成都市第二人民医院

网站运维及安全服务项目报价表

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 项目 | 内容 | 用途 | 数量 | 报价（万/年） | 备注 |
| 网站运维及安全服务项目 | 成都市第二人民医院官网（域名：[www.cd2120.com](https://www.cd2120.com/)）运行维护服务、安全运维服务、ipv6服务等。详见网站服务要求。 | 在不改变现有系统体系架构和功能模块的情况下，提供官网技术支持及安全运维保障。 | 3年 |  |  |

报价公司：

联系方式：

日期：

成都市第二人民医院

网站运维及安全服务项目服务要求

1.网站运维服务及网站安全服务

1.1 采购内容：成都市第二人民医院官方网站（cd2120.com）运维服务及网站安全服务采购

1.2 供应商需对现运行的官网提供运维服务（现有网站系统的基础上进行网站维护服务）及云服务器系统的安装、更新和维护，安全设置和现有网站管理系统的安全漏洞补丁升级；根据云服务的安全公告及时打补丁；WEB运行环境的安装与配置。

1.3 供应商需对网站部署SSL证书、WEB应用防火墙、主机安全（安全中心）、日志审计（态势感知）、堡垒机等安防服务产品，确保通过网站三级等保测评，顺利拿到等保三级备案证书及测评报告。（需提供以成都市第二人民医院为主体的证明），定时查看，及时处理并有运维报告。

1.4Web应用防火墙

1.4.1 服务商提供的服务可适用于公有云、私有云和混合云及传统环境等场景，并支持多场景的统一实施和管理；

1.4.2 服务商提供的服务支持反向代理防护模式和主机防护模式；

1.4.3 服务商提供的服务网站漏洞防护:支持HTTP检测，持文件上传防护，通过自定义禁止上传的文件类型，对上传至web服务器的信息进行检查;

1.4.4 服务商提供的服务支持目录漏洞防护，支持禁止浏览畸形文件，支持短文件名防护;

1.4.5 服务商提供的服务支持网页后门（webshell）查杀，分为静态查杀引擎和动态查杀引擎；

1.4.6 服务商提供的服务支持资源防盗链防护，支持特定资源防护，通过对某些特定资源的进行防护，不允许被下载或被盗用。保护模式有资源路径保护 和 资源类型保护。

1.4.7 服务商提供的服务内容防护模块:支持网站后台防护，支持响应内容防护;

1.4.8 服务商提供的服务支持CC攻击防护：支持通过主动防御系统防御CC攻击。

1.4.9 服务商提供的服务支持黑白名单管理：支持通过设置IP地址为黑名单地址或者白名单地址，调整指定IP/IP段对网站的访问权限。支持的设置有白名单、黑名单、封禁区域、爬虫白名单。

虚拟补丁：支持在无需打补丁的情况下，通过其他方式进行非法攻击拦截，完成漏洞防护。

1.4.10 服务商提供的服务支持攻击分析：支持对攻击事件源和攻击源事件的分析；支持从多个维度挖掘攻击者IP的地理信息、活跃度、攻击手法特征、攻击次数、攻击服务器范围等并进行画像分析和威胁程度排名，提供攻击IP风险分布图、攻击IP地理分布图、最近30天攻击IP列表。

1.5安全中心

1.5.1 资产清点:服务商需要通过安全中心服务进行资产管理，能够定期获取并记录主机上的Web站点、Web容器、Web应用、Web应用框架、账号、计划任务、端口、数据库、进程、第三方组件、环境变量、Jar包、系统安装包、软件应用、内核模块等信息。

服务商需要对主机开启各类监控包括登录监控、完整性监控、操作审计、进程监控、资源监控、性能监控、会话监控，能确保第一时间发现服务器问题。

1.5.2 入侵检测：服务商需要处理各类入侵事件及具有高度威胁的事件，支持识别并处置的入侵威胁事件包括：病毒木马、网页后门、反弹shell、异常账号、日志删除、异常登录、异常进程、系统命令校验等。服务商需要对接国内外主流病毒查杀引擎，采用不少于4个的多引擎查杀，可检测出恶意进程及软件，并提供隔离、信任等功能。

1.5.3 安全体检：服务商可主动发起主机深度检测，检测的项目包括：系统漏洞、弱口令、高危账号、配置缺陷、病毒木马、网页后门、反弹shell、异常账号、日志删除、异常进程、系统命令校验等。

1.5.4 安全基线：服务商需要对服务器操作系统（Windows和Linux）配置和web容器配置的基线内容进行检查，可以设置合规基线检测的基线模板，设置模板基础信息、规则信息，支持自定义基线检测。

