附件：

1.项目名称：2025年度医院门户网站运维和安全服务采购项目。

2.最高限价：3.8万元，超过限价的报价其响应文件作无效处理。

**★**3.服务要求：

医院门户网站部署在西部数码云平台，本次采购门户网站运营维护和日志审计系统、Web应用防火墙、SSL证书、IPV6改造等安全服务。保障门户网站日常正常运营，且需通过三级等级保护测评和备案，服务周期为一年，详细服务需求清单如下：

|  |  |  |  |
| --- | --- | --- | --- |
| **一、日志审计系统功能清单** | | | |
| 数据监控 | 数据概要 |  | 支持查看常规统计信息（当日数据概要）、最新日志信息、Windows、Linux等各种分类日志数据信息； |
| 资产状况 |  | 支持查看所有已采集到日志信息的服务器相关信息、包括所有资产、监控资产、历史资产三大分类； |
| 安全事件 |  | 支持查看告警规则及事件规则定义筛选后呈现的日志信息 |
| 系统运行 |  | 支持查看日志审计系统本身的设备状态信息（包括CPU、内存、存储空间、证书信息）、日常运行状态及最新系统日志； |
| 检索分析 | 日志检索 |  | 支持通过时间范围加上单一条件针对所有日志进行检索分析； |
| 事件检索 |  | 支持通过时间范围加上单一条件针对事件日志进行检索分析； |
| 告警检索 |  | 支持通过时间范围加上单一条件针对告警日志进行检索分析； |
| 高级检索 |  | 支持通过日志属性、入库时间、日志类型及日志子条件（可多级子条件）进行组合式高级检索，并支持保存日志检索模板； |
| 文件检索 |  | 支持通过时间范围加上单一条件针对文件日志进行检索分析； |
| 报表分析 | 手动任务 |  | 支持查看手动生成的报表信息（支持导出） |
| 计划任务 |  | 支持查看周期自动生成的报表信息（包括日、周、月） |
| 报表管理 |  | 支持内置各种合规性报表、实用性报表及自定义报表； |
| 数据采集 | 日志导入 |  | 支持将本地存放日志包导入至日志审计中进行查看归类存储； |
| SYSLOG |  | 支持将各类syslog日志进行更精细的划分，如分类为cisco、H3C、绿盟等； |
| SNMP |  | 支持将各类snmp日志进行更精细的划分，如分类为cisco、H3C、绿盟等； |
| OPSEC LEA |  | 支持采集OPSEC LEA相关日志； |
| 镜像数据采集 |  | 支持采集各类数据库日志、文件传输日志、网站访问日志等； |
| 文件定时采集 |  | 支持采集各类应用文本日志，如apache、tomcat、weblogic等； |
| 远程定时采集 |  | 支持采集远程定时型日志，如mysql transaction log、snmp设备信息等； |
| 原始文件采集 |  | 支持采集原始文本日志包进行存储； |
| 策略管理 | 内置策略 |  | 支持http数据自动归并策略、用户口令猜测关联分析策略、web访问数据策略； |
| 实时规则 |  | 支持内置上百种实时告警规则及支持用户自定义各类规则； |
| 业务策略 |  | 支持添加数据库业务三层策略、支持建立数据库模型策略； |
| 知识库 |  | 支持上传常用FAQ文本、以供排错； |
| 数据管理 | 数据备份 |  | 支持根据日志属性及时间范围进行数据备份，支持下载； |
| 数据恢复 |  | 支持将已下载的备份数据文件导回日志审计中进行查看； |
| 数据归档 |  | 支持查看自动归档数据及下载该数据； |
| 归档设置 |  | 支持根据磁盘配额、存储周期、归档策略进行自动数据归档配置； |
| 系统配置 | 用户管理 |  | 支持用户及用户组创建、支持三权分立、支持日志权限及管理范围划分； |
