附件1

正（副）本

致：赣州市妇幼保健院

**项**

**目**

**咨**

**询**

**文**

**件**

**项目名称：网络安全运维服务项目**

**响应供应商名称：**

**日期： 年 月 日**

## 一、系统咨询响应函

致：赣州市妇幼保健院

（响应供应商名称）系中华人民共和国合

法企业，我方就参加本次投标有关事项郑重声明如下：

一、我方完全理解并接受系统咨询公告所有要求。

二、我方提交的所有响应文件、资料都是准确和真实的，如有虚假或隐

瞒，我方愿意承担一切法律责任。

三、我方承诺，以后的项目采购不高于此次系统咨询结果，系统性能参数、

配置、维保不低于此次项目咨询结果。

四、与此次项目咨询相关一切正式往来信函请寄：

地址 ： 传真：

电话 ： 电子邮件：

法定代表人或被授权人（签字）：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

响应供应商名称（公章）

年 月 日

## 二、服务项目、服务描述、价格

1、服务期间，响应供应商需按照医院要求完成各项安全检查工作，协助医院建立完善各项信息安全管理制度。

2、为加强本院业务系统云上及云下安全统筹运营能力，拉通云上安全防护能力与本地安全防护能力的统一管理，统一协调，加强云上应用及本地应用的网络访问控制精细度，缩小风险暴露面，降低安全风险，需监测所有云上与本地的网络威胁攻击事件，进行分析与溯源确保安全事件的及时发现与处置，保障云上数据中心与本地数据中心的安全统筹，定期输出完整安全运营报告。

