国药东风总医院
SDFGH 湖北医药学院附属东风医院

采 购 文 件

项目名称：国药东风总医院互联网边界安全相关设备维保及升级服务项目

2025 年 1 月

采购文件

一、采购书

1. 项目名称：国药东风总医院互联网边界安全相关设备维保及升级服务采购项目
2. 项目概况：详见采购文件
3. 项目限价：15 万元
4. 质保期限：自安装验收合格后之日起三年
5. 交货方式、地点：

   运输方式：由报价人自行确定（包装费、运输费及保险费，包含在总报价内）

   交货地点：湖北省十堰市大岭路 16 号

   收货单位：国药东风总医院

6. 货款结算方式： 甲方收到乙方开具的年服务费全额增值税发票，按照季度进行付款。每季度完成服务合格后，向乙方转账支付服务费
7. 报价时间：2025 年 1 月 3 日至 2025 年 1 月 8 日止
8. 报价方式：纸质报价文件（活页装订，编制页码，加盖骑缝章），一式两份
9. 采购人联系方式：

   联系单位： 国药东风总医院招标办

   招标办　　陈静　　13907280772

   信息中心　　何永钢　　18986911234

国药东风总医院

一、项目采购要求

1. 基本要求

1.1 供应商资质要求：

1.1.1 供应商应是注册于中华人民共和国的独立企业法人，满足采购文件要求资格的企业；

1.1.2 符合政府采购法第二十二条规定的供应商资格条件：

①具有独立承担民事责任的能力；

②具有良好的商业信誉和健全的财务会计制度；

③具有履行合同所必需的设备和专业技术能力；

④有依法缴纳税收和社会保障资金的良好记录；

⑤参加采购活动前三年内，在经营活动中没有重大违法记录；

⑥法律、行政法规规定的其他条件。

1. 1.1.3 应遵守《中华人民共和国政府采购法》《中华人民共和国民法典》《中华人民共和国产品质量法》等相关法律法规。

1.2 交货期：合同签订后，根据采购人实际需求，发送至采购人指定地点；

1.3 质量要求：经国家相关部门检测合格，有产品合格证、产品检测报告。

1.4 本项目不接受联合体投标，不允许转包。

2. 技术要求

2.1 投标产品需满足的性能、材料、结构、外观、质量、安全、技术规格、物理特性等要求；

2. 2.2 符合国家及行业其他现行的有关技术规范、质量标准及要求；

2.3 所投标产品质保期不低于三年，该项做为评标的计分项；

3. 2.4 中标人提供免费培训，至使用人员能够正常操作；

2.5 中标人应有相应的供货流程以及应急方案。对于提前识别和预防可能发生的重大隐患事故，提供完善详细的处理方案和处置措施；

2.6 中标人对招标人由于产品引发的医疗投诉（或纠纷）所产生的费用，由中标人承担。

2.7 本次中标价格为合同执行价格，如遇该产品在市内任何医院价格调整低于我院采购价时，应第一时间提供最新调价单并及时告知。

3 质保期、售后服务及验收要求

3.1 质保期：在产品有效期内出现非人为质量问题，中标人承诺无条件更换，以保证科室日

常工作使用；

3.2 中标人必须对于出现因不符合质量标准的产品负责包退包换（不合格产品包括产品质量问题、生产日期等）；

4 包装、保险及发运、保管要求

4.1 包装必须是制造商原厂包装，其包装均应有良好的防湿、防潮、防雨、防腐的措施。凡由于包装不良造成的损失和由此产生的费用均由中标人承担；

4.2 中标人负责将产品到现场过程中的全部运输，包括装卸车、现场的搬运及配合分发等；

4.3 必须提供产品清单，按清单验收产品；

4.4 货物至采购人指定的使用现场的包装、保险及发运等环节和费用均由中标人负责。

5 其它要求

5.1 投标人需要上传电子报价单，统一为 EXCEL 格式。

5.2 投标人应递交纸质版报价文件 2 份,递交时纸质文件按要求密封。密封包应写有业主和项目名称、供应商名称。封口骑缝处以显著标志密封,并加盖供应商公章。

5.3 书面报价文件与电子报价文件应当一致,若出现不一致的情况,以书面报价文件为准。若评标委员会认定书面报价文件与电子报价文件之间的关键项不一致,且影响评审时,评标委员会可否决其报价。

国药东风总医院互联网边界安全相关设备维保及升级服务采购需求

1．采购需求清单

序号	名称	子项	服务周期	单位
1	互联网边界安全相关设备维保及升级服务	边界安全态势感知系统维保及升级服务	3	年
		数据中心防火墙系统维保及升级服务	3	年
		上网行为管理系统维保及升级服务	3	年

