

招 标 文 件

招标编号：ZHBRJ202201-26

项目名称：态势感知系统

招标内容：态势感知管理平台 威胁探针

湖北日报传媒集团招标采购部

2022 年 6 月

投标邀请函

请合格的投标人就“态势感知系统”采购项目提交密封投标文件。

有意向的投标人可在2022年6月10日—6月16日时间内,上午9:00至11:00时,下午2:30时至4:00(北京时间)到本部领取招标文件,或在湖北日报客户端、荆楚网客户端、<http://www.cnhubei.com> 下载招标文件。

投标人如有疑问,可致电胡先生,15972202401。

所有投标书应于2022年6月23日下午17:00前送达本部,逾期将不予接受。

开标一览表请单独封装在一个投票信封内,并注明“开标一览表”字样,放在投标文件正本中。

地址:武汉市武昌区东湖路181号楚天传媒大厦招标采购部B0132室

电话:027-88568112

联系人:胡先生

邮政编码:430077

湖北日报传媒集团招标采购部

2022年6月8日

第一章 投标人须知附表

序号	名称	内容规定
1	招标人	招 标 人：湖北日报传媒集团招标采购部 地 址：湖北省武汉市武昌区东湖路 181 号楚天传媒大厦 B0132 室 邮 编：430077 联 系 人：胡先生 电 话：027-88568112
2	项目名称	态势感知系统
3	投标人报名时间	2022 年 6 月 9 日至 2022 年 6 月 16 日 16 时 00 分止
4	投标截止时间	2022 年 6 月 23 日下午 17 时 00 分
5	递交投标文件地点(即开标地点)	武汉市武昌区东湖路 181 号楚天传媒大厦 B0132 室
6	投标文件份数	贰份(一正一副，并提交投标文件电子档，相关文件及资料不予退还)
7	评标小组的组建	评标小组构成：不少于 5 人，且为奇数。
8	中标通知	在中标通知书发出前，招标人将电话联系中标单位。
9	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；除招标文件中有特别规定外，仅适用于招标投标阶段的规定，按招标公告（投标邀请书）、投标人须知、评标办法、投标文件格式的先后顺序解释；同一组成文件中就同一事项的规定或约定不一致的，以编排顺序在后者为准；按本款前述规定仍不能形成结论的，由招标人负责解释。

第二章 投标人须知

一、项目介绍

- 1、项目名称：态势感知系统
- 2、招标单位：湖北日报传媒集团招标采购部
- 3、招标方式：公开招标
- 4、招标内容：态势感知管理平台 威胁探针

二、合格投标人条件

- 1、资格要求：依法依规登记设立，具有独立法人资格，并符合本招标文件资质能力要求的投标人；
- 2、信誉要求：遵守国家法律法规，诚实守信，信用中国近两年无市场不良行为记录。
- 3、如投标人代表不是法定代表人，须在投标文件中提供《法定代表人授权委托书》
- 4、参与本次招标投标活动的各方应对招标文件和投标文件中的商业和技术秘密保密，否则应承担相应的法律责任，并赔偿招标人因此遭受的损失。
- 5、投标人具有对所提供服务的维护能力。

三、招标文件说明

- 1、投标人应仔细阅读招标文件中的所有内容，按照招标文件及要求，详细编制投标文件，并保证投标文件的正确性和真实性。
- 2、投标人获取招标文件后，应仔细检查招标文件中的所有内容，如有疑问，应及时向招标人提出。
- 3、不按招标文件的要求提供的投标文件将被拒绝。
- 4、招标文件发出后，投标人在提交投标文件截止时间前，招标人如需对招标文件进行补充和修改，并发布相关澄清公告，澄清文件视为该招标文件的组成部分。

四、投标文件要求

（一）根据评标需要，投标人应按招标文件要求的格式制作投标文件，并装订成册。投标文件应包括下列部分：

- 1、投标函（按附件1格式）；

- 2、投标保证金（按附件 2 格式）；
- 3、法定代表人身份证明；
- 4、法定代表人授权委托书（按附件 3 格式）；
- 5、投标人相关资格证明文件。（正本必须提供加盖公章的彩色影印件，否则将被作无效投标处理）