3、服务内容：

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 序号 | 服务类别 | 服务项 | 服务  细项 | 服务描述 | 数量 | 单位 | 服务输出 |
| 1 | 网络安全驻场服务 | 人员驻场 | 网络安全运营人员（1名） | 提供1名具备CISP证书的网络安全运营专家驻场1年，负责提供技术支撑和响应，满足网络安全防护建设及优化过程中的各类需求。驻场专家应具备安全服务需求中常态化网络安全服务以及实战化安全运营服务过程中所需的全部网络安全技能，包括但不限于网络安全监测、风险评估、事件响应、事件处置、渗透测试等方面，确保能够提供高质量、专业化的网络安全服务。 | 1 | 项 | 每月月底驻场专家根据实际工作内容提供1份当月《安全巡检报告》；《日常运维周报》、《日常运维月报》；《安全加固报告》等 |
| 2 | 日常运维 | 安全运维 | 提供日常安全设备巡检、风险协助整改、日常安全审计、基线配置核查、安全加固、迎检支撑、安全检查等服务。 |
| 3 | 事件上报 | 事件告警 | 建立及时准确的安全事件预警上报体系，在事件分类的基础上，进一步研究针对各类安全事件的响应对策，快速向招标人及相关方推出安全预警信息及解决方案，并协助招标人根据实际情况制定应急预案，针对监管单位通报或最新暴出的高危漏洞，第一时间确认通报是否属实，以及漏洞是否在招标人单位存在，漏洞影响范围等。 |
| 4 | 专项网络安全服务 | 漏洞管理 | 漏洞扫描服务 | 每季度开展1次漏洞扫描等漏洞识别服务，挖掘主机操作系统、中间件、数据库、安全设备等相关设备或应用的漏洞信息，定位未修复的漏洞，并提供漏洞修复建议，协助招标人完成漏洞修复。 | 1 | 项 | 每季度完成漏扫后3个工作日内提供1份《漏洞扫描报告》 |
| 5 | 渗透测试 | 渗透测试服务 | 每季度对招标人指定信息系统开展周期性的渗透测试服务，以模拟黑客攻击的手段，从攻击者角度发现招标人的网络安全风险，先一步攻击者发现网络相关漏洞，防止被攻击者利用。 | 每季度完成渗透测试后3个工作日内提供1份《渗透测试报告》 |
| 6 | 专项检查 | 专项检查服务 | 每季度开展专项安全检查行动，专项检查内容包括但不限于：弱口令排查、违规接入与设备外联风险排查、公众号小程序专项检测等，并输出检查报告，配合完成整改。 | 每季度专项安全检查后3个工作日内提供1份《专项检查报告》 |
| 7 | 策略管理 | 策略管理服务 | 每月进行安全策略的梳理和检查，定期针对日常安全监测和安全风险检查的结果进行综合分析研判，识别网络安全风险、脆弱性和不合规配置项，从整体网络安全技术防护策略的角度提出准确、有效的改进措施，指导和协助开展策略配置调优，确保安全策略符合标准要求，使设备的安全防护能力有效发挥；以持续提升安全运行和防护能力。 | 每月完成安全策略检查后3个工作日内提供1份《分析研判报告》 |
| 8 | 项目管理 | 项目管理服务 | 组织项目资源、把控项目质量、跟踪项目进度，每季度完成季度总结汇报等。同时对接招标人各业务部门，以及院外业务系统、等保测评机构、监管机构等。 | 每季度末提供1份《项目总结报告》 |
| 9 | 安全管理制度 | 安全管理制度服务 | 结合新的政策要求以及招标人的具体需求，动态补充安全管理制度，并与原有制度相融合，安全管理制度的建设需要覆盖安全方针、管理办法、实施规范、记录表单等多级安全管理制度文件，指导全集化安全工作的实施及优化。 | 每年根据新政策及招标人要求提供1份《安全管理制度》 |
| 10 | 等保2.0 | 等保2.0建设服务 | 在提供设备的基础上，提供等保咨询人员，保障招标人安全技术水平满足等保要求，通过顺利等保测评。 | 每年等保测评前提供1份《等保差距分析报告及整改方案》 |
| 11 | 能力成熟度 | 能力成熟度评估及优化 | 为了确保服务质量，每年开展一次安全能力成熟度评估及优化工作，提供安全能力评估、安全流程优化、安全制度优化、安全工具优化和运营人员优化等服务。 | 每年度完成能力评估工作后3个工作日提供1份《能力成熟度评估及优化方案》 |
| 12 | 重保服务 | 重要时期安全保障服务 | 在攻防演习、春节、两会、国庆及发生安全事件等重要时期提供安全值守保障及应急响应服务。 | 每年重保期间安排2人值守并提供1份《重保服务方案》 |
| 13 | 风险评估 | 安全风险评估服务 | 每年开展1次系统性的信息安全评估，全面识别、评估和量化招标人面临的潜在威胁、漏洞和可能带来的负面影响，并支撑招标人有针对性的采取安全措施和策略，以减小风险的发生概率和影响程度，从而确保招标人信息系统的安全稳定运行。 | 每年开展安全风险评估后3个工作日内提供1份《安全风险评估报告》并提出相应整改建议 |
| 14 | 系统检测 | 系统安全检测服务 | 新系统上线前，开展安全检测，包括渗透测试、漏洞扫描、代码审计等，对发现的安全隐患，指导修复并复测，确保信息系统所有安全隐患修复完成，保障系统安全后再上线。为招标人系统上线落实完善的管理流程。 | 新系统上线前提供《系统安全检测报告》并提出相应整改建议 |
| 15 | 攻防演练 | 攻防演练服务 | 每年为招标人组织一次单位内的实战化攻防演练服务，提供演练平台和攻击团队，组织攻防演练行动。 | 每年根据招标人要求组织攻防演练，提供1份《攻防演练方案》并组织演练活动 |
| 16 | 应急响应 | 应急响应服务 | 如遇突发安全事件，为招标人提供专业的应急响应支撑服务，帮助招标人快速、准确应对突发事件。 | 解决突发安全事件后3个工作日内提供1份《安全事件处理报告》 |
| 17 | 安全培训 | 安全意识 | 全院安全意识提升培训 | 每年对招标人单位全员开展1次安全意识提升培训。 | 1 | 项 | 根据招标人指定时间安排培训，提供《安全培训PPT》 |
| 18 | 安全技术 | 安全技术培训服务 | 根据招标人对单位安全技术人员的专业能力要求，以线上线下结合的培训方式，每年度集中培训1次。 |

