秒新建连接24万；可扩展IPSEC VPN、SSL VPN、三权分立模块；支持扩展IPS入侵防御、WAF、URL过滤及AV防病毒功能；要求支持芯片硬件加速技术，实现硬件资源充分利用，保障设备处理效率，提供第三方权威证明材料 |
| 安全功能模块 | 配置入侵防御功能及默认包含3年规则库升级授权。 |
| **集成技术支持** | 工作模式 | 支持路由、交换、虚拟线、Listening、混合工作模式；  |
| 路由交换 | 支持RIP、OSPF、BGP4、QinQ、PIM-SM、PIM-DM；（提供截图） |
| 支持策略路由，支持根据入接口、源/目的IP地址、协议、用户、应用、选路算法、探测等多种条件设置策略路由；  |
| 链路聚合 | 支持手动和LACP链路聚合，可根据源/目的MAC、源/目的IP、源/目的端口、五元组、端口轮询等条件提供不少于10种链路负载算法。（提供截图） |
| IP/MAC绑定 | 支持IP/MAC绑定，支持跨三层绑定，支持IP/MAC绑定表导入导出，以便对IP/MAC绑定关系进行批量操作；  |
| 地址转换 | 支持多种地址转换，支持源/目的NAT、双向NAT、NoNAT转换方式；支持源IP转换同一性；支持端口块地址转换和EIM地址转换 |
| DNS Doctoring | 支持DNS Doctoring功能，能够将来自内部网络的域名解析请求定向到真实内网资源，提高访问效率，同时支持通过配置多条 DNS Doctoring，实现内网资源服务器的负载均衡（提供截图）； |
| 媒体业务接入 | ★支持H.323、SIP等媒体协议,符合GB/T 28181-2016《安全防范视频监控联网系统信息传输、交换、控制技术要求》及TC/OP(XZ)2B-185-2017相关技术要求，提供权威测试报告； |
| 访问控制 | ★支持一体化安全策略配置，可以通过一条策略实现五元组、源MAC、源地区、目的地区、域名、应用、服务、时间、长连接、并发会话、WEB认证、IPS、AV、URL过滤、高级威胁防护、WAF、邮件安全、数据过滤、文件过滤、僵木蠕防御、审计、防代理、APT等功能配置,简化用户管理；（提供截图） |
| 提供策略分析功能，支持策略命中分析、策略冗余分析、策略冲突检查、策略包含分析，可在WEB界面显示检测结果；（提供截图） |
| 网络接入 | 支持RADVD、ND、RIPng、OSPFv3、BGP4+，支持IPv6静态、动态组播路由；（提供截图） |
| 支持NAT64、NAT46、NAT66地址转换，支持6to4隧道、ISATAP隧道；（提供截图） |
| 访问控制 | ★支持IPv6安全控制策略设置，能针对IPv6的目的/源地址、目的/源服务端口、区域、服务、时间、扩展头属性等条件进行安全访问规则的设置（提供截图）； |
| 支持IPv6域名控制，支持对多级域名进行控制，域名对象支持通配符； |
| 安全防护 | 支持对IPv6报文进行病毒防御、入侵防御、URL过滤、抗DDOS、WAF防护、僵木蠕、流量控制、连接限制、文件过滤、数据过滤等；（提供截图） |
| 资源虚拟化 | 支持在一台物理设备上划分出128个相互独立的虚拟系统（提供截图） |
| 功能虚拟化 | 支持配置文件、系统服务、路由、链路聚合、安全策略、NAT策略、带宽管理、认证策略、IPV6功能、URL过滤、病毒过滤、WAF、僵木蠕、高级威胁防护、内容过滤、邮件安全、审计、报表、防代理等安全功能虚拟化；  |
| 负载均衡 | 支持用户服务器的负载均衡，保证用户关键服务的有效性； |
| 防火墙在链路高数据量情况下，可以实现防火墙网络地址转换动态负载均衡，提供第三方权威证明文件； |
| 为保证产品功能健壮性，要求产品研发厂商通过软件成熟度CMMI5认证，提供第三方权威证明文件。 |
| 操作系统 | 可在发生系统故障时，实现系统自动修复。提供第三方权威证明文件； |
| 入侵防御 | 支持独立的入侵防护规则特征库，特征总数在5500条以上（提供截图），能对常见漏洞进行安全防护，兼容国家信息安全漏洞库（提供权威资质证明）； |
| ★厂商需具备强大的漏洞和攻防研究能力，为CNNVD一级支撑单位和CNVD技术组成员（提供证明材料），能够确保每周至少更新1次攻击特征库； |
| DDOS防御 | 支持针对IP、ICMP、TCP、UDP、DNS、HTTP、HTTPS、SIP、NTP等协议进行DDOS防护；支持预定义和自定义策略模板；（提供截图） |
| 支持TCP DDOS防护，采用阀值检查、源/目的限流、源认证、会话检查等方式综合进行SYN FLOOD、SYN-ACK FLOOD、FIN FLOOD、RST FLOOD、FRAG FLOOD、连接耗尽等攻击防护；（提供截图） |
| 支持NTP DDOS防护，采用阀值检查、源/目的限流、源认证等方式综合进行NTP REQUEST FLOOD、NTP REPLY FLOOD攻击防护；（提供截图） |
| 支持SIP DDOS防护，采用阀值检查、源/目的限流、源认证方式进行SIP FLOOD攻击防护；（提供截图） |
| 支持HTTPS DDOS防护，采用阀值检查、源/目的限流方式进行HTTPS FLOOD攻击防护；（提供截图） |
| URL过滤 | 支持超过80类、1000万的URL地址分类库，用户可对搜索引擎、微博、网购、求职、婚恋、娱乐、恶意网站、赌博、色情、反动、暴力、迷信等网站进行全面管控； |
| 支持自定义URL分类和地址，支持URL黑/白名单，支持自定义阻断页面； |
| 内容过滤 | 内置内容过滤功能，支持基于http、ftp、telnet、smtp、pop3协议的内容过滤策略，可对FTP上传/下载的文件名进行过滤，同时支持过滤FTP信令：上传文件、下载文件、删除文件、重命名文件、创建目录、删除目录、列出目录等，邮件过滤支持对发件人、收件人、主题、内容、附件等进行过滤；（提供截图） |
| Web攻击防护(需另外购买) | 支持独立的WAF引擎，WAF防护特征总数在1300条以上，可对常见Web攻击进行防护；  |
| 高级威胁防护 | 内置高级威胁防护，可对DGA、隐蔽信道、恶意加密流量进行检测，支持监控高级威胁检测数据，并进行可视化展示； |
| 支持与APT联动，获取APT监测设备上的威胁检测结果，实现协同防护；（提供截图） |
| 内置行为分析功能，对新建连接数、并发连接数、流量等数据进行统计分析，建立业务行为基线，对异常行为进行告警；支持行为分析监控展示，可展示不同行为分析策略的实时数据和基线数据趋势； |
| 邮件安全 | 内置邮件安全防护功能，支持邮件过滤、邮箱防暴力破解、邮件泛洪攻击防护、邮件黑、白名单检测；（提供截图） |
| 资产管理 | 支持资产管理，可查看资产详情、安全防护策略，并对资产进行分组和防护优化； |
| 智能防护 | 支持对网络资产进行一键检查，获取网络中资产信息、分析资产安全状态，一键完成风险资产安全防护； |
| 漏扫联动 | 支持与漏扫联动，获取漏扫资产信息，提供资产脆弱等级、安全评分等信息，并可对资产设置安全防护策略；（提供截图） |
| EDR联动 | 支持与EDR联动，获取EDR资产信息，提供资产IP、资产状态、安全状态、资产详情等信息，并可对资产按照安全状态、资产类别、操作系统等分类进行统计；支持监督网络中主机安装EDR客户端；（提供截图） |
| DLP联动 | 支持与DLP产品联动，获取DLP设备检测到的具有威胁的五元组信息，防火墙进行动态阻断；（提供截图） |
| 数据库审计联动 | 支持与数据库审计产品联动，获取数据库审计设备检测到的具有威胁的五元组信息，防火墙进行动态阻断；（提供截图） |
| ★**资质和服务要求** | 产品资质 | 信息安全产品自主原创证明； |
| 防火墙密码检测证书； |
| 信息安全产品分级评估（EAL4+）； |
| 国家信息安全漏洞库兼容性资质； |
| 所投厂商具备云安全成熟度模型CS-CMMI 5认证，提供证书复印件 |
| 投标产品应该是被广泛应用的成熟产品，在国内市场具有较高的市场份额，近3年市场占有率排名不应低于前3名。须提供知名第三方机构（如IDC）出具的市场占有率排名有效证明材料。 |
| 服务 | 原厂商五年硬件保修，因该设备是我单位重要等保安全设备，中标七个工作日内，我单位有权利要求中标公司提供样机对所投产品功能逐一验证，如果发现有不满足要求，将有权追究相关代理商和厂商虚假应标的责任。 |

**4.3APT**

|  |  |  |
| --- | --- | --- |
| **指标** | **指标项** | **详细要求** |
| ★**基本要求** | 硬件配置 | 接口配置≥7个千兆电口，≥4个千兆光口，≥2个万兆光口，含HA口、管理口,冗余电源；CPU≥10核20线程\*2,内存≥128G，系统盘≥250GB SSD,硬盘≥12T。 |
| 产品架构 | 软硬一体化标准机架式设备，单台设备即可完成对APT攻击全生命周期的监测及数据分析与风险预警功能。 |
| 软件规格 | 要求提供APT高级威胁检测软件一套，系统应具备流量采集、文件还原、文件静态和动态沙箱检测、web攻击检测、异常行为分析、数据分析与风险预警等功能，能够检测已知/未知恶意文件，0Day/nday漏洞利用，Web攻击，恶意扫描攻击等；还支持对失陷主机、DGA域名、动态域名、隐蔽信道、异常协议等异常通信行为进行分析告警。为保障产品运行的安全及稳定性，要求产品设计、开发、生产及售后服务符合TL9000-H-S-V相关标准要求；提供第三方权威证明材料。 |
| 性能 | 综合监测吞吐5Gbps；全功能All\_In\_One设备，旁路部署，单台设备具备文件还原、文件静态检测、文件动态沙箱检测、web攻击检测、流量检测、数据分析与风险预警等功能。为保证产品功能健壮性，要求具备产品成熟度CMMI5认证（提供第三方证明）； |
| 部署环境 | 支持在IPv4、IPv6、IPv6和IPv4混合网络环境下提供APT攻击全生命周期的监测及数据分析与风险预警功能。 |
| 规则库升级 | 支持规则库离线、在线以及自动升级。默认包含3年应用特征库升级许可。 |
| 分布式部署 | 支持APT设备多级分布式部署，通过级联管理中心对多台APT设备集中管理，包括收集告警信息，查看节点系统状态，下发策略等。 |
| **集成技术支持** | 审计协议 | 支持常见网络协议的解析，包括DNS、HTTP、FTP、SMTP、POP3、IMAP、SMB、HTTP proxy等协议报文；支持协议还原流量大小自定义。（提供功能截图） |
| 文件还原 | ★支持解析还原包括邮件文件（EML）、Office（Word、Excel、PPT、RTF）、WPS、PDF、HTML、JS、PE（EXE、DLL等）、压缩包（ZIP、7Z、RAR等）、脚本文件（BAT、VBS、CMD、Powershell）、图片文件（PNG、JPG等）、APK等70余种默认文件格式。（提供功能截图） |
| 支持检测文件格式自定义，如：新增.do后缀类型的文件，系统对此类型文件进行实时检测。（提供功能截图） |
| 检测引擎 | 具备动态行为检测引擎、机器学习检测引擎、威胁情报检测引擎、AV检测引擎、CVE检测引擎、YARA规则检测引擎等文件检测引擎，且每种检测引擎均可输出各自检测结果。（提供功能截图） |
| 文件静态信息检测 | 支持文件静态信息检测，应能分析文件的PE信息，证书信息，字符串信息以及样本文件的数字签名有效性，能够识别伪装的恶意代码文件。 |
| 文件hash检测 | 具备独立的文件HASH库检测引擎，发现已知的恶意文件；文件HASH库支持100+万个以上已知恶意文件MD5特征。 |
| 支持对所有已检测过的文件HASH进行统一存储，并提供搜索、查看、重新检测功能。（提供功能截图） |
| 机器学习 | 支持3种以上机器学习算法模型（静态检测模型、动态检测模型、静态和动态混合检测模型）对文件进行威胁判定，且每种机器学习模型会对所支持的样本文件进行检测，输出不同的机器学习算法对样本恶意与非恶意的判定结果。（提供功能截图） |
| YARA规则匹配 | 支持自定义YARA匹配规则和快速集成第三方YARA规则，通过匹配恶意文件特征的描述信息有效识别恶意软件，极大优化文件检测执行效率。（提供功能截图） |
| 沙箱检测 | 支持动态沙箱检测技术检测恶意文件（流量还原出的文件或直接上传的文件），通过动态执行可疑文件，发现已知/未知的漏洞利用行为，识别已知/未知木马、僵尸、蠕虫、病毒等恶意代码文件。 |
| 沙箱行为监测 | 支持检测文件运行期间的漏洞利用行为，支持对缓存溢出、ROP、堆喷射等漏洞利用行为的检测。 |
| ★沙箱支持安装包程序释放物检测，沙箱能够自动完成安装包类型样本的安装，检测安装包中隐藏的恶意释放物，同时支持shellcode提取，能将shellcode反汇编成汇编代码。（提供功能截图） |
| 沙箱能够监控恶意软件对文件系统和系统注册表的操作，能够对进程操作、模块行为以及进程的异常处理情况进行监控，能够对进程调用API情况和对窗口的操作行为进行监测。（提供功能截图） |
| 沙箱支持对恶意文件样本的网络行为进行监测，记录文件联网通信会话，并支持在线查看通信会话详情，会话内容支持以16进制和ASCII两种格式进行展示。（提供功能截图） |
| 沙箱逃逸检测 | 具备业内领先的沙箱逃逸行为检测技术，针对特种木马、病毒等恶意文件反虚拟机检测行为进行检测和分析，避免恶意文件逃逸沙箱检测。 |
| 威胁行为展示 | 沙箱引擎支持以可视化的对象实体图的方式来查看样本的威胁行为信息。（提供截图证明） |
| 沙箱引擎支持对恶意样本的活动行为截图保存，并可在线查看恶意行为截图详细信息。（提供截图证明） |
| 离线检测 | 支持手工上传本地样本和远程url链接地址下载文件进行文件检测。（提供截图证明） |
| 样本下载 | 支持将系统还原出的文件进行加密，加密密码可自定义设定。支持将加密后的文件下载到本地进行复核。（提供功能截图） |
| 沙箱环境自定义 | 支持用户自定义沙箱虚拟机联网配置，至少支持不联网、可联网、使用虚拟网络联网等模式。（提供功能截图） |
| 支持沙箱检测虚拟执行策略自定义，自定义策略类型包含发现威胁执行、未发现威胁执行、始终执行、始终不执行4种。（提供功能截图） |
| 检测配置 | 支持文件检测多种策略设定，包括：检测文件大小自定义、虚拟机模板切换、自定义指定类型文件的特征等。 |
| 失陷主机检测 | 支持信誉检测机制，通过C&C信誉库（黑IP、黑URL、黑域名）来检测木马（如：ZeuS、Feodo等）、僵尸、蠕虫等恶意代码的活动行为。 |
| 支持通信流量特征检测，基于流量中的通信特征，来检测木马、僵尸、蠕虫等恶意代码的主机上线、文件操作、屏幕监控等活动行为。（提供功能截图） |
| 支持基于威胁情报&流量特征的威胁事件会话PCAP文件记录、存储和PCAP文件在线查看功能。 |
| Web攻击检测 | 支持对Web应用攻击行为进行检测，包括恶意扫描攻击、漏洞利用行为、注入攻击，XSS，CSRF、文件包含、目录遍历等常见web攻击类型。（提供功能截图） |
| ★支持根据相似关系构建僵尸群落，进行分析，发现僵尸网络间的内在关系，更有效的跟踪和研究僵尸网络背后的黑客组织的行为模式，提供第三方证明文件。 |
| 支持对Webshell控制行为进行监测。 |
| 支持Web攻击事件会话PCAP文件记录、存储和PCAP文件在线查看功能。 |
| 隐蔽信道检测 | 支持隐蔽信道通信检测功能，能够在看似正常的流量中识别木马的隐藏传输行为，并具备对通信会话的PCAP文件记录、存储以及在线查看功能。 |
| 异常通信检测 | 支持不少于4项异常通信行为检测功能，包括但不限于动态域名、DGA域名检测、异常协议、异常心跳等。（提供功能截图） |
| 支持动态域名检测，能够检测大量频繁访问常见动态域名的可疑行为，如3322.org等。（提供功能截图） |
| 防火墙联动 | 支持与防火墙联动实现网络攻击检测与阻断的闭环。支持自定义五元组信息的阻断策略。（提供功能截图） |
| 时间序列关联分析 | 支持时间序列关联分析，以内网资产或者指定的外部IP地址作为基础，以时间、检测事件作为条件呈现当前资产或者IP的威胁态势情况。需要支持交互式操作，用户可以按照时间段、威胁类别、攻击次数、外网IP进行过滤筛选。（提供功能截图） |
| KILLCHAIN关联分析 | 支持交互式的KILLCHAIN可视化分析功能，对攻击过程智能化关联分析，方便还原攻击过程，对攻击进行溯源追踪。（提供功能截图） |
| 支持在单一界面内对系统检测到的各类攻击行为按照网络杀伤链不同阶段进行展示，以全局的视图呈现网络中指定资产遭受到的攻击情况并支持按照攻击阶段、威胁类别、时间周期进行过滤筛选。（提供功能截图） |
| 网络安全知识库 | 提供网络安全知识库，能够为系统检测的威胁信息并提供知识说明。知识库内容包括威胁类型、威胁标签、描述信息、受影响范围、处置建议、参考信息、代码示例、流量示例、安全普及知识、时间线等信息。（提供功能截图） |
| 资产信息录入 | 支持重点资产信息录入，信息包括：资产IP、资产类型、归属人、所属区域、操作系统、MAC地址、归属人等信息。 |
| 资产维度分析 | 支持重点资产监控，以资产维度进行威胁分析与统计，展示重点资产所遭受攻击的攻击阶段，攻击源，攻击类型等信息，便于客户直观的对重点资产安全状况进行了解和查看。 |
| 威胁感知地图 | 支持对实时攻击态势进行动态地图展示，在动态地图中可按日或按周展示全球地图和中国地图的攻击源到目的地址的攻击路径。（提供功能截图） |
| 数据分析展示 | 支持大屏展示实时告警信息，包括攻击源目的IP，通信协议，攻击类型，告警次数等详细信息，并支持告警信息展示界面自定义。 |
| 支持大屏展示攻击阶段分布信息，将攻击过程按照入侵植入，远程控制，未知攻击进行分类展示，并支持攻击阶段分布展示界面自定义。 |
| 威胁态势监控 | 支持当天或一周的威胁态势监控，威胁态势信息通过统计攻击次数，威胁趋势，威胁分布，威胁排名等信息并以攻击类型和地区分布两方面进行详细展示。 |
| 告警信息展示 | 支持以威胁等级、事件类型、协议类型等对告警事件进行分类，并可按照自定义攻击源目的IP、检测信息、时间等条件进行分类查询，同时支持自定义列展示信息。 |
| 报表查询 | 支持对指定时间段内所有事件或指定分类事件（文件、失陷主机、漏洞攻击、WEB检测、异常行为）的统计信息进行查询。 |
| 报表导出 | 支持自动导出报表，将定时导出的报表发送到指定邮箱中。 |
| Syslog配置 | 支持将告警日志发送给第三方Syslog服务器。支持日志外发策略自定义，包括对转发事件类型（系统告警事件、文件检测事件、流量检测事件、Web攻击检测事件、审计事件、性能日志）、转发地址、转发端口、协议类型等进行配置。 |
| 邮件告警 | 支持将告警信息以邮件形式发送到策略设定的接收人查收。（提供功能截图） |
| **其他要求** | ★产品资质 | 中华人民共和国公安部颁发的《计算机信息系统安全专用产品销售许可证》 |
| 中国信息安全认证中心颁发的《IT产品信息安全认证证书》，测试标准为ISCCC-TR-083-2018《APT安全监测产品安全技术要求》 |
| IPV6金牌证书 |
| 中华人民共和国国家版权局颁发的《计算机软件著作权登记证书》 |
| 服务 | 原厂商五年硬件保修 |

