附件1

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**

**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、服务内容：

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **序号** | **服务名称** | **基本配置** | **数量** | **单位** | **总价** |
| 1 | 驻场运维服务 | 1、提供1人驻场，按照要求进行日常安全运维服务，进行日常巡检、一般巡检、常规故障处理等日常工作。驻场期间提供相应的运维日志、及巡检报告；  2、提供每年至少一次应急响应服务、提供应急预案、应急演练等应急服务。提供《应急演练方案》； 3、一年一次的风险评估服务，其中包括：漏洞扫描（针对漏扫发现的漏洞进行处理，包括云主机及终端电脑等设备），基线核查，风险分析等。评估结束后提供《系统安全评估报告》、《系统安全漏洞扫描报告》、《系统安全配置检查报告》；每季度提供一次策略优化、网络设备安全加固、安全设备安全加固、主机系统安全加固、应用系统安全加固等服务，加固后提供《安全加固报告》； 4、一年一次的渗透测试服务，通过模拟黑客使用的工具、分析方法对网站及业务系统进行安全测试，并结合智能工具扫描结果，由高级工程师进行深入的手工测试和分析，识别工具弱点扫描无法发现的问题。主要分析内容包括逻辑缺陷、上传绕过、输入输出校验绕过、数据篡改、功能绕过、异常错误以及其他专项内容。测试结束后输出《渗透测试报告》并提供加固建议； 5、提供“护网行动”前的安全加固工作以及“护网行动”时的驻场值守服务，至少提供1人直至“护网行动”结束。护网前提供护网专项行动工作方案，护网期间提供安全保障服务日报、结束后提供护网总结报告；  6、协助单位迎接网信办、公安部门等上级单位的安全检查工作，详细解读安全检查细则，制定安全迎检规范和计划，协助进行安全检查工作。 7、在用户单位重大会议和法定节假日（国庆、春节等）期间，提供安全保障工作，协助处理信息安全事件。包括前期的安全检查、应急响应、现场/电话值守等准备工作，确保在重要敏感时期的网络安全。  8、提供一年二次安全意识及日常安全办公培训，安全培训服务前，出具一份《安全培训计划》、《安全培训教材》，文档中会详细的列出本次培训的课件和培训的计划，以便有针对性的进行本次培训，达到培训的效果。 | 1 | 年 |  |
| 2 | 网络访问控制服务 | 提供一年网络访问控制服务。运维期提供网络访问控制服务配置报告。服务中使用的工具具备以下功能：  1、能够提供基于源/目的IP地址、安全区、应用/应用过滤器、协议/端口、时间、用户、安全模板/模板组等，对经过网络的流量进行多维度的的安全访问控制； 2、可不通过主机扫描等技术，也不需要在主机上安装任何插件，即可识别内网主机的操作系统、杀毒软件、浏览器等信息，可自定义操作系统、浏览器、杀毒软件的风险等级，并支持预置风险等级； 3、提供应用过滤器，至少支持4个维度进行过滤，能够将通过应用过滤器筛选出来的应用直接生成模板供用户统一管理使用； 4、能同时辨识IPv4和IPv6通讯流量，支持IPv6环境下攻击检测技术和基于IPv6地址格式的安全检测； 5、可针对网络病毒、蠕虫、间谍软件、木马后门、扫描探测、暴力破解等恶意流量进行检测，检测时所用的特征库数量大于8000种； 6、帮助用户提供入侵规则分类，根据规则分类能够更便捷的制定防护策略。如勒索、挖矿、SQL注入、XSS注入、webshell、命令代码执行、内存破坏、类型混淆、反序列化、信息泄露、目录遍历、文件操作漏洞、注入攻击、重定向漏洞、CSRF、僵木蠕、拒绝服务、弱口令、欺骗劫持、扫描类攻击等； 7、能够识别敏感数据，同时针对敏感数据外发提供检测，能够识别敏感数据信息含身份证号、银行卡、手机号等。 | 1 | 年 |
| 3 | WEB应用防护服务 | 提供一年WEB应用防护服务。运维期提供WEB应用防护报告。服务中使用的工具具备以下功能：  1、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； 2、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； 3、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； 4、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； 5、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； 6、能够兼容所有类型Web服务器，如IIS、Apache、IBM http server、WebSphere、WebLogic、Tomcat、Jboss、Resin等； 7、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； 8、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； 9、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。 | 1 | 年 |