2．技术服务具体要求

2.1 边界安全态势感知系统维保及升级服务具体要求

服务内容：对现有态势感知系统升级或提供更高性能的态势感知系统服务；主要功能要求以

下：

指标项	服务要求（标*为核心参数）
基本要求	能够及时发现威胁、阻断威胁、取证、溯源、响应、处置来自互联网的风险，能够实现智能检测、智能运维、智能防御，助力用户完成全流程威胁事件闭环。
服务模式	针对威胁告警定期进行巡检服务，出具威胁报告和处置建议，每年不低于 4 次
★联动要求	保证态势感知系统维保升级之后能与现有出口防火墙联动， 作为交付依据。
漏洞利用攻击检测（语义分析引擎）	支持通过漏洞利用攻击检测模型，对命令执行、XML 实体注入、未授权访问、权限绕过、解析漏洞、非 Web 攻击、SQL、XSS、CSRF、SSRF、拒绝服务、后门、反序列化、代码执行、代码注入、文件上传、权限不当、信息泄漏、未授权访问、不安全的配置、XXE、Xpath 注入、LDAP 注入、目录穿越、扫描器探测、水平权限绕过、垂直权限绕过、文件修改、文件读取、文件删除、逻辑错误、CRLF 注入、模版注入、点击劫持、缓冲区溢出、整数溢出、格式化字符串、条件竞争、超时等漏洞利用攻击行为进行深度检测，并输出安全事件
	★支持基于语义分析的漏洞利用检测，对 sql 注入、XSS、命令注入行为进行语义分析检测，并输出安全事件（提供产品功能截图证明并加盖原厂公章）
	支持通用漏洞利用检测，通过分析各类漏洞利用的相同点，形成通用漏洞检测规则，可用于发现 0day 安全事件
反弹 shell 检测	★支持通过反弹 shell 检测模型，对执行代理工具 shell 等黑客发起的攻击行为（加密丨非加密）进行深度检测，并输出安全事件（提供产品功能截图证明并加盖原厂公章）
	支持黑客常规反射 shell 行为检测，并输出安全事件
加密流量检测	支持加密流量指纹 JA3、JA3S 和 SSL 检测
	支持加密情况下反弹 shell 检测
异常扫描行为检测	支持有效识别 nmap、sqlmap、Gobuster、WebCruiser、N-Stalker、W3af、Awvs、Netsparker 等类型扫描器发起的网络扫描行为，并输出安全事

	件
	支持黑客扫描 webshell 后门检测，准确识别黑客扫描 webshell 后门行为，并输出安全事件
	支持有效识别常见的端口扫描、目录扫描、主机存活扫描等扫描活动；能够有效识别特定场景下 Fastjson 探测、利用空间测绘引擎收集各类资产信息等活动，并输出安全事件
	支持有效识别 crawlergo 爬虫等各类爬虫探测行为，并输出安全事件
信息收集行为检测	支持针对 Fastjson 版本信息探测、Weblogic 黑名单探测等应用信息收集行为进行有效检测，并输出安全事件
	支持利用空间测绘引擎收集信息等行为检测，并输出安全事件
挖矿行为检测	支持通过挖矿分析模型，对主机与矿池通信连接行为、协议等进行深度检测，检测矿池包含但不限于：XMRig 工具、Stratum 挖矿协议等，并输出安全事件
自动化攻击工具检测	★支持各类扫描、漏洞利用、远控、横向移动、webshell、权限维持工具检测，检测工具类型不少于 260 种；（提供产品功能截图证明并加盖原厂公章）
虚拟化环境检测	专项支持如 VMware、vcenter、esxi 等针对虚拟化环境的攻击检测支持，并输出安全事件
Webshell 攻击检测	支持通过 Webshell 攻击检测模型对常见 Webshell 工具发起的攻击行为进行深度检测，工具类型包含但不限于：蚁剑、冰蝎、哥斯拉等；支持 Webshell 攻击检测，并输出安全事件
远程代理攻击检测	支持 HTTP 代理下使用 ABPTTS、Chisel、reGeorg、Tunna、Neo-reGeorg 等渗透工具进行远程代理攻击行为检测，并输出安全事件
	支持非 HTTP 代理下使用 Earthworm、frp、Ngrok、nps、Stowaway、Termite、Venom 等渗透工具进行远程代理攻击行为检测，并输出安全事件
	支持通过商业远控检测模型，对 AnyDesk、向日葵、Teamview、ToDesk 等商业远程工具发起的远程控制行为进行检测、并输出安全事件
隐蔽隧道检测	支持 ICMP 隧道深度检测；支持对 icmptunnel、icmpsh、Nishang 等隧道检测工具发起的隧道构建行为进行识别，并输出安全事件