**4.4多功能探针**

|  |  |  |
| --- | --- | --- |
| **指标** | **指标项** | **详细要求** |
| ★**基本要求** | 性能要求 | 2U,6个千兆电口，4个千兆光口，2个万兆光口,冗余电源,4个扩展槽位,最大并发连接数：500W，综合威胁检测能力：10000Mbps。为保证产品功能健壮性，要求具备产品成熟度CS-CMMI5认证（提供第三方证明）； |
| 设备管理 | 支持B/S管理模式，无需安装独立的控制台软件署。 |
| 支持对设备WEB页面、命令行方式配置管理，可直接从web中实现命令行方式管理。（提供截图证明） |
| 软件规格 | 要求提供僵尸网络木马和蠕虫监测软件一套，集合攻击检测、僵木蠕检测、DDoS检测、恶意程序检测、APT检测、WEB安全检测、虚拟沙箱、元数据提取、流量分析九大功能，即九合一全流量检测探针。软件通过深度解析网络流量，结合特征匹配、异常行为分析、机器学习技术、虚拟沙箱等技术，实现迅速、精准识别网络中各种已知和未知网络威胁。为保障产品运行的安全及稳定性，要求产品设计、开发、生产及售后服务符合TL9000-H-S-V相关标准要求；提供第三方权威证明材料。 |
| 规则库升级 | 默认包含3年应用特征库打包升级许可，包含攻击检测规则库、应用识别库、地理信息库、僵尸主机规则库、威胁情报库、URL分类库。 |
| 支持对规则库自动更新、手动更新、导入等升级方式。 |
| 支持特征库升级无缝加载技术，整个升级过程检测引擎无间断工作。 |
| 支持攻击检测规则库、应用识别规则库、URL分类规则库、僵尸主机规则库、威胁情报库、地理信息库，各规则库相互独立。（提供截图证明） |
| **集成技术支持** | 攻击检测 | 支持独立的攻击检测引擎，支持8500种以上的攻击规则库。（提供截图证明） |
| 支持扫描探测、暴力猜解、拒绝服务攻击、后门控制、溢出攻击、代码执行、非授权访问攻击、注入攻击、URL跳转、跨站攻击、Webshell、浏览器劫持、文件漏洞攻击等多种常见攻击行为。攻击行为涉及WEB应用、文件传输、邮件、数据库、远程访问、远程过程调用、基础服务、工控、加密等多种业务。（提供截图证明） |
| ★支持工控漏洞攻击、车联网漏洞攻击、物联网漏洞攻击。如对施耐德PLC、Siemens S7、IGSS SCADA、RealWin、SERVER-WEBAPP、罗克韦尔、 Netgear DGN1000系列路由器、Belkin N750 F9K1103无线路由器、DGN2200、欧姆龙FINS TCP读取控制器、Iconics Genesis、华为HG532路由、Vivotek智能摄像头等系统或设备漏洞攻击检测。（提供截图证明） |
| 支持对攻击逃逸的检测，包括IP分片逃逸行为攻击，TCP流重组乱序逃逸行为攻击检测、协议端口重定向逃逸行为攻击检测等类型。 |
| 支持对SMTP、POP3、IMAP、FTP、TELNET、LDAP、RDP等服务的弱口令登录行为检测，采用弱口令字典和口令强度两种方式检测，可自定义口令度规则，如密码长度、密码字符类型等。（提供截图证明） |
| 支持暴力破解攻击行为检测，包括SMTP服务暴力破解、POP3服务暴力破解、IMAP服务暴力破解、FTP服务暴力破解、TELNET服务暴力破解等。支持自定义周期和告警阈值。（提供截图证明） |
| 僵尸木马蠕虫病毒检测 | 采用僵尸主机与控制主机异常通信行为检测的方式，具有独立的僵尸主机特征库，能够对10000种以上僵尸主机行为进行监测，包括僵尸网络行为、木马控制行为、蠕虫活动行为、挖矿行为、勒索软件行为、移动端木马控制行为、APT行为等多类型的僵尸主机行为。（提供截图证明） |
| 支持对检测到的控制主机数量、僵尸主机数量实时统计，记录控制主机的活跃次数，控制了多少僵尸主机、地理位置监控，且支持以地图的形式展现控制主机的地理分布。 |
| 支持实时分析统计僵木蠕事件的控制主机、僵尸主机以及事件总次数，并对TOP10排名。提供僵木蠕事件的详细信息，如：影响操作系统、描述、解决方法等。 |
| 恶意程序检测 | ★支持对恶意程序实现特征检测、机器学习检测、内置虚拟沙箱检测等多种检测方式，并且多种检测方式相互独立、互不影响；支持专业沙箱设备联动检测。（提供截图证明） |
| 机器学习检测能够对目标文件实时检测实时还原效果，不依赖规则库检测实现对未知恶意程序检测。 |
| 沙箱设备联动检测支持将被检测的文件自动发送到沙箱设备，沙箱设备检测后自动返回结果，无需人工操作，整个检测过程自动化处理。 |
| 支持对使用HTTP、FTP、SMTP、POP3、SMB、DNS、NFS、IMAP等非加密协议以及HTTPS、FTPS、SMTPS、IMAPS等加密协议传输的文件检测。（提供截图证明） |
| 支持对压缩类（包括RAR、7Z、ZIP、GZ、CAB等压缩类型）、Windows可执行类（包括exe、dll等）、Linux可执行类（包括SO、ELF等）、移动端类型（包括APK、SIS等）、OFFICE类、PDF、RTF、JAR等多种文件类型检测。 |
| 支持对恶意文件还原捕获，可自定义捕获文件大小，支持对恶意文件、疑似恶意文件、无风险文件还原。支持对还原捕获的恶意文件使用FTP服务、SFTP服务外发第三方平台。（提供截图证明） |
| ★支持详细记录被检测文件信息，包括文件文件名 、首次传播时间 、文件哈希 、文件类型 、文件大小(字节) 、传播次数 、威胁指数。（提供截图证明） |
| 支持按恶意程序类型、文件类型、应用协议类型对恶意程序图形化统计。支持对恶意程序Top10统计，并且统计传输次数。 |
| 支持对传输的恶意程序以源、目主机两种维度统计，包括主机所属区域、传播的恶意文件数、涉及的攻击次数。 |
| APT检测 | 支持通过威胁情报检测已知APT事件，通过恶意程序检测未知APT事件，通过僵尸行为规则库检测已知的APT组织。 |
| 支持识别摩诃草APT组织、隐士(Hermit) APT组织、DarkHydrus APT组织、APT 28组织、APT29(Cozy Bear)组织、APT33组织、APT34组织、Donot (APT-C-35)组织、OceanLotus APT组织、朝鲜STOLENPENCIL APT组织、Windshift APT组织、TransparentTribe APT组织等全球多个APT攻击组织。（提供截图证明） |
| WEB安全检测 | 支持对SQL注入攻击、跨站攻击、浏览器劫持攻击、URL跳转攻击、WEB远程代码执行攻击、WEB缓冲区溢出攻击、WEB漏洞攻击、Webshell上传攻击、WEB越权攻击、WEB扫描攻击、目录遍历攻击、WEB口令暴力破解攻击等多种类型的WEB攻击检测。 |
| 虚拟沙箱 | 支持模拟仿真沙箱环境，对文件进行扫描分析、脱壳分析、动态行为分析等深度检测，脱壳分析支持多层壳、虚拟 机保护壳、自定义壳、高级包裹器。 |
| 威胁情报 | 本地嵌入独立的威胁情报库，不依赖其他设备或情报平台，即可独立的实现威胁情报检测能力。（提供截图证明） |
| 威胁情报库数量超过790万，可通过手动添加、批量导入的方式自定义威胁，并且满足威胁白名单能力。（提供截图证明） |
| 威胁情报支持对恶意IP/域名访问、恶意URL、恶意文件传输行为检测。 |
| 支持对属性未知的IP地址、URL地址、MD5值在线检测。 |
| 对命中的威胁情报事件，支持按威胁源主机TOP10、恶意文件TOP10实时统计。支持对威胁源主机分布、恶意文件分布图形化实时统计。 |
| 加密流量检测 | 支持卸载SSL，实现对HTTPS、SMTPS等加密流量的分析检测。（提供截图证明） |
| 溯源取证 | 支持攻击取证、僵尸主机取证、恶意程序取证、威胁情报取证，取证类型支持报文取证和样本文件取证两种形式。（提供截图证明） |
| 支持将威胁事件日志信息和取证文件相互关联，通过对威胁基本信息检索即可获取全面的威胁信息 |
| 威胁处置 | 支持对入侵攻击、僵木蠕行为、恶意程序传播、APT攻击、WEB攻击、访问非法URL/域名、恶意IP访问等安全事件阻断处置。 |
| 支持通过发送RSET包阻断。 |
| 支持防火墙联动，实现联动阻断恶意事件的通信。防火墙阻塞时间可自定义。 |
| 元数据提取 | ★支持对TCP/UDP流量、ICMP流量、HTTP流量、邮件流量、FTP流量、DNS流量、NFS流量、SMB流量、SSL流量、LDAP流量、RDP流量等多种常见流量深入内容层解析元数据；支持对HTTPS流量、加密邮件流量、FTPS流量等多种加密流量深。入内容层解析元数据。（提供截图证明） |
| 元数据解析内容包括邮件发件人、邮件收件人、邮件主题等邮件信息，传输文件协议、文件名称、文件大小、文件类型、MD5值、传输方向等文件信息，以及加密证书名称、证书颁发机构、证书使用者、证书内容等加密证书信息。（提供截图证明） |
| 流量分析 | 支持按接口对报文流入流出速率实时监控，每分钟对接收的报文按传输层协议、网络层协议、报文字节大小等多维度进行统计分析。对各接口的流量趋势按天、周、月图形化记录。 |
| 支持对流量从应用维度详细分析，支持记录统计各应用的总流量消耗、上下行流量消耗、当前上下行速率、连接总数等。记录每种应用天、周、月的流量趋势图。并且分析记录应用的主机访问详情，包括主机IP、总流量消耗、连接数等信息。 |
| 支持对3600多种的应用流量分析。 |
| **其他要求** | ★产品资质 | 计算机信息系统安全专用产品销售许可证（设备专属证书，非复用其他产品证书） |
| 国家信息安全漏洞库兼容性资质证书 |
| 计算机软件著作权登记证书 |
| 服务 | 原厂商五年硬件保修 |

**4.5态势感知**

|  |  |  |
| --- | --- | --- |
| **指标** | **指标项** | **详细要求** |
| ★**产品基本要求** | 操作系统 | 为保障产品运行的安全及稳定性，要求产品设计、开发、生产及售后服务符合TL9000-H-S-V相关标准要求；提供第三方权威证明材料。 |
| 产品性能 | 系统立足客户视角分别从全网、威胁、安全底图、安全处置、资产、漏洞、攻击、僵木蠕、网站监测、终端十个视角进行安全数据采集、监测、分析、研判和展示，满足不同行业的实时态势感知、准确安全监测、及时应急处置等目标 、提升风险识别效率和安全处置能力 。主要包括：安全事件一键溯源、自动化响应编排、可视化分析场景管理、多重安全分析、多维度资产视角、联动式设备管理、多算法安全事件校验、海量数据处理性能、多厂商探针灵活接入。 |
| 日志源接入 | 满足现有安全设备和未来五年内所有网络与安全设备的日志源接入，包含软件五年升级。 |
| **集成技术支持** | 大屏展示 | 支持态势大屏展示，包括全网态势、资产态势、**漏洞态势**、攻击态势，支持大屏展示时间设置，支持态势大屏中相关信息下钻跳转到对应的详细页面 |
| 支持拖拽方式自定义大屏界面展示顺序，**支持多种地图、拓扑展示方式，包括但不限于世界、全国、省份、拓扑等**，支持logo、标题、大屏超时设置。（提供截图）。 |
| 全网态势 | 支持全网资产概述、高危资产、漏洞、告警趋势、安全日志趋势、告警统计、最新告警名称和影响范围、热点威胁等内容的相关展示 |
| 支持3D地球动态展示攻击过程，支持以不同攻击线颜色区分攻击级别 |
| 资产态势 | ★支持通过轮播进行资产总量、漏洞总数、日志总数相关信息的展示，支持按资产类型及失陷状态进行展示，支持按漏洞级别进行展示，支持按日志级别进行展示（提供截图）； |
| 支持重点威胁对资产的影响分析，支持至少5种重点威胁，支持分析每种威胁影 响的资产数量 |
| 漏洞态势 | ★支持漏洞态势分析，包括漏洞总体情况、漏洞类型分布、漏洞级别分布、高危漏洞排行TOP5、漏洞排行TOP10、最新漏洞发现趋势、高危漏洞类型排行、漏洞级别对比（提供截图）； |
| 攻击态势 | 支持以全球地图实时展示网络攻击态势，支持以不同颜色攻击线展示攻击过程，支持攻击源和攻击目的国家名称展示，支持攻击目的进行光晕显示 |
| 日志监测 | 支持日志概览，包括日志源数量、安全日志数量、审计日志数量、安全日志级别分布、安全日志类型排名、日志量趋势，支持概览时间设置； |
| 支持对接同品牌及第三方安全设备的日志，包括但不限于防火墙、入侵检测、流量分析、蜜罐等（提供截图）； |
| 支持分布式部署采集代理，支持不同采集代理的状态监控，包括但不限于状态、CPU、内存、接收速率、归一化数量、归并数量等 |
| 漏洞监测 | 支持联动漏扫设备、手动导入漏扫报告两种方式实现漏洞数据采集，支持同品牌及第三方漏扫设备联动，支持excel、zip等类型的漏扫报告导入（提供截图）； |
| 支持漏洞监测任务添加、查询、**批量启动、批量删除**等操作管理（提供截图）。 |
| 性能监测 | ★支持资产性能监测概览，支持监测设备总数、异常数、主机异常数、网络设备异常数、安全设备异常数展示，支持监控资产性能状态占比、性能告警TOP10、规则类型事件分布、CPU使用率TOP10、内存使用率TOP10、磁盘使用率TOP10，支持性能监控详细列表，包括IP、资产名称、归属安全域、资产类型、性能状态、连通状态、CPU使用率、内存使用率、磁盘使用率、操作等（提供截图）。 |
| 漏洞处置 | 支持通过漏洞视角进行漏洞的查询展示及处置，展示信息包括时间、漏洞名称、漏洞编号、漏洞级别、漏洞分类、影响范围，支持按照TXT、CSV、EXCEL进行导出； |
| 支持漏洞详情查看，包括漏洞基本信息及影响范围，影响范围以列表形式展示受影响资产的名称、IP、类型、所属业务系统、漏洞状态等信息，支持按多种方式对漏洞进行处置，处置方式包括新发现、重现、确认、误报、已消除、已防范； |
| 安全预警 | 支持按照预备预警、正式预警规则进行安全预警规则管理，支持预警规则自定义配置，配置内容包括但不限于预警名称、预警类型、预警级别、预警内容、可能后果、解决方案、发送方式、负责人、资产影响范围等细颗粒度的关联配置。 |
| 处置配置 | 支持按预设规则进行告警，支持告警规则的新建、删除、启用、禁用、编辑，支持按照分组进行告警规则管理，告警规则内容包括规则名称、告警名称、过滤器、应用范围、告警类型、告警级别、告警内容、负责人、可能后果、解决方案、**影响范围**、响应方式、触发方式、归并字段；响应方式包括登录显示、邮件、**工单、企业微信群**等（提供截图）。 |
| 建模分析 | 支持内置至少30种分析模型，包括但不限于失陷状态、FTP登录失败、敏感文件信息泄露、成功暴力破解、文件上传漏洞等，支持模型查看、启用、停用等操作，支持模型批量删除、批量启用、批量停用，支持导入内置模型，状态为启用的模型不允许操作，支持按照模型名称、模式、模型状态、模型分类、关注度进行过滤查询（提供截图）。 |
| 资产概况 | 支持全局展示资产概况，包括但不限于全部资产数/安全域数、等保业务系统数/业务系统数、已同步主库资产数/备库资产数、安全域资产分布TOP5、业务系统定级分布、主库资产类型分布等。 |
| ★支持多视角全网拓扑管理，包括管控设备拓扑、资产拓扑、业务拓扑，支持自定义拓扑及主动扫描探测拓扑，支持编辑及保存拓扑，支持拓扑图的整体拖拽和缩放操作，支持对单个节点拖拽操作，支持查看拓扑图节点关联的资产设备概览、告警列表、漏洞列表等安全属性详细信息（提供截图）。 |
| 资产属性管理 | 支持资产属性信息管理，包括认证信息、类型配置、物理位置、资产用户、漏洞、补丁。 |
| IP资源管理 | 支持IP集合管理，支持IP集合列表展示，展示信息包括IP集合总数、IP集合名称、地址范围、标签、应用情况、时间等，支持对IP集合进行新增、修改、查看、删除、批量删除、下载模板、导出、导入、定位下发等操作，支持IP定位库管理，支持IP定位库上传、IP定位下发，支持IP定位库上传（提供截图）。 |
| 安全报告 | ★治理中心支持统计概览，包括但不限于安全报告、合规审计日志、应急预案、跟踪文档、待整改业务系统展示，支持待整改业务系统排名、最新安全报告排名、最新跟踪文档等信息，最新安全报告支持下载（提供截图）； |
| 合规审计 | 支持合规审计，审计设备类型包括但不限于主机、安全设备、网络设备、业务应用、中间件、数据库（提供截图）； |
| 支持简洁审计模式，查询条件支持10种以上字段，包括但不限于日志名称、日志级别、传输协议、应用协议，支持查询时间范围设置（提供截图）； |
| 支持高级审计模式，查询条件支持时间范围、日志级别、所属区域、地址/端口/协议、日志信息等（提供截图）。 |
| 等保管理 | 支持等保概览，包括但不限于统计等保业务系统数、已备案业务系统数、测评通过业务系统数、待整改业务系统数、已测评总次数、已整改总次数等统计信息，支持等保业务系统列表展示、等保业务系统等级分布统计、业务系统整改次数排名TOP5、业务系统测评次数排名TOP5、业务系统等保过程记录（提供截图）； |
| ★**资质要求** | 软著证书 | 平台需具备国家版权局颁布相关软件著作权（系统名称具备“态势分析”“安全运营”字样）。须提供证明加盖公章，证明中明确包括“态势分析”“安全运营”两个关键词信息，否则视为不满足 |
| 销售许可证 | 平台需具备公安部颁布的销售许可证（系统名称具备“态势分析”“安全运营”字样）。须提供证明加盖公章，否则视为不满足。 |
| 技术能力 | 《网络安全态势感知技术标准化白皮书 (2020版)》编写单位 |
| 国产化 | 1. 平台需具备信创服务器（基于鲲鹏920）国产化兼容认证；
2. 平台需具备信创操作系统V20(UOS) 国产化兼容认证；

3）平台需具备国产通用安全数据库管理系统兼容性认证证书； |
| **其它要求** | IPV6 | IPv6 Ready Logo 认证证明 |
| 演示环境要求 | 中标方需在中标通知书发出后于3个工作日内根据甲方要求提供演示环境，演示环境需具备招标要求中的全部要求，否则视为不满足 |

