**安徽华佗智慧中医药服务平台采购项目**

**（二次）更正公告**

一、项目基本情况

原公告的采购项目编号：BZSJ2024CG190号

原公告的采购项目名称：安徽华佗智慧中医药服务平台采购项目（二次）

首次公告日期：2024年8月8日

二、更正信息

更正事项：□采购公告☑采购文件 □采购结果

更正内容：质疑1. 招标文件第四章采购需求-硬件清单-3.双活超融合集群：一、提供承诺函，要求与现有超融合实现无缝兼容储双活、虚拟机双向平滑漂移。二、服务器虚拟化模块：2.支持无代理跨物理主机的虚拟机映射，且虚拟机迁移到其它物理主机后，仍能正常使用迁移前所在物理主机上的资源，对于业务的自适应能力、使用便捷性更佳；三、网络虚拟化模块：2.支持对oracle、sqlserver、Weblogic、国产数据库等数据库及中间件监控，实现对数据库的语句的故障定位排错，执行时延分析；4.分布式防火墙基于监测虚机IP地址和端口进行东西向流量隔离控制，并提供实时拦截日志，以及支持“数据直通旁路”功能，方便出现问题快速定位问题；6.提供虚拟路由器、虚拟交换机等设备的连通性探测功能，能够定位到出现故障的虚拟网络设备，排查到ACL策略配置错误；四、存储虚拟化模块：2.支持多种硬盘状态检测监控及告警，包括“健康”状态、“亚健康”状态、“故障”状态，不同状态的硬盘在UI上呈现不同的特征或告警，让用户能够区分处理；3.支持回收站一键还原已删除的虚拟机，可恢复30天内已删除的虚拟机；五、云管理平台：5.云平台具备对资源池中CPU、网络、磁盘使用率等指标进行实时的数据统计功能，并支持针对租户使用的CPU、内存和存储等维度的资源进行计费，并提供报表功能。以上参数要求仅深信服一家厂家满足，有严重的倾向性的问题。

回复:市场上主流厂家（包含但不限于SmartX、浪潮、中国电子云）均满足此配置要求。当前主流超融合厂家为华为、华三、深信服等厂商，贵单位给出的建议厂商都是在云计算领域，且奇安信、360和绿盟都无超融合产品。故按招标文件执行。

质疑2. 招标文件第四章采购需求-硬件清单-5.主动防御系统：▲2、支持多样性的挖矿检测手段，能够检测挖矿信息、矿池域名解析、挖矿阶段、矿池协议等；矿池协议告警须提供虚拟币种类别；挖矿告警须提供专项告警页面，独立于其它告警；能够自动解析DNS响应的矿池及IP地址。▲9、支持失陷主机智能研判：支持追踪到失陷主机IP号，攻击阶段数，命中规则数，攻击次数，是否外联，风险值等能力；能够提供攻击详情分析，包含攻击结果，攻击者信息，攻击时间线，攻击规则汇总，入侵检测攻击上下文等；支持报告详情下载。以上参数属于深信服主动防御系统独有，限制了其他设备厂商公平参与的机会的问题。

回复：市场上主流厂家（包含但不限于奇安信科技、亚信安全、深信服科技等）均满足此配置要求。故按招标文件执行。

质疑3. 招标文件第四章采购需求-硬件清单-6.WEB应用防护系统：2、支持旁路流量牵引部署方式，通过BGP路由牵引和SNAT回注方式对流量进行过滤；旁路部署对镜像流量分析的同时实现阻断功能，产品具备专门的阻断接口设置和对端MAC地址设置功能；3、支持静态路由、策略路由等路由配置；支持802.1Q协议，支持Vlan解码，在Trunk线路上部署并提供防护；支持ARP协议，对静态、动态ARP进行绑定；5、支持威胁情报中心联动功能，基于FTP或FTPS协议登录云端；对威胁情报中心提供的相关数据运用到产品防御策略中，提供基于僵尸网络、恶意IP、扫描刺探、Webshell、代理IP、漏洞利用、暴力破解、恶意代码以及木马蠕虫等情报类型； 7、支持蜜罐防御功能，提供伪造的后台管理系统页面防御功能；8、支持检测TCP并发链接数，TCP新建链接数，TCP带宽（c2s），UDP带宽（c2s），ICMP带宽（c2s），HTTP GET 速率，HTTP POST 速率，HTTP 其他请求速率，DNS 查询请求速率，并发IP数量等单用户和总量进行自定义阈值配置；9、支持windows、linux的32位与64位操作系统的网页防篡改功能，并提供相应的客户端下载功能；10、支持安全态势大屏实时展示，可通过产品自带的实时态势监测模块进行攻击态势地图展示，包含对源地域、目标资产、安全防护攻击类型、攻击趋势、HTTP并发请求及实时事件统计；11、支持移动终端管理功能，支持移动终端对设备的一键管控功能，支持网站一键下线的终端应急措施。以上参数属于深信服WER应用防护系统独有，限制了其他设备厂商公平参与的机会的问题。

