**官网回迁与综合运维服务项目**

## 项目背景

医院官网因历史客观原因，一直存放于区域信息中心的服务器机房，由于官网的等保测评合规要求，为进一步满足医院宣传管理、信息发布、日常运营、安全运维等工作需要，降低网站日常管理的综合维护成本、完善医院管理服务体系等方面考虑，现需将官网回迁到本院机房并提供专业化的综合运维服务。

本项目要求对医院网站提供综合的网站回迁与部署配置服务，提供SSL证书采购与配置服务，提供服务器基线扫描与应用安全扫描服务、网页防篡改系统服务、应急演练服务、现场服务支持、网站SEO优化服务、2022年度等保测评（二级）服务、流量监测服务等，进一步密切协助医院相关科室做好信息发布管理、推广宣传管理、安全检查、安全防护、安全日常巡检、网络设置、安全管理和日常维护、流量监测等网站相关的所有综合运维服务工作。

## 项目建设清单

|  |  |  |
| --- | --- | --- |
| **序号** | **建设内容** | **详细技术要求** |
| 1 | 官网回迁与部署配置服务 | 1. 提供官网系统程序的源文件程序和数据库文件； 2. 针对官网程序和数据库进行整体的备份打包，包含WEB站程序文件、数据库文件、WEB站附件等网站相关的所有数据数据的100%无缝迁移； 3. 在官网系统进行回迁后，提供对官网系统软件授权的更新和加密； 4. 对回迁后的官网系统进行基础配置和安全策略检查，提供官网系统回迁后的服务器配置与数据库配置等配置服务，检查系统运行日志，查看是否有异常运行记录，对可能发生的问题进行积极预防，确保回迁后的业务可用； 5. 对回迁后的系统进行数据库备份、日志备份等备份服务。每日备份系统服务器数据目录并检查备份运行情况。 6. 协助进行灾难恢复；数据安全性评估、灾难事件分析。 7. 在服务器、数据库、存贮、网络及工作站各个环节，提供持续的优化服务，保障业务整体性能。 |
| 2 | 官网SSL证书服务 | 1. 根据单位的项目的相关安全接口配置需要，进行官网域名的SSL证书购买和部署实施; 2. SSL证书为泛域名证书，支持一个域名及其下属的所有二级域名加密，无数量限制（二级域名可无限自定义，可随时修改）。 3. SSL证书加密强度支持40/56/128 位自适应加密，支持128-256位加密（支持2048/3072/4096公钥加密）。 4. SSL证书加密算法需支持RSA+ECC+DSA以及SHA256签名算法并完全支持最新TLS1.3版本。 5. 支持所有主流SSL协议，支持IIS，Tomcat，Apache，nginx，云服务器负载均衡等多种服务器环境。 6. 支持日常的台式电脑和移动设备，支持主流浏览器、操作系统，支持5G网络及IPV6地址加密访问。 7. SSL证书签发地必须在国内，需确保SSL的正确部署和相关IP的HTTPS安全访问; 8. 根据医院的服务器和防火墙端口映射的业务进行SSL证书的配置。 |
| 3 | 服务器基线扫描与应用安全漏洞扫描服务 | 1. 针对服务器进行基线安全扫描，严格按照国内信息安全等级保护要求和CIS组成的基准要求，涵盖官网服务器的操作系统、Web应用、数据库等。 2. 要求提供主机系统漏洞发现、开放端口扫描、弱口令检测及配置脆弱性检测，并对扫描检测结果进行分析、形成报告，提供解读及指导服务，方便医院信息安全管理员对主机的安全进行检查和分析，及时修复漏洞、提高系统安全防护能力。 3. 通过对服务器主机信息和行为进行持续监控和细粒度分析，快速精准地发现安全威胁和入侵事件，并提供灵活高效的问题解决能力，为医院官网系统提供安全检测和响应能力。 4. 通过细粒度分析系统内潜在的风险与合规问题，一键任务化检测,基线检查结果可视化，及时发现Web应用漏洞、弱口令、风险文件、错误配置等，。 5. 全方位检测网站服务器系统存在的脆弱性，提供无死角的风险状况视图，先于攻击者发现安全问题，及时进行修补。 6. 自动识别应用配置缺陷，通过比对攻击链路上的关键攻击路径，发现并处理配置中存在的问题，降低可被入侵的风险。