**4.6安全资源池**

|  |  |  |
| --- | --- | --- |
| **指标** | **指标项** | **详细要求** |
| **基本要求** | 系统性能 | 2U,6个千兆电口,4个万兆光口,冗余电源,CPU:Intel 处理器\*2颗 10核心支持超线程， 内存：128G内存， 系统盘：256G\*1 SSD， 数据磁盘：4T\*2 raid 0， 接口：6个千兆电口, 4个万兆光口。三节点部署。 |
| **云安全管理平台** | 软件规格 | 要求提供云安全管理平台软件一套，支持提供虚拟化防火墙、虚拟化堡垒机、虚拟化日志审计、虚拟化数据库审计、虚拟化网络审计、虚拟化基线管理、虚拟化Web应用防火墙、虚拟化负载均衡、虚拟化终端威胁防御（EDR）、虚拟化VPN、虚拟化漏扫等安全产品的能力。（提供产品功能截图） |
| 平台要求 | ★安全资源池内所有虚拟化安全产品皆为云安全管理平台安全厂商自研。（提供官网产品截图） |
| **★用户支持按月开通安全组件。本次招标需要安全组件包括但不限于日志审计、数据库审计、堡垒机、漏洞扫描、EDR。**为保障产品运行的安全及稳定性，要求产品设计、开发、生产及售后服务符合TL9000-H-S-V相关标准要求，具备云安全成熟度模型CS-CMMI 5认证，提供第三方权威证明材料。 |
| 支持可以通过控制台单点登录到安全组件管理页面，无需再次输入账号密码。 |
| 支持在云安全管理平台控制台页面显示SAAS化EDR模块授权信息、可视化方式显示EDR服务Agent总数、agent在线数、agent离线数等相关信息。（需提供产品功能界面截图） |
| ★支持多区域部署，用户可通过为不同的区域配置不同的安全组件。（需提供产品功能界面截图） |
| 服务编排支持以可视化的方式方便用户规划创建自己的业务网络，用户可以通过拖拽的方式直观的管理自己的计算网络资源。用户可基于资产信息定义IP五元组流量信息，并可定义流量路径，并关联流量定义实现流量编排。 |
| 默认支持平台管理员、租户管理员、普通用户三种角色支持自定义用户权限对功能模块进行控制，并且可设置功能权限只读或者读写。（需提供产品功能界面截图） |
| 支持创建、删除、修改、查询租户、租户账号。 |
| 支持管理员在创建用户时生成初始密码，并可重置用户密码。 |
| 支持显示平台资源信息，如宿主机运行状态、CPU利用率、内存利用率、磁盘利用率；支持显示申请的实例状态、实时流速、网络总流量、CPU温度等信息，并用可视化图表的方式展示CPU、内存、磁盘占用趋势，网络总流入流出速率趋势（提供界面截图并加盖公司公章) |
| 支持显示安全实例运行状态，可查看安全实例详细信息，如（cpu/内存/磁盘信息、历史流量/流量趋势信息、网络接口状态等）（提供界面截图并加盖公司公章) |
| 支持安全实例态势大屏展示，以可视化的形式显示安全实例列表、安全实例告警状态、安全实例资源信息、以及安全实例资源分布（需提供产品功能界面截图） |
| 支持运维监控态势大屏展示，以可视化的形式显示系统服务状态、物理主机资源信息、IP使用率信息、平台告警信息（需提供产品功能界面截图） |
| 支持安全态势大屏展示、以可视化的形式显示攻击类型排名、攻击源Top5、被攻击主机Top5、安全事件趋势、安全事件排行、威胁终端排行等信息（需提供产品功能界面截图） |
| 支持实时监测日志中包含的关键事件信息和日志产生的频率，从频繁发生的事件日志中发现潜在的危害事件，并产生潜在危害告警日志。可根据不同的事件场景灵活配置监测的事件相关信息、监测时间窗口、监测阀值和告警日志内容。 |
| 支持新建、编辑、复制、删除、启用和停用告警策略；告警日志支持按时间和告警类型等维度筛选；告警类型至少包括：网络攻击告警、WEB攻击告警、DDoS攻击告警、防病毒告警、未知威胁事件告警等；支持自定义告警规则；支持查看告警策略详情，详情至少包括：策略名称、过滤规则、报警级别、规则分组、报警内容等。（需提供产品功能界面截图） |
| 支持单个license可实现云安全管理平台授权和安全组件授权导入；支持许可自动化导入激活安全产品，实现安全产品自动化激活，包括云防火墙、云WAF、云堡垒、云日志审计、云数据库审计、云网络审计、云负载、云基线等等所有安全产品许可的自动化导入激活。 |
| 云安全管理平台相关运行日志，包括服务状态、调试日志等所有用户登录到云安全管理平台以后执行的存在风险的操作，如安全实例关机、重启、删除，用户删除，租户删除，开通新服务等 |
| 支持系统运行诊断分析，诊断系统各平台的服务状态；支持网络抓包诊断分析，可设置区域、物理主机、物理网口、租户、IP、端口等条件进行抓包分析。（需提供产品功能界面截图） |
| 支持查看磁盘使用情况显示磁盘节点信息、磁盘使用情况以及操作日志、告警日志、审计数据所占磁盘空间大小；支持以磁盘利用率、数据类型、时间等条件设置磁盘清理规则，定期清理磁盘空间（需提供产品功能界面截图） |
| ★支持级联管理功能，一个主管理平台可以管理多个分支管理平台，并且主管理平台能够显示下级管理平台的IP地址、地理位置、在线状态、上线时间等信息（需提供产品功能界面截图） |
| 支持修改云安全管理平台的系统名称、公司名称以及页面logo等信息（需提供产品功能界面截图） |
| 支持通过云安全管理平台下载安全组件技术白皮书和用户手册等相关附件信息（提供界面截图并加盖公司公章） |
| **★资质要求** | **产品资质** | 云安全管理平台需具备中华人民共和国公安部颁发的《计算机信息系统安全专用产品销售许可证》 |
| 云安全管理平台需具备中华人民共和国国家版权局颁发的《计算机软件著作权登记证书》 |
| 云安全管理平台需具备公安部第三研究所安全防范与信息安全产品及系统检测实验室颁发的《云计算产品信息安全认证》 |
| 云安全管理平台需具备CSA云计算信息安全专业权威认证《云计算产品信息安全认证CSA CSTAR》 |
| 云安全管理平台需具备IPv6 Ready Logo认证 |
| **服务** | 原厂商五年硬件保修 |

**4.7漏洞扫描组件**

|  |  |  |
| --- | --- | --- |
| **指标** | **指标项** | **详细要求** |
| **基本要求** | 总体要求 | 支持IPv4/IPv6双协议栈地址场景漏洞扫描； |
| 支持多个系统升级包并存，系统升级包文件数量不少于3个（提供截图）； |
| 支持在WEB界面网络诊断，包含PING、TRACEROUTE、TCP、HTTP、DNS多种诊断方式（提供截图）； |
| ★支持防火墙联动功能，防火墙能根据漏扫提供的资产信息对重要资产信息进行防护，根据漏洞信息自动生成防护规则，保护内网安全（提供截图）； |
| 支持限制webui、ssh、telnet方式登陆最大并发管理数，超出限额时，处理策略可选提示不能登陆和踢掉最不活跃的用户（提供截图）； |
| 支持磁盘管理功能，能查看和搜索历史扫描收集信息，选择删除无用的数据信息，并可设置磁盘告警。（提供截图）； |
| 支持WSUS补丁服务器联动功能（提供截图）； |
| 安全性 | 产品应支持对系统配置进行备份、恢复功能，保证产品系统数据的安全性，为保障产品运行的安全及稳定性，要求产品设计、开发、生产及售后服务符合TL9000-H-S-V相关标准要求；提供第三方权威证明材料。 |
| ★规则库升级 | 默认包含3年应用特征库升级许可。 |
| **厂商** | 漏洞研究 | ★请提供设备厂商连续三年为CNVD原创漏洞报送突出贡献单位的证明；（提供证明文件）； |
| **集成技术支持** | 仪表板 | 支持首页全面展示风险分布及趋势图表，包括主机风险分布、站点风险分布、漏洞风险分布、漏洞top10、资产风险值趋势、资产风险分布趋势 |
| 系统漏洞扫描能力要求 | 支持扫描系统漏洞数量大于140000种，web漏洞数量大于2200种,数据库大于2500种，CVE漏洞数大于60000（提供截图）； |
| 产品漏洞库应涵盖目前的安全漏洞和攻击特征，漏洞库具备至少CVE、CNCVE、CNVD、BUGTRAQ、CNNVD编号； |
| 支持扫描主流操作系统、web服务器、数据库、网络主机、移动设备、应用及软件的安全漏洞（提供截图）； |
| 允许管理员配置扫描通知，在扫描任务运行开始时向被扫描的资产发送扫描通知（提供截图）； |
| 支持扫描虚拟机安全漏洞，如VMWare、EXSI、KVM、XEN、XenServer、HyperV，可扫描漏洞数量大于1500条（提供截图）； |
| 支持扫描大数据组件的安全漏洞，如Spark、Splunk、Kafka、Storm、Cassandra、Ambari、Impala、Solr、Oozie、Hbase、Hadoop等； |
| 支持网络打印机、摄像头、移动终端等设备的漏洞发现（提供截图）； |
| 支持对扫描任务进行克隆、搜索、导出、删除、查看等操作，支持断点续扫功能（提供截图）； |
| 扫描对象支持手动输入、批量文件导入及资产树导入，支持填写排除目标（提供截图）； |
| 支持配置扫描任务最大并发线程数，可根据网络空闲状态调整漏洞扫描的并发进程数量； |
| 扫描目标支持ip、域名、网段、子网的组合配置； |
| 登录扫描支持ssh、smb、snmp、esxi、mysql、db2、postgresql、mssql、ftp、imap、pop3、pop2、rsh、rexec、rlogin、smtp、telent、gbase、dmdb、oracle等类型（提供截图）； |
| 支持DB2、FTP、IMAP、MSSQL、MYSQL、Oracle、POP3、POSTGRES、RDP、Redis、RTSP、SMB、SMTP、SNMP、SSH、TELNET、TOMAT等的弱口令探测（提供截图）； |
| 端口扫描支持TCP CONNECT、TCP SYN、TCP FIN、UDP等多种方式； |
| 提供标准通用端口、快速扫描端口、全部TCP端口、指定端口四种扫描策略（提供截图）； |
| 主机存活探测支持ARP ping、ICMP ping、TCP ping、UDP ping、TCP SYN Ping、TCP ACK Ping等多种方式（提供截图）； |
| 支持对DB2、MSSQL、MySQL、Oracle、GBASE、DMDB等主流数据库进行登陆认证扫描；（提供截图） |
| 支持危险插件开关，支持扫描前提示被扫描主机； |
| Web漏洞扫描要求 | 扫描对象支持手动输入、批量文件导入及站点组导入，支持填写排除目标（提供截图）； |
| 支持站点分组管理功能，可批量导入站点信息，并支持在站点管理下针对站点组或者单个站点直接开启扫描任务； |
| 支持站点组、单站点风险在线报表和站点特有属性配置（提供截图）； |
| http认证类型支持auto、basic、digest、ntlm（提供截图）； |
| SSL认证支持输入私钥并导入软证书（提供截图）； |
| 支持认证自动登录，提供用户名密码登录、自定义表单登录、cookie登录、登录录制等功能（提供截图）； |
| 支持通过代理服务器扫描目标url，代理报文可选http、http1.0、socks4、socks4a、socks5、socks5h等多种类型（提供截图）； |
| 支持自定义路径，对有爬取限制链接进行深度扫描（提供截图）； |
| 支持排除路径名，可自定义无需爬取的URL链接（提供截图）； |
| 支持排除后缀名，可自定义无需爬取的文件后缀名（提供截图）； |
| 支持自定义http请求，包括UserAgent、http cookie、http header、超时时间、重试次数、表单输入（提供截图）； |
| 支持被动扫描功能，通过代理获取审计页面（提供截图）； |
| 爬取策略支持广度优先、深度优先，支持自定义子目录深度、最大页面数、页面最大响应长度（提供截图）； |
| 支持智能审计功能，提供智能算法对页面进行审计（提供截图）； |
| 口令猜解 | 支持DB2、FTP、IMAP、MSSQL、MYSQL、Oracle、POP3、POSTGRES、RDP、Redis、RTSP、SMB、SMTP、SNMP、SSH、TELNET、TOMAT等的弱口令探测（提供截图）； |
| 支持自定义口令猜测时间、猜测频率、猜测次数、最大并发线程数（提供截图）； |
| 支持chrome、IE、Firefox等浏览器配置核查（提供截图）； |
| 支持FW、IPS、IDS、防毒墙、ACM等安全设备配置核查（提供截图）； |
| 支持Elasticsearch、ZooKeeper、Spark、HDFS、Kafka、HBase、Hive、Sqoop、Yarn-MR、Impala等大数据组件的配置核查（提供截图）； |
| 报表能力 | 支持在线报表，可详细展示任务综述信息、站点列表、漏洞列表、对比分析及参考标准，漏洞分布支持风险等级过滤查看（提供截图）； |
| 综述报表可展示详细的任务信息，包括任务名称、类型、开始时间、任务耗时、摘要信息等（提供截图）； |
| 站点报表支持展示危险级别、站点信息、漏洞信息、外部站点，支持基于站点树展示漏洞分布及漏洞信息（提供截图）； |
| 主机报表支持展示主机风险、漏洞信息，及主机详细的端口信息、端口Banner信息、安装软件信息、操作系统类型（提供截图）； |
| 支持漏洞生命周期管理，包括未修复、确定、忽略、修复、已验证五种状态（提供截图）； |
| 支持同一任务的最近两次扫描结果对比，展示漏洞状态的变更情况（提供截图）； |
| 内置包含弱口令猜测、Web扫描、系统扫描的多类型报表模板，同时支持自定义模板（提供截图）； |
| 支持扫描任务中自动生成报表，包含html、pdf、word、excel、wps、xml等多种格式类型，可通过设置邮箱自动发送（提供截图）； |
| 报表支持综述报表及主机报表，可自定义安全结论（提供截图）； |

**4.8数据库审计组件**

|  |  |  |
| --- | --- | --- |
| **指标** | **指标项** | **详细要求** |
| **基本要求** | 审计查询 | 支持按数据库实例、数据库名、用户名、数据库表名、表字段名、操作类别、SQL语句、响应时间、连接时长、会话ID、关联规则ID、操作结果、SQL返回结果集、数据库客户端程序、数据库服务器端程序等作为查询和统计条件 |
| 报表 | 支持WORD、PDF、CVS、XLS、HTML等格式导出报表 |
| 告警 | 支持通过声光、邮件、短信等方式对审计日志、系统日志进行告警 |
| 系统部署 | 支持单点旁路、多点多级部署 |
| IPv6环境 | 支持IPv6网络环境下的数据库审计，可识别IPv6的相关主体与客体资源 |
| 操作系统 | 为保障产品运行的安全及稳定性，要求产品设计、开发、生产及售后服务符合TL9000-H-S-V相关标准要求；提供第三方权威证明材料。 |
| ★云审计功能 | 默认一个云审计代理/Agent授权；最高支持15个云审计代理/Agent授权 |
| **集成技术支持** | 数据库类型 | 支持Oracle、SQLServer、MySQL、DB2、Sybase、Informix、PostgreSQL、Teradata等数据库系统 |
| 支持Cache、Hive、Hana、clickhouse、Tibero、Solr、MongoDB、HBase、ElasticSearch、Redis等国际主流数据库系统 |
| 支持KingBase、DaMeng、Oscar、GBase、Inspur\_KDB、Highgo、GaussDB等国内主流数据库系统 |
| 主流业务协议审计 | 支持HTTP、Telnet、FTP、SMTP、IMAP、POP3的审计 |
| 主流业务协议审计查询 | HTTP协议支持按HTTP访问域、URL、请求类型、请求文件、Cookie、返回码等34个分项作为查询和统计的条件 |
| Telnet协议支持按telnet命令、返回信息等20个分项作为查询和统计的条件 |
| FTP协议支持按ftp命令、传输文件信息、ftp用户名、密码等23个分项作为查询和统计条件 |
| 邮件协议支持按邮件主题、附件、发送ip等24个分项作为查询和统计的条件 |
| 细粒度审计信息 | 系统支持详细的审计日志，审计元素包括执行人who、执行内容what、执行时间when、执行地点where、执行方式how、影响范围Range、执行结果ResultSet， |
| 数据库协议审计查询 | 支持按五元组、数据库实例、数据库名、用户名、数据库表名、表字段名、告警级别、VLANID、操作类别、SQL语句、响应时间、连接时长、会话ID、关联规则ID、操作结果、SQL返回结果集、数据库客户端程序、数据库服务器端程序等57个分项作为查询和统计条件 |
| 双向审计 | 支持数据库请求和返回的双向审计，特别是返回字段和结果集、返回码、SQL错误信息、返回行数、执行时长等内容 |
| 支持通过返回行数控制返回结果集审计大小，降低系统开销。可配置返回行数，不低于100万行 |
| 数据库自动发现 | 支持从数据库流量中自动识别数据库，从流量分析结果中自动判别包含的数据库类型、版本、地址、端口、发现时间、会话时长、总事件数等信息，并且自动添加到待监控审计列表，无需用户提供网段、数据库地址等信息。 |
| 数据库监控 | 支持依据数据库实例监控各个数据的数据库类型、活跃会话数、总会话数、负载等信息 |
| 支持依据数据库实例监控各个数据库的连接池、缓冲区、表空间、死锁、CPU、内存、硬盘等信息，可自定义告警阈值进行健康评估 |
| 支持自定义时间条件进行各个数据库的会话趋势、SQL操作趋势、安全趋势、访问源趋势的图表展示 |
| 支持自定义审计精确到秒级的流入流出总流量趋势、总体新建与并发会话数趋势、总体资源占用率趋势 |
| 弱口令扫描 | 支持数据库服务器弱口令扫描，扫描出的弱密码支持脱敏显示 |
| ~~★~~SQL操作统计 | 支持各类SQL操作数量以及占比情况（提供截图） |
| 应用流量监听 | 支持审计各个应用协议的流量大小和数据包数量，并以图表形式进行排名； |
| 支持自定义时间查看各个协议审计的流量趋势图，直观展示应用流量的监听情况 |
| 设备运行状态 | 支持首页直观展示数据库审计系统的运行情况，比如并发连接数、每秒新建连接速率、版本号、运行时间以及CPU、内存、硬盘等资源占用情况 |
| 数据库攻击行为审计 | 支持对针对数据库的 XSS 攻击行为、SQL 注入攻击行为，利用漏洞攻击等行为进行审计，并进行实时报警；（提供截图证明） |
| SQL错误统计 | 多个维度展示错误占比及趋势，从源IP维度以柱状图展示SQL错误数（TOP10） （提供截图） |
| SQL错误分析 | 以列表形式给出出错原因、出错信息以及解决办法（提供截图） |
| ★SQL效率分析 | 以饼图展示正常SQL与慢SQL占比情况、TOP10慢SQL的详细分析：TOP排名信息、事件ID、数据库名、目的ip、协议类型、源ip、sql响应时间、操作类型、具体sql语句等要素 （提供截图） |
| SQL错误知识库 | 支持不少于20000条SQL错误码，知识库至少体现SQL错误码、出错信息、出错原因、解决办法等内容； （提供截图） |
| 实名审计 | 支持以姓名、部门、域名、主机名、源MAC、邮箱、电话、数据来源等要素为条件的实名审计（提供截图） |
| 会话回放 | 支持会话回放功能,并至少支持0.5倍速、1倍速、1.5倍速、2倍速、4倍速五级播放速度调节（提供截图） |
| 翻译功能 | 实现对SQL语句报警内容自定义成中文自然语言的描述功能，便于非技术人员理解报警内容； |
| 数据查询 | 支持基于数据库[时间、源/目的IP、](file:///C%3A%5CUsers%5Czzs%5CDesktop%5C%E9%97%AB%E5%AE%8F%E6%B6%9B%5C%E6%B0%B8%E5%98%89%E5%8E%BF%E5%A4%A7%E6%95%B0%E6%8D%AE%E5%B1%80%5C%E5%A4%A9%E8%9E%8D%E4%BF%A1%E6%95%B0%E6%8D%AE%E5%BA%93%E5%AE%A1%E8%AE%A1%E7%B3%BB%E7%BB%9F%E6%8E%A7%E6%A0%87%E5%8F%82%E6%95%B0%EF%BC%88%E5%AE%8C%E6%95%B4%E7%89%88%EF%BC%89.docx#_多维度查询)数据库名、应用协议、数据库表名、字段值、预处理SQL、SQL关键词、数据库返回码、SQL响应时间、数据库操作类型、影响行数等条件的审计查询。 |
| 边查询边统计机制，页面采用异步加载技术，保障查询和统计效率 |
| 查询方式支持精确查询与模糊查询两种模式，并支持自定义保存当前查询条件，为后续查询提高便捷 |
| 复杂SQL审计能力 | 支持超长SQL语句审计，至少不低于2M |
| 支持嵌套SQL语句的审计 |
| 准确审计绑定变量的SQL语句 |
| 有效分割、准确审计主流数据库协议的多SQL语句 |
| 端口重定向 | 支持端口重定向审计，在服务器端口变化动态协商为其他端口时同样能精确审计。 |
| 阻断功能 | 支持针对源IP/端口操作的所有请求直接阻断 |
| 特殊紧急情况可阻断风险数据库的所有操作 |
| 支持与公司防火墙联动阻断功能 |
| 基线管理 | 支持基于SQL操作进行基线构建和基线管理，支持引用基线进行告警配置 |
| 业务关联审计 | 支持插件方式和非插件方式的业务关联审计，支持B/S业务系统三层关联审计，实现java web环境100%准确关联，包括但不限于Tomcat、Weblogic、Jboss服务器 |
| 白名单审计 | 支持白名单审计：系统使用审计白名单将非关注的内容进行过滤，降低了存储空间和无用信息的堆砌，白名单内容包括但不限于SQL语句、数据库类型、业务URL地址、数据库名、HTTP访问域等；  |
| 探针管理 | 对无法镜像流量的审计场景，支持多种类型操作系统的探针部署，适配的操作系统至少包括以下几种： WinSer2003/2008/2012/2016、Centos、opensuse、redhat、Ubuntu、中标麒麟SV1.2-龙芯、银河麒麟SV1.3-飞腾、银河麒麟server-飞腾等、AIX5/6（提供截图） |
| ★操作系统 | 安全操作系统采用冗余设计，可在设备命令行启动过程中选择主备系统，为保障产品研发稳定性，所投厂商具备云安全成熟度模型CS-CMMI 5认证，提供证书复印件 |
| IPv6环境 | 支持IPv6网络环境下的数据库审计，可识别IPv6的相关主体与客体资源 |
| 云检测 | 支持云检测，可对本单位部署的同一品牌的多台审计或者多类型安全设备（版本号、序列号、型号、运行时长、CPU和内存占用、并发和新建连接数、设备流量等）进行远程统一检测，保障各设备的安全稳定运行（提供截图） |
| 系统抓包 | 支持抓包工具（可配置抓包个数、源和目的IP、协议等）、系统巡检、网络诊断、规则库升级（提供截图） |
| 一键巡检 | 支持系统本身主要运行功能服务模块的运行状态巡检，保证系统安全稳定运行 |
| ★配置与策略 | 支持系统配置文件和系统策略的密文导入导出，不可设置为明文（提供截图） |
| 系统角色 | 支持本地认证、Radius、LDAP等用户认证方式，支持添加系统管理员、审计管理员、安全管理员等角色 |
| ★安全浏览器管理 | 支持红莲花、密信等安全浏览器登录管理设备，该类浏览器支持国密算法SM2/SM3/SM4，安全性非常高（提供截图） |
| 系统登录安全设置 | 支持用户密码复杂度（高、中、低）设置、最大登录失败次数设置 |
| 系统登录连接数设置 | 支持webui/ssh/telnet方式登录系统的最大连接数设置 |
| 日志外发 | 支持Syslog、SNMP、kafka等方式外发日志（提供截图） |
| 磁盘管理 | 支持手动、自动方式的磁盘清理，可根据剩余空间、保存时限等条件灵活设置，磁盘空间占用情况的检查频率可灵活设置：10min、30min、1h、3h、6h、24h等时长 （提供截图），支持存储外发。 |
| 告警方式 | 支持通过声光、邮件、短信等方式对审计日志、系统日志进行告警通知 |
| 系统部署 | 支持单点旁路、多点多级部署 |
| 高可靠性 | 支持双机热备 |
| 告警级别 | 支持告警级别划分，至少分为七类，例如：紧急、警告、一般等级别，以便运维人员作出不同响应（提供截图）  |
| 报表模板 | 支持等保、萨班斯法案报表模板以及自定义报表，可以按日、周、月等周期自动生成报表（提供截图） |
| 报表格式 | 支持WORD、PDF、CVS、XLS、HTML等格式导出报表，并可通过邮件自动发给相关人员 |