1.5.5 病毒防护：服务商能提供病毒防护和主动防护功能，需要支持暴力破解防护、扫描防护、病毒防护、IP黑白名单、端口安全防护、访问控制、进程行为控制、反弹shell监控、远程登录防护、本地提权防护。

1.6堡垒机

1.6.1 服务商提供的服务可用于集中管理资产权限，全程监控操作行为，实时还原运维场景，保障云端运维身份可鉴别、权限可管控、风险可阻断、操作可审计，助力等保合规。

1.6.2 服务商提供的服务建立统一安全运维通道，通过运维权限细粒度管控、风险命令实时阻断、密码无感知托管、操作行为录播审计等，解决“众多资产难管理”、“运维职责权限不清晰”以及“运维事件难追溯”等问题。

1.6.3 服务商提供的服务支持权限细粒度划分，有效防止越权行为导致的敏感数据泄漏事件发生

1.6.4 服务商提供的服务支持高危风险命令实时阻断，保障运维过程中的业务系统安全；

1.7SSL证书

1.7.1 网站数据加密

1.7.2 提升网站用户访问网站的安全性

1.7.3企业级SSL证书，浏览器上有https提示并有绿锁标记。

1.7.4 品牌选择：GeoTrust、GlobalSign、CFCA、Symantec等主流品牌。

1.7.5 域名类型：通配符域名（泛域名）。

1.8日志审计
1.8.1 提供威胁情报源管理功能，支持本地威胁情报管理和在线威胁情报联查接口管理功能；本地威胁情报管理支持手工录入、批量导入和定时远程FTP下载；威胁情报种类至少支持IP、域名、URL和文件HASH。

1.8.2 支持用户通过平台接口针对URL、IP、未知文件信息进行云端情报查询，获取URL、IP、可疑文件的威胁情报，帮助用户判断威胁程度；支持定时从云端获取情报和手工获取的方式

1.8.3 平台内置信誉库、地理信息库、漏洞库，并可持续更新

1.8.4 平台支持针对日志或事件类型生产新的事件关联规则配置，规则包括对日志或事件的统计，属性值比较的配置，支持配置滑动时间窗口和定时时间窗口。

支持的告警事件规则包括:

（1）事件数告警

用户可以创建基于搜索结果的告警触发条件，在一个给定的时间范围内触发告警的阈值数。例如，用户可以设置告警条件为5分钟内搜索结果计数超过10次（基于时间戳）。

（2）字段统计告警

字段统计告警为您提供针对字段内容的告警设置，在触发条件中用户需要填写字段名，统计方式可以在下拉框中选择，cardinality（独立计数）、sum （求和）、avg（平均值）、max（最大值）、min（最小值）。例如，告警触发条件为：clientip在5分钟之内某个ip的计数值超过10。

1.8.5 提供的日志支持包括：入侵防护日志、应用管理日志、认证日志、防病毒日志、数据防泄漏日志、Web安全日志、运行日志、高级威胁日志、url过滤日志、VPN日志、waf日志、内容审计日志、数据库审计日志、无线热点发现日志等。

1.8.6 提供的支持能够对海量应用安全审计日志进行稳定、高速、容错的持续采集。具体包括：

（1）高可靠：数据传输过程失败重复和虑重机制，保障一致性；

（2）低时延：流式数据处理，秒级数据分发；

（3）可复用：7天数据缓存，数据可被多次订阅；

（4）软硬结合冗余：采用硬件设备负载均衡和服务器硬件、软件集群工作模式确保高可用。

1.8.7 提供的支持包括定时备份：包括支持对日志数据、系统管理数据等重要数据自动定期备份至备份服务器，保障系统在出现重大故障时可快速恢复正常状态。

1.8.8 攻击分析：分析模块包含【自动化分析引擎】和【交互式分析功能组成】，其中自动化引擎包括：关联分析引擎、定向攻击引擎和问题资产引擎，采用实时计算方式根据预定义规则模型产生告警事件、问题资产。交互式分析功能针对安全分析师提供查询、搜索、统计、透视调查、扩线溯源等高级分析功能，分析师结合自身安全知识背景发现深层次问题，提升研判分析工作效率。

