遵义市播州区人民医院
People's Hospital Of Zunyi City Bo Zhou District

遵义市播州区人民医院
关于外联安全建设项目采购的内部竞争性磋商公告

一、项目基本情况

项目编号：BYC-2023-ZX009

项目名称：外联安全建设项目采购

采购方式：内部竞争性磋商

采购限价： \

资金来源：自筹

采购需求：

项目编号	产品名称	数量	单位	采购限价	备注
BYC-2023-ZX009	外联安全建设项目采购	1	批	\	

技术参数及服务要求

序号	服务项	服务内容要求	数量	单位	备注
1	网闸	1.内网接口：不少于6个10M/100M/1000M电口（其中包含1个管理口、1个HA口），6个SFP插槽，2个SFP+插槽。外网接口：不少于6个10M/100M/1000M电口（其中包含1个管理口、1个HA口），6个SFP插槽，2个SFP+插槽。 2.整机吞吐量700M，并发连接数不低于6万，系统延迟小于1ms。 3.采用“2+1”系统架构，即由两个主机系统和一个隔离交换专用硬件组成；隔离交换矩阵基于专用芯片实现，保证数据在搬移的时间内，内、外网隔离卡与内、外网系统为断开状态。 ★4.内外网主机系统分别支持双系统引导，并可在WEB界面上直接配置启动顺序，在A系统发生故障时，可以切换到B系统；且支持系统(包括配置)备份；（提供产品功能界面截图证明，并加盖原厂公章）； ★5.支持HTTPS的Web方式管理，实现了远程管理信息加密传输；（提供产品功能界面截图证明，并加盖原厂公章）； 6.支持断点续传；支持增量传输、发送后删除、发送后转移、改名传输等发送策略；支持文件传输方向可控，实现单向或双向传输； ★7.可对用户的客户端版本和进程进行检查，进行准入控制；（提供产品功能界面截图证明，并加盖原厂公章） 8.支持对外开启WEB服务，供用户登录进行文件上传/下载操作;支持两种文件存储方式,设备本地硬盘或远端samba共享。; ★9.支持单主键、多主键表结构；数据库同步客户端（非浏览器）支持Windows、Linux等主流平台，均具备图形化管理界面；支持Oracle、SQLServer、Sybase、Db2、MySQL、MongoDB等主流数据库；支持病毒检测； 10.支持同种数据库间（同构）和不同种数据库间（异构）的	1	台	