- （1）法人或者其他组织的营业执照等证明文件，自然人的身份证明；
- （2）具备履行合同所必需的设备和专业技术能力的证明材料；
- （3）采购活动前 3 年内在经营活动中没有重大违法记录的书面声明；
- （4）具备法律、行政法规规定的其他条件的证明材料。
- （5）招标文件要求或投标人认为需提供的其它相关资格证明材料。

6、投标报价

（1）投标报价应包括招标文件及所注明的全部内容以及为完成上述内容所必须的部署、运输、安装、调试、税金等全部费用；一经中标，合同金额在合同期限内不做调整。

（2）投标人未计入或计算的招标范围内的设备及配件将被视为已包含在其投标报价中，投标人没有填写单价或合价的项目，招标人将拒绝承认和接受投标报价中未列出的任何费用，并认为这些项目的费用已经包括在报价单的其它单价或总价之中。

（3）投标方在运输和安装所需要的设备工具及人员的食宿由投标方自行解决。甲方为投标方提供必要的帮助。

（4）当单价与数量的乘积和总价不一致时，以单价为准。除非评标小组认为有明显的小数点错误，此时则以总价为准，并修改单价。

7、其他

以上资料如有复印件，须在复印件上加盖投标人公章。

投标文件须由投标人法定代表人或授权代理人签字，当由授权代理人签字时，须同时提交《法定代表人授权委托书》。

投标文件均需打印或用不褪色的书写工具书写，投标文件任何行间插字、涂改和增删，必须由投标人盖章确认方为有效。

投标文件一式二份（正本壹份，副本壹份）正本和副本如有不一致处，以正本为准。同一数字的表达不一致时，以大写为准。

投标文件装袋后应进行密封、封口应粘贴封口条，写上开标启封时间、加盖投标人单位公章和法定代表人印章。封口密封条贴在密封袋两端处且不得有任何修饰和其他痕迹。如果投标文件没有按上述要求密封，招标人将不承担投标文件提前开封的责任。

投标有效期为提交投标文件截止之日起 60 天，在此期限内，凡符合招标公告和招标文件的投标文件均保持有效。本次投标文件资料均不退还。

（二）投标人出现以下情况之一，其投标文件作废：

- 1、投标文件中有弄虚作假的内容。在签订合同之前，招标人如发现中标人的投标文件有弄虚作假内容，招标人可拒绝与其签订合同。
- 2、投标文件附有招标人不能接受的条件。
- 3、投标有效期不足。
- 4、按照相关法律法规，应视为废标的情形。

五、技术要求

1、态势感知管理平台技术要求

技术指标	指标要求
★硬件性能要求	平台采用软硬件一体架构 支持横向平滑扩展，可以通过增加硬件设备数量的方式，扩展平台集群的计算处理性能。 硬件性能要求：标准 2U 机架式硬件设备，CPU$\geq$20 核，内存$\geq$256GB，磁盘可用容量$\geq$40TB，接口要求$\geq$4 个千兆电口，$\geq$2 个万兆光口（含模块），冗余电源。 数据采集和处理性能$\geq$20000EPS 支持接入日志源数量$\geq$50 个 支持通过多种类型的安全、泛安全类数据接入采集解析，支持通过 TCP，UDP，Syslog，webService、SSH、JDBC、WMI、FTP、SNMP、SFTP、目录、文件等采集协议 支持自适应解析，采集自动匹配解析大部分设备日志能力
★大屏展示	支持不同安全视角的大屏展示功能，包括全网安全态势感知大屏、安全事件态势、通报预警态势、资产态势大屏等。支持态势大屏中相关信息下钻跳转到对应的详细页面。（要求提供截图并加盖厂商公章）
	支持对大屏界面进行二次微调，例如更换界面 logo
	支持安全态势的可视化呈现，以大屏的方式从攻击事件、资产安全、追踪溯源、运行监测等多个维度进行可视化展示，（要求提供截图并加盖厂商公章）