1.9云服务器租赁：

1.9.1 阿里云服务器为华东1（杭州）可用地区的服务器。

1.9.2 4vCPU 内存8GiB 。

1.9.3 x86计算架构。

1.9.4 环境部署为CentOS，7.7.64位镜像。

1.9.5 云盘达到50G+500G，固定带宽为10M。

1.10技术指导及技术支持支援：现有网站内容运维操作培训指导，投标人应提供安全技术支持，提供24小时的热线支持，发生网络安全响应时间：1小时。若电话中无法解决，2小时内到达现场进行维护，并应于24小时内完全解决故障，提交完整的事件分析报告，详细说明事件原因、经过和处理方式等，而且对以后整改的方向提供适当的解决方案，提供维护报告。

1.11 供应商需24小时受理甲方的维护请求，同时医院反馈工单享有优先处理权；日常维护中，供应商随时做到无限次系统重启；提供固定的网络IP和100M共享网络带宽峰值可达10M，全年365天永不断电的电源和恒温恒湿的机房网络环境；24\*7客户服务电话，并保证24\*7小时有人接听。供应商无权复制、传播、转让、许可或提供他人甲方存放在服务器上的任何资料、软件、数据等资源，否则应承担相应的责任。

1.12 因供应商原因，造成服务器网络中断，供应商应第一时间提出并实施解决方案。

1.13 供应商不得在医院租赁服务器上架设其他和甲方无关的网站。

1.14 供应商需定期对托管服务器的安全运行状况进行巡查和维护，若有问题及时处理并通知医院信息中心，提供巡查维护报告。

1.15供应商需完成域名cd2120.com的域名解析、续费等操作。

1.16网页出现信息错误时，立即处理，在30分钟内更正。

1.17提出现有板块更新求及新增板块内容求时，在半小时内响应，2小时内完成更新。有专人负责甲方单位官网（中英文及手机）的美工、版块制作维护，提供24小时电话咨询服务，及时处理更新要求。

1.18提供多类型文档、图片、视频文件的上传下载，可进行外部网页链接。

1.19日常维护中英文网站电脑版、手机版，信息同步及时。

1.20提供网站浏览情况月分析、半年分析、年度分析、网站内容导出、导入等数据备份功能。

1.21网站具有一键关停功能，有专人专班应急处置。

1.22网站信息安全性、稳定性、保密性措施，网站响应体系等内容待信息中心提出专业意见建议。

1.23能根据医院及相关科室需要，负责二级网站、跳转端口等建设，提供相应配合。

1.24网站安全符合等保三级标准，测评未达到三级要求需配合整改到位（整改内容需要对现有的网站系统所有漏洞进行修复，网站管理系统及服务器、数据库等所有漏洞（高、中、低）进行修复，包括且不限各种文件制度的编写等）。

1.25配合医院进行漏洞扫描、渗透测试等安全测试并对发现的问题立即进行整改，直至通过测试。

1.26具备防攻击、防入侵、防篡改、防病毒等技术措施，具备拦截、封堵等功能。

1.27有机器审核方式，实现7\*24小时监控巡查，支持人工团队对机器审核告警的内容进行复核，内容审核必须覆盖网页内容、用户账号、用户头像图片和通讯群组名称、昵称、简介、备注等

1.28建立有害信息快速处置制度措施，支持发现违法有害信息1分钟内处置并在后台保留原始记录，即原始发布信息内容、发布时间、发布者使用IP及端口等。

1.29具备封禁特定账号、禁止新建账号、禁止分享、禁止留言及回复、控制特定发布来源、控制特定地区或指定IP账号登陆、禁止客户端推送、切断与第三方应用的互联互通等措施。

1.30制定并公开用户隐私协议，不得超范围采集非服务所需的个人信息。

1.31明示加入的第三方SDK，以及第三方SDK收集信息的理由与用途。

1.32落实容灾备份，一旦服务中断可立即切换恢复。

1.33制定包含处置违法信息发布、DDoS攻击、勒索病毒、网页篡改、木马、数据泄露等各类网络安全事件的应急预案，定期开展应急演练。

1.34重大活动举办期间组织网络安全技术及运维团队开展7\*24小时值班值守，随时应急响应。

1.35提供节假日banner图、通知栏等的制作与更新，提供的所有素材、图片、视频等乙方必须保证具有版权，甲方无偿使用。

1.36ipv6服务

1.36.1 达到上级单位对医院门户网站IPv6要求，门户网站完全支持IPv6环境下运行，实现“IPv6第二级链接支持率”、“IPv6第三级链接支持率”和"支持度评分"，达到三项评测指标要求。

1.36.2 所有涉及第三方产品的采购、安装、调试均由乙方组织负责完成，并保证其正常运转和售后服务，乙方承担因此而发生的一切合理费用。

1.37 其他要配合医院的工作。