回复：市场上主流厂家（包含但不限于奇安信科技、亚信安全、深信服科技等）均满足此配置要求。按招标文件执行。

质疑4. 招标文件第四章采购需求-硬件清单-7.网络台式感知探针：▲1、硬盘容量≥128G minisata SSD，提供承诺函，承诺与现有态势感知平台实现无缝对接，提供5年产品质保及软件升级；2、支持命令注入检测、PHP代码检测、XSS攻击检测、Webshell上传检测、SQL注入检测、XXE攻击检测、JAVA代码检测、SQL非注入型检测、MYSQL解析增强、php反序列化检测等自定义配置启用，针对命令注入检测、SQL注入检测等类型支持自定义高检出、低误报模式。3、支持IP，IP组，服务，访问时间等定义违规访问策略，主动建立针对性的业务和应用访问逻辑规则，针对目标IP（组）已开放的服务，白名单策略只允许白名单里的IP（组）在指定的时间内访问，其他时间或其他IP的访问均被视为违规，黑名单策略禁止黑名单里的IP（组）在指定的时间内访问，否则将被视为违规。4、支持检测出网络中的网络拓扑设备进行绘制，更直观可视化查看网络整体情况5、支持基于IP和域名的旁路阻断，能够在实时镜像的流量中发现恶意IP并实现实时阻断，支持24小时/7天/最近30天/永久或者自定义时间阻断威胁。6、支持HTTP未知站点下载可执行文件、浏览最近30天注册域名、浏览恶意动态域名、访问随机算法生成域名、暴力破解攻击、反弹连接、IRC通信等僵尸网络行为检测。以上参数属于深信服网络态势感知探针独有，限制了其他设备厂商公平参与的机会的问题。

回复：市场上主流厂家（包含但不限于奇安信科技、亚信安全、深信服科技等）均满足此配置要求。按招标文件执行。

质疑5. 招标文件第四章采购需求-硬件清单-8.备份一体机：4、支持对X86架构物理机、虚拟机、超融合架构和云主机等多种平台提供持续数据保护 (CDP) ，备份时间粒度最小可达百万分之一秒，实现近乎零的 RPO 。5、配置定时备份无限授权许可，配置无限制客户端定时备份授权许可以及无限制虚拟机定时备份授权许可。6、支持在千兆网络环境下，无论数据量大小，在 15 分钟内完成裸机恢复，快速恢复应用系统对外提供服务，最大程度减少业务中断时间。确保业务始终保持连续运行，避免因数据丢失或系统故障造成的损失。9、支持可无需停止备份任务，即可随时随地进行验证，确保数据始终处于可恢复状态，支持同时验证多个备份点。 11、支持按时间节点编排自动的主机验证计划，无需停止备份任务，按照设定时间节点开启和释放自动化验证主机所需资源。12、支持X86/虚拟机/云主机的整机快照、持续数据保护、分钟级业务恢复重建、数据去重与合并、多级恢复验证（WindowsSever和linux备份代理程序，无系统X86/虚拟机/云主机裸机、WindowsSever、linux国产操作系统还原代理）；12T灾备容量授权。以上参数属于深信服备份一体机独有，限制了其他设备厂商公平参与的机会的问题。