★威胁检测	海量数据的聚合分析可以发现潜在威胁，通过资产信息、安全知识库、弱点库三个维度聚合分析事件是否存在威胁，并形成关联事件，发现潜在威胁。
资产中心	支持通过流量自动发现资产，支持发现终端、服务器。
	支持对识别到的资产进行编辑，如添加主机名，划分系统和安全域
	支持以单个 IP 地址、IP 区间、子网掩码等 3 种模式录入安全域信息
脆弱性感知	支持具备弱口令风险、明文传输风险、HTTP 配置风险、中间件配置风险、数据库配置风险、服务配置风险等配置风险检测规则。并且对弱口令风险能显示账号密码和登入方式。（要求提供截图并加盖厂商公章）
	支持 Webshell 请求、XSS 攻击、SQL 注入、远程代码执行、命令注入、远程文件包含、本地文件包含、文件上传、路径遍历、信息泄露、越权访问、XXE 注入、网页篡改、SSRF 攻击等 Web 攻击检测，提供产品配置界面截图证明，并加盖公章。（要求提供截图并加盖厂商公章）
	支持通过总览、威胁源视角、受威胁资产视角，综合展示告警状态分布、告警级别分布、告警类型分布、告警阶段分布、告警趋势图（要求提供截图并加盖厂商公章）
	支持以告警归类视图、攻击者归类视图、受害主机归类视图查看告警信息，快速统计告警、攻击者、受害主机出现频率及关联情况（要求提供截图并加盖厂商公章）
	支持自动化溯源，可自动化复现受害者从最开始的遭受攻击到权限维持各个阶段的黑客行为，包括攻击入口溯源。支持基于可视化的形式展示威胁的影响面，通过大数据分析和关联检索技术，能够直观的看到失陷主机的威胁影响面，同时基于列表模式展示攻击、违规访问、风险访问、可疑行为、正常访问等详细信息。（要求提供截图并加盖厂商公章）

分析与处置中心	支持横向威胁分析，包括横向威胁总览、横向攻击、违规访问、可疑行为、风险；其中横向风险总览包括发起横向威胁主机排行、遭受横向威胁排行、横向威胁类型分布、横向威胁趋势。
	支持外连威胁分析，包括对外威胁总览、对外攻击、可疑行为、隐蔽通信、违规访问、服务器风险访问；其中外连威胁总览包括外连威胁主机类型分布、存在外连威胁 IP 排行、外连目标地区（国外）排行、外连威胁类型分布、外连威胁趋势。（要求提供截图并加盖厂商公章）
	支持挖矿专项检测，可实时查看挖矿各个攻击阶段，包括感染挖矿病毒、与控制端建立通信、获取挖矿任务、尝试挖矿、挖矿成功等；挖矿风险态势、受影响主机等维度分析统计。（要求提供截图并加盖厂商公章）
	支持横向访问服务器流量分析，包括应用流量趋势、协议趋势；支持服务器视角和来访分支视角，其中服务器视角可展示服务器 IP、总流量、源 IP 数量、连接失败数、最大并发，并支持以表格形式导出数据。（要求提供截图并加盖厂商公章）
报告中心	支持导出主机安全风险报告，报告内容包括业务与终端风险摘要、业务风险与终端详情分析，提供危害解释和参考解决方案；适用于日常处理安全问题的运维人员。也支持自定义时间导出报告。（要求提供截图并加盖厂商公章）
功能联动	支持与第三方安全设备，例如防火墙，ips，等进行联动处置，对发现的威胁进行自动化处置，阻断攻击流量。（要求提供第三方接入列表）（要求提供截图并加盖厂商公章）
	支持自动化编排的自定义处置流程策略的设置，灵活剧本设置，融入事件自动处置流程，节省运维处置时间，根据客户实际需要对接所需同品牌或者第三方品牌安全设备进行安全事件处置。（需提供厂商承诺函并加盖原厂商公章）
产品及厂商资质	★要求所投产品具备计算机信息系统安全专用产品销售许可证，提供有效证书复印件。