	支持 DNS 隧道深度检测；支持对 dns2tcp、iodine、dnscapy、dnsteal、DnsShell、OzymanDNS 等 DNS 隧道构建行为进行识别，并输出安全事件
	支持通过 ICMP 隐蔽隧道检测模型，对未知 ICMP 隐蔽隧道进行分析，并输出安全事件
	支持通过 DNS 隐蔽隧道检测模型，对未知中继型 DNS 隐蔽隧道进行分析，并输出安全事件
主机受控检测	支持通过 DGA 域名检测模型，对黑客利用随机字符生产 C&C 域名逃避检测的行为进行深度检测；检测模型能够覆盖基于算数算法编码、基于哈希表示、基于辞典组合、基于排列组合等方式生成的随机域名及黑客行为，并输出安全事件
	支持通过 C2 检测模型对 Cobalt Strike HTTP 上线、Cobalt Strike DNS 上线、Metasploit TCP 上线、Metasploit HTTP 上线等远控活动进行深度检测，并输出安全事件
	内网主机疑似失陷后对外异常攻击
登录风险检测	支持通过登录检测模型，对登录过程中输入的弱口令进行深度检测，并输出安全事件
	支持通过登录检测模型，对登录爆破行为进行深度检测，并输出安全事件
	★支持对部分非明文传输密码的登录协议弱口令进行检测，如 mysql、pgsql，并输出安全事件（提供产品功能截图证明并加盖原厂公章）
内网横移检测	支持内网中各类漏洞攻击行为检测，如永恒之蓝，并输出安全事件
	★支持内网横移手段的检测，如 Windows 通过 SMB/DCERPC 远程添加服务、Windows 通过 SMB/DCERPC 共享添加计划任务、通过 PsExec 进行远程控制等，并输出安全事件。（提供产品功能截图证明并加盖原厂公章）
	★支持内网权限提升手段的检测，如 MS14-068、Zerologon CVE-2020-1472、PrintNightmare 等，并输出安全事件（提供产品功能截图证明并加盖原厂公章）
	★支持内网权限维持手段的检测，如 Kerberos 万能钥匙（Skeleton

	Key），并输出安全事件（提供产品功能截图证明并加盖原厂公章）
	★支持内网环境中敏感行为、危险调用检测检测，如 Kerberos 票据加密方式降级、LDAP 敏感操作等，并输出安全事件（提供产品功能截图证明并加盖原厂公章）
	支持内网环境中账户爆破检测、如 kerberos 账户爆破、SMB 账户爆破、LDAP 账户爆破
攻击链检测	支持通过攻击杀伤链模型从侦查、入侵、命令与控制、横向移动、达成目标等阶段对各类攻击进行层次划分，利用攻击特征、攻击结果、攻击时序等因素进行综合分析对事件进行标识
威胁情报集成	支持矿池类情报告警，并输出安全事件
	支持病毒、木马类情报告警，并输出安全事件
	支持 c2 类情报告警，并输出安全事件
攻击结果研判	★支持通用失败研判，对攻击事件进行分析，判断此次攻击结果是否为失败
	支持命令执行成功研判，对攻击事件进行分析，判断此次攻击结果是否为成功
	★支持文件读取成功研判，对文件读取类攻击事件进行分析，判断此次攻击结果是否为成功
	★支持弱口令登录结果研判，对弱口令登录事件，判断弱口令是否有效
	★支持登录接口爆破结果检测，对登录爆破检测，判断是否爆破成功，并输出安全事件
	★支持 SQL 注入成功研判，对 SQL 注入类事件进行分析，判断此次攻击结果是否为成功
	★支持反连成功研判，对反弹 shell、ssrf、jndi 等攻击，提取反连 IP/域名，分析受害主机是否连接该 IP/域名，判断此次攻击结果是否为成功（提供产品功能截图证明并加盖原厂公章）
旁路阻断	支持通过 TCP RST 方式旁路对攻击会话发送双向 RST 包，关闭攻击会话以达到阻断攻击目的
	支持添加阻断策略，阻断对象包括 IP、IP+端口等；支持设置策略失效时间