| 资产管理 |  | 支持主机及主机组创建、支持对主机IP地址、主机名、主机类型、实时监控类型的自定义； |
| 安全策略 |  | 支持密码长度、密码复杂度设置、支持双因素认证、支持账户自动锁定、支持系统超时设置、支持日志审计系统IP访问范围限制； |
| 系统管理 | 授权许可 | 支持查看设备基本信息和使用授权，并可导入新的授权证书文件； |
| 证书生成 | 支持根据IP或域名生成日志审计认证证书； |
| 网络设置 | 支持配置及更改日志审计IP地址、网关； |
| 配置管理 | 支持配置备份、配置恢复； |
| 时间同步 | 支持修改当前系统时间、也可以配置NTP服务器自动同步； |
| 辅助接口 | 支持配置邮件、syslog、snmp trap、短信网关等方式输出告警信息； |
| 系统升级 | 支持对系统版本进行升级； |
| 系统告警配置 | 支持将日志审计自身系统日志输出告警； |
| 设备管理 | 支持关闭设备、重启设备、系统备份、系统恢复； |
| 运维管理 | 支持与同品牌堡垒机进行数据联动 |
| 帮助 | 用户手册 |  | 支持下载日志审计用户手册PDF版 |
|  | | | |
| **二、Web应用防火墙功能清单** | | | |
| 攻击防护 | | | 实时对云防御规则库优化和分发虚拟补丁程序，为安全基础为零的业务系统、API、移动APP、小程序提供99.99%的安全防御支持 |
| 安全合规 | | | 参照《网络安全等级保护基本要求》和《中华人民共和国网络安全法》的规定，助力政企业务系统快速合规合法。 |
| 站锁替身 | | | 自创替身技术，虚拟补丁服务，采用主动发现、协同防御的方式将Web安全问题化于无形。 |
| 7\*24专家服务 | | | 安全运维专家团队 7x24 小时全天候监控，确保 Web 业务始终保持高效流畅的体验。 |
| 专属防护 | | | WEB应用防火墙 |
| 浏览器安全检查 |
| 区域防御控制 |
| 精准访问控制 |
| 拟态防御 |
| 深度防御 | | | 在线锁 |
| 防黑锁 |
| 整站锁 |
| 高级扫描防护 |
| 弱口令防护 |
| 基础服务 | | | 端口支持 |
| IP黑白名单 |
| 敏感时期特殊防护 | | | 重点保障时期攻击防护 |
| 1. 通过防御SQL注入、XSS跨站脚本、常见Web服务器插件漏洞、非授权核心资源访问等恶意行为攻击，过滤海量恶意CC攻击，避免网站资产数据泄露，保障网站的安全与可用性。 2. 业务带宽：不低于20M 3. 防护域名：不低于10个   （1个主域名+9个关联子域名） | | | |
|  | | | |
| **三、SSL证书功能清单** | | | |
| 安全可信标识展示 | | | 将网址中的“HTTP”升级为“HTTPS”协议，并使浏览器对网站加注“安全”标识。 |
| 支持国密SSL证书 | | | 满足政企国产/国密SSL证书应用需求。 |
| 多平台支持 | | | 支持微信小程序、苹果应用商店（App Store）SSL上架要求。 |
| 数据传输加密 | | | 数据加密传输，防运营商流量劫持、网络钓鱼、广告代码注入。 |
| 为网站业务系统提供HTTPS加密防劫持、防篡改、防钓鱼假冒安全服务，消除浏览器“不安全”警告，有利于保障客户信息安全、增强网站可信度、提升网站搜索排名。更支持国密SSL证书，使用SM2算法加密通信，满足国密改造合规要求。 | | | |
|  | | | |
| **四、IPV6升级改造要求** | | | |
| 域名一致性 | | | 网站www的IPv6域名要与IPv4域名为同一域名； |
| 地址可解析性 | | | 网站www域名能够实现多个地点多链路解析到IPv6地址； |
| 首页访问成功率 | | | 网站首页IPv6可以访问，且访问成功率大于100%； |
| 内容布局一致性 | | | 通过IPv4访问和IPv6访问网站，内容和布局应保持完全一致； |