		同步；支持数据库表及字段级的同步；支持同步库中初始数据功能； 11.支持对多种（如 MySql、SqlServer、Oracle、DB2、Sybase）等主流数据库系统的安全访问；提供数据库访问用户的过滤和控制；持访问时段控制；提供数据库传输告警事件的日志； ★12.采用自有知识产权的病毒防范引擎引擎（提供相关专利证明，并加盖原厂公章），支持抗攻击功能，能够识别和防御 SYNFlood、ICMPFlood 等攻击。			
2	未知威胁发现设备	1. 1U 标准机架式设备，接口数量≥6 个千兆电口，吞吐量≥1.5Gbps，内存≥32G，硬盘容量≥4T，可扩展插槽≥2 个，沙箱个数≥1 个，电源：冗余电源。 2.支持侦测各种文件型病毒，如勒索病毒、木马、僵尸、后门等，并支持多种高危病毒的侦测； 3.支持威胁流量与协议异常检测，如勒索病毒、零日攻击、网络蠕虫、木马、后门、僵尸、间谍软件、网络漏洞、网页威胁（网页漏洞、跨网站攻击）、暴力攻击、数据库注入攻击等； ★4.支持多样性的挖矿检测手段，能够检测挖矿木马投递、挖矿木马横向移动行为、挖矿软件、矿池域名解析、矿池连接、矿池协议等，需提供产品功能截图； 5. 支持自动研判功能，能够对攻击方向、攻击结果进行自动判定，并在告警中展示攻击结果。对于聚合后的告警，能展示不同攻击结果的次数。 ★6.支持内置沙箱系统，内置沙箱允许用户导入自定义镜像，需提供产品功能截图； 7. 支持按照网络攻击、挖矿、扫描、暴力破解、恶意文件、威胁情报等告警进行分类，需提供产品功能截图； 8. 支持威胁分类统计数据，排名前五的病毒事件，失陷风险最高的 TOP5 主机，攻击源和攻击目标地理位置展示。 9. 能够以文件为中心，溯源整个文件的流转记录，并以图形化方式展示出来，需提供产品功能截图； ★10.支持失陷主机的智能研判，能够追踪到失陷主机 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，需提供产品功能截图；	1	台	
3	态势感知	1. 2U 机架式机箱，内存≥256GB，硬盘总容量≥48TB（支持 RAID），网口≥6 个千兆电口；配备双电源。 2.支持日志源数量≥200 个；最大支持接入探针流量≥2Gbp；数据采集和处理性能≥20000EPS。 3.支持通过 TCP，UDP，Syslog，WebService、SSH、Telnet、JDBC、WMI、FTP、SNMP、FTP、SFTP、HDFS、目录、文件等采集协议，实现 100+种常用设备的告警日志直接接入平台，无需单独部署日志采集设备； 4.支持提取 IP、端口、域名、URL 等信息与本地威胁情报库的失陷库碰撞，命中威胁情报生成告警，需提供产品功能截图； 5.支持设置事件类型、事件等级、处置状态、攻击阶段等查询	1	台	

		条件，筛选出符合条件的安全事件，需提供产品功能截图； 6.支持规则引擎和融合建模，对原始日志或内部事件，进行关联、聚合分析等操作后形成安全事件；基于安全规则分析、融合关联分析引擎，对多源告警进行关联，支持对告警进行聚合，安全告警中识别出安全事件，治理告警风暴； 7. 支持资产探测任务，以 IP 或者 IP 段、端口或者端口段进行扫描，能够识别操作系统、开放端口、开放服务、MAC 地址、资产名称，所得的资产数据可以自动或者人工确认装载到资产数据库进行统一管理，需提供产品功能截图； 8.支持基于 IP 的威胁狩猎，实现风险钻取分析功能，可根据攻击者和受害者等不同纬度的风险要素对整网安全进行逐层分析和逐级追踪，可以从系统内所有的 IP 进行下钻分析，聚合关联与该 IP 相关的所有安全告警与访问信息，以时序方式呈现资产遭受的攻击全过程需； 9.支持在狩猎查询阶段，根据不同的时间维度，查看可疑 IP 的基本资产信息，并且能够查看该 IP 的威胁情报信息，提供产品功能截图； 10. 支持安全报告模板，提供安全日报、安全周报、安全月报等报告生成功能，报告内容包括系统的资产信息、安全告警、监测结果、处置建议等信息。 11.支持对原始日志的全文检索，可通过来源 IP、目标 IP、源端口、目的端口、威胁类型、威胁等级、资产组、时间段等单个条件或多种条件进行组合查询； 12. 兼容云主机深度安全防护系统应用软件联动，提供服务器病毒一键查杀、Web 病毒一键查杀、挖矿检测防护、主机异常监控、勒索漏洞防护、漏洞攻击防护、应用漏洞防护、资产勒索防护、域名勒索防护等剧本，需提供产品功能截图； 13. 支持从网络流量被动发现资产信息，探测到的资产数据自动装载到资产数据库，支持记录资产变更记录； 14. 支持不少于 9 块态势大屏，包括综合态势、安全告警、外部威胁、横向威胁、外连威胁、脆弱性威胁、恶意程序、资产态势、资产画像，大屏显示支持 3D 效果。 15. 支持大屏轮播，可以指定轮播的大屏和时间；可批量或者单独设置大屏的过滤参数包括是否情报命中、安全域、组织机构，需提供产品功能截图。			
商务要求					
1	服务期限要求	包含三年的维护期，提供设备的现场维护和一年四次巡检服务。			
2	交货期及地点	签合同后的 30 日内交货，遵义市播州区人民医院院内			