	支持阻断记录功能，可以查看阻断相关 IP、策略以及阻断时间等信息，并可以按照时间、IP、端口、阻断策略等条件对阻断记录进行快速筛选
联动阻断	支持联动防火墙对检测到的攻击 IP 进行阻断，并可查看阻断记录
	★支持与 HIDS 产品联动，将检测到的攻击 IP 下发到主机侧做快速隔离处置
	★支持与 WAF 产品联动，将检测到的攻击会话下发到 WAF 做快速阻断处置

2.2 数据中心防火墙系统维保及升级服务

指标项	服务要求（标*为核心参数）
服务内容	提供现有奇安信防火墙（奇安信 NSG5000 系列火墙）维保及升级服务，或更新为更高性能的数据中心防火墙产品，包含 3 年全功能模块升级订阅服务包（含应用识别库、URL 分类特征库、病毒防护特征库、入侵防御特征库升级服务及威胁情报订阅服务）

2.3 上网行为管理系统维保及升级服务

指标项	服务要求（标*为核心参数）
服务内容	提供现有上网行为管理（奇安信 NI5200-30）维保及升级服务或更新为更高性能的上网行为管理产品，包含 3 年 URL 库、应用协议库定期更新服务，提供软件版本功能优化与性能提升。

4. 评分标准

评标项目	评标分项	分值	子项目及分值
价格评审（30 分）	投标报价	30 分	报价得分统一采用低价优先法计算，即满足招标文件要求且最后报价（落实政府采购政策进行价格调整的，以调整后的价格计算）最低的供应商的价格为评标基准价，其价格分为满分。其他供应商的价格分统一由评标委员会按照下列公式计算：报价得分=（评标基准价 / 投标报价)×30%×100
商务评审（20 分）	类似业绩	3 分	供应商提供近三年（至响应文件递交截止时间往前推算三年，以合同签订时间为准）类似项目业绩，每提供一个得 1 分，最多 3 分（提供合同扫描件加盖公章，未提供不得分）。
	拟派人员	4 分	1、供应商拟派项目负责人具有 IT 服务项目经理及信息系统项目管理师（高级）得 1 分；（提供项目负责人近 3 个月的社保证明和证书扫描件并加盖供应商章，未提供不得分。） 2、供应商拟派团队人员具有 CISP 证书（种类涵盖 CISO、CISE 和 CISP-PTE 等）的，每提供一项得 1 分，本项目最多得 3 分。（提供人员近 3 个月的社保证明和证书扫描件并加盖供应商章，未提供不得分。）
	履约能力	7 分	1、供应商具有有效的 CCRC 信息安全服务资质认证(安全集成)二级及以上证书得 4 分。（提供证书扫描件并加盖供应商章，未提供不得分。） 2、供应商具有有效的信息技术服务运行维护标准符合性（ITSS）证书二级及以上证书得 3 分。（提供证书扫描件并加盖供应商章，未提供不得分。）
	体系认证	6 分	1、供应商具有有效的 ISO20000 IT 服务管理体系认证证书，得 2 分； 2、供应商具有有效的 ISO27001 信息安全管理体系认证证书，得 2 分； 3、供应商具有有效的 ISO9001 质量管理体系认证证书，得 2 分； 备注：以上认证证书应同时提供认证证书及在“国家认证认可监督

			管理委员会（https://www.cnca.gov.cn/）”官网查询截图，一个不提供 扣 2 分，全部提供得 6 分。
技术评审（50 分）	技术参数响应情况	43 分	所有投标产品的技术参数，性能及功能完全满足招标文件要求，标注★号为重要技术指标，每出现一项不满足要求的，扣 3 分，其它一般功能技术指标，每出现一项不满足要求的，扣 1 分，扣完为止。（标注★的技术参数须按招标文件 “采购需求及相关要求”中提供相应证明材料，否则视为不响应。）
	培训方案	2 分	投标人应根据本项目得采购需求和投标人要求提供详细的培训方案及培训计划，提升采购人相关产品运维水平。根据培训人员、时间、内容的合理性、可操作性得 2 分；方案较合理性、具有可操作性得 1.5 分；方案一般、可行性低得 1 分
	服务方案	5 分	具有完善具体可行的服务方案和服务能力，服务便捷、响应速度快，各阶段服务方案详尽，满足采购人需求，得 5 分; 有提供服务方案，且有一定的可行性，服务较便捷，响应及时，各阶段服务方案完整， 基本满足采购人需求，得 3 分; 有提供服务方案，但可行性不强，服务内容及各阶段服务计划完整性有缺漏，得 1 分；未提供方案不得分。
总分		100 分	