| 二、三级链接支持率 | | | 网站二三级链接IPv6访问支持率应达到100%； |
| [外链可访问性](https://www.west.cn/cloudhost/ipv6sky.asp" \t "_blank) | | | 能够彻底解决IPv6外链问题，且深度不小于5层； |
| 访问流畅性 | | | 网站www域名解析时延及网站首页访问时延不大于300毫秒； |
| 访问稳定率 | | | 网站全网IPv6可稳定访问不小于100%； |
|  | | | |
| **五、官网运营维护** | | | |
| **一、网站维护服务细则：**  1、向医院提供网站、域名、空间运营维护服务。  2、域名维护服务：提供免费域名dns维护、解析、实名认证、过户等常规服务；特殊需要可单独申请。  3、ICP备案代理：根据中华人民共和国国务院令第292号《互联网信息服务管理办法》规定，国家对提供互联网信息服务的ICP实行许可证制度，所有的主机用户都必须办理ICP备案才能使用，代理提交申请备案、接入备案、变更备案。  4、代理第三方平台账号（如微信公众平台、微信开放平台、支付宝、苹果开发者平台、安卓类开发者平台等）的注册、认证、年审，其中所涉及材料和费用由医院提供。  5、免费网络推广：免费为客户通过程序关键词优化，提交到各大搜索引挚，如百度、google、搜搜等搜索平台。  6、后台操作培训：由供应商客服人员进行专业的后台操作培训，演示网站后台管理操作，讲述网络营销技巧以及网络推广方式；培训方式:远程培训4次/年、上门培训每年 2次/年。  7、网站修改：在免费维护期内，对本单位网站内容免费修改（指在不改变网站主框架设计和功能结构前提下做网站文字的修改和变更）。  8、资料上传：若医院没有网络维护人员，将免费为医院上传网站资料以及修改网站资料，资料由医院整理以及提供（详细见服务内容）。  9、咨询服务：对网站运营或其他IT相关服务有疑问，可以致电咨询，将由专门人士跟踪服务，并给出相关解决方案以提参考。  10、数据备份：每周对网站数据进行云备份，以防网站出问题，用于应用数据的修复。  11、电话应急服务：提供公司服务电话和技术员手机，7X24小时为你服务（一般故障10分钟内恢复；重装服务器系统2-3小时；硬件故障1-2天恢复）。  12、灾难性问题发生后，2小时内响应，48小时内恢复数据；  13、当医院网站运行程序出现异常、病毒攻击、空间不稳定等故障，及时提供服务，保证1个工作日之内恢复网站正常运作，3个工作日内采取相应补救措施。  **二、服务内容**：  **基础服务**1、域名dns维护、解析、转发、实名认证、过户等常规服务；特殊需要单独申请（域名代续费（不清楚域名购买地）、代域名注册服务等）；2、基础产品图片处理，如修改分辨率、添加水印、调色、扫描等；  3、添加产品或者案例信息；  4、添加新闻资讯其中修改公司简介、网页电话号码、联系方式不限次数；  5、网站音视频服务转换音频格式服务;DV拍摄制作企业记录片：医院自行提供，免费转换和上传；  6、协助网站转移、部署；  7、网站内容备份：每周对网站进行云备份，若需要数据库备份文件每月可申请1次；  8、ICP申请备案、接入备案、变更备案；四川省公安局安网备案；第三放平台账号申请（如微信公众号、支付宝、安卓类平台的申请、认证、年审，每年1次，所涉及费用和材料由医院提供）；  9、常规搜索引擎免费收录；  10、网站增值服务：  电话支持：7\*24小时热线服务  **设计服务**   1. 制作专题宣传静态页面   2、网站制作专题网页  3、首页设计局部调整  4、设计站内banner广告/横幅广告  程序服务   1. 修改首页内容布局   2、处理、隐藏或者删除页面；导航名称、页面电话、文档类等文案修改 3、网站病毒查杀；4、协助处理网络黑客攻击；  5、制作网站内浮动、弹窗广告；  6、第三方代码安装（网站访客统计、客服、推广代码等）。  **网站运营维护服务**  1.服务器保障服务  网络安全检查、网络流量检查、服务器硬件资源占用情况检查。服务器操作系统及时打补丁升级。服务器定期病毒查杀、实时监测安全情况，及时处理安全情况，使服务器能安全良好的运行。  2.数据备份与恢复保障服务  数据备份（网站文件、CMS程序、定制开发程序、数据库文件）的备份以及恢复，网站遭到破坏时能在最短时间能恢复。当系统发生灾难性问题后，会在12小时内及时响应，48小时内恢复所有数据。当网站运行程序出现异常、病毒攻击、空间不稳定等故障，及时提供服务且保证一个工作日内恢复网站正常运行，两个工作日内采取相应补救措施。  3.网站内容服务  安排排一名资料编辑人员为本单位提供网站内容编辑上传服务，且将会对本单位网站上传的图片进行处理，保证网站页面的加载速度。同时，该人员提供网站CMS系统操作培训服务，医院相关人员遇到问题可向该人员反馈，若该人员能解答则可及时得到响应的解答，若该人员不能及时解答，则提交至相关人员处，由其他人员及时处理并反馈处理结果。在服务期限内，除提供文字资料编辑上传、修改、删除服务外，还可提供不改变网站主框架设计和功能结构前提下的其他修改服务，如：修改网站的图片、Banner设计、JS动画效果制作、Button设计等。  **网站应用程序维护服务**  1.软件保障维护  CMS系统和定制开发程序的升级、Bug和漏洞的修复、网站前台页面正常运行、数据库防注入等。其中，定期对CMS系统进行漏洞修复，且每年对CMS系统进行一次功能升级，使用系统更方便，且系统功能更强大。定期对网站和CMS系统进行漏洞安全扫描，对高危漏洞进行及时修复，防止网站出现安全问题。  2.网站安全保障服务  安装安全扫描软件，实时监控网站能否正常打开、是否被篡改和被注入，发现问题及时通知相关人员并进行修复。一般问题，在一个工作日内解决，并形成问题解决报告。本单位接受上级单位检查时，将协助医院处理上级单位形成的检查报告，并形成相应的问题解决报告，方便医院向上级单位汇报处理结果。  3.网站应急保障服务  编写网站预案，在网站遇到紧急突发情况时能有效应对，采取相关措施保障网站正常运行，同时相关技术和客服人员，提供7\*24小时不间断的应急保障服务，且可随时电话咨询了解相应技术问题。  4.现场处理服务  在网站应用程序出现故障时，若公司技术工程师远程不能解决，则该技术工程将继续保证远程监测故障，并派遣另一位工程师在故障发生后2小时内到达办公地点现场处理。同时保证每年至少3次不定期派服务人员到达办公地点现场维护及处理相关问题，如遇产品问题，停留至问题解决。  **网站监测分析服务**  1.网站性能监测  使用专业权威的性能监控平台对网站性能进行监测，主要采取监测节点、监测对象、检测指标三中手段进行性能监测。针对本单位的情况，主要从对象和指标进行监测，下面具体介绍详细内容。  1)监测对象  针对医院网站，主要监测的对象有：图片、页面、视频文件、动态行为和上传过程。监测图片、页面和视频文件主要是因为用户比较关注资源的加载和视频的播放速度。而监测动态行为和上传行为主要针对内部工作人员。  2)监测指标  指标一般包括这几个方面，平均响应时间、可用性、首包时间、DNS 时间、建连时间、内容下载时间、SSL 握手时间（对 HTTPS 协议监测）、重定向时间。其中可靠性指访问成功率，该值越高越好；建连时间指用户和 WEB 服务器建立 TCP/IP 连接消耗的时间；首包时间指用户浏览器发起 HTTP 请求结束开始，到收到 WEB 服务器返回的第一个数据包的消耗时间。SSL 握手时间是针对 HTTPS 网站特有，重定向时间是配置了301或302跳转所对应的时间。  2.网站流量统计  网站流量统计主要分为三个方面：网站流量指标、用户行为指标和浏览网站方式，这些统计分析能帮助本单位工作人员从不同的方面分析网站运营的效果，同时可以看出用户最主要了解的内容，从而多放置相关咨询，方面患者的就医诊疗，下面详细介绍统计的内容。  