回复：此为备份一体机硬件服务器的基础需求，且市场上主流厂家（包含但不限于奇安信科技、亚信安全、深信服科技等）均满足此配置要求。故按招标文件执行。

质疑6. 招标文件第三章评审办法（三）综合评审表服务技术方案技术参数响应，“技术参数须满足项目需求，每满足一项带“▲”参数的得 2分，满分 52 分。注：招标文件中要求提供的相关证明材料（如资质证书、检测报告、截图等），硬件部分，供应商在投标时按照招标文件采购需求硬件技术参数的要求提供资质证书、检测报告、截图、承诺函等；软件部分，供应商在投标时提供响应承诺函。未按要求响应的视为该项负偏离，则不予得分。” 1、招标文件第四章采购需求3.3建设清单3.3.2硬件清单万兆交换机参数中“6.设备支持 AAA、RADIUS 认证、HWTACACS、PKI 等安全特性，提供官网截图并加盖公章；”。2、招标文件第四章采购需求3.3建设清单3.3.2硬件清单主动防御系统参数中“▲2、支持多样性的挖矿检测手段，能够检测挖矿信息、矿池域名解析、挖矿阶段、矿池协议等；矿池协议告警须提供虚拟币种类别；挖矿告警须提供专项告警页面，独立于其它告警；能够自动解析DNS 响应的矿池及 IP 地址。”。3、招标文件第四章采购需求3.3建设清单3.3.2硬件清单主动防御系统 参数中“▲9、支持失陷主机智能研判：支持追踪到失陷主机IP号，攻击阶段数，命中规则数，攻击次数，是否外联，风险值等能力；能够提供攻击详情分析，包含攻击结果，攻击者信息，攻击时间线，攻击规则汇总，入侵检测攻击上下文等；支持报告详情下载；”。

回复：1、招标文件第四章采购需求3.3建设清单3.3.2硬件清单万兆交换机参数中“6.设备支持 AAA、RADIUS 认证、HWTACACS、PKI 等安全特性，提供官网截图并加盖公章；”。该项不做修改，按原招标文件执行。

2、招标文件第四章采购需求3.3建设清单3.3.2硬件清单主动防御系统 参数中“▲2、支持多样性的挖矿检测手段，能够检测挖矿信息、矿池域名解析、挖矿阶段、矿池协议等；矿池协议告警须提供虚拟币种类别；挖矿告警须提供专项告警页面，独立于其它告警；能够自动解析DNS 响应的矿池及 IP 地址。”该项不做修改，按照原招标文件执行。

3、招标文件第四章采购需求3.3建设清单3.3.2硬件清单.主动防御系统 参数中“▲9、支持失陷主机智能研判：支持追踪到失陷主机 IP 号，攻击阶段数，命中规则数，攻击次数，是否外联，风险值等能力；能够提供攻击详情分析，包含攻击结果，攻击者信息，攻击时间线，攻击规则汇总，入侵检测攻击上下文等；支持报告详情下载；”。该项不做修改，按照原招标文件执行。

质疑7. 招标文件中第四章采购需求.3.3建设清单3.3.2硬件清单中，非▲项的参数未明确在何时进行核验的问题。

回复：招标文件第四章采购需求6. 其他要求.三、注意事项：“3.对于“采购需求”中要求提供（具有）的证书、检测报告及其他有关证明文件，投标时不作要求，供货时交采购人核验，如发现弄虚作假或不能提供齐全的，将向政府采购监管部门报告，按有关规定进行处理。如有关要求与本条内容不一致，则以本条内容为准。”对此种情形已有明确规定。不做修改，按原招标文件执行。

质疑8. 采购需求-硬件清单标▲项，要求不明确的问题。

回复：按招标文件执行，招标文件中要求提供的证明材料须按要求提供，未要求提供证明材料的，投标人须提供承诺函。

更正日期：2024年8月16日

三、其他补充事宜

1.本更正公告为采购文件组成部分，与采购文件具有同等法律效力。之前发布的文件与本公告不一致的，以本公告为准。

2.其他事项暂不作调整，请按采购文件执行。

四、凡对本次公告内容提出询问，请按以下方式联系。

1.采购人信息

名称：亳州市中医院

地址：亳州市谯城区北一环与魏武大道交叉口西200米

联系方式：0558-5515970

2.采购代理机构信息

名 称：亳州市公共资源交易中心

地 址： 亳州市希夷大道455号市政务服务中心五楼F519室

联系方式： 0558-5991075

3.项目联系方式

项目联系人： 马工

 电 话： 0558-5991075

2024年8月16日