| 4 | 全网安全态势分析服务 | 提供一年全网安全态势分析服务。运维期提供全网安全态势分析报告。服务中使用的工具具备以下功能：  1、支持300+设备日志解析规则查看以及筛选，包括但不限于网络设备（防火墙、交换机、网关）、安全设备（入侵检测设备、WEB攻击防护设备、APT检测设备、防火墙、网络审计、流量探针等）、终端主机日志、数据库等； 2、服务支持对失陷资产进行判定并提供失陷资产的判定依据，包括但不限于失陷资产概要信息、攻击结果、攻击链分布阶段、失陷资产的攻击过程及过程判定依据如攻击特征、流量上下文、关联的告警日志及流量日志以及pcap包下载，并可快速扩展该失陷资产的全部攻击事件以及该失陷资产攻击者发起的攻击、该失陷资产的同类型威胁事件； 3、支持针对漏洞扫描结果生成漏洞处置单，支持对漏洞处置单闭环处理，可设置漏洞处置单状态包括：新增、待修复、已修复、已验证、单次忽略、永久忽略； 4、支持将监测网络安全情况的态势进行呈现，态势呈现包括但不限于综合态势、威胁态势、脆弱性态势、环境感知态势、运维响应态势； 5、支持对网络环境中威胁、漏洞、资产各种事件多种运维方式进行可视化呈现，包括但不限于人工处置的各类型运维事件的状态统计、数量统计、自动化编排和响应的时长统计、数据量统计以及任务数统计等； 6、支持对威胁、失陷主机、漏洞等事件进行统一运维处理，提供统一入口； 7、服务支持对各类运维事件进行运维处置，包括但不限于提交研判人员进行分析、忽略、误报、处置、优先处理、加入白名单、生成报告、联动封堵设备封堵处置、邮件通报、工单通报等； 8、支持针对攻击IP、域名、会话进行封堵，支持黑名单、流量牵引等方式配合安全设备进行封堵。 | 1 | 年 |
| 5 | 病毒防护服务 | 对内网900台windows电脑终端、112台windows服务器及45台Linux服务器提供一年病毒防护服务。运维期提供病毒防护配置报告。服务中使用的工具具备以下功能：  1、要求能直观的展示终端信息、病毒趋势统计、病毒类型排行、病毒排行、终端危险排行等全网统计情况。并随时对网络中威胁发生的情况进行查询，能组合时间、IP、机器名、病毒名称、病毒类型等信息全方位定位、展示。 2、支持实时显示客户端的状态及终端基本信息，包括客户端连接状态、服务状态；终端机器名称、IP地址、MAC地址、操作系统、显卡信息、内存大小、当前版本信息和物理位置等信息，支持终端信息导出。 3、支持对客户端进行统一管理，统一下达指令。支持对终端进行分组及批量分组，支持分组导入、导出。支持对终端进行单/多标签标记，进行部分操作，方便管理。 4、支持统计分析客户端上报的威胁日志，包含终端/部门/责任人危险排行统计、防御类型分布统计、病毒类型分布统计、病毒排行统计、病毒趋势统计等，要求支持管理员操作，日志记录追踪；支持控制中心-客户端交互操作，日志记录追踪，便于问题定位。 5、支持漏洞集中修复、统一修复高危漏洞、统一修复所有漏洞，并展示以做补丁和未做补丁的信息。要求支持配置补丁从控制中心下载/从外网下载两种方式。 6、支持设备控制功能，可管控U盘、便携设备、USB无线网卡、USB有限网卡、打印机、光驱、蓝牙设备。 | 1 | 年 |
| 6 | 内外网数据交互服务 | 提供一年内外网数据交互服务。运维期提供内外网数据交互配置报告。满足部分办公电脑及内网电脑能同时访问内外网，通过制定相应的规则策略，实现医院内网与外网隔离和自有协议数据摆渡，同时实现两网业务系统间的数据实时或定时、双向安全交换，实现业务数据的互联互通。支持内网到外网、外网到内网、双向的文件传送；支持文件传输方向可控，实现单向或双向传输；支持文件传输时的身份认证及加密传输功能；支持对文件类型的黑白名单控制。支持FTP访问、数据库传输及同步。支持身份认证功能：采用用户名和密码、IP地址、MAC地址、IP与MAC绑定、Radius、网页认证等多种组合方式实现客户端访问控制。具有实时入侵检测机制，支持对SMTP、FTP、DNS、DOS/DDOS攻击、PortScan的检测。 | 1 | 年 |

3、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0.5%；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1%。 |
| 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0.5%，第二次及以后，在上一次罚则的基础上，金额加1%。 |
| 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0.5%；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1%； |
| 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0.05%，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。 |
| 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0.05%，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。 |
| 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0.05%，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。 |
| 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0.025%，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0.025%，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0.025%，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**