**4.9日志审计组件**

|  |  |  |
| --- | --- | --- |
| **指标** | **指标项** | **详细要求** |
| **基本要求** | 系统部署 | 支持单级部署；支持代理分布式部署采集日志； |
| 数据采集 | 支持安全设备、网络设备、中间件、服务器、数据库、操作系统、业务系统等不少于26类300种日志对象的日志数据采集；支持日志归一化处理； |
| 采集方式 | 支持Syslog、SNMP Trap、Netflow、JDBC、WMI、FTP、SFTP、SCP、文件等方式进行数据采集；支持通过Agent采集日志数据 |
| 数据存储 | 对所管理设备的日志原始数据完整存储，支持数据本地集中存储； |
| 数据查询 | 基于时间轴展示数据分布，能够通过时间轴进行查询分析； |
| 告警 | 支持首页展示当日告警情况统计；支持展示当日最新告警TOP10、TOP30和TOP50； |
| 报表 | 基于时间轴展示数据分布，能够通过时间轴进行查询分析。智能报表创建，每添加一个日志源，系统自动分析日志源类型进行相应报表创建，无需人工干预，报表和资产一一对应。 |
| ★日志源授权 | 提供≥200日志源授权 |
| **集成技术支持** | 系统性能 | 日志采集峰值：10000EPS；日志采集均值：5000EPS； |
| 数据存储能力：压缩加密存储，压缩比不低10:1；日志存储不低于10000条/M ；支持百亿级数据交互式多条件查询，百亿级数据查询响应时间小于10s； |
| 数据采集 | 支持安全设备、网络设备、中间件、服务器、数据库、操作系统、业务系统等不少于26类300种日志对象的日志数据采集； |
| 支持Syslog、SNMP Trap、Netflow、JDBC、WMI、FTP、SFTP、SCP、文件等方式进行数据采集；支持通过Agent采集日志数据； |
| 系统内置已支持设备种类清单，提供设备日志外发配置建议指导； |
| 支持日志归一化处理，将不同设备所产生的不同格式的难以理解的日志数据进行统一格式化处理，提炼出有用信息清晰、明确的展示给管理者； |
| 支持实时自动刷新每个日志源的实时日志列表，支持在实时日志界面通过选择过滤器来监视所关注的特定类型的日志； |
| 支持首页展示日志采集总量统计，可按不同日志源种类分类显示日志总量及大小，并支持导出；（提供截图） |
| 对于尚未支持的设备类型日志进行新增采集支持，在页面上传升级文件或增加配置文件即可；支持主动、被动相结合的数据采集方式； |
| ★支持独立展示每个被采集源最近24小时的日志数量趋势，便于掌握设备的安全事件情况，支持独立展示每个设备日志的最新采集时间，便于了解设备日志的采集状态；（提供截图） |
| 支持对日志流量非常大但是日志重要程度低的syslog类型日志源进行限制接收速率，降低对系统资源的占用，保障重要日志的收集；  |
| ★支持对文本类型日志源进行限速采集，匀速采集日志，防止对系统资源产生突发冲击；（提供截图） |
| 支持对每个日志源设置过滤条件规则，自动过滤无用日志； |
| 支持日志转发给第三方系统平台，支持设置多个日志转发IP地址，支持转发格式化日志或仅转发原始日志； |
| 数据存储 | 支持对所管理设备的日志原始数据完整存储，支持数据本地集中存储、网络存储； |
| 支持根据设备重要程度设置独立设置每个被采集源的日志、报表数据存储时间为1个月、3个月、6个月和永久保存等参数；（提供截图） |
| 支持存储空间图像化、动态监控，超过阀值进行告警。支持从存储空间、存储时间多维度进行动态监控； |
| 支持日志备份功能，支持本地备份和FTP备份方式，支持自动备份和手动备份。 |
| 数据查询 | 支持首页以全国地图、全球地图展示最近24小时日志访问源和访问目的的分布，能根据颜色区分访问来源和访问目的数据量大小，能够通过首页地图快速下钻查询指定区域的日志详细信息；（提供截图） |
| 支持实时日志查询，支持历史备份文件导入查询；支持等于、不等于、大于、小于、正则表达式等查询条件；支持多条件组合查询； |
| ★支持为不同类型日志设置不同的查询条件和显示条件；（提供截图） |
| 支持原始日志全文检索； |
| 支持在查询结果页面上直接下钻二次查询，快速定位关键日志，还可以返回上次查询条件；查询结果可将归一化日志和原始日志同屏对比显示； |
| 支持展示日志查询情况，包括查询条件命中数、日志总量、查询耗时等信息； |
| 查询结果支持分页显示；支持查询结果格式化日志、原始日志导出； |
| ★支持在日志查询结果上针对源IP、目的IP、操作、源端口、目的端口等字段一键快速统计，以饼图方式展示，对于源IP和目的IP（公网地址）还支持以中国地图、世界地图方式展示，在统计图上能够进行点击下钻查询对应条件的日志结果； |
| 支持查询结果快速统计，可自定义统计主题规则，支持将多个主题添加为一个统计任务，以分、时、周、月、年定时执行自动统计，将统计结果报表发送到指定邮箱； |
| ★支持基于时间轴展示日志数据分布，能够通过时间轴进行查询分析； |
| 告警管理 | 支持首页展示当日告警情况统计；支持展示当日最新告警TOP10、TOP30和TOP50；（提供截图） |
| 内置系统运行相关告警规则，包括检测到新日志源、节点掉线、主动日志源长期不外发日志、存储上限告警、主机认证失败等，可启用/禁用规则； |
| 支持安全告警概况、安全告警趋势的统一展示，实时告警可根据级别、规则类型等进行分类；  |
| 支持实时告警展示，可根据告警规则、告警级别两个维度进行实时告警监视，并可对刷新事件间隔进行设定； |
| 支持根据告警级别、告警规则类型、规则名称、时间范围、事件名称、设备IP、源IP、目的IP等方式快速检索安全事件告警，检索结果支持Excel等格式导出；（提供截图） |
| ★支持基于时间轴展示告警数据分布，能够通过时间轴进行查询分析；（提供截图） |
| 支持在告警事件查询界面直接显示触发告警的关联日志，也支持点击跳转到日志查询界面。 |
| 支持告警抑制规则设定，防止报警信息短时间内大量发送。 |
| 告警响应方式 | 支持邮件、Snmp Trap、声音、声光、短信、一信通响应、数据库响应等多种告警方式，支持报警内容引用字段变量参数。 |
| 统计报表管理 | ★系统内置上百种报表模版，支持自动实现智能报表创建，每添加一个日志源，系统自动分析日志源类型进行相应报表创建，无需人工干预，报表和资产一一对应；（提供截图） |
| 报表支持基于全国地图、全球地图进行访问源、访问目的追踪。 |
| 支持自定义统计日志数据形成报表，支持统计分析报表以PDF、word、execl、html等方式导出；支持实时报表、计划报表。 |
| 日志源管理 | 支持手动添加日志源，管理员可以对日志源进行查看、批量修改、添加、编辑、删除以及启\禁用的操作； |
| 支持对重点日志源的关注设置，并可通过关注列表快速查看重点日志源的状态、当日日志量、采集日志总量、最近接收时间、业务组等基础信息； |
| 支持按照日志源名称、IP地址、日志源类型、接受时间及状态等维度对日志源列表进行排序；支持为日志源指定类型、名称、IP地址、收集节点、收集方式、以及日志源启停状态等属性信息； |
| 支持日志源在线状态监测告警，实时监测日志源的可用性，可显示每个日志源采集日志的最近时间，实时展示每个日志源最近一天日志趋势变化； |
| 支持以业务角度将日志源进行分组，支持在日志查询时以业务组进行查询，支持在首页拓扑展示时以业务组进行展示； |
| ★支持基于拓扑图的日志源相关数据信息快速查看；支持通过拓扑下钻查看对应日志源的日志、报表、告警数据。（提供截图） |
| 系统管理 | 支持用户按角色管理，支持三权分立； |
| 支持将日志源管理权限分配给不同的操作管理员，不同用户管理不同日志源的日志，互不干扰； |
| 支持设置非法用户访问控制策略；系统具有防恶意暴力破解账号与口令功能，口令错误次数可设置，超过错误次数锁定，锁定时间可设置。 |
| 支持将常用IP地址或IP地址网段标记为自定义名称，在日志查询界面可以在IP列中对应悬浮显示自定义名称； |
| 支持系统肤色设置，可根据喜好对系统主题颜色进行红色、蓝色切换。 |

**4.10堡垒机组件**

|  |  |  |
| --- | --- | --- |
| **指标** | **指标项** | **详细要求** |
| **部署方式** | 工作模式/高可用 | 采用物理旁路部署，不改变现有网络结构；支持双机部署，保证系统发生故障时的可用性；支持自建集群部署：支持无缝横向扩展，轻松应对高并发需求；为保障产品运行的安全及稳定性，要求产品设计、开发、生产及售后服务符合TL9000-H-S-V相关标准要求；提供第三方权威证明材料。 |
| ★**基本要求** | 资源授权 | 提供≥200资源授权，用户数不限制；支持后续扩展 |
| **集成技术支持** | 用户管理 | 支持用户的增删改查、锁定、激活，进行用户全生命周期管理，支持用户批量导入和导出；支持用户清理功能 |
| 角色管理 | 支持系统管理员、保密管理员、密码管理员、安全审计员、保密员、运维管理员、操作员七种角色，同时也可按需分配角色权限，权限间相互制约； |
| 认证管理 | 支持本地认证和三方认证服务器接入认证，如AD、LDAP、Radius服务器； |
| 支持密码认证、证书认证、USBKEY认证、人脸识别等双因素认证方式； |
| 证书管理 | ★支持第三方证书用户自行上传用作校验的CA证书和CRL列表；本地CA支持根证书的重新生成及替换；支持根据根证书签发出客户端证书；支持发布生成吊销列表；支持国密证书认证。（提供截图） |
| 用户分组 | 归属层级化部门分组管理；用户组与部门关联，支持部门隔离；支持授权和规则配置用户组； |
| 消息管理（公告） | ★支持管理员通过发布公告的形式，发送通知给所有指定用户；（提供截图） |
| 认证服务器同步 | 支持通过AD域服务器和LDAP服务器进行用户同步； |
| 资产管理 | 支持混合云资源的管理，即公有云及局域网资源，支持主机、服务器、网络设备、安全设备、数据库等的资产管理；满足公有云、云资源池、数据中心多种运维场景； |
| 支持首页动态展现资源总量、活动用户、实时会话、待审批工单、当日运维记录、资产运行状态、今日运维总数、今日运维时长TOP10、今日告警总数、今日运维指令TOP10等信息，方便管理员实时查看系统运行情况掌握资产会话连接情况。 |
| 支持资源分类和资源系统类型管理：内置常见资源分类和资源系统类型，可自定义添加资源分类、资源系统类型和资源服务类型； |
| 自动发现 | 公有云设备支持一键更新发现功能；支持自动扫描网段内主机并支持导入系统（提供截图） |
| 云同步 | 支持华为云、阿里云、腾讯云主机同步功能； |
| 资产组管理 | 支持资产组的增删改查； |
| 收藏夹 | 支持运维清单收藏夹功能，可将常用运维资产添加至收藏夹，便于运维。 |
| 资源导入导出 | 支持资源（包括服务和资源账号）批量导入导出功能； |
| 批量运维 | 支持创建不同资产，不同协议的批量运维登录 |
| 特权切换 | 支持以普通管理模式登录网络设备或主机并自动切换到特权模式。 |
| 应用编排 | 支持应用编排，应用发布运维除了内置标准客户端，可自定义其他类型客户端进行运维，如VMware等 |
| Session导出 | 支持Xshell、Xftp、SecureCRT客户端的session文件导出 |
| 账号抽取和推送 | 支持将堡垒机中的账号推送到服务器，或者是直接将服务器中的账号抽取到堡垒机，不用再手动建立。 |
| 密码托管 | 支持对已添加的设备账号进行密码托管，从而实现单点登录功能； |
| 账号改密 | 自动对数据库、Windows、Linux等设备进行账号改密，改密支持手动和定期任务，密码配置支持全局策略和手工指定，密码复杂度支持按策略随机生成； |
| ★支持改密结果自动发送到制定改密计划的管理员邮箱；密码采用密码信封加密保存，以保证安全性；支持密码分段发送。（提供截图） |
| 密钥登录 | 支持字符类协议可通过ssh密钥的方式登录服务器。 |
| 批量操作 | 支持账号批量修改、删除等操作； |
| 登录方式 | 支持自动、半自动、手动三种登录方式； |
| 账号稽查 | ★支持账号稽查功能，报表可生成孤儿账号、幽灵账号和僵尸账号（提供截图） |
| 授权管理 | 支持按照用户、用户组、资产、资产组、管理协议、资产账号进行一对一、一对多、多对一、多对多授权； |
| 运维策略 | 支持会话、指令、剪切板上下行、文件上传下载的约束行为； |
| 登录策略 | 支持对用户/IP/mac地址/登录时间进行控制； |
| 运维工单 | 支持内置工单运维，操作员可根据工作需求临时申请设备运维工单，管理员审批后可直接运维，过期失效； |
| 授权关系 | ★提供授权关系查看功能，图形化直观展示用户、资产、协议、账号的授权关系；（提供截图） |
| 访问策略 | 支持对运维时间、运维地址、运维操作指令、操作行为的限定，触发策略后进行告警、再审、阻断等； |
| 组管理 | 支持地址、时间、指令单独组配置，进行批量管理； |
| 单点登录 | 支持访问SSH、RDP、Telnet、FTP、SFTP、VNC、数据库等资产；支持无须记忆多个设备账号和密码，实现账号密码代填功能；支持自动、半自动、手动三种登录方式；支持进行协议/工具扩展； |
| 页面调用客户端 | 支持通过web页面调用SecureCRT、XShell、putty工具单点登录。（提供截图） |
| Html5技术 | 设备访问支持最新的html5技术，在同一WEB窗口页签中，无需JAVA应用插件或调用本地应用客户端，即可实现对目标设备的快速运维；（提供截图） |
| c/s运维 | 支持SecureCRT、XShell、WinSCP、Mac Terminal等客户端直接连接堡垒机进行代理运维目标资产； |
| 会话分享 | 支持会话请求远程协助，且协同会话保持实时同步； |
| 国际化 | 支持国际化，支持界面切换中英文显示。 |
| 临时运维 | 支持临时运维功能，管理员可针某些用户开启临时运维功能，操作员在管理员未添加资产并授权时，时间紧急情况下，可临时运维。 |
| 操作审计 | 支持对用户和管理员的认证登录、操作和配置管理进行日志记录；支持改密任务的审计记录； |
| 图形协议审计 | ★图像审计采用OCR图像识别技术，通过加载训练过的运维图片集合，可以识别图形操作中的快捷方式标题、窗口内容中的文本信息；（提供截图） |
| 行为追溯 | ★支持追溯功能，支持运维追溯查询和改密追溯查询。（提供截图） |
| 字符文件传输协议审计 | 支持字符协议SSH、TELNET和文件传输协议FTP、SFTP的协议审计，审计详细的操作指令及操作录像，同时可根据每条指令快速定位其操作录像；支持通过应用发布实现字符协议和文件传输协议的命令级审计；和图形审计的双重审计效果，命令级审计便于重现真实的完整操作命令，图形审计便于直观的查看到真实的操作行为，并支持通过搜索操作语句或执行结果中关键字定位审计回放； |
| 数据库审计 | 支持通过应用发布实现数据库操作的命令级审计和图形审计的双重审计效果； |
| 全文检索 | ★支持全文审计检索。可以对操作行为中的用户信息、资产信息、管理地址信息、管理方式信息、操作命令信息、操作结果信息进行全文检索、过滤，极大提高查询效率，更方便的进行用户关联追溯。（提供截图） |
| 视频回放 | 操作过程的录像回放时，支持暂停，支持设置播放速度，支持过滤静止，方便录像的查看；WEB在线视频回放方式重现维护人员对服务器的所有操作过程。离线回放重现维护人员对服务器的所有操作过程（回放文件下载到本地播放）； |
| 会话、指令关联 | 优化会话审计功能，可通过会话操作记录直接定位到指令，也可通过指令直接定位到审计会话，且字符型运维记录下载shell格式指令。 |
| 监控告警 | 支持对在线会话的实时监控和即时阻断，避免违规操作；支持对目标设备自身健康状况进行监控及告警行为； |
| 审计报表 | 报表针从会话、指令等多个维度进行统计；系统内置丰富报表统计模板：协议运维排名、资产运维次数top10、资产运维趋势top10、用户运维趋势top10、协议运维趋势、用户运维次数top10、指令分布top10、top10指令资产分布、指令用户分布top10、指令资产账号分布、指令排名、指令趋势、风险指令次数、风险指令top10等多种类型报表模板。报表功能支持自定义审计查询条件，包括：时间范围、用户、资源、资源账号、IP、关键字等条件；报表导出格式支持Excel、PDF、HTML；支持邮件和FTP两种外发方式；支持报表统计历史记录； |
| 自动改密 | 自动对Windows、Linux等设备进行账号改密，可设定周期性改密； |
| 自动化运维 | ★支持自动执行运维脚本。运维脚本分为内置和自定义两种。支持脚本类型为sh和exp、py、c语言四种；（提供截图） |
| 部门管理 | 最大支持24个层级级部门分权功能，本部门的运维管理员只能查看、管理本部门的用户和设备；（提供截图） |
| 安全管理 | 支持HTTPS方式和Console方式进行管理； |
| 支持管理口与业务口分离； |
| 虚拟化 | 支持对堡垒机虚拟为多台逻辑堡垒机，虚拟堡垒机之间实现独立配置、独立数据。实现IT资源的动态分配、灵活调度、跨域共享，提高IT资源利用率。 |
| 内置VPN | ★支持SSLVPN功能，可内置VPN功能，实现数据的加密传输。（提供截图） |
| 日志管理 | 支持将本机日志、告警日志通过SYSLOG、邮箱等进行外发和告警； |
| 数据维护 | 支持配置数据和审计数据的备份、自动清理，支持备份数据通过FTP方式远程备份；支持磁盘映射手动/自动清理； |
| 时间同步 | 支持配置时间同步服务器，进行时间自动校对，保障审计的有效性和准确性； |
| 网络诊断 | 支持使用ping、transroute工具、tcp端口进行连接测试； |
| WEB界面 | 支持通过WEB升级系统版本、重启系统、关机； |