4、服务工具清单

本次项目服务过程中，需要响应供应商自行携带满足网络安全工作所需的软、硬件服务工具，具体所需的服务工具性能要求如下：

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 服务工具 | 数量 | 工具性能要求 |
| 1 | 边界安全防护服务工具 | 2套 | 1、网络层吞吐量≥4G;应用层吞吐量≥2G;防病毒吞吐量≥600M;IPS吞吐量≥600M;全威胁吞吐量≥450M;并发连接数≥200万;HTTP新建连接数≥6万;SSL VPN推荐用户数≥20; IPSec VPN 最大接入数≥300;IPSec VPN吞吐量≥270M;规格:1U; 电源:单电源; 接口≥8千兆电口; 2千兆光口SFP  2、支持路由，网桥，单臂，旁路，虚拟网线以及混合部署方式。  3、具备静态路由和多播路由，支持RIP、OSPF、BGP等动态路由协议。  4、具备ARP代理功能，对指定地址的ARP请求使用指定接口的MAC地址应答，实现保护内网主机。  5、支持NAT穿透技术ALG，支持FTP、TFTP、SQLNET、PPTP、RTSP、SIP 、H.323等协议。  6、产品支持3种以上的用户认证方式,包含但不限于单点登录、本地账号密码、外部账号密码认证。  7、产品支持多维度流量控制功能，支持基于IP地址、用户、应用、时间设置流量控制策略，保证关键业务带宽日常需求。  8、产品支持异常数据包攻击防御，防护类型包括IP数据块分片传输防护、Teardrop攻击防护、Smurf攻击防护、Land攻击防护、WinNuke攻击防护等攻击类型。  9、产品支持对SMTP、HTTP、FTP、SMB、POP3、HTTPS、IMAP等协议进行病毒防御。  10、产品支持基于IMAP、FTP、RDP、VNC、SSH、TELNET、ORACLE、MYSQL、MSSQL等应用协议进行深度检测与防护。  11、产品支持安全策略有效性分析功能，分析内容至少包括策略冗余分析、策略匹配分析、风险端口风险等内容，提供安全策略优化建议 |
| 2 | 流量采集服务工具 | 1套 | 1、网络层吞吐量≥1Gbps，应用层吞吐量≥350Mbps；规格：2U，内存大小≥8G，硬盘容量≥480GB SSD，电源：冗余电源，接口≥6千兆电口+2万兆光口SFP+  2、支持自动识别内网的服务器及其开放的服务与端口，支持以列表形式显示资产IP、提供的服务及其开放的端口、设备类型、操作系统等信息。  3、支持多种类型弱口令策略可选；支持自定义FTP弱口令检测，规则设置如空口令、用户名和密码相同、长度、弱口令列表等；支持口令暴力破解检测不同类型（FTP/WEB登录）的爆破次数。  4、支持智能语义引擎检测，可针对http隧道、java反序列化保护等类型进行自定义设置  5、支持通过白流量过滤的方式，过滤安全网站访问，提升性能。  6、审计白名单支持源目IP、源目端口和日志类型、日志来源  7、支持列表形式展示阻断记录，展示维度包括：最近阻断时间、阻断类型、阻断对象、源IP、源端口、目的IP、目的端口、阻断次数等信息  8、支持访问检测日志，包括正常访问、风险访问、违规访问  9、支持对接CWPP原始流量，包括DNS\HTTP\RDP协议流量传输到探针检测。  10、提供三权分立的用户管理能力：系统管理员、审计管理员、安全管理员、普通管理员四个角色相互独立；同时支持IP绑定的登录安全设置。普通管理员角色的权限可自定义模块页面的编辑和查看权限。  11、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 |
| 3 | WEB应用防护服务工具 | 1套 | 1、标准机架式，交流双电源；≥1个RJ45串口，≥2个GE管理口，≥6个千兆电口(3对Bypass)，≥4个千兆光口，≥2个接口扩展槽（4GE/4SFP），网络层吞吐量≥4Gbps，应用层吞吐≥1Gbps  2、支持非法文件上传防护，有效识别文件上传行为，并对上传行为的内容做安全检测，可以根据需要禁止上传以下文件类型：PE(windows Executable File)、ELF(linux Executable File)、PHP web shell、Linux shell、Power shell(windows Script File)、Java shell、Asp shell、Perl shell、Python shell及Ruby shell；  3、支持针对主流Web服务器及插件的已知漏洞进行防护。