采购需求

**一、项目概况**

1、项目名称：江苏医药职业学院网站云防护服务项目

2、项目地点：江苏医药职业学院

3、总体要求

随着网络安全法的颁布和实施，我国对于网络安全的重视空前提高，高校网站在《关键信息基础设施安全保护条例》中被列为关键信息基础设施需要在等级保护基础上进行增强防护。我校网站云防护体系建立，旨在提升对于网站安全状况的感知、提供多维网络攻击防护能力，保障网站高可用性，实现网络安全风险管理闭环。

本次服务要求中标单位采用专职服务团队人员加后端专家服务团队人员的方式进行整体服务实施。服务方需成立不少于10人的后端专家服务团队，安排高素质的后端支撑人员配合专职服务团队人员，完成招标人提供所要求的网站云防护服务项目和相关技术支持。同时，后端专家服务团队需具备丰富的漏洞挖掘能力、专业的渗透测试能力、数据安全能力及专业的应急响应支撑能力，以应对针对我校网站群的各种网络安全攻击及安全事件。提供在线专家的7×24小时应急响应，当发生安全事件时能够及时响应并协助处置

4、设备清单

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 设备名称 | 基本规格参数 | 数量 | 备注 |
| 1 | 网站云防护服务 | 主动加强对网站群的实时动态防御，保障各类网站的安全，建立常态化监测防御、预警通知与安全分析报告和应急保障。通过7\*24小时攻击预警和通知服务，使网站管理和维护人员能够实时获取网站群内所有网站的安全状况；能够通过周期性的检查，发现网站群内所有网站存在的安全漏洞并及时告警；实现在线网站安全专家的7×24小时应急响应。 | 1套 | 网站云安全防护服务 |

**二、主要技术指标：**

|  |  |
| --- | --- |
| **指标项** | **指标要求** |
| 防护能力 | 支持无限制IPv4访问带宽、无限制QPS，支持弹性资源调配，特殊情况下可为网站动态分配节点及带宽资源，保障网站正常运行 |
| 产品部署 | 无需对原有网络拓扑进行任何更改，需将CNAME别名指向云防护平台 |
| 智能DNS | ★支持根据客户不同服务的运营商智能选择不同的DNS进行解析，并支持解析负载功能**（需提供截图证明，加盖投标人公章）** |
| 端口自助配置 | 为了满足业务需要，要求能够对网站除80、443以外的非标准端口提供防护，并可以自助配置 |
| https网站防护支持 | 支持HTTPS网站防护，可支持SSL证书上传到防护服务器 |
| 非标准端口防御 | ★提供所有支持的http协议防护端口>300个；https协议防护端口>100个，提供防护平台端口统计表**（需提供截图证明，加盖投标人公章）** |
| Web防火墙 | 可防护SQL注入、命令注入、跨站脚本、文件包含、信息探测等常见攻击，防止网站因为漏洞导致被篡改，被拖库，被入侵。 |
| Webshell防护 | 使用WebShell进行攻击尝试和试图访问WebShell的IP地址将被屏蔽，可在整站设置中修改屏蔽时间 |
| IP黑白名单 | 可根据IP地址，建立黑名单或白名单，阻止或者允许特定IP进行访问 |
| 智能攻击识别 | 精准识别上百种自动化扫描和攻击软件，并阻断其所有请求 |
| 后台锁 | 禁止非授权IP访问网站后台管理地址或重要页面 |
| 防盗链 | 保护网站图片、压缩包等资源文件不被其它站点盗用 |
| 拦截黑白名单 | 设置不进行防护的IP地址（IP白名单）、不允许访问的IP地址（IP黑名单）和不经过防护的URL地址（URL白名单） |
| 日志下载 | 提供日志下载功能，并区分原始日志，攻击日志和CC攻击日志下载 |
| 网站访问情况 | 包括请求数、总流量、网站浏览人数，搜索引擎引导量，遭受攻击次数等，并能按时间端统计的网站访问量 |
| 网站安全状况 | 包括各种攻击发生次数，攻击IP、来源（国家）等 |
| 网站安全评级 | 网站安全、危险等评级，可显示历史攻击次数 |
| 攻击扫描统计 | 可显示攻击者的扫描情况，包括时间、攻击URL，攻击者IP及归属地，攻击类型等 |
| 攻击统计数据 | TOP5攻击来源国家、TOP5攻击来源城市、TOP5攻击来源IP |
| IPV6防护 | ★提供不少于100个二级域名的IPV6防护服务，无限制IPv6访问带宽、无限制IPv6访问QPS。支持在不改变网站既有配置得情况下，无缝提供访客IPV6访问；提供IPV6 DNS解析服务，该IPV6 DNS具有抗DNS DDoS能力； |
| 实时防御和追踪 | 基于世界地图和中国地图两种视角，实时防御和追踪系统可以直观地查看目前网站的安全状况，被攻击情况，攻击地域分布、攻击类型分布、攻击 IP 情况，以及遭受攻击的具体网址等情况 |
| 防护节点组 | ★提供良好的用户访问体验，全国云防护集群节点IP段≥20个、线路类型≥60个，且覆盖移动、电信、联通国内三大主流运营商，提供IP段、线路类型明细**（需提供截图证明，加盖投标人公章）** |
| 设备生产厂商资质 | 产品具备工信部颁发的中华人民共和国增值电信业务经营许可证（互联网接入服务业务（全国）、内容分发网络业务类（全国）  中国信息安全测评中心颁发的《国家信息安全漏洞库兼容性资质》证书。**（提供有效期内证书复印件并加盖投标人公章）** |