**4.11自适应安全防护**

|  |  |  |
| --- | --- | --- |
| **指标** | **指标项** | **详细要求** |
| ★基本要求 | Agent要求 | 采用进程级别安全探针，不对运行的业务应用进行代码注入，对java、PHP、JAVASCRIPT、JAVA、CG、.Net语言的web应用提供安全防护，所投厂商具备云安全成熟度模型CS-CMMI 5认证，提供证书复印件 |
| 支持主流windows、linux操作系统，以及中标麒麟、银河麒麟等国产操作系统。兼容各大云平台，为保障产品运行的安全及稳定性，要求产品设计、开发、生产及售后服务符合TL9000-H-S-V相关标准要求；提供第三方权威证明材料。 |
| 授权要求 | 300个服务器功能授权。包括但不限于winserver、中标麒麟、银河麒麟及各版本linux操作系统， 针对服务器操作系统进行病毒查杀，提供主动防御系统防护等功能。系统默认支持LinuxServer，含三年升级服务。 |
| 集成技术支持 | 多维度展示 | 具备直观的首页展示页面，至少包含主机资产、全网风险趋势、风险主机与风险排行，其中主机资产信息至少包含账号、端口、进程、数据库、容器的数量。 |
| 资产发现 | 采用多种探查方法，如包括“ARP 缓存分析”、“Ping 扫描”、“Nmap 扫描”，自动排除网络设备，主动发现网络环境中已安装安全探针的主机和未安装安全探针的主机的信息，包含IP地址、MAC地址、操作系统、安装状况、最近扫描方式等，支持以模板xlsx格式手动导入资产。 |
| 基本信息采集 | 支持采集主机的基本信息，包含主机名、IP、连接IP、MAC地址、系统安装时间、操作系统；Agent在线情况、Agent版本、Agent规则库、Agent上线时间、Agent安装时间、Agent ID；支持设置部门、使用人、类型、物理位置与标签。可以对单个主机进行资产预览，包含账户、端口、进程、软件、数据库、容器、web服务、web应用、web框架，关联风险与威胁。（提供截图） |
| ★进程信息采集 | 支持采集主机上的进程信息，包含进程名、进程ID、父进程ID、内存使用量、进程命令、启动时间、运行用户、所属用户组、软件包、状态信息。（提供截图） |
| ★账号信息采集 | 支持采集主机上的账号信息，包含采集账号名、账号状态、账号类型、最近登录时间、账号主目录、UID、GID、登录方式、sudo权限、shell、密码状态信息（提供截图） |
| web服务采集 | 支持采集主机上的Web服务，包含服务名、版本、启动用户、二进制路径、安装路径、配置文件路径。（提供截图） |
| Web站点采集 | 支持采集主机上的Web站点，包含域名、站点标题、服务类型、站点端口、端口访问性、协议、运行用户、主目录、主目录所有者、拥有者权限、启动的命令参数。 |
| Web应用采集 | 支持采集主机上的Web应用，包含应用名、版本、站点域名。（提供截图） |
| Web框架采集 | 支持采集主机上的Web框架，包含框架名、框架语言、框架版本。（提供截图） |
| 数据库信息采集 | 支持采集主机上的数据库信息，包含数据库名、版本、监听端口、协议、运行用户、绑定IP、配置文件路径、日志文件路径、数据路径。 |
| 端口信息采集 | 支持采集主机上的端口信息，包含端口、访问性、绑定IP、协议、进程名、进程路径、进程ID、状态、运行用户、所属用户组、进程启动时间、启动参数。（提供截图） |
| 容器信息采集 | 支持采集运行容器与容器镜像，包含运行容器的ID、镜像、命令、创建时间、状态、端口、容器名；包含容器镜像的仓库、标签、镜像ID、创建时间、大小。（提供截图） |
| 资产双维度查看 | 操作系统、硬件信息、软件信息、账号信息、端口信息、进程信息、启动项、内核模块、数据库、web服务、web站点、web应用、web框架、容器等资产支持从资产、主机维度进行统计，通过资产统计相关的主机数量，通过主机统计相关资产。（提供截图） |
| 系统漏洞检测 | 支持对主流windows系统、linux系统进行漏洞检测，对漏洞进行分析，支持打补丁。 |
| 中间件漏洞检测 | 支持检测中间件漏洞，包括但不限于Apache、IIS6、IIS7、IIS8、IIS10、JBoss、Nginx、Tomcat、Weblogic、Websphere。 |
| 数据库漏洞检测 | 支持检测数据库漏洞，包括但不限于MSSQL，Oracle、Sybase、Informix、DB2、MySQL、Redis、Mongodb。 |
| 弱口令检测 | 支持检测操作系统弱口令、数据库弱口令、应用弱口令，应包括：SSH、RDP、MySQL、FTP等。 |
| 支持管理密码字典，支持自定义简单密码，支持设置通过前缀密码、连接符、后缀密码等特征组合进行密码检测的字典。 |
| 支持配置白名单规则，按照应用、账号、账号状态、密码类型加入白名单。 |
| 支持对弱密码隐藏密码值、明文查看密码值以及查看弱密码修复详情。 |
| 异常账号 | 对高权限账号、空密码账号、用户名和密码相同的账号、可sudo账号、是否限制su成root帐号进行检测识别，对危险程度进行评级，提供忽略、信任处置动作。 |
| ★病毒查杀 | 具备对蠕虫、木马、内核后门等流行病毒的实时监测能力，需包含类型、病毒名称、病毒ID，通过集中管理平台对病毒进行处理与溯源。 |
| 具备快速扫描、全盘扫描、自定义扫描方式，支持设置扫描是否自动处理，提升病毒处置效率；（提供截图） |
| 具备威胁行为、主机双维度入侵分析能力，按照不同病毒ID统计未处理主机与相关主机；按照不同主机IP统计未处理病毒数量与病毒总数。 |
| 暴力破解 | 对暴力破解行为进行实时检测，根据SSHD、FTP服务类型进行停封，支持设置攻击检测周期、攻击次数阈值与处理方式（包含仅记录和记录自动停封）。 |
| 按照服务类型、IP地址设置白名单和黑名单。（提供截图） |
| 具备威胁行为、主机双维度的入侵分析能力，按照暴力破解使用的服务统计相关主机；按照不同主机统计未封停的次数与暴力破解记录。（提供截图） |
| 异常登录 | 按照异常IP、异常区域、异常时间、异常账号对异常登录行为进行实时检测，展示威胁事件详情，包含主机IP、登录区域、登录账号、来源、登录时间、异常类型等。（提供截图） |
| 具备威胁行为、主机双维度的入侵分析能力，按照异常登录类型统计相关主机数量；按照不同主机IP统计异常登录次数。 |
| Webshell后门 | 对ASP、ASPX、PHP、JSP等 Webshell后门进行实时检测，展示威胁事件详情。（提供截图） |
| 具备快速扫描、全盘扫描、自定义扫描方式，支持设置扫描是否自动处理，提升后门处置效率。 |
| 策略支持 | 通过源/目的地址、端口、协议（TCP、UDP、ICMP、IGMP、GGP、PUP、IDP、ND、ESP、AH、RDP、GRE、SKIP、RAW）、流量方向等维度配置放行、阻止等访问控制规则；（提供截图） |
| 策略配置与查看 | 支持配置多条微隔离策略，可根据需求进行启用或禁用，并且支持通过生效状态、策略名称、协议等维度进行筛选搜索； |
| 策略下发 | 支持通过调整微隔离策略顺序调整生效的优先级；微隔离策略支持按照主机/主机组/IP组进行配置下发。 |
| ★基线支持 | 支持CIS、等保2.0合规基线检查标准，并且能够定制扩展合规基线检查标准。 |
| 操作系统基线检测 | 支持操作系统（包括A但不限于BC-Linux、Suse、CentOS、RedHat等）的基线检测。 |
| 中间件基线检测 | 支持中间件（包括但不限于Apache、Nginx、Tomcat、Weblogic等）的基线检测。 |
| ★安全态势分析 | 具备安全态势大屏，对整体主机威胁态势进行分析，包含主机在线情况、全网风险趋势、资产清点、病毒、Webshell、弱口令、暴力破解、风险主机、告警动态。（提供截图） |
| 资质要求 | 软著 | 计算机软件著作权登记证书 |

**注：防火墙、态势感知为此次采购核心设备。**

**五、人员及服务要求**

1、★所有设备如需植入或有针对服务器或终端的，均要求支持信创服务器、信创电脑终端、信创中间件、信创数据库等；

2、★所有设备的操作界面应支持信创电脑终端；

3、★投标人需承诺支持态势感知产品与市级态势感知同类产品数据对接；

4、★投标人应按甲方要求在电子政务外网环境内完成所投设备的安装、调试等集成服务；

5、★投标人需承诺提供至少1人驻点永嘉协助公共数据一体化平台运维工作开展。

注：支持国产信创设备为强制要求。

**六、付款方式：**

**在合同签订后乙方提供合同总金额5%的履约保证金；**

1、合同签订后15个工作日内,甲方向乙方支付合同总额的30%（具体预付约定落实需以预付当月永嘉县财政库款情况为前提）；

2、该项目经相关部门初步验收合格，自正式上线试运行之日起15个工作日内，甲方向乙方支付合同总额的60%；

3、该项目通过最终验收后15个工作日内，甲方向乙方支付剩余合同总额的10%，同时项目进入免费维护期。

**履约保证金转为系统免费维护保证金，在硬件五年免费维护期到期后十个工作日内向中标人一次性无息退还。**

注：根据《浙江省财政厅关于坚决打赢疫情防控阻击战进一步做好政府采购资金支持企业发展工作的通知》（浙财采监〔2020〕3号）及《永嘉县财政局关于做好政府采购相关工作应对新冠肺炎疫情支持中小企业共渡难关的通知》（永财采监〔2020〕47号），双方协商决定付款比例，具体每笔款项支付视财政部门资金拨付情况而定。

**七、实施要求**

1、项目进度要求

**本项目由中标方负责的设备集成、调试、测试到上线试运行自合同签订起不得超过60天。**投标人必须响应并承诺上述要求，并在投标文件中编制具体的施工组织设计和详细时间进度表。

2、项目实施、检验、验收要求

验收时必须提供本项目所有的软件系统、接口清单并按本项目技术文件、合同、承诺等要求进行验收。

（1）要求编写完整、可行的系统实施方案，包括但不限于项目管理、服务承诺、系统设计、系统开发、系统测试等方案。

（2）要求完成项目实施、测试及系统切换工作，并阐述系统的项目实施方案及进度、测试方案。

（3）要求中标方提供本项目中所有交付物清单（包括项目文档、用户手册和系统管理手册等），所有通信协议和标准规范必须完全向永嘉县大数据管理中心开放并整理成册提交，作为系统验收依据。

3、项目技术团队要求

承建本项目的技术团队应具有丰富的开发经验和明确的责任分工，投标人须提供承建本项目技术团队详细的成员名单和各自所承担过的项目经历的实证。中标方的技术团队项目主管须具有丰富的项目开发管理经验。在本项目实施过程中（正式验收前），承担项目的技术团队应保持稳定连续，各成员未经采购方书面同意不得随意进行调换和减少。

**八、售后服务与技术支持**

在本项目验收后，中标方须及时向采购方提供必要的软件运行和开发、升级的技术支持。

1、中标方应保证提供不少于硬件五年、软件**三年**的质保期，包括软件质保及技术服务。质保期从项目验收之日算起。在质量保证期内，中标方应免费负责对运行中出现的故障进行处理。每年进行现场售后服务不少于二次，每季度提供定期系统、软件检查，保证运行稳定。质量保证期内中标单位未能按要求提供服务的，采购方有权没收质量保证金作为处罚。

2、中标方应根据本技术文件要求、合同、承诺规定，在质量保证期内免费提供软件升级服务。中标方应根据要求和待升级软件的特点，提供现场或其它方式的升级服务。免费维护期满后，凡不涉及软件系统调整的，中标方能电话或远程网络解决的技术服务均免收取服务费用。

3、在质保期满以后，投标人应提供成本价售后服务（含升级费用），在接用户通知后投标人应在24小时内响应。

4、投标人应在投标书中明确说明有效期后的升级服务方式和费用情况，供采购方参考。

**九、文档要求**

电子文档是项目不可分割的部分，要求提供如下文档：

1、项目实施期间：需求规格说明书、系统概要设计、项目实施过程中衍生的其它相关资料；

2、项目实施后：系统试运行和测试报告、故障诊断与排除手册、系统安装包等；

3、培训期间：培训计划、用户使用手册、管理员使用手册、安装部署手册、运维手册；

4、其他需要提交的材料。

**十、其他要求**

1、 如招标文件中遗漏了必须具备的系统或模块，请投标人在投标文件中指出，并提出解决方案供采购人、采购机构参考；中标人有义务保证采购人系统的完整性，如项目实施过程中因缺少模块或组件导致采购人系统无法正常运行，中标人须承诺免费提供。

2、 投标人须保证所提供产品具有合法的版权或使用权，本项目采购的产品，如在本项目范围内使用过程中出现版权或使用权纠纷，应由中标人负责，采购人不承担任何责任。

第三部分 供应商须知

**一、说明**

1、本次采购工作是按照《中华人民共和国政府采购法》、《政府采购货物和服务招标投标管理办法》及相关法律规章组织和实施。

2、供应商必须对全部内容进行投标报价，只对部分内容进行投标报价的供应商将按无效投标处理。

3、无论投标过程中的作法和结果如何，供应商自行承担投标活动中所发生的全部费用。采购人有权选择中标供应商的服务范围。

4、本次采购采用商务投标文件与技术资信文件分别评审，评标委员会首先评审供应商技术资信部分，技术资信部分无效的供应商不进入商务报价评审。

5、供应商须自行现场勘察，确认采购人的实际需求，取得准确的报价依据。如果认为招标文件描述或所列范围、面积与实际情况有较大出入，请在规定的招标质疑截止时间前列出详细的异议意见和数据向采购代理机构书面反映，逾期不得再对招标文件的条款提出质疑，视为接受招标文件，投标供应商中标后不得以各种理由提出增价要求，否则做投标违约处理，采购人有权取消其中标资格。

6、**本项目采购预算见采购公告。**

7、投标供应商认为为完成本招标文件规定的项目承包内容所发生的直接成本、间接成本、利润、税金、政策性文件规定的费用等一切费用均应计入投标报价，凡未列入的将被认为均已包含在投标报价中，今后不得以任何理由追加或调整。

8、**供应商如果报名后不来参与本次投标要在投标截止前3天给予书面告知及其理由。**

9、本项目对符合财政扶持政策的中小企业（小型、微型）、监狱企业、残疾人福利性单位给予价格优惠扶持，执行节能产品政府强制采购和优先采购政策，执行环境标志产品政府优先采购政策；

10、根据浙江省财政厅《关于坚决打赢疫情防控狙击战进一步做好政府采购资金支持企业发展工作的通知》（浙财采监〔2020〕3号）和永嘉县财政局《关于做好政府采购相关工作应对新冠肺炎疫情支持中小企业共渡难关的通知》（永财采监〔2020〕47号）文件精神，永嘉县财政局积极协同永嘉县相关金融机构，加快推广政采贷、履约保函等政府采购金融服务。各中标供应商可直接在政采云上申请政采贷也可以通过线下申请政采贷活动，永嘉县域内金融机构政采贷服务业务介绍详见采购公告“政采贷融资”，如有需要可直接联系。

11、投标人代表指全权代表投标人参加投标活动并签署投标文件的人。如果投标人代表是法定代表人（负责人）的，仅须提供身份证扫描件；如果投标人代表不是法定代表人（负责人），须持有《法定代表人（负责人）授权书》。

12、中标供应商必须是已申请加入浙江省政府采购供应商库的，未申请加入的请到浙江省政府采购网申请加入：<http://www.zjzfcg.gov.cn/new/zytz/257927.html> 。

13、采用最低评标价法的采购项目，提供相同品牌产品的不同投标供应商参加同一合同项下投标的，以其中通过资格审查、符合性审查且报价最低的参加评标；报价相同的，采取随机抽取方式确定，其他投标无效。

使用综合评分法的采购项目，提供相同品牌产品且通过资格审查、符合性审查的不同投标供应商参加同一合同项下投标的，按一家投标供应商计算，评审后得分最高的同品牌投标供应商获得中标人推荐资格；评审得分相同的，采取随机抽取方式确定，其他同品牌投标供应商不作为中标候选人。