1)网站流量指标  网站流量统计指标常用来对网站效果进行评价，主要指标包括：  ·独立访问者数量（unique visitors）；  ·重复访问者数量（repeat visitors）  ·页面浏览数（page views）；  ·每个访问者的页面浏览数（Page Views per user）；  ·某些具体文件/页面的统计指标，如页面显示次数、文件下载次数等。  2)用户行为指标  用户行为指标主要反映用户是如何来到网站的、在网站上停留了多长时间、访问了哪些页面等，主要的统计指标包括：  ·用户在网站的停留时间；  ·用户来源网站（也叫“引导网站”）；  ·用户所使用的搜索引擎及其关键词；  ·在不同时段的用户访问量情况等。  3)浏览网站方式  用户浏览网站的方式相关统计指标主要包括：  ·用户上网设备类型；  ·用户浏览器的名称和版本；  ·访问者电脑分辨率显示模式；  ·用户所使用的操作系统名称和版本；  ·用户所在地理区域分布状况等。  **网站防入侵服务**  常见的网站攻击方式有网站篡改、流量攻击、数据库攻击、恶意扫描和域名攻击，为了使网站能够正常稳定的运行，我们应该清晰掌握攻击网站的方式，以及掌握防入侵的具体方法。针对以上列举的常见攻击方式，我们将详细描述，并提出解决方案。  1.网页篡改  网页篡改主要是针对网站程序漏洞，植入木马（webshell、跨站脚本攻击），篡改网页，添加黑链或者嵌入非本站信息，甚至是创建大量目录网页。网站信息被篡改，将导致本站访客不信任，搜索引擎(百度为例)和安全平台(安全联盟为例)检测到你的网站被挂马，会在搜索结果提示安全风险，搜索引擎和浏览器都会拦截访问。具体的解决方式有：  程序设置：更换程序、更新补丁、修补漏洞、设置权限、经常备份  漏洞查杀：使用360网站检测、360主机卫士等软件，可实现漏洞的检测和查杀。  申诉平台：安全联盟  2.流量攻击  流量攻击分为CC攻击和DDOS攻击，其中CC攻击是指借助代理服务器模拟多个用户不停的对网站进行访问请求，DDOS攻击是指控制多台电脑向网站发送访问请求。流量攻击中，以CC攻击最为普遍，采用大量数据包淹没一个或多个路由器、服务器和防火墙。CC攻击会使服务器CPU达到峰值100%，网站瘫痪无法正常打开，IIS停止服务，出现503状态无法自动恢复;百度蜘蛛无法抓取网站，清空索引及排名，流量下滑。常见的处理方式有：  选择大型安全有防火墙的主机服务商，如阿里云、西部数码和新网互联等。  网站监控：可使用360网站监控  CDN防护：可使用加速乐、云盾等进行CDN防护  服务器：推荐使用服务器安全狗、网站安全狗等软件对服务器进行监测。  3.数据库攻击  数据库攻击常见的方式为SQL注入，即通过把SQL命令插入到Web表单提交或输入域名或页面请求的查询字符串，最终达到欺骗服务器执行恶意的SQL命令。若网站数据库被入侵，会使网站用户信息泄露，数据表被篡改。数据库被篡改比网页文件被篡改危害大得多，因为网页都是通过数据库生成的。针对数据库攻击采用以下方式处理。  1、网站程序开发时，编写防SQL注入的程序，使网站的安全性得到了提高。  2、在各种信息提交框处加验证。  3、对数据库安装数据库防火墙。  4.恶意扫描  恶意扫描是指为了攻击网站人为的通过工具自动扫描漏洞，主要为了发现漏洞，进而攻击网站。将会通过关闭闲置端口，修改默认端口的方式防止恶意扫描。  5.域名攻击  常见的域名攻击手段有：DNS域名劫持和域名泛解析，其中DNS域名劫持是指伪造DNS服务器，指引用户指向错误的一个域名地址，域名泛解析指域名被泛解析很多二级域名网站指向黑客网站，如指向博彩网站等。这种攻击会使网站引起搜索引擎、安全平台不信任从而降权标黑。解决方式为：选择大型稳定的域名解析商，锁定解析，并且会实时监测域名解析，如发现异常将会及时处理。 | | | |