**防护站点数量：主域名及子域名合计约100个站点左右**

**三、质量和服务要求：**

1、所供产品必须符合国家标准，设备和配件为全新原装，功能符合使用要求，保证为正规渠道供货的正宗原厂产品。须提供良好的售后服务，终身提供技术支持。

2、供货方式、时间及地点要求：

合同签订后30天内设备运抵江苏医药职业学院校内指定地点，并完成安装及调试。

3、质保期及服务要求：

（1）培训及售后服务：现场完成安装、调试之后，由中标方工程师提供免费操作培训。培训内容主要包括设备原理、基本操作要领、设备简易故障排除和维护保养知识等。

（2）须提供售后服务团队人员名单清单和联系方式。

（3）质保期：提供至少 1 年的免费质保期，自验收合格之日起计算。质保期内中标人需提供7×24小时热线服务、须定期上门进行例行检查，并做好记录，以保证设备正常运行。对于采购方的服务通知，中标方必须在接到通知后1小时内予以响应，若有必要，中标方工程师必须2小时内到达现场，常见问题 4小时内处理完毕。若大问题在48小时内未能有效解决，中标方须免费提供同档次的设备给予采购方临时使用。

服务期：合同签订后7天内完成前期准备，经学校信息中心确认具备正式开展服务的条件后，进入正式服务期，正式服务期为一年。一年期满，服务质量达到我校相关要求，且履约情良好的，在采购人同意的情况下，可续签一年（续签不得超过两次）；

4、验收方法及验收标准：

货物发运前，必须对系统的质量、规格、性能等方面的技术数据进行综合检验，需随系统提供检验合格证书和原产地证明书。 现场安装、调试结束后，中标方和采购方相关人员按验收标准进行验收。验收标准为招标文件、投标文件、合同中的相关技术及服务条款内容。

5、服务质量考核

为评价中标方提供的服务质量，每季度对中标人的安全服务进行考核评分（百分制），年度考核评分为每年四个季度考核的平均分。详细考核机制如下表：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **考核** | **考核项目** | **分值** | **评价描述** | **评分** |
| 工作考核  90分 | 任务完成效率 | 40 | 未充分规划、在规定时间内不能完成任务 | 每次扣5分 |
| 任务完成质量 | 50 | 出现质量异常（投诉、失误、返工） | 每次扣3分 |
| 出现严重质量异常（投诉、失误、返工） | 每次扣6分 |
| 出现因安全服务导致的宕机超过4小时 | 每次扣10分 |
| 响应需求被动，消极处理问题 | 每次扣5分 |
| 人员考核  10分 | 服务质量 | 10 | 不注重沟通，遇到问题以强硬或回避的态度来应对 | 每次扣2分 |
| 服务态度差，甲方收到投诉 | 每次扣5分 |

**考核说明：**

1.考核初始赋值 100分。考核表格包括但不限于以上内容，在实际运作中不断完善。每个考核项目扣分项最多将该项分值扣至0分。

2.每季度考核分数在60到80分之间，将要求中标方对安全服务团队责任人进行谈话，并责令整改。每季度考核分数≦60分，中标方须更换安全服务实施人员，更换人员须符合安全服务人员要求。如无法更换符合要求的安全服务人员，甲方将终止合同，并拒付剩余合同款项。

3.年度评分将作为考核中标方服务质量的依据，作为下一次安全服务招标对中标方评价的重要参考依据。