非单一产品采购项目，防火墙、态势感知认定为核心产品， 多家投标人提供的核心产品品牌相同的，按前两款规定处理。

**二、供应商资格条件**

按招标公告要求。

**三、招标文件**

1、招标文件

1.1、招标文件约束力

▲**供应商一旦获取了本招标文件并参加投标，即被认为接受了本招标文件中所有条款和规定。**

1.2、招标文件的组成

招标文件由招标文件总目录所列内容及补充资料等组成。

2、招标文件的澄清

供应商对招标文件如有质疑或需要澄清，以书面形式或在政采云（在线询问和质疑系统）中向采购人、采购代理机构提出，但通知不得迟于规定的质疑时间前使采购代理机构收到，采购代理机构将用书面形式予以答复。如有必要，可将不说明来源的答复书面发给各有关供应商并予以公告。**任何口头答复均不作为投标依据。**

3、招标文件的修改

3.1、在投标截止时间前，采购人有权澄清或者修改招标文件，并以书面形式（补充、更正文件）通知供应商。补充、更正文件作为招标文件的组成部分，对所有投标供应商均有约束力。

3.2、澄清或者修改的内容可能影响投标文件编制的，采购人或者采购代理机构在投标截止时间至少15日前，以书面形式通知所有获取招标文件的潜在投标供应商；不足15日的，采购人或者采购代理机构顺延提交投标文件的截止时间。

3.3、补充、更正文件在浙江政府采购网（http://www.zjzfcg.gov.cn/）予以公告公布。**供应商须在开标前一日自行查看是否有补充更正文件，并按补充更正文件要求磋商响应，否则责任自负。**

**四、投标文件**

1、投标文件

1.1供应商提交的投标文件以及供应商与采购人就有关投标的所有来往函电均应使用中文。供应商可以提交用其它语言印制的资料，但必须译成中文，在有差异和矛盾时以中文为准。

1.2供应商提交的投标文件报价均采用人民币报价。

1.3供应商应仔细阅读招标文件中的所有内容，按照招标文件及招标要求，详细编制投标文件。并对招标文件的要求做出实质上响应。实质上响应的投标应该是与招标文件要求的条款没有重大偏离的投标。未实质上响应的投标文件将被拒绝，但允许在基本满足招标技术要求的前提下出现的微小差异。

1.4供应商必须按招标文件的要求提供相关技术参数、资料，包括采用的计量单位，并保证投标文件的正确性和真实性。投标文件全部内容应保持一致，否则可能导致不利于其投标的评定甚至被拒绝。技术和商务如有偏离均应填写偏离表。

1.5供应商应仔细阅读招标文件中的所有内容，按照招标文件要求，详细编制投标文件，所有文件资料必须是针对本次投标。不按招标文件的要求提供的投标文件可能导致被拒绝。

2、投标文件的组成

**投标文件由资格证明文件、报价文件部分和技术资信部分三部分组成。**

**2.1、资格证明文件部分组成**

|  |  |
| --- | --- |
| **序号** | **内容** |
| 1 | 投标供应商的营业执照（或事业法人登记证书或其它工商等登记证明材料）、税务登记证（如为多证合一仅需提供营业执照（或事业法人登记证书或其它工商等登记证明材料），扫描件加盖公章） |
| 2 | 投标供应商最近一年度的资产负债表、损益表或利润表(新成立的公司，必须提供情况说明） |
| 3 | 具有履行合同所必需的设备和专业技术能力的承诺函（附件一） |
| 4 | 依法缴纳税收和社会保障资金的承诺函（附件二） |
| 5 | 参加政府采购活动前3年内（新成立不满三年的组织机构自成立之日起算）在经营活动中没有重大违法记录的声明函（附件三） |
| 6 | 投标供应商特定资格条件证明：无。 |
| 7 | 投标供应商“信用中国”(www.creditchina.gov.cn)；“中国政府采购网”（www.ccgp.gov.cn）信用记录查询网页截图（采购公告发布之日至响应文件递交截止时间前） |
| 8 | 与参加本次项目同一合同项下政府采购活动的其他供应商不存在单位负责人为同一人或者直接控股、管理关系的承诺函（附件四） |
| 9 | 投标供应商参与政府采购活动投标资格声明函（附件五） |
| 10 | 供应商法定代表人（负责人）授权书（附件六） |

**2.2、报价文件部分组成**

|  |  |
| --- | --- |
| **序号** | **内容（▲报价一览表、分项报价表（若有）供应商必须提供，否则不能通过符合性审查的，责任自负）** |
| **1** | **报价一览表（附件七）** |
| **2** | **分项报价表（附件八）** |
| 3 | 享受小微企业（含监狱企业、残疾人福利性单位）价格折扣须按供应商单位性质提供以下相关的证明材料：（1）《中小企业声明函》（原件，加盖供应商公章，格式见招标文件第四部分）（2）监狱企业参加政府采购活动时，应当提供由省级以上监狱管理局、戒毒管理局(含新疆生产建设兵团)出具的属于监狱企业的证明文件（原件或扫描件加盖公章）。在政府采购活动中，监狱企业视同小型、微型企业，享受评审中价格扣除政策。（3）残疾人福利性单位声明函（原件，加盖供应商公章，格式见招标文件第四部分）在政府采购活动中，残疾人福利性单位视同小型、微型企业，享受评审中价格扣除政策。 |

**2.3、商务技术文件部分组成**

|  |  |
| --- | --- |
| **序号** | 内容 |
| **资信部分（▲序号1、2项供应商必须提供，否则不能通过符合性审查的，责任自负。）** |
| 1 | 投标函（附件九） |
| 2 | 法定代表人（负责人）诚信投标承诺书（附件十） |
| 3 | 供应商相关资质、资信或信用证书、获奖证书等（如有则提供，扫描件加盖有效公章） |
| 4 | 2018年1月1日以来投标供应商有同类项目业绩（附件十一） |
| 5 | 其它须说明的资料（如有则提供） |
| 技术部分（如资料提供不齐全，将可能导致不利的评定） |
| 6 | 商务、技术偏离表（附件十二） |
| 7 | 项目实施方案、供货（如有，包括品牌、型号、规格等）、人员情况等 |
| …… | …… |
| …… | 根据采购文件中的采购内容与技术要求、评标细则，需要提供的其它文件和资料。 |
| …… | 其它供应商须说明的资料（如有则提供） |

**注：金融、保险、通讯等特定行业的全国性企业所设立的区域性分支机构，以及个体工商户、个人独资企业、合伙企业，如果已经依法办理了工商、税务和社保登记手续，并且获得总公司（总机构）授权或能够提供房产权证或其他有效财产证明材料（在投标文件中提供相关材料），证明其具备实际承担责任的能力和法定的缔结合同能力，可以独立参加政府采购活动，由单位负责人签署相关文件材料。**

3、投标文件编制

3.1本项目通过“政采云平台（www.zcygov.cn）”实行在线投标响应（电子投标）。供应商应通过“政采云电子交易客户端”，并按照本采购文件和“政采云平台”的要求编制并加密投标文件。

3.2投标人应当按照本章节 “投标文件组成”规定的内容及顺序在“政采云电子交易客户端”编制投标文件。其中 “技术资信文件”中不得出现本项目投标报价，如因投标人原因提前泄露投标报价，是投标人的责任。

3.3本采购文件“投标文件格式”中有提供格式的，投标人须参照格式进行编制（格式中要求提供相关证明材料的还需后附相关证明材料），并按格式要求在指定位置根据要求进行签章，否则视为未提供；本文件“第六部分 投标文件格式”未提供格式的，请各投标单位自行拟定格式，并加盖单位公章并由法定代表人（负责人）或其授权代表签署（签字或盖章），否则视为未提供。

3.4投标文件内容不完整、编排混乱导致投标文件被误读、漏读或者查找不到相关内容的，是投标人的责任。

3.5投标文件因字迹潦草或表达不清所引起的后果由投标人负责。

3.6 投标人没有按照本章节 “投标文件组成”要求提供全部资料，或者没有仔细阅读采购文件，或者没有对采购文件在各方面的要求作出实质性响应是投标人的风险，由此造成的一切后果由投标人自行承担。

4、投标文件的签章

4.1投标文件的签章要求：投标人须知前附表；

4.2投标文件应由投标人法定代表人（负责人）或其授权代表签章，并时加盖投标人公章（电子签章）。

4.3电子签章操作指南详见采购公告附件《供应商项目采购-电子招投标操作指南》。

5、投标文件的形式

5.1投标文件的形式：见投标人须知前附表；

5.2“电子加密投标文件”：“电子加密投标文件”是指通过“政采云电子交易客户端”完成投标文件编制后生成并加密的数据电文形式的投标文件。

5.3“备份投标文件”：“备份投标文件”是指与“电子加密投标文件”同时生成的数据电文形式的电子文件（备份标书），其他方式编制的“备份投标文件”视为无效的“备份投标文件”。

6、投标文件的份数

6.1投标文件的份数：见投标人须知前附表。

7、投标报价

7.1、供应商应按招标文件中《开标一览表》及《投标分项报价表》（如有）填写投标报价及分项报价（如果）。

7.2、本次招标只允许有一个报价，有选择的报价将不予接受。

7.3、投标报价应按包含以下费用。

包括服务期的设备的人工费（含工人工资、奖金、房补、劳保福利、社保、意外保险、工伤费、教育培训费、暂住费及处理一切伤亡事故等费用）、工具材料费、安全文明作业装备费、企业应缴税金和应得利润、应急等完成合同所需的一切本身和不可或缺的所有工作开支、政策性文件规定计合同包含的所有风险、责任等各项全部费用并承担一切风险责任。

**供应商在投标报价中应充分考虑所有可能发生的费用，否则采购人将视投标综合单价中已包括所有费用。**

**供应商对在合同执行中，除上述费用及招标文件规定的由中标供应商负责的工作范围以外需要采购人协调或提供便利的工作应当在投标文件中说明。**

填写报价表格时，各项费用应如实填写。

8、采购人要求分类报价是为了方便评标，但在任何情况下不限制采购人以其认为最合适的条款签订合同的权利。

9、投标文件的有效期

9.1 自投标截止时间起90天内，投标文件应保持有效。有效期短于这个规定期限的投标将被拒绝。

9.2 在特殊情况下，采购人可与供应商协商延长投标文件的有效期，这种要求和答复均应以书面形式进行。

9.3 供应商可拒绝接受延期要求。同意延长有效期的供应商不能修改投标文件。

10、投标人如发生下列情况之一，将上报同级政府采购监督管理部门，追究其责任：

1. 投标人在采购文件规定的投标有效期内撤回投标；
2. 中标人未按中标通知书中规定的时间与采购人签订合同；
3. 投标人在采购文件中提供虚假技术指标及参数，经评标委员会确认属实的。
4. 经同级政府采购监督管理部门审查认定投标人有违反《中华人民共和国政府采购法》等有关法律法规的行为。

**五、投标文件的密封**

1、投标文件的递交

1.1投标文件的上传、递交：见投标人须知前附表。

2、 “电子加密投标文件”解密和异常情况处理。

2.1“电子加密投标文件”解密：见投标人须知前附表。

**3、 投标文件的补充、修改或撤回**

3.1供应商应当在投标文件递交截止时间前完成投标文件的上传、递交，并可以补充、修改或者撤回投标文件。补充或者修改投标文件的，应当先行撤回原文件，补充、修改后重新上传、递交。投标文件递交截止时间前未完成上传、递交的，视为撤回投标文件。投标文件递交截止时间后递交的投标文件，“政采云平台”将予以拒收。

3.2投标文件递交截止时间后，投标人不得撤回、修改投标文件。

**4、投标文件的备选方案**

4.1投标人不得递交任何的投标备选（替代）方案，否则其投标文件将作无效标处理。与“电子加密投标文件”同时生成的“备份投标文件”不是投标备选（替代）方案。

**六、开标和评标**

**1、开标形式**

1.1 采购组织机构将按照采购文件规定的时间通过“政采云平台”组织开标、开启投标文件，所有供应商均应当准时在线参加。

**2、 开标准备**

2.1开标的准备工作由采购组织机构负责落实。

2.2采购组织机构将按照采购文件规定的时间通过“政采云平台”组织开标、开启投标文件，所有供应商均应当准时在线参加。投标人如不参加开标大会的，视同认可开标结果，事后不得对采购相关人员、开标过程和开标结果提出异议，同时投标人因未在线参加开标而导致投标文件无法按时解密等一切后果由供应商自己承担。

**3、开标流程（两阶段）**

3.1开标第一阶段

**（1）向各投标人发出电子加密投标文件【开始解密】通知，由供应商按采购文件规定的时间内自行进行投标文件解密。投标人在规定的时间内（开标时间起30分钟内）无法完成已递交的“电子加密投标文件”解密的，如已按规定递交了备份投标文件的，将由采购组织机构按“政采云平台”操作规范将备份投标文件上传至“政采云平台”，上传成功后，“电子加密投标文件”自动失效；**

**（2）开启投标文件，进入资格审查；**

**（3）资格审查通过的投标人的技术资信文件进入符合性审查、技术评审；**

**（4）第一阶段开标结束。**

**备注：开标大会的第一阶段结束后，采购人或采购代理机构将对依法对投标人的资格进行审查，资格审查结束后进入符合性审查和技术资信文件的评审工作，具体见本章节“投标人资格审查”相关规定。**

3.2开标大会第二阶段

**（1）符合性审查、技术资信文件的评审结束后，举行开标大会第二阶段会议。首先在“政采云平台”系统平台上公布符合性审查、技术资信评审无效供应商名称及理由；公布经技术资信评审后有效投标人的名单，同时公布其技术资信部分得分情况。**

**（2）开启通过符合性审查、技术资信文件评审有效投标人的商务（报价）文件，在“政采云平台”系统平台上公布开标一览表有关内容，同时当场制作开标记录。开标结束后，由评标委员会对报价的合理性、准确性等进行审查核实。**

**（3）评审结束后，在“政采云平台”系统平台上公布中标（成交）候选供应商名单，及采购人最终确定中标或成交供应商名单的时间和公告方式等。**

**特别说明：如遇“政采云平台”电子化开标或评审程序调整的，按调整后程序执行。**

**4、 投标人资格审查**

4.1开标大会第一阶段结束后，采购人或采购代理机构首先依法对各投标人的资格进行审查，审查各投标人的资格是否满足采购文件的要求。采购人或采购代理机构对投标人所提交的资格审查材料仅负审核的责任。如发现投标人所提交的资格审查材料不合法或与事实不符，采购人可取消其中标资格并追究投标人的法律责任。

4.2投标人提交的资格审查材料无法证明其符合采购文件规定的“投标人资格要求”的，采购人或采购代理机构将对其作资格审查不通过处理（无效投标），并不再将其投标提交评标委员会进行后续评审。

4.3单位负责人为同一人或者存在直接控股、管理关系的不同供应商参加同一合同项下的政府采购活动的，相关投标人均作资格无效处理。

**5、评标**

**5.1评标由采购人依法组建的评标委员会负责，并独立履行下列职责：**

1）审查投标文件是否符合招标文件要求，并做出评价；

2）要求供应商对投标文件有关事项做出解释或者澄清；

3）按照招标文件确定的评标办法确定中标人，并对其排序；综合得分最高的供应商推荐为中标人；

4）向采购人或者有关部门报告非法干预评标工作的行为。

5）根据采购人的授权确定中标人名单；

**5.2评标应当遵循下列工作程序：**

1）投标文件初审。初审为符合性检查。

（1)符合性检查。依据招标文件的规定，从投标文件的有效性、完整性和对招标文件的响应程度进行审查，以确定是否对招标文件的实质性要求做出响应。

2）澄清有关问题。对投标文件中含义不明确、同类问题表述不一致或者有明显文字和计算错误的内容，评标委员会可以书面形式要求供应商做出必要的澄清、说明或者纠正。供应商的澄清、说明或者补正应当采用书面形式，由其授权的代表签字，并不得超出投标文件的范围或者改变投标文件的实质性内容。

**实质上没有响应招标文件要求的投标将被拒绝。供应商不得通过修正或撤消不合要求的偏离从而使其投标成为实质上响应的投标。**

**评标委员会对投标文件的判定，只依据投标文件内容本身，不依靠开标后的任何外来证明。**

3）比较与评价。按招标文件中规定的评标方法和标准，对资格性检查和符合性检查合格的投标文件进行商务和技术评估，综合比较与评价。

4）推荐中标人候选人名单，并根据采购人的授权确定中标人。

**5.3 ▲投标人存在下列情况之一的，投标无效:**

1）投标文件未按招标文件要求签署、盖章的；

2）不具备招标文件中规定的资格要求的；

3）报价超过招标文件中规定的预算金额或者最高限价的；

4）投标文件含有采购人不能接受的附加条件的（包括招标文件中明确要求不得偏离的招标要求，存在负偏离的）;

5）仅提交“备份投标文件”的；

6）对关键条文的偏离、保留或反对，例如关于付款方式、完工期、免费质保期、适用法律法规、标准、税费等其他内容；

7）存在串标、抬标或弄虚作假情况的；

8）法律、法规和招标文件规定的其他无效情形（或出现重大偏差）。

**5.4 ▲评标委员会发现投标文件有下列情形之一的属于重大偏差(评标委员会按少数服从多数原则认定),按照无效投标处理：**

**1）未按招标文件要求编制或字迹模糊、辨认不清的投标文件；**

**2）供应商技术资信投标文件中出现投标报价；**

**3）除5.3条款以外，出现其它明显不符合技术规格、技术标准的要求或不满足招标文件技术规格书中的主要参数的投标文件；**

**4）除5.3条款以外，出现投标服务内容与招标文件对比出现较大偏差；商务报价明细表计算错误，出现较大差错；**

**5）除5.3条款以外，出现其它不符合招标文件中规定的实质性要求的投标文件，是否为偏离实质性要求由评标委员会认定。**

**5.5 开启供应商商务报价文件后发现价格、数量有误，其投标价将按下述原则处理：**

1) 任何有漏去一些小项货物或服务的投标将被视为其费用已包含在投标综合单价中，投标价格不予调整。如果供应商不接受上述处理方式，将作为无效投标。

2) 任何有多报一些小项工程或服务的投标其投标价不予调整，如果该供应商中标，则合同价格必须为核减掉多报的一些小项工程或服务后的价格。如果供应商不接受上述处理方式，将作为无效投标。

3）对于计算错误的其投标价不予调整，如果该供应商中标，如其投标价格计算错误导致多报者合同价格予以据实核减，少报者合同价格不予调整。如果供应商不接受上述处理方式，将作为无效投标。

4）对于计算错误，多报或漏报的一些小项工程或服务的仅仅为非实质性重大偏差范围内的偏离，并经过评标委员会按少数服从多数原则认定为细微偏差，评审时其投标价不予调整。**如认定为重大偏差的，做无效投标处理。**

**5.6▲评标委员会认为投标人的报价明显低于其他通过符合性审查投标人的报价，有可能影响产品质量或者不能诚信履约的，将要求其在合理时间内在“政采云平台”上作出在线澄清并提供书面说明，必要时提交相关证明材料；投标人不能证明其报价合理性的，评标委员会应当将其作为无效投标处理。**

**5.7如果投标人代表拒绝按评标委员会要求在“政采云平台”作出在线回复且无其他有效回复方式的，评标委员会可以对其作出否决投标处理。**

5.8 经澄清后，若偏差仍存在，且不可接受，则投标文件将被认定为“没有实质性响应采购文件要求”，按无效投标处理，不再进入下一步评审。评标委员会在评标中，不得改变招标文件中规定的评标标准、方法和中标条件。

5.9 评标时如遇到招标文件未规定的特殊情况，由评标委员会按少数服从多数原则集体决定处理。

**5.10评标委员会对未中标的供应商不作解释。同时根据政府采购法实施条例第四十条规定，本项目不对供应商公布详细的评审情况，不公布具体评标细则中小项得分。**

6、投标文件的澄清

6.1 **为有助于投标文件的审查、评价和比较，评标小组可以在“政采云平台”在线询标或其他有效形式要求投标人对同一份投标文件含义不明确或同类问题表述不一致的内容（采购文件其它地方有规定处理方法的除外）作必要的澄清或说明，投标人应采用在线回复或其他有效形式在询标规定时间内进行澄清或说明（需盖电子签章或实体公章），但不得超出投标文件的范围或改变投标文件的实质性内容。凡属于评标小组在评标中发现的计算错误并进行核实的修改不在此列**。