	★要求具备国家版权局颁发的软件著作权登记证书 考虑到国产化进程，本次采购态势系统支持信创产品
★服务要求	态势感知基于大数据架构，为了保证使用稳定可靠，以及前期交付产品的服务质量，原厂商应具有专业的大数据安全分析团队和云安全团队。
★质保授权	提供原厂商对本项目的授权和售后服务承诺函并加盖原厂公章 提供 5 年硬件质保及软件升级服务

2、威胁探针技术要求

★硬件性能指标及部署方式	探针数量=2 个 探针 1：标准 2U 机架式专用设备，吞吐$\geq 5\text{Gbps}$，万兆光口（含模块）≥ 4 个 探针 2：标准 2U 机架式专用设备，吞吐$\geq 10\text{Gbps}$，万兆光口（含模块）≥ 8 个 旁路部署，支持探针同时接入多个镜像口，每个口相互独立不影响，要求与态势感知平台产品同品牌。
★基础检测功能	旁路部署在核心交换机位置，不影响服务器处理性能和网络架构，通过接入核心交换机镜像流量，提供流量威胁检测分析，实现进行基于网络流量的恶意威胁分析，深度解析各种传播数据，从而发现各种网络入侵攻击等威胁行为，从而进行预防，同时将流量检测数据推送至态势感知系统进行集中存储分析，用于网络安全事件追踪和事件评估等。
敏感信息检测	支持敏感数据检测能力，具备弱口令风险、明文传输风险、HTTP 配置风险、中间件配置风险、数据库配置风险、服务配置风险等。（要求提供截图并加盖厂商公章）
★漏洞利用攻击检测	支持 Database 漏洞攻击、DNS 漏洞攻击、FTP 漏洞攻击、Mail 漏洞攻击、Network Device、Scan 漏洞攻击、System 漏洞攻击、Telnet 漏洞攻击、Tftp 漏洞攻击、Web 漏洞攻击等服务漏洞攻击检测。（要求提供截图并加盖厂商公章）

	支持 Application 漏洞攻击、File 漏洞攻击、Scan 漏洞攻击、Shellcode 漏洞攻击、System 漏洞利用攻击、Web Activex 等客户端漏洞攻击检测。（要求提供截图并加盖厂商公章）
异常流量检测	为满足溯源取证需求，对威胁告警进行调查分析，针对威胁告警支持原始数据包取证分析，告警详情支持查看、下载 PCAP 包。（要求提供截图并加盖厂商公章）
高级检测	支持传输安全检测日志，包括网络攻击检测日志、漏洞利用攻击检测日志、僵尸网络检测日志
	支持传输协议审计日志，包括 https 协议日志、http 协议审计日志、DNS 协议审计日志、邮件协议审计日志、SMB 协议审计日志、AD 域协议审计日志、WEB 登录审计日志、FTP 协议审计日志、Telnet 协议审计日志、ICMP 协议审计日志、LLMNR 协议审计日志。
违规访问检测	支持 IP，IP 组，服务，端口，访问时间等定义访问策略，主动建立针对性的业务和应用访问逻辑规则，包括白名单和黑名单方式。
管理功能	支持对设备进行运维操作； 可实时监控设备的 CPU、内存、存储空间使用情况； 能够监控监听接口的实时流量情况。
★部署	支持多台采集器同时部署于客户网络不同位置并将数据传输到同一套分析平台
★产品及厂商资质	要求所投产品具备计算机信息系统安全专用产品销售许可证，提供有效证书复印件。
	要求具备国家版权局颁发的软件著作权登记证书，提供有效证书复印件。
	要求所投产品具备中国国家信息安全产品认证证书，提供有效证书复印件。
★质保授权	提供原厂商对本项目的授权和售后服务承诺函并加盖原厂公章 提供 5 年硬件质保及软件升级服务

注：带“★”为必须满足指标

六、开标、评标及合同授予

（一）评审

- 1、检查投标文件是否完整、资格证明是否齐全、有无计算上的错误。
- 2、同一数值的表达不一致时，以文字表达为准。如投标人不接受对其错误的修正，其投标将被拒绝。
- 3、对于投标文件中不构成实质性偏差的不正规、不一致、或不规则，招标人可以接受，但这种接受可能会影响投标人的综合得分。
- 4、在详细评审前，评标委员会审查每份投标文件是否实质上响应招标文件的要求。
- 5、实质上没有响应招标文件要求的投标书将被拒绝。