及时发现并处理服务器与应用系统的配置缺陷，有效解决潜在安全隐患。 7. 采用Agent探针式扫描，及时、精准地发现服务器主机系统需要打的重要补丁。同时，深入检测系统中应用、内核模块、安装包等，各类软件的重要更新，智能提取急需修复的补丁。 8. 基线扫描检查项类别包含访问控制、身份鉴别、安全审计、资源控制、入侵防范等多个类别。 9. 持续关注国内外服务器相关的安全动态及漏洞利用方法，通过基于agent的持续监测与分析机制，能迅速与庞大的漏洞库进行比对，精准高效地检测出来系统漏洞。   10、结合多个病毒检测引擎，能够实时准确发现主机上的病毒进程，并提供多角度分析结果，以及相应的病毒处理能力。 |
| 4 | 官网网页防篡改系统服务 | 1. 网页防篡改系统采用事前阻止+事后恢复作为网页防篡改方案，通过操作系统底层驱动技术实现事前阻止网页篡改行为，通过高效率的文件同步技术实现网页篡改后的实时恢复，通过深度扫描网页木马发现隐藏的已存在的网页木马，从根本上解决页面篡改，挂马，暗链等网页风险问题。 2. 在资产概况中可以查看所有绑定该中心的服务器信息,包括名称、分组、标签、IP、操作系统、终端版本等。可以按照模板名称的维度和按照资产的维度去查看当前已创建策略模板。 3. 可根据实际现场需要配置网页防篡改/发布配置/网站漏洞/cc 攻击/网站访问控制/网马查杀等功能项。 4. 在终端详情界面可以对服务器进行重启，查看服务器ip，MAC 地址，系统环境信息，网马库更新时间，终端版本等信息。在监听端口中可以看到系统占用的端口号，网络协议，对应进程，端口绑定ip 5. 网页防篡改可保护对象设置的目录及子目录下的文件无法被修改，支持例外设置，新增子规则对子目录设置例外。 6. 网站访问控制可以对一些特定的请求在网站漏洞防护之前直接进行阻断或拦截。网站漏洞防护，可对网站常见的 SQL 注入攻击、XSS 跨站、Web 容器及应用漏洞进行实时防护。 7. 智能检测并防御 CC 攻击，保证网站正常服务能力。可调节高、中、低三个防护等级，可自定义拦截提示 8. 可对单个或者多个资产进行网马查杀或者网马处理网页防篡改保护系统基本包；可以对不同的资产设置不同的扫描路径，支持同时对多个资产的多个目录进行网马查杀 9. 设置扫描路径后，检测路径下的网站后门，检测结果可放入隔离区并删除或放入信任区。 |
| 5 | 官网应急演练服务 | 1. 在官网回迁后，提供应急演练整体的现场服务1次。 2. 针对官网系统和医院的实际情况，模拟网站被篡改后提供详细可操作的演练脚本方案。 3. 演练方案中的流程和内容应包括如下环境准备、演练开始、故障诊断、应急决策、指挥处置、发布信息、系统恢复、演练总结等多个环节。 4. 通过演练，检验医院网站篡改预案以及应急演练方案的完善性和指导性，同时提高医院相关工作人员与其他部门/机构的协同能力。 5. 通过后续应急的演练总结，完善应急演练方案、改进应急操作及流程、全面提高网站篡改事件的应急响应能力。 |
| 6 | 官网现场与日常运维质保服务 | 1. 提供运行环境（操作系统、数据库）变更，网络环境、服务器变动或机房搬迁引起的移机的支持等服务。 2. 系统定期主动的远程检查服务，内容包括：服务器磁盘空间检查、数据库自动备份检查、应用程序备份检查、系统运行速度检查、系统日志异常运行记录检查等。 3. 提供官网的服务器安全运维服务，包括服务器部署环境排查、系统应用检查、安全配置、安全策略、系统备份、文档归存等综合安全运维服务。 4. 根据省市政务数据局和市网安部门的安全要求规范选择较高版本的数据库进行安装与权限设置服务；提供官网的数据库安全运维服务，包括数据库策略、数据库配置、数据库备份等服务。 5. 根据省市政务数据局和市网安部门的安全要求规范进行系统的部署与配置；根据省市政务数据局和市网安部门的安全要求规范进行堡垒机等安全运维。提供省网络信息安全中心要求的主机安全防护工具（安全狗） 6. 配合网安等安全主管部门的相关安全检查和扫描渗透； 7. 