6.2 若投标文件中所提交的证书、证明等材料若出现已过有效期、时间或其他主要信息不明确，且投标人书面澄清（书面澄清仅限在投标文件递交截止时间前所提交投标文件及相关材料中未被评标委员会审查出的内容）亦不明确的，评审过程中将不予认可，不再寻求外部证据（外部证据包括投标人在澄清过程中申请补交的证明材料或网络查询结果等非投标文件本身内容）。

6.3 供应商对投标文件的澄清不得寻求、提供或允许改变投标价格等实质性内容。

7、禁止供应商相互串通投标。
7.1、有下列情形之一的，视为供应商相互串通投标：
（一）不同供应商的投标文件由同一单位或者个人编制；
（二）不同供应商委托同一单位或者个人办理投标事宜；
（三）不同供应商的投标文件载明的项目管理成员为同一人；
（四）不同供应商的投标文件异常一致或者投标报价呈规律性差异；
（五）不同供应商的投标文件相互混装；
**7.2、经评标委员会认定供应商进行串通投标的，评标委员会可以对相关供应商做出无效投标处理，并上报政府采购管理部门进行进一步处理。**

8、评标原则

**8.1 ▲投标截止时或评审过程中有效投标供应商不足三家的，不予开标或评标。**

9、确定中标候选人

9.1本次招标由评标委员会推荐中标候选人，采购人根据评标委员会的推荐结果进行最终确认。

9.2评标委员会依据法律、法规及采购文件有关规定在有效标中按投标人的最终得分（即技术分与商务分之和）高低进行排序，得分前二名的投标人推荐为中标候选人与备选中标人（得分相同投标报价低的排序第一；得分且投标报价相同的，由评标委员会成员抽签决定排序）。

9.3若出现以下情形之一，采购人可视具体情况确定是否由备选中标人为中标人或重新组织招标：

1）中标候选人放弃中标资格；

2）中标候选人因不可抗力提出不能履行合同；

3）中标候选人未能在规定时间内与采购单位签订合同；

4）经质疑，采购人审查后，中标候选人确实在本次采购活动中存在违法违规行为或其他原因使质疑成立的。

9.4采购人、采购代理机构及评标委员会对未中标的供应商不作解释。同时根据政府采购法实施条例第四十条规定，本项目不对供应商公布详细的评审情况，不公布具体评标细则中小项得分。

10、评标细则详见“评标原则及方法”。

11、 可中止电子交易活动的情形

11.1采购过程中出现以下情形，导致电子交易平台无法正常运行，或者无法保证电子交易的公平、公正和安全时，采购组织机构可中止电子交易活动：

* + 1. 电子交易平台发生故障而无法登录访问的；
		2. 电子交易平台应用或数据库出现错误，不能进行正常操作的；
		3. 电子交易平台发现严重安全漏洞，有潜在泄密危险的；
		4. 病毒发作导致不能进行正常操作的；
		5. 其他无法保证电子交易的公平、公正和安全的情况。

11.2出现前款规定情形，不影响采购公平、公正性的，采购组织机构可以待上述情形消除后继续组织电子交易活动；影响或可能影响采购公平、公正性的，应当重新采购。

**七、授予合同**

1、决标

1.1、评标结束后，评标委员会按照招标文件确定的评标办法推荐中标供应商。

2、中标通知书

**2.1、采购人依法确认中标供应商后，代理机构在浙江省政府采购网上公告中标结果，公告期限为1个工作日。同时向中标供应商发出中标通知书。**

2.2、中标通知书对采购人和中标人具有法律约束力。中标通知书发出后，采购人改变中标结果或者中标人放弃中标的，应当承担法律责任。

**2.3、中标无效**

1）发现中标供应商资格无效或中标供应商放弃中标或拒绝与采购人签订合同的,采购人可以按照评审报告推荐的中标候选人名单排序，确定下一候选人为中标供应商，也可以重新开展政府采购活动。
 2）有《中华人民共和国政府采购法实施条例》第七十一条、第七十二条、第七十三条、第七十四条规定的违法行为之一，由政府采购监管部门依法处理。

4、签订合同

4.1 中标供应商须主动联系采购人或采购代理机构领取中标通知书。中标供应商应当在中标通知书发出之日起30日历天内与采购人签订合同。中标供应商未经采购人许可，在规定时间内未到采购人处与采购人签订合同，则视为拒签合同。

4.2 招标文件、中标供应商的投标文件及投标修改文件、评标过程中有关澄清文件及经双方签字的询标纪要（承诺）和中标通知书均作为合同附件。

4.3 拒签合同的责任

中标供应商在规定时间内（30日历天）借故否认已经承诺的条件、拒签合同或拒交履约保证金者，以投标违约处理，赔偿采购人由此造成的直接经济损失；采购人重新组织招标的，所需费用由原中标供应商承担。

4.4 采购人在授予合同时有权对采购的服务予以增加或减少，但不得对单价或其他的条款和条件做任何改变。

第四部分 政府采购政策功能相关说明

一、小、微企业（含监狱企业、残疾人福利性单位）扶持政策说明

1、文件依据

（1）关于印发《政府采购促进中小企业发展管理办法》的通知（财库〔2020〕46号）

（2）浙江省省财政厅《关于开展政府采购投标人网上注册登记和诚信管理工作的通知》（浙财采监〔2010〕8号)

（3）《工业和信息化部、国家统计局、国家发展和改革委员会、财政部关于印发中小企业划型标准规定的通知》（工信部联企业[2011]300号）

（4）财政部、司法部《关于政府采购支持监狱企业发展有关问题的通知》（财库〔2014〕68号）

（5）《财政部 民政部 中国残疾人联合会关于促进残疾人就业政府采购政策的通知》（财库〔2017〕 141号）

（6）《浙江省财政厅 浙江省经济和信息化委员会关于简化中小企业类别确认流程有关事项的通知》（浙财采监〔2018〕2号)

2、享受小微企业价格折扣应具备的条件与价格折扣比例

（1）在货物采购项目中，货物由中小企业制造，即货物由中小企业生产且使用该中小企业商号或者注册商标；
（2）在工程采购项目中，工程由中小企业承建，即工程施工单位为中小企业；

（3）在服务采购项目中，服务由中小企业承接，即提供服务的人员为中小企业依照《中华人民共和国劳动合同法》订立劳动合同的从业人员。
在货物采购项目中，供应商提供的货物既有中小企业制造货物，也有大型企业制造货物的，不享受本办法规定的中小企业扶持政策。

以联合体形式参加政府采购活动，联合体各方均为中小企业的，联合体视同中小企业。其中，联合体各方均为小微企业的，联合体视同小微企业。

（3）本项目对小型和微型企业产品的价格给予6%的扣除，用扣除后的价格参与评审。

3、享受小微企业价格折扣应提供以下证明材料：

（1）《中小企业声明函》（原件，加盖投标人公章，格式见附件1）

4、享受监狱企业价格折扣应提供以下证明材料（投标文件商务（报价）标中，不提供的不享受价格折扣）：

（1）监狱企业参加政府采购活动时，应当提供由省级以上监狱管理局、戒毒管理局(含新疆生产建设兵团)出具的属于监狱企业的证明文件（原件或扫描件加盖公章）。在政府采购活动中，监狱企业视同小型、微型企业，享受评审中价格扣除政策。

5、享受残疾人福利性单位格折扣应提供以下证明材料（投标文件技术资信标中，不提供的不享受价格折扣）：

（1）残疾人福利性单位声明函（附件2）；

6、非单一产品采购，无法核实（按投标文件资料）全部货物均为小微企业（含监狱企业、残疾人福利性单位）制造；或小微企业（含监狱企业、残疾人福利性单位）提供其他制造商制造的货物且无法核实（按投标文件资料）制造商是否为小微企业（含监狱企业、残疾人福利性单位）的，不享受价格折扣。

**附件1：**

**中小企业声明函（货物）**

本公司（联合体）郑重声明，根据《政府采购促进中小企业发展管理办法》（财库﹝2020﹞46 号）的规定，本公司（联合体）参加 （单位名称） 的 （项目名称） 采购活动，提供的货物全部由符合政策要求的中小企业制造。相关企业（含联合体中的中小企业、签订分包意向协议的中小企业）的具体情况如下：

1. （标的名称） ，属于 行业 ；制造商为 （企业名称） ，从业人员人，营业收入为万元，资产总额为万元 ，属于 （中型企业、小型企业、微型企业） ；

2. （标的名称） ，属于 行业 ；制造商为 （企业名称） ，从业人员人，营业收入为万元，资产总额为万元，属于 （中型企业、小型企业、微型企业） ；

……

以上企业，不属于大企业的分支机构，不存在控股股东为大企业的情形，也不存在与大企业的负责人为同一人的情形。

本企业对上述声明内容的真实性负责。如有虚假，将依法承担相应责任。

企业名称（盖章）：

日 期：

**中小企业声明函（工程、服务）**

本公司（联合体）郑重声明，根据《政府采购促进中小企业发展管理办法》（财库﹝2020﹞46 号）的规定，本公司（联合体）参加 （单位名称） 的 （项目名称） 采购活动，工程的施工单位全部为符合政策要求的中小企业（或者：服务全部由符合政策要求的中小企业承接）。相关企业（含联合体中的中小企业、签订分包意向协议的中小企业）的具体情况如下：

1. （标的名称） ，属于 行业 ；承建（承接）企业为 （企业名称） ，从业人员人，营业收入为万元，资产总额为万元 ，属于 （中型企业、小型企业、微型企业） ；

2. （标的名称） ，属于 行业；承建（承接）企业为 （企业名称） ，从业人员人，营业收入为万元，资产总额为万元，属于 （中型企业、小型企业、微型企业） ；

……

以上企业，不属于大企业的分支机构，不存在控股股东为大企业的情形，也不存在与大企业的负责人为同一人的情形。

本企业对上述声明内容的真实性负责。如有虚假，将依法承担相应责任。

企业名称（盖章）：

日 期：

**注：1 从业人员、营业收入、资产总额填报上一年度数据，无上一年度数据的新成立企业可不填报。**

**附件2**

**残疾人福利性单位声明函**

本单位郑重声明，根据《财政部 民政部 中国残疾人联合会关于促进残疾人就业政府采购政策的通知》（财库〔2017〕 141号）的规定，本单位为符合条件的残疾人福利性单位，且本单位参加\_\_\_\_\_\_单位的\_\_\_\_\_\_项目采购活动提供本单位制造的货物（由本单位承担工程/提供服务），或者提供其他残疾人福利性单位制造的货物（不包括使用非残疾人福利性单位注册商标的货物）。

本单位对上述声明的真实性负责。如有虚假，将依法承担相应责任。

投标人全称（盖章）：

日 期：

**备注说明：**

**1、如中标，将在中标公示中将此声明函予以公示，接受社会监督；**

**2、投标人提供的《残疾人福利性单位声明函》与事实不符的，依照《政府采购法》第七十七条第一款的规定追究法律责任。**

第五部分 合同格式（仅供参考）

本条款为甲乙双方必须遵守的基本条款，甲乙双方也可根据实际情况另签合同条款，正式合同以双方签字盖章的文本为准。

 甲方：永嘉县大数据管理中心

 乙方：

 鉴于甲方于2021年 月 日接受乙方对的投标，双方根据《中华人民共和国民法典》和本项目的招标文件、投标文件及其投标中的承诺，经双方协商，同意签订本合同，共同遵守：

**1.合同内容**：依据招标文件及招标人规定的服务内容。

**2.合同价格**

本合同总价为人民币万元。

**3、项目实施时间：**

**软件开发、调试、测试、上线试运行自合同签订起不得超过60天。**

**4. 合同说明**

甲、乙双方经过协商，就甲方希望获得乙方开发、生产的软件的使用许可达成以下合同。

**5.许可软件清单、费用支付及许可范围**

5.1许可软件清单。根据本合同约定的条款及条件，乙方同意授予、甲方同意接受下表所列许可证软件的使用许可。

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 名称 | 品牌、版本号 | 备注 |
|  |  |  |  |

5.2 费用支付。

**在合同签订后乙方提供合同总金额5%的履约保证金；**

1、合同签订后日内,甲方向乙方支付合同总额的30%；

2、所有项目经相关部门初步验收合格，自正式上线试运行之日起日内，甲方向乙方支付合同总额的60%；

3、所有项目通过最终验收后日内，甲方向乙方无息支剩余合同总额的10%。

**履约保证金转为系统免费维护保证金在硬件五年免费维护期到期后十个工作日内向卖方一次性无息退还。**

**6. 相关服务**

乙方为甲方提供如下免费服务：

6.1乙方为甲方提供硬件五年（50个月），软件三年（36个月）的软件免费升级技术升级与支持服务。

6.2上述许可软件的安装、调试及相关实施服务。

6.3三年的免费技术支持服务时间从企业推广完成经企业确认后起计算；

6.4在产品的生命期内，提供免费电话技术，但因程序本身的问题，而导致功能与说明书上不符、或程序运行错误等，乙方需提供免费完善其功能或修正其错误的技术支持；

6.5双方可就该软件系统三年免费维护期满后的维护与技术支持服务等内容另外签署服务合同。服务内容与合同规定的三年期免费服务标准内容一致。

**7.产品保证**

7.1乙方保证交付的软件均符合说明书或使用手册所述功能，并由软件验收测试的成功完成予以证明。验收测试的成功完成应被视为该许可软件能达到说明或使用手册所述功能的决定性证据。但本保证不适用于：

7.1.1乙方之外的任何人对该许可软件作任何方式的修改；

7.1.2甲方未按许可软件所附说明书或用户手册的规定使用软件；

7.1.3由于甲方原因或第三方产品的故障、网络故障等使软件无法正常运行。

如果许可软件未能按照说明书或使用手册的功能运行，乙方应负责对许可软件进行修正或者在修正不能的情况下，免费为甲方更换符合规定的许可软件。如果上述二种方法均不可行，甲方有权终止许可软件不符合规定部分的使用许可，并由乙方返还甲方已经支付该部分的使用许可费。

7.2从本项目软件系统终验合格，正式交付使用之日起一年内，许可软件的储存载体、加密附件出现非人为的物理损坏、乙方应根据甲方的书面要求给予免费修正更换，对人为损坏或遗失则需适当收费。

**8.产品验收**

8.1甲方对产品外部瑕疵的异议，应在收到该许可软件之日当面提出。

8.2乙方在甲方指定场所完成许可软件的安装和调试工作（包括个性化改造及适应性修改部份），并与甲方一起按许可软件的说明书或使用手册规定的技术指标和参数对该软件进行验收测试，验收测试合格后，甲方和乙方代表共同在验收合格证明书上签字。验收分为初验和终验：

**9.免责条款**

乙方对甲方因许可软件遗失、被盗、被误用或被擅自修改、计算机设备故障、操作失误等情况造成的损失不负责任。

**10.软件著作权**

许可软件的著作权归 （甲乙方）共有。

乙方承诺：本合同规定的软件系统（包括个性化改造及适应性修改部份）是独立、可稳定运行的系统，不需要另外依靠第三方软件的支持；本软件如与甲方在用其它第三方软件冲突，由乙方负责解决；乙方已依法进行了计算机软件著作权登记，或已经通过由有关部门组织的验收，准予在甲方所处行业或部门推广应用；甲方在使用过程中，不会遭遇知识产权方面的阻碍。

**11.保证金**

乙方在合同签订后，向甲方递交本次合同金额5%的履约及免费技术支持保证金，从本项目软件系统终验合格，正式交付使用之日起五年内，软件系统运行正常，技术支持良好，无质量和服务问题，维护期满后7天内原额（无息）退还保证金。

**12. 违约责任**

本合同签订生效即具有法律效力，双方必须严格遵守，如有一方违约，其必须承担违约责任并赔偿对方因此而遭受的全部损失。具体如下：

（1）乙方未按时交货（包括个性化改造），并在规定时间内完成安装、调试，或所提交的软件系统商品达不到合同规定的指标，乙方应当承担违约方式和违约金额如下：每超期10天，扣合同金额的**0.5 %**；累计超期30天，甲方有权终止执行合同，并没收履约保证金。

（2）甲方逾期支付货款的，自逾期之日起，向乙方每日偿付合同总价**0.5 %**的违约金；需方无正当理由拒绝付货款的，应向乙偿付合同总价 **5 %**的违约金。

**13.争议解决**

凡由本合同引起的或与解释或执行本合同有关的任何争议，双方应首先通过友好协商或调解解决。若协商或调解不成，双方约定：向甲方所在地的仲裁，仲裁应依据该委员会当时的仲裁规则进行；仲裁裁决是终局的，对双方都有约束力；仲裁费用应由败诉方承担，除非仲裁裁决另有裁定。

**14．合同生效及其他**

14.1 合同应在双方签字盖章并在甲方收到乙方提供的履约保证金后开始生效。

14.2 本合同一式柒份，双方各执叁份，采购代理机构执一份，具有同等法律效力。

14.3下列文件构成本合同的组成部分：

 （1）合同主要条款 （2）合同的特殊条款

 （3）售后服务条款 （4）中标通知书

 (5) 投标分项报价表 (6) 技术规格、商务条款偏离表

 (7) 招标内容及要求 （8）合同补充条款或说明（如有的话）

 (9)履约保证金 (10) 承诺书 （含询标记录和优惠条件）

14.4如需修改或补充合同内容，经协商，双方应签署书面修改或补充协议，该协议将作为本合同的一个组成部分。

甲方：（印章） 乙方：（印章）

全权代表:（签字） 全权代表:（签字）

地址： 地址：

邮政编码： 邮政编码：

电话： 电话：

传真： 传真：

开户银行： 开户银行：

帐号： 帐号：

第六部分 投标文件格式

一、资格文件部分格式

**附件一**

具有履行合同所必需的设备和专业技术能力的承诺函

永嘉县大数据管理中心：

温州市中概工程管理咨询有限公司：

我方 （供应商）承诺具有履行合同所必需的设备和专业技术能力。如有虚假，采购人可取消我方任何资格（投标/中标/签订合同），我方对此无任何异议。

特此承诺！

投标供应商（盖章） ：

法定代表人（负责人）或授权代表（签字或盖章）：

日期：

**附件二**

依法缴纳税收和社会保障资金的承诺函

永嘉县大数据管理中心：

温州市中概工程管理咨询有限公司：

我公司郑重声明，我公司严格依法缴纳税收和社会保障资金，本文件中所提供的相关材料均真实有效，不存在虚假、造假行为。如有违反，愿承担一切责任。

特此承诺！

投标供应商（盖章） ：

法定代表人（负责人）或授权代表（签字或盖章）：

日期：

**附件三**

参加政府采购活动前3年内在经营活动中没有重大违法记录的声明函

永嘉县大数据管理中心：

温州市中概工程管理咨询有限公司：

我方 （供应商）具有良好的商业信誉，依法缴纳税收和社会保障资金，未被列入失信被执行人名单、重大税收违法案件当事人名单、政府采购严重违法失信行为记录名单，参加本次政府采购活动前3年内在经营活动中没有重大违法记录（没有因违法经营受到刑事处罚，没有被责令停产停业、被吊销许可证或者执照、被处以较大数额罚款等行政处罚，没有因违法经营被禁止参加政府采购活动的期限未满情形）。如有虚假，采购人可取消我方任何资格（投标/中标/签订合同），我方对此无任何异议。