Web服务器应覆盖主流服务器：apache、tomcat、lightpd、NGINX、IIS等；插件应覆盖：dedecms、phpmuadmin、PHPWind、shopex、discuz、echsop、vbulletin、wordpress等；  4、支持盗链防护，能够有效识别网页盗链行为，避免用户网页资源被滥用；支持Cookie安全机制；支持敏感关键字自定义；  5、支持暴力破解防护，可针对指定URL进行暴力破解防护，支持多种方式的登陆，支持referer检测，支持阈值和检测周期的自定义；  6、支持对攻击源地址进行智能阻断，支持永久封禁或者自定义IP封禁时间（秒/分钟/小时），并且可以手工解除解禁；  7、能够兼容所有类型Web服务器，如IIS、Apache、IBM http server、WebSphere、WebLogic、Tomcat、Jboss、Resin等；  8、当需要对外发布网站时，本次服务支持一键启停服务器组中所有节点的防护；  9、支持多服务器节点的多层级管理，支持多节点划分到防护群组、管理域等多业务层级进行管理；  10、能够支持增、删、改、重命名、修改属性等篡改行为的检测和阻断。 |
| 4 | 端点安全管理服务工具 | 1套 | 提供200个服务器客户端,780个PC客户端授权 1、支持自定义拦截终端软件弹窗，可在终端设置自动拦截骚扰弹窗开关。  2、支持应用管控功能，内置常用的系统应用，包括IM、下载工具、代理工具、办公软件等，并且支持新增自定义应用，辅助客户限制恶意软件、盗版软件的使用，加强正版软件配置规范建设，事前可拦截终端进程运行，事中可结束终端应用的运行，事后可审计进程管控日志  3、支持显示攻击事件命中的ATT&CK相关技术，并对此技术做简要说明。便于用户了解攻击者的操作行为和目的，评估整体影响面  4、支持内存马检测功能，在检测到进程被注入和进程新建时，主动调用内存马检测引擎进行相关进程扫描检测，检测到内存马后产生告警并可提供举证信息（进程信息、检测时间等）  5、支持基于终端侧采集记录的行为数据，对文件变更、进程变更、网络连接、DNS查询等多种行为，在全网中搜索命中指定条件的端点和行为，进行高级威胁的狩猎对全网终端发起威胁狩猎，挖掘潜伏攻击  6、支持对已停止更新的Windows系统的全网一键清点，管理员可快速筛选出全网已停止更新的Windows系统的数量和具体的终端  7、支持按照扫描网段、扫描方式、扫描协议、扫描端口对终端进行扫描，及时发现尚未纳入管控的终端  8、支持暴露面梳理功能，可以快速识别环境中暴露在外网的端口及应用，当检测到有来自于外网的IP地址访问时，判定该资产为外网暴露面资产，帮助用户高效梳理资产脆弱面  9、可通过多维度引擎进行漏斗式检测，保障查杀效果在低误报率的情况下保持高检出率  10、支持agent性能保护兜底机制，可设置agent主进程、威胁检测、病毒查杀等进程的资源占用阈值，当进程资源占用达到阈值时，进程会自动重启  11、服务器全量版支持全面防护：文件实时监控、勒索诱饵防护、静态文件AI引擎、动态勒索行为AI引擎、勒索攻击对抗、无文件攻击防护、RDP二次认证、SSH二次认证、可信进程防护、关键目录加固、Webshell防护、无文件攻击防护  灵敏检测：恶意文件检测、暴力破解检测、网端联动杀毒 |
| 5 | 威胁检测响应服务工具 | 1套 | 1、支持网络侧遥测数据采集20种，包含脆弱性风险、访问风险、服务探测、主机探测、网站攻击、后门通信、账号爆破、攻击利用、邮件攻击、Dos攻击、黑链、漏洞攻击、黑客工具、数据库攻击利用、访问恶意文件、感染病毒、行为异常、流量异常、登录异常、流量审计日志、Payload等  2、支持自定义仪表盘，内置安全事件/告警视图、资产视图、脆弱性风险视图、风险资产视图等模板，展示图表样例包括条形图、水平条形图、趋势图、饼图、表格、指标、Markdown等，可编辑背景及标题样式，可全局预览  3、支持自定义可视化组件，可设置组件类型（包括柱形图、水平条形图、趋势图、饼图、表格、指标、Markdown等形式）、资产范围、聚合维度（字段、排序）、度量（字段、计算方式）。  4、支持自定义报告生成，包括时间、报告组件、可视化组件、图标设置及文字编辑，可上传自定义页眉和自动化目录生成，支持预览和导出。  5、支持数据分析，支持内置CC通信、VPN安全、主机异常、堡垒机安全、恶意软件、扫描探测、拒绝服务、暴力破解、漏洞利用、网站攻击、邮件安全等维度的数据分析规则不低于100条。可自定义新增匹配或统计规则，可启用或禁用解析规则。  6、支持多面板功能，用户可以在安全告警页面增加/删除/修改告警面板并保存下来，方便后续使用 |