根据国家信息安全漏洞共享平台(CNVD)、省网络安全应急响应平台、市网络与信息安全信息通报中心等省市区网安部门的漏洞扫描、预警等进行及时反馈、快速排查、应急处置等服务。协助院方人员进行灾难恢复、数据安全性评估、灾难事件分析。 8. 提供包括官网系统的BUG修改，原有官网功能的接口变更、对于工作量小于3个工作日的官网功能变动予以二次开发，如工作流程微调、HIS接口变动、政策新要求等服务 9. 提供系统升级、技术答疑、日常咨询等技术支持。   10、提供电话、微信、邮件、传真等多种类型的技术支持服务，协助和指导院方的技术人员确定故障原因，找出解决办法予以解决，完成相关服务。  11、如遇到重大故障，运维厂商需承诺并可实现10分钟内响应，30分钟内工程师到达现场提供现场技术服务。  12、重大节假日以及特殊时期，为医院开通24小时服务，对服务需求随时响应。  13、在运维和质保服务过程中，需结合医院实际情况，提供信息化规划指导、安全咨询、技术咨询等网站相关的服务。 |
| 7 | 网站SEO优化服务 | 1. 针对医院品牌和网站进行在百度搜索、360搜索等主流搜索平台的综合推广服务，强化医院的互联网综合品牌影响力。 2. 结合医院实际需求，针对医院官网在搜索平台进行官网认证. 3. 针对医院名称进行关键词的SEO优化。 4. 针对医院的地理位置、地图标注进行检查和更新。 5. 针对医院、各科室、各专家的关键词进行搜索优化。 6. 梳理医院相关介绍的词条目录，汇总医院和科室的相关图文信息、视频素材。按月、按季度、按年进行针对医院科室和专家进行百度百科词条的创建与更新。 7. 严格按照相关的搜素平台规则，如百度百科、百度知道、百度文库等频道搜索的具体规则要求来编辑图文信息，对各信息进行标注和内容的出处引用。 |
| 8 | 2022年度等保测评（二级）服务 | 1. 以等级保护为标准开展安全建设运营，让安全建设更加体系化、标准化。配合医院官网系统开展等保测评工作，配合服务包括定级、备案、安全建设和整改、信息安全等级测评、信息安全检查等多个阶段。配合医院网站后期信息安全等级保护测评复评工作，修复网站系统可能存在的漏洞或缺陷，提升网络系统的安全防护能力，保证业务的连续性。配合医院单位网站取得《信息安全等级保护测评结果通知书》。 |
| 9 | 网站全流量监控分析系统 | 1.专用机架式设备，高度≥2U，CPU内核不少于14核\*1，设备内存不低于96GB，持续运行设备最大存储空间≥32TB，磁盘应采用RAID5冗余模式；  2.支持至少包括2个千兆电口，支持扩展接口模块；  3.支持冗余交流电源，单电源模块故障不影响设备正常运行，故障电源更换支持热插拔。  4.设备支持旁路部署，可通过交换机端口镜像或使用流量分流设备采集流量数据，数据采集可以多接口同时进行采集。  5.系统支持B/S架构，可直接解码数据包，对会话流进行还原，可查看会话流内容；  6.能够实时捕获网络中的通讯数据包，每秒流量处理能力≥1Gbps，并可提取网络元数据，对元数据和通讯数据包进行存储；可根据用户实际需求，配置相应的存储空间，无软件授权限制  7.系统支持自动提取网络元数据，包括HTTP、HTTP body MD5、DNS、POP3、SMTP、Mysql、ICMP、SSH、证书、cert、smb、radius、DHCP、socks、irc、krb5、BGP、isis、ldap、数据包载荷等20类以上元数据日志提取，元数据字段个数不少于300种。  8.支持网络行为精细分析能力，能够对重点关注的应用进行监控和报警，如SMTP，POP3，HTTP，FTP，DNS等应用进行检测和报警，发现可疑的行为能够进行深入到数据包级的分析  9.要求设备内置勒索病毒、挖矿、APT组织等安全事件的专题规则库，可配置自动调查任务通过专题规则库持续检测高危安全事件或政策要求的安全事件，对最新安全事件进行自查自排，及时发现中招主机，对已中招主机进一步扩线分析调查，彻底清除网络中潜在的安全威胁，避免进一步扩散 |