（二）合同授予

- 1、《中标通知书》将作为签订合同的依据，也是合同文件的组成部分。
- 2、招标人发出中标通知书之后，双方基于招标文件和投标文件订立合同。
- 3、正式合同文本经双方确定后，投标人应及时签字、盖章，填写签署日期，尽快送达本部。

七、售后服务

投标人必须依据招标文件、投标文件及合同相关条款提供相应的售后服务。在合同约定的服务期内，投标人在接到招标人系统故障报告后，15分钟内响应，30分钟内做出诊断，2小时内达到现场并给出初步诊断，4小时内解决故障或提供替代方案（备件），若需返厂维修，维修期内提供备件不低于投标产品的性能指标。其他常规巡检、软件（固件）升级等周期性维护项目，以合同约定为准。

八、说明

本招标文件未尽事宜，按国家相关法律法规规定执行。

附件 1

投 标 函

致：湖北日报传媒集团招标采购部：

_____（投标单位全称）授权_____（全权代表姓名）_____（职务）为全权代表，参加贵方组织的_____（招标项目名称）招标的有关活动。我方已充分理解贵方本项目招标公告及招标文件的全部内容，包括补充、修改、澄清、答疑文件（如果有），我方接受招标文件的全部条款，且无任何异议。

如我方中标，我方保证按投标报价的优惠折扣签订合同，不因其他任何情况而改变折扣比率。

如我方中标，我方保证忠实地执行双方签订的合同，按贵方的委托要求按期、按质、按量履行合同义务。若在合同执行的过程中，发现货物质量、规格、性能、数量等有差异，我方一定尽快更换或退货，并承担相应的经济责任。

我方同意在本招标项目开标时间起 60 天内，遵守本投标文件的承诺，且在此期限内具有约束力。

本投标函附录是本投标函的组成部分。

在签订合同前，贵方的中标通知书连同本函及附录，对双方具有约束力。

与本投标有关的一切正式往来函件请寄：

地址：_____ 邮编：_____

电话：_____ 传真：_____

投标单位（公章）：_____

法定代表人（或授权人）签字并盖章_____

年 月 日

附件 2

投 标 保 证 书

湖北日报传媒集团招标采购部：

- 1、我方一定严格遵守相关法律法规参与本次项目投标。
- 2、若我方中标，按照贵方的招标文件，积极配合招标人签订合同，并按合同要求承担本项目的实施。
- 3、在正式合同订立之前，本投标书连同贵方中标通知书、以及其他文件和附件成为约束双方的合同。
- 4、我方对出具的业绩表、人员一览表以及反映我方实力及信誉的各种证明材料的真实性负责。如有虚假行为，无条件同意贵方取消我方的投标资格和中标资格。
- 5、我方同意从定标日起至双方签订的合同有效期内，严格遵守本投标书的各项承诺。本投标书始终对我方具有法律约束力。
- 6、我方承诺，若中标，本投标书中人员安排不做更换。

投标单位：（公章）

邮政编码：

投标单位地址：

法定代表人或其授权的代理人：（章）

联系电话：

传真号码：

日期： 年 月 日

附件 3

法定代表人授权委托书

本授权书声明：注册于_____（地址）的
（单位全称）的法定代表人_____（法定代表人姓名、职务）授权_____（被
授权人姓名、职务）为本单位的合法代理人，并将以本单位名义处理一切与
_____（招标项目名称）招标投标活动中的有关事宜，代理人（被
授权人）在本项目投标及合同中所签署的一切文件和处理的一切有关事宜，我单
位均予承认。

本授权书于_____年____月____日签字生效，特此申明。

法人授权代表（被授权人）情况：

姓名：_____ 性别：_____ 年龄：_____ 职务：_____

联系地址：_____

邮编：_____ 电话：_____ 传真：_____

授权单位（公章）：_____

法定代表人（签字或盖章）：_____

法人授权代表（被授权人）（签字）_____

授权日期：_____

注：无投标单位公章及法定代表人签章的视为无效授权。

年 月 日

