附件1：采购项目配置需求

1.产品名称：四川省妇幼保健院网站系统升级及安全加固服务

2.数量：1套/年;

3.技术参数要求：

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **产品名称** | **年度预计用量** | **技术参数** |
|  | **服务要求** | **/** | **★本次安全加固升级需在医院现有的网站管理系统基础上进行安装部署，并获得原网站管理系统开发公司的授权。****★进行安装部署时，期间加固升级中会对原系统进行改造，该方面需要原系统开发公司协助并且所产生的服务费用都由中标方承担。****★按照等保三级要求进行日常安全运维，并协助通过每年重保活动和等保三级测评及整改，整改内容需要对网站系统所有漏洞进行修复，需要原系统开发公司协助并且所产生的服务费用都由中标方承担。** |
|  | **Web应用防火墙** | 1 | 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；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；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;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;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；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。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;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。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。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。 |
|  | **安全中心** | 1 | **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。**★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。**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。**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。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。 |
|  | **堡垒机** | 1 | ★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。★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。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★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 |