特此承诺！

投标供应商（盖章） ：

法定代表人（负责人）或授权代表（签字或盖章）：

日期：

**附件四**

**与参加本次项目同一合同项下政府采购活动的其他供应商不存在单位负责人为同一人或者直接控股、管理关系的承诺函**

永嘉县大数据管理中心：

温州市中概工程管理咨询有限公司：

我方郑重承诺，我方此次参加本项目的投标，与参加本次项目同一合同项下政府采购活动的其他供应商不存在单位负责人为同一人或者直接控股、管理关系。如有虚假或隐瞒，愿意承担一切后果。

特此承诺！

投标供应商（盖章） ：

法定代表人（负责人）或授权代表（签字或盖章）：

日期：

**附件五**

**供应商参与政府采购活动投标资格声明函**

|  |  |
| --- | --- |
| 项目名称 |  |
| 项目采购编号 |  |
| 时 间 | 投标截止时间： |
| 1、根据政府采购法第二十二条规定，我单位满足以下条件，并已经在技术资信部分投标文件中提供了相应的证明材料：（一）具有独立承担民事责任的能力； 　　（二）具有良好的商业信誉和健全的财务会计制度； 　　（三）具有履行合同所必需的设备和专业技术能力； 　　（四）有依法缴纳税收和社会保障资金的良好记录； 　　（五）参加政府采购活动前三年内，在经营活动中没有重大违法记录； 　　（六）法律、行政法规规定的其他条件。 2、根据财政部与有关部门联合签署了《关于对重大税收违法案件当事人实施联合惩戒措施的合作备忘录》(发改财金〔2014〕3062号)、《失信企业协同监管和联合惩戒合作备忘录》(发改财金〔2015〕2045号)、《关于对违法失信上市公司相关责任主体实施联合惩戒的合作备忘录》(发改财金〔2015〕3062号)、《关于对失信被执行人实施联合惩戒的合作备忘录》(发改财金〔2016〕141号)、《关于对安全生产领域失信生产经营单位及其有关人员开展联合惩戒的合作备忘录》(发改财金〔2016〕1001号)，依法限制相关失信主体参与政府采购活动。我单位不存在上述文件规定依法限制参与政府采购的情况，并提供“信用中国”、 “中国政府采购网”查询网页截图（公告发布之日至投标截止时间）。**3、我单位没有被各地、各级财政部门限制参加政府采购活动，且在限制期内：****4、清楚知道参加本项目采购活动的其他所有供应商名称，本单位与其他所有供应商之间均不存在利害关系。****5、我单位参与本项目政府采购活动3年内其它重大违法记录（重大违法记录，是指供应商因违法经营受到刑事处罚或者责令停产停业、吊销许可证或者执照、较大数额罚款等行政处罚）情况声明：**6、我单位符合本项目特定资格条件： 的要求，并在技术资信部分投标文件中提供了相应的证明材料（招标文件没有要求特定资格条件的，本条款空格处可以空白）本公司所提交的本声明和陈述均是真实的、准确的。若与真实情况不符，本公司愿意承担由此而产生的一切后果。我方提供了全部能提供的资料和数据，我们同意遵照贵方要求出示有关证明文件。 |
| 供应商名称（加盖盖章）： |
| 法定代表人（负责人）或授权代表（签字或盖章）： |
| 签署日期： |

**备注：▲投标供应商必须提供本声明，不提供按无效投标处理。**

附件六

法定代表人（负责人）授权书

（采购人名称）：

本授权委托书声明：我 （法定代表人（负责人）姓名） 系 （供 应 商 名 称） 的法定代表人（负责人），现授权委托 （单 位 名 称） 的 （授权代表姓名） 为我公司法定代表人（负责人）授权代表，参加贵处组织的 （招标项目名称，括号中填写项目编号） 项目投标，全权处理本次招投标活动中的一切事宜，我承认授权代表全权代表我所签署的本项目的投标文件的内容。

授权代表无转授权，特此授权

授权代表： 性别 ：

职务：年龄：

详细通讯地址： 邮政编码：

电话： 传真：

 投标人： （盖章）

 法定代表人（负责人）： （签字或盖章）

授权委托日期： 年 月 日

|  |
| --- |
| **（授权代表身份证扫描件或影印件）** |

二、报价文件部分格式

**附件七**

报价一览表

项目名称： 项目编号： 人民币（元）

|  |  |  |
| --- | --- | --- |
| **项目名称** | **投标总价（人民币元）** | **备注** |
|  | **（大写）****（小写）** |  |

说明：

1. **▲不提供此表格将被视为没有实质性响应招标文件。**
2. **▲投标总价须与投标分项报价表中的总计价相一致。**

投标人全称（盖章）：

法定代表人（负责人）或授权代表（签字）：

日 期： 年 月 日

**附件八**

**二、投标分项报价表**

**项目名称： 项目编号：**价格单位：人民币（元）

|  |  |  |
| --- | --- | --- |
| 序号 | 项目内容 | 报价 |
| 1 |  |  |
| 2 |  |  |
| 3 |  |  |
| 4 |  |  |
| 5 |  |  |
| 总 计 价 |  |

**说明：**

1. **▲总计价应与“开标一览表”中投标总价相一致。**

**2. ▲不提供投标分项报价表的投标文件将被视为未实质性响应招标文件。**

**3. 本表可在不改变格式的情况下根据具体需要自行增减。**

投标人全称（盖章）：

法定代表人（负责人）或授权代表（签字或盖章）：

日 期： 年 月 日

三、商务技术文件部分格式

**附件九**

投 标 函

 （采购人） ：

（供应商全称）授权 （授权代表名称）（职务、职称）为授权代表，参加贵方组织的（招标项目名称）（括号内填投标编号） 招标的有关活动，并对该项目进行投标。为此：

1、提供投标须知规定的全部响应文件。

2、我方对服务期承诺如下：按招标文件要求完成本项目。

3、保证遵守采购文件中的有关规定和收费标准。

4、保证忠实地执行采购人、成交供应商双方所签的合同，并承担合同规定的责任义务。

5、供应商已详细审查全部采购文件，包括采购文件补充文件（如有）。我方完全理解并同意放弃对这方面有不明及误解的权力。如果采购文件有相互矛盾之处，我方同意按采购人的理解处理。

6、愿意向贵方提供任何与该项投标有关的数据、情况和技术资料，完全理解贵方不一定接受最低价的投标或收到的任何投标。

7、利益冲突：近三年内直至目前，我公司与本项目的采购人、采购代理机构没有任何的隶属关系。

8、我单位没有被各地、各级财政部门限制参加政府采购活动或曾被各地、各级财政部门限制参加政府采购活动但已不在限制期内。

9、投标有效期内不撤销投标文件；强行撤销的，承诺按采购预算金额的2%赔偿对采购组织机构造成的损失。

10、中标或者成交后，按采购文件规定与采购人签订合同。拒绝签订合同的，承诺按采购预算金额的 2%对采购人进行赔偿；赔偿金额不足以弥补采购人损失的，承诺继续承担超过部分的损失。

11、中标或者成交后，按采购文件规定的采购代理服务费标准，承诺在签订合同前向采购代理机构支付采购代理服务费。

12、本投标自开标之日起90天内有效。

13、如有列情形之一的，我方愿意被取消成交资格（如成交），同时继续承担其他一切法律后果，并不再寻求任何旨在减轻或免除法律责任的解释：

(1)提供虚假材料（承诺）谋取成交、成交的；

(2)采取不正当手段诋毁、排挤其他供应商的；

(3)与采购人、其它供应商或者采购代理机构恶意串通的；

(4)向采购人、采购代理机构行贿或者提供其他不正当利益的；

(5)在招标采购过程中与采购人进行协商谈判的；

(6)拒绝有关部门监督检查或提供虚假情况的。

14、与本投标有关的一切往来通讯请寄：

地址：

邮编：电话：传真：

供应商全称（盖章）：

法定代表人（负责人）或授权代表（签字或盖章）：

日期：

**附件十**

**法定代表人（负责人）诚信投标承诺书**

本人以企业法定代表人（负责人）的身份郑重承诺：

将遵循公开、公平、公正和诚信信用的原则参加 项目（项目编号： ）的投标；

一、杜绝以收取管理费等形式的一切挂靠、违法转包、分包行为；并选派有丰富经验、无不良行为记录的在项目管理人员、技术人员，严格按招标文件、投标文件及合同等要求保证拟派人员的到岗率。

二、投标文件所提供的一切材料都是真实、有效、合法的。

三、不与其他投标人相互串通投标报价，不排挤其他投标人的公平竞争，不损害招标人或其他投标人的合法权益。

四、不与采购人或采购代理机构串通投标，不损害国家利益，社会公共利益或其他人的合法权益。

五、不向采购人或者评标委员会成员行贿以牟取中标。

六、不以其他人名义投标或者以其他方式弄虚作假，骗取中标。

七、不在开标后进行虚假恶意投诉。

八、我单位没有被政府机关列入失信被执行人名单、重大税收违法案件当事人名单、政府采购严重违法失信行为记录名单及其他不符合《中华人民共和国政府采购法》第二十二条规定条件的情形：

九、没有被各地、各级财政部门禁止参加政府采购活动，且在限制期限内：

十、参与本项目政府采购活动3年内没有重大违法记录情况。

本公司若有违反本承诺内容的行为，愿意承担法律责任，包括不限于：愿意接受相关行政主管部门作出的处罚；给采购人造成损失的，依法承担相应的赔偿责任。

法定代表人（负责人）或授权代表（签字或盖章）：

投标供应商（盖章）

承诺书签署日期： 年 月 日

**备注：▲投标供应商必须提供本承诺书，不提供按无效投标处理。**

**附件十一**

**2018年1月1日以来投标供应商有同类项目业绩**

项目名称： 项目编号：

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 序号 | 采购单位 | 项目名称 | 销售数量（台） | 签约日期 | 联系人 | 联系电话 | 备注 |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |

注：投标供应商可按此表格式复制，需后附合同及相关材料扫描件加盖公章。

供应商全称（盖章）：

法定代表人（负责人）或授权代表（签字或盖章）：

日期：

**附件十二**

偏离表

项目名称： 项目编号：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 内 容 | 采购文件条目 | 采购文件规格要求 | 投标文件对应规格 | 说 明 |
| 技术偏离 |  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
| 商务偏离 |  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

注：1、不填写此表视为完全响应招标文件内容；

2、“技术规格偏离表”必须按照招标文件要求逐条如实填写，根据投标情况在“说明”项填写正偏离或负偏离，完全符合的填写“无偏离”，并在投标文件中逐条提供响应技术规格要求的直接证据。

投标单位名称（盖章）：

法定代表人（负责人）或授权代表（签字或盖章）：

 日 期： 年 月 日

**附件十三**

**（1）项目负责人情况表**

项目名称： 项目编号：

|  |
| --- |
| 1、一般情况 |
| 姓 名 |  | 年 龄 |  | 学 历 |  |
| 毕业学校 |  | 专 业 |  | 职 务 |  |
| 职 称（或资格） |  | 拟任何职 |  | 参加工作时间 |  |
| 2、个人简历 |
| 时 间 | 专业工作经历 |
|  |  |
|  |  |
| 3、负责类似项目业绩 |
| 序号 | 项 目 名 称 | 该项目中任何职 |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

注：1、本表应附相关证书、社保等证明。

2、本表可在不改变格式的情况下根据具体需要自行增减。

投标供应商全称（盖章）：

法定代表人（负责人）或授权代表（签字或盖章）：

日 期： 年 月 日

**（2）项目组人员一览表**

项目名称： 项目编号：

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 姓名 | 性别 | 年龄 | 学历/职称 | 专业 | 专业工作年限 | 拟任何职 | 是否常驻（填：是或否） |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |

注：1、本表应附所列项目组成员相关证书、社保等证明。

2、此表仅提供了表格形式，可按此表格复制。

投标供应商全称（盖章）：

法定代表人（负责人）或授权代表（签字或盖章）：

日 期： 年 月 日

**附件十四**

产品配置及主要技术参数

 招标编号： 项目名称：

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 序号 | 货物名称 | 品牌产地 | 主要规格 | 数量 | 免费质保期 | 备注 |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

注：1、放置技术资信标中

2、所投产品详细配置、技术应另页描述。

3、相当于不带价格的详细报价表，必须提供，所有项目均需在本表体现

投标供应商全称（盖章）：

法定代表人（负责人）或授权代表（签字或盖章）：

日 期： 年 月 日

第七部分 评标定标办法

根据《中华人民共和国政府采购法》等有关政府采购法规，结合本次所要采购服务的实际，按照公平、公正、科学、择优的原则选择中标供应商，特制定本评标办法。

一、总则

评标工作遵循公平、公正、民主、科学的原则和诚实、信誉、效率的服务原则。本着科学、严谨的态度，认真进行评标。择优选定服务供应商，确保服务质量，最大限度的保护当事人权益，严格按照招标文件的商务、技术要求，对投标文件进行综合评定，提出优选方案，编写评标报告。评标委员会必须严格遵守保密规定，不得泄漏评标的有关情况，不得索贿受贿，不得接受吃请和礼品，不得参加影响公正评标的有关活动。对落标供应商，评标委员会不作任何落标解释。供应商不得以任何方式干扰招投标工作的进行，一经发现其投标文件将被拒绝。

二、评标组织

评标工作由采购人依法组建的评标委员会负责，评标委员会由采购人代表以及评标专家库中随机抽取的有关技术、经济专家共同组成。评标全过程由采购管理部门监督整个开标、评标和定标过程。

三、评标程序

1、开标后，采购人或采购代理机构对各投标人的资格进行审查；然后评标委员会对合格投标人的进行符合性审查，按照招标文件中规定的评标方法和标准，对符合性审查合格的投标文件进行商务和技术评估，综合比较与评价。

2、由评标委员会根据评审报告推荐综合得分第一名的供应商为中标人。如果第一名得分相同，以报价低的优先；报价也相同，以抽签随机决定。

3、中标人放弃中标，或者因不可抗力提出不能履行合同，或者招标文件规定应当提交履约保证金、签订合同而在规定的期限内未能提交、签订合同的，采购人可以取消其中标资格。并按供应商评标排序从高到低排序依次确定新的中标人或重新组织采购。

4、如果无候选供应商，或者侯选供应商因前款规定的同样原因不能签订合同的，本次采购失败，重新组织采购。

5、其它参见本采购文件第三部分：“供应商须知” 中的相关内容。

**四、评分细则**

一、商务报价评分30分

**1、以供应商有效投标价中的最低价为评标基准价，得满分30分。商务报价评分结算公式为:投标报价得分=****(评标基准价／投标报价)×30%×100。**

**注：符合招标文件规定条件的小、微企业（或监狱企业、残疾人企业），给予评标价格折扣（6%）。**

**2、本项目采购预算见采购公告。**如果所有供应商的报价均超出采购最高限价且采购人确认不能支付的情况，本次采购做流（废）标处理。如果仅仅某个（些）供应商的商务报价超出采购最高限价则该供应商按无效投标处理。

二、技术、服务、资信业绩综合评分70分

|  |  |  |
| --- | --- | --- |
| 评定项目 | 分值 | 备注 |
| 投标供应商资质 | 0-13分 | 1、投标供应商具有质量体系认证证书、环境管理体系认证证书、职业健康安全管理体系认证证书、信息技术服务管理体系认证证书（认证范围包含硬件运维服务），每提供一个证书得1分，最高得4分。2、投标供应商具有信息技术服务运营维护ITSS证书，得3分。3、投标供应商具有云管理服务评估证书（卓越级），得3分。4、投标供应商具有CMMI3及以上认证证书，得3分。注：①以上证书需提供复印件加盖投标人公章，否则不得分；②如投标人是金融、保险、通讯等特定行业的全国性企业所设立的区域性分支机构的，则上级机构（上级机构指总公司或总公司设立浙江省省级、温州市市级分支机构）具有以上证书均认可。 |
| 投标供应商同类业绩 | 0-3分 | 自2018年1月1日以来投标供应商有同类项目业绩，每个有效业绩1分。注：提供合同扫描件，业绩认定时间以合同签订时间为准。 |
| 技术力量 | 0-12分 | 1、投标供应商拟派服务于此次项目的项目负责人（一名）同时具有信息系统项目管理师（高级）、HCIE-CDO（华为认证云运维专家）或同级别的运维专家、ITSS IT服务项目经理的得4分,只具有其中一个证书得1分，2个证书的得2分。2、投标供应商拟派服务于此次项目的安全负责人（一名）同时具有CDPSE（数据隐私解决方案工程师）证书、CISSP (ISC)²证书（注册信息系统安全专家）、信息安全工程师证书（中级或以上）的得4分，只具有其中一个证书得1分，2个证书的得2分。3、投标供应商拟派服务于此次项目的项目团队具有大数据技术（中级及以上）、CDA数据分析师、MySQL OCP、CISP-CISE（注册信息安全工程师），每提供1类证书得1分，最多得4分。（同一人员不重复计分）注：以上人员须提供相关证书及所在磋商供应商单位连续缴纳近三个月的社保证明（若公司注册时间未满三个月的，出具书面说明）并加盖公章。 |
| 投标产品性能、参数符合性 | 0-30分 | 根据投标产品技术指标参数的响应情况，由评委打分，均无负偏离的得满分30分：1.标注“★”的重要技术参数负偏离的，每项扣1分2.其他技术参数偏离（包括不提供采购文件中要求的证书、测评报告、截图等无法证明无实际负偏离）的每项扣0.5分，备注：实质性条款除外；技术指标中的参数需逐条对应答复，如查实有任一投标产品技术参数有造假行为，将取消其中标资格。 |
| 核心设备厂商资质和能力 | 0-4分 | 投标供应商所投产品核心设备厂商具备以下能力认证，每提供一个证书得1分，最高得4分：1.具备信息系统建设及服务能力评估资质CS4级证书；2.具备中国保密协会出具的中国保密协会会员证书；3.具备工业信息安全产业发展联盟颁布的工业信息安全应急服务支撑单位证书；4.具备公安部第一研究所颁发的信息安全等级保护安全建设服务机构能力合格证书。 |
| 技术方案 | 0-2分 | 根据总体框架的设计方案、技术实现、思路清晰、设计合理、技术先进、结构完整进行评分，由评委综合打分。最高得2分。 |
|
| 售后服务方案 | 0-3分 | 1、根据售后服务承诺的范围和完善程度（包括售后服务标准、服务人员配备、故障响应修复时间方式及保障措施），由专家评审，最高可得1分。2、根据供应商售后服务网点的配置情况，由专家评审，最高可得1分。3、根据供应商是否针对本次项目建立专业的培训计划及培训服务，由专家评审，最高可得1分。 |
| 优惠条件 | 0-3分 | 1、企业专线一条（服务期三年，下行速率1G，含至少1个固定IP），0-1分2、根据供应商所投优惠条件综合对比打分，0-2分。 |

三、说明

1、每个供应商最终得分=技术资信部分分值（所有评标委员会成员打分的算术平均值）+商务报价部分分值。

2、评标委员会推荐得分最高的供应商为中标供应商，如果得分相同则以抽签决定，并编写评标报告。

3、所有分值计算保留小数点后二位，小数点后三位四舍五入。

参见本招标文件第三部分：“供应商须知” 中的相关内容，未尽事宜按有关法律规定处理。

四、注意事项

为确保评标工作的顺利进行，防止因泄密或其它意外而造成不良后果及影响，凡参加评标工作的人员都必须认真执行下面规定：

1． 在评标工作期间，所有分发的投标文件、资料等仅限于在评标场所中使用，不得带往其它地方。

2． 评标人员及工作人员不得在公共场合谈论有关评标内容。

3． 评标人员及工作人员不得以书信、电讯、口述等方式将有关评标内容（如资料、投标文件、报价、评标方式、评标委员会的决定、评标人员名单等）披露给未参加评标的任何无关人员，包括上级领导、同级和下级人员，任何与评标无关的人员（包括亲朋好友和同事）不得进入评标场所。

4． 任何需要向投标人进行询标的问题必须经评标委员会成员签字并由主询标人提出。在询标期间，对于涉及本规定保密范畴的所有内容，主询标人不得向投标人透露。

5． 任何评标人员和工作人员不得对外公布评标的一切内容。