5、服务考核及违约赔偿

院方按照以下责任考核制度和处罚机制定期对中标人进行考核，责任考核制度和处罚机制均在合同签订之日起3个月后开始生效。

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 考核大类 | 考核项目 | 考核说明 | 罚则 |
| 1 | 技术 | 网络安全 | 因恶意病毒、安全攻击事件造成网络故障（不含设备故障类）影响超过20%的部门人员无法正常使用，包括无法连接互联网或内网正常连接请求无法响应等，造成网络瘫痪不可用。 | 网络瘫痪超过1小时不可用，扣除本年度安全服务合同金额1%；网络瘫痪超过2小时不可用，扣除本年度安全服务合同金额2%。 |
| 2 | 终端安全 | 发生内网终端安全病毒大面积传播，终端中病毒数量高于10%。 | 首次发生，扣除本年度安全服务合同金额1%，第二次及以后，在上一次罚则的基础上，金额加2%。 |
| 3 | 终端安全 | 因终端安全问题造成业务部门业务中断或门急诊业务中断。 | 业务部门业务中断超过1小时未修复，门急诊业务中断超过0.5小时未修复，扣除本年度安全服务合同金额1%；业务部门业务中断超过2小时未修复，门急诊业务中断超过1小时未修复，扣除本年度安全服务合同金额2%； |
| 4 | 质量 | 服务文档质量 | 交付文档的质量不能满足客户模板及内容要求的 | 首次发生,扣除本年度安全服务合同金额0.1%，第二次及以后，在上一次罚则的基础上，金额加20%，每次罚款金额以0.5%为上限。 |
| 5 | 问题解决质量 | 发生服务质量问题后，是否能够给出合理的解释，以及完整、有效的解决方案。不能给出相关方案的。 | 首次发生，扣除本年度安全服务合同金额0.1%，第二次及以后，在上一次罚则的基础上，金额加20%，每次罚款金额以0.5%为上限。 |
| 6 | 服务 | 服务专业性 | 服务人员是否具备相应技术素质和工作能力，出现不满足技术要求的。 | 首次发生，扣除本年度安全服务合同金额0.1%，第二次及以后，在上一次罚则的基础上，金额加20%，每次罚款金额以0.5%为上限。 |
| 7 | 服务及时性 | 是否按照既定时间完成服务成果提交，出现不满足要求的。 | 首次发生，扣除本年度安全服务合同金额0.05%，第二次及以后，在上一次罚则的基础上，金额加20%，每次罚款金额以0.5%为上限。 |
| 8 | 服务态度 | 服务人员因工作态度问题被友邻部门投诉。 | 首次发生，扣除本年度安全服务合同金额0.05%，第二次及以后，在上一次罚则的基础上，金额加20%，每次罚款金额以0.5%为上限。 |
| 9 | 服务满意度 | 每季度开展1次服务满意度调研，若服务满意度为不满意。 | 首次发生，扣除本年度安全服务合同金额0.05%，第二次及以后，在上一次罚则的基础上，金额加20%，每次罚款金额以0.5%为上限。 |

在服务期间内出现以下场景，中标方需要向医院支付服务违约金：

一、网络勒索损失

在服务期间内，我院发生网络安全事件受网络攻击、网络安全威胁而被勒索、敲诈，导致产生下列损失和费用，中标方需进行全额赔付：赎金、咨询处理网络勒索事件第三方专业机构的费用以及对能提供逮捕、定罪勒索人信息的举报人的奖励。

二、安全工作不利被开罚单损失

因网络安全工作开展不利（如日志留存不符合要求、存在重大高危漏洞等），导致医院被第三方检查机构或监管机构开出网络安全罚单，中标方对罚单金额进行全额赔付。

三、数据丢失泄露损失

在服务期间内，因本地运维人员未及时监测并阻断黑客入侵等攻击行为，造成医疗数据丢失泄露所产生损失和费用，中标方需进行全额赔付并对数据进行修复找回。

## 三、法定代表人授权书（非法人代表参与投标时提供）

致:赣州市妇幼保健院

（响应供应商法定代表人名称）是 （响应供应商名称）的法定代表人，特授权 （被授权人姓名及身份证代码） 表代表我单位全权办理上述项目的设备咨询、投标、谈判、签约等具体工作，并签署全部有关文件、协议及合同。我单位对被授权人的签字负全部责任。在撤消授权的书面通知以前，本授权书一直有效。被授权人在授权书有效期内签署的所有文件不因授权的撤消而失效。

被授权人签字：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 法定代表人签字：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

响应供应商名称（公章）

年 月 日

|  |
| --- |
| 粘贴法人身份证明**（复印件正、反两面）**  粘贴被授权人身份证明**（复印件正、反两面）** |

## 四、响应供应商关于无重大违法记录书面声明函

致：赣州市妇幼保健院

我公司在参加本次政府采购活动前三年内，在经营活动中没有因违法经营受到刑事处罚或者责令停产停业、吊销许可证或者执照、较大数额罚款等重大违法记录。

特此声明。

法定代表人或被授权人（签字）：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

响应供应商名称（公章）

年 月 日

## 五、响应供应商资格证明文件

1、营业执照、税务登记证、机构代码证（三证（五证）合一的提供三证（五证）合一证件）

**六、其他证明文件**