贵州航天医院信息安全 APT 平台及漏洞扫描系统采购议标邀请书

建设单位	贵州航天医院		
项目名称	信息安全 APT 平台及漏洞扫描系统采购		
招标方式	招标邀请		
投标供应商资质要求	1、投标企业资质：（1）企业法人营业执照，（2）税务登记证，（3）法人身份证复印件。 2、投标人资质：（1）法人签字授权书，（2）投标人身份证及复印件。 3、设备生产厂家授权及售后服务承诺函（复印件并加盖生产厂家公章）。 4、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书面声明。 5、上述资质需盖鲜章和签字。提供一份正本，二本以上副本。		
工期要求	20 天		
议标技术要求	详见本附件		
建设地点	贵州省遵义市大连路贵州航天医院		
报名时间	2020 年 9 月 10 日	地点	贵州航天医院信息科
邀请截止时间	2020 年 9 月 15 日 17：00	地点	贵州航天医院信息科
竞争性谈判时间	2020 年 9 月 17 日 14：10	地点	远程会诊中心
评标办法	综合评标:产品、价格、服务、解决方案等		
联系电话	商务及技术咨询电话：0851－28690308		
传真	0851-28691113　　E-mail:791364169@qq.com		

贵州航天医院

2020 年 9 月 10 日

附件：信息安全 APT 平台及漏洞扫描系统采购要求

二、产品商务要求

1. 产品要求：国内知名品牌，通过相关权威机构认证，符合信息安全相关管理规范。

2. 单位负责人为同一人或者存在直接控股、管理关系供应商，不得参加同一项下的政府采购活动；为采购项目提供整体设计、规范编制或者项目管理、监理、检测等服务的供应商，不得再参加该采购项目的其他采购活动。

3. 供应商技术人员具有所投产品的认证资格证书或具有 CISP（国家注册安全认证工程师）证书、并提供社保缴纳证明。

4. 供应商需书面承诺中标后设备在 20 个工作日内供货并安装调试完成。

5. 免费提供送货卸货至用户指定地点、安装、操作与调试，同时系统安装后提供操作培训及相关系统操作手册。

6. 需提供设备厂家针对本次项目加盖公章的承诺书原件，提供原厂安装及技术服务。

二、采购要求及数量

1. 推荐设备是目前市场上使用的主流产品；系统满足医院信息安全使用要求。

2. 医院不承诺最低价中标；

3. 产品参数及数量

序号	货物名称	数量	技术规格、参数要求	附件材料
1	APT 攻击预警平台	1	1.硬件规格：一体化 2U 标准机架式设备；冗余电源；内存≥16G； 硬盘容量≥1T，千兆电口≥6 个，吞吐率：网络层≥1Gbps；应用层≥500Mbps；支持 WEB 检测≥HTTP 最大并发数 7 万/秒；支持邮件检测：邮件处理数≥100 万封/24 小时；文件检测≥3 万个/24 小时； 2.支持一键登录排错平台，对系统进行深度配置和排错，	

			支持一键检测故障、配置核对、表分区检查、表检测、同步验证、信息收集等功能。 3.部署方式：支持旁路部署和分布式部署，对探测器可以添加、删除，显示探测器版本、状态和IP，管理中心可实现告警统一管理；可自定义管理中心和探测器之间的数据传输速率、时间、发送目录等参数； 4.支持全流量检测，可根据需求打开或关闭全流量检测功能； 5.支持解析HTTP、FTP、SMTP、POP3、SMB、IMAP、DNS、Mysql、MSSQL、DB2、Oracle、HTTPS、SMTPS、POP3S、IMAPS等协议报文（HTTPS、SMTPS、POP3S、IMAPS加密协议解析需要导入服务器私钥证书），并提供审计协议类型的端口号配置，可根据需要变更端口号；支持LDAP登录行为识别；支持VXLAN镜像流量解析检测； 6.支持检测WEB攻击、异常访问、恶意文件攻击、远程控制、WEB后门访问、发件人欺骗、邮件头欺骗、邮件钓鱼、邮件恶意链接、DGA域名请求、SMB远程溢出攻击、WEB行为分析、隐蔽信道通信、暴力破解（包括SSH、TELNET、RDP、FTP暴力破解）、挖矿等风险； 7.支持对私网地址IP地理位置信息添加，在产生告警时，定义IP可正常显示所属地理位置信息； 8.可支持详细展现告警级别、时间、威胁名称、状态、客户端IP、客户端IP所在地理位置、服务端IP、服务端IP所在地理位置、报文、操作等信息，包含请求URL、请求类型、请求内容、请求头、Host、User-Agent、Accept、Accept-Language、Accept-Encoding、Accept-Charset、Keep-Alive、Connection、Cookie、请求参数、响应码、返回长度等信息	
2	漏洞扫描	1	1.规格参数：标准式机架设备、≥6个千兆电口、≥1TB硬盘；最大并发扫描任务数≥10个；授权可扫描总数量至少512个无限制范围IP地址；配置漏洞扫描、数据库漏洞扫描、系统及软件漏洞扫描、端口及服务探测、弱口令扫描授权。 2.支持IPV6 3.系统为B/S架构，并采用SSL加密通信方式，用户可以通过浏览器远程方便对产品访问操作，支持多用户同时登陆操作。 4.提供三权分立的账户体系，支持上下级部门管理，非上下级的不同部门任务、资产隔离。提供审计功能，能	

			够对登陆日志、操作日常进行记录和查询，并可以将日志导入导出操作。 5.系统内置不同的策略模板如针对Linux、Windows操作系统等模板，同时允许用户定制扫描策略；用户可定义扫描范围、定义扫描端口、扫描使用的参数集等具体扫描选项。 7.支持Windows系列操作系统，支持Linux主流操作系统（Centos、Redhat、Debian、Fedora、Ubuntu、Suse等），支持Unix主流操作系统（AIX、HPUX、Solaris等）；支持对Web、FTP、电子邮件等应用系统、Apache等web中间件服务器以及Office等常用软件进行漏洞扫描； 8.可以自定义扫描端口范围、端口扫描策略 9.提供采用SMB、SSH等协议对Windows、Linux系统进行登录授权扫描。 10.具备弱口令扫描功能，提供多种弱口令扫描协议，包括SMB、RDP、SSH、TELNET、FTP、SMTP、IMAP、POP3、MySQL、MSSQL、REDIS、RTSP等协议进行弱口令扫描，允许用户自定义用户、密码字典。 11.支持发现非默认端口启动的服务，支持服务的协议识别、版本 12.可根据端口识别出的软件版本提供可能存在的相关漏洞列表 13.支持HTML、WORD、PDF、XLS报告格式 14.产品提供Web应用漏洞扫描功能,支持对Discuz、大汉CMS、PHPCMS、DEDECMS、ECSHOP、WordPress、eWebEditor、FCKeditor、Struts2等国内外常见第三方组件扫描	

贵州航天医院信息科

2020-09-10