**以上标注“★”号的为本次采购项目的的实质性要求，供应商应全部满足。**

报价表

|  |  |  |
| --- | --- | --- |
| 序号 | 项目名称 | 报价（元） |
| 1 | 2025年度医院门户网站运维和安全服务采购项目 |  |
| 合计金额（大写）： | | |

**注：**

1.报价应是最终用户验收合格后的总价，包括设备运输、保险、代理、安装调试、培训、税费、系统集成费用和采购文件规定的其它费用。

2.“品目及报价表”为多页的，每页均需由法定代表人或授权代表签字并盖投标人印章。

3.如有多种规格，请按每种规格分别报价。

供应商名称：（盖章）

法定代表人或授权代表（签字）：

日期：

响应表

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 文件要求 | 响应文件响应 | 响应/偏离 |
|  |  |  |  |
|  |  |  |  |

注意：竞标人必须据实填写，不得虚假响应，虚假响应的，其响应文件无效并按规定追究其相关责任。

投标人名称（加盖公章）：XXX

法定代表人或单位负责人或授权代表（签字或盖章）：XXX

日 期：XXX年XXX月XXX日

**质量保证书**

：

（制造商家名称）是在 .（国名）依法登记注册的，其地址现在 。其主要营业地点现在 。

作为供应商，我方承诺，为本次招标提供的货物为原厂制造、合法渠道供应的全新产品。我方保证以投标合作者来约束自己，并对该投标共同承担和分别承担招标文件中所规定的义务。

供应商单位名称： （盖章）

供应商单位法定代表人或授权代表（签字）：

日期：

附：授权销售产品清单

**法定代表人身份授权书**

（采购单位名称）：

本授权声明： （投标人名称） （法定代表人姓名、职务）授权 （被授权人姓名、职务）为我方 “ ”项目投标活动的合法代表，以我方名义全权处理该项目有关投标、签订合同以及执行合同等一切事宜。

特此声明。

法定代表人签字：

授权代表签字：

投标人名称： （加盖公章）

日期：

★说明：上述证明文件附有法定代表人、被授权代表身份证复印件（加盖公章）时才能生效。

无围标、串标行为承诺书

本公司郑重承诺：我公司自觉遵守《中华人民共和国政府采购法》和《中华人民共和国政府采购法实施条例》的有关规定，我公司在参加本次采购活动中，无以下围标、串标行为：

1.不同供应商的投标文件由同一单位或者个人编制；

2.不同供应商委托同一单位或者个人办理投标事宜；

3.不同供应商的投标文件载明的项目管理成员或者联系人员为同一人；

4.不同供应商的投标文件异常一致或者投标报价呈规律性差异；

5.不同供应商的投标文件相互混装；

6.不同供应商的投标保证金从同一单位或者个人的账户转出；

7.不同供应商的董事、监事、高管、单位负责人为同一人或者存在控股、管理关系的不同单位参加同一采购项目；

8.供应商之间事先约定由某一特定供应商中标、成交；

9.供应商之间商定部分供应商放弃参加采购活动或者放弃中标、成交；

10.法律法规界定的其他围标串标行为。

我公司承诺在本项目采购活动中，与采购人不存在关联关系，与其他投标单位不存在关联关系。如被查实在本项目采购活动中存在围标、串标的，本公司将承担法律责任，接受相应的法律法规处罚。

投标人法人代表或委托代理人（承诺人） ：

投标人：（公章）

日期： 年 月 日