★本项目不接受联合体投标。

其它要求：详见《采购文件》

二、合格供应商应当具备的资格条件

（一）一般条件要求：符合《政府采购法》第二十二条之规定，分公司投标的，必须由具有法人资格的总公司授权。

1、在中华人民共和国境内注册取得有效的营业执照、组织机构代码证、税务登记证（或营业执照三证合一），具有独立法人资格或其他组织机构及法人委托文件；

2、提供具备履行合同所必需的设备和专业技术能力的证明材料（自行承诺）；

3、提供供应商 2021 年度或 2022 年度资产负债等财务报告[新注册企业提供当年内]；

4、提供供应商近 3 个月依法纳税证明材料及缴纳社会保障金的证明材料【新注册企业提供当年内或者依法不用纳税及缴纳社保的证明材料】；

5、提供供应商 1 年以上无违法不良记录的证明材料及供应商主体信用记录【新注册企业提供当年内】；

6、其它特别指明要求提供的材料、证明等；项目属特种行业的提供相应资证。

（二）诚信资格要求：提供购买标书当日至谈判前一天任一时间，在“信用中国”网站[www.creditchina.gov.cn，包括行业失信被执行人、重大税收违法案件当事人名单、政府采购严重违法失信名单]、中国政府采购网[政府采购严重违法失信行为记录名单http://www.ccgp.gov.cn/cr/list]的查询记录截图[完整清晰]。

三、报名与采购文件获取

1、报名与采购文件获取时间：2023 年 6 月 19 日-2023 年 6 月 27 日[8:00-11:30;14:00-17:30]**[周末、中午休息、节假日除外]**，供应商须在规定的时间内到指定地点获取本采购文件，并登记备案，如在规定时间内未获取采购文件并登记备案的供应商均无资格参加。

2、报名方式：电子邮件报名

3、报名邮箱：3266520453@qq.com

4、参与本项目报名的投标人请在电子邮件主题：注明公司名称、竞标的设备名称。

正文注明公司名称、授权委托人姓名和联系方式、竞标的设备名称，另扫描以下资料作为附件同发报名邮箱：

1）三证合一的营业执照副本（复印件加盖公章）；

2）法定代表人授权委托书附法定代表人及授权委托人身份证正反两面复印件（复印件加盖公章）；

3）特殊行业注册证或许可证（复印件加盖公章）；

4）诚信资格证明材料、无违法不良记录证明（复印件加盖公章）；

四、响应文件递交须知

1、截止时间

2023 年 6 月 28 日 14：30 时上班时间[中午休息、周末、节假日除外]，逾期送达的文件拒不接收。

2、投响应文件密封方式：档案袋封装

五、开标时间和地点

1、时间：2023 年 6 月 28 日 14 时 30 分[北京时间]。

2、地点：遵义市播州区人民医院远程医疗中心二楼开标室

六、信息公开媒介：http://www.zysbzqrmyy.cn 遵义市播州区人民医院[官网]

七、保证金

供应商递交响应文件前，应提交人民币 0 元的保证金。望供应商以法律规范、行业标准自律谈判行为，不恶意扰乱投标规则和采购秩序，一经发现则列入

八、评标办法摘要

1、合格供应商须提供规范有效的响应文件[1 正 1 副]对项目要求、技术参数、配置要求进行实质性响应。

2、综合评标法。

3、开标条件：响应报价≧3 家。

九、联系方式

1、主管科室：信息科

联系人及电话： 李先生 18076239198

2、办理科室：总务科

联系人及电话： 罗女士 19184538868

3、地址：遵义市播州区人民医院远程医疗中心二楼开标室

十、请严格遵守疫情防控相关规定。

遵义市播州区人民医院总务科

2023 年 6 月 19 日