## 服务需求响应情况一览表

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **服务项目** | | **服务内容** | **服务**  **时间** | **是否**  **响应** |
| ★医院信息系统安全服务 | 安全巡检 | 对安全设备和重要的安全信息资产每季度进行安全巡检，并出具安全巡检报告。 | 每季度 |  |
| 安全扫描  渗透测试 | 1.保障南通市第二人民医院的安全性，对网络、安全设备、主机设备进行安全扫描及渗透测试。  2.对安全隐患提出相应的解决建议方案。 | 每季度 |  |
| 风险评估 | 准确掌握南通市第二人民医院信息系统当前的安全总体状况，查找系统中可能存在的安全弱点和缺陷，能够有针对性的实施安全建设和整改。 | 每半年 |  |
| 等保服务 | 1.根据国家相关法律法规的要求，设计甲方的等级保护所需方案，提供等级保护相关咨询、进行等级划分、等级保护策略的部署及等级保护相关的其他工作，同时配合各个相关部门的检查。  2.配合完成本次甲方信息系统的等级保护测评服务，包括：1个三级系统。 | 1次 |  |
| 项目咨询服务 | 包含从项目立项、前期调研、可行性研究、方案设计、设备选型参考，招标书的制作以及项目管理辅助，项目验收辅助的整体的咨询服务解决方案。 | 按照甲方实际需求 |  |
| 网络与信息安全体系设计 | 提供信息安全防御体系、监控体系、应急体系、重要的基础设施和组织架构等体系建设的咨询服务，并制订合适的安全策略、措施和方案。 |  |
| 网络与信息安全规划及解决方案设计 | 提供信息系统建设的规划和方案设计服务。 |  |
| 等级保护测评咨询服务 | 提供定级备案咨询、差距评估咨询、整改方案设计咨询、测评咨询服务。 |  |
| 信息安全通告服务 | 安全通告服务以邮件、电话、走访等方式，将安全技术和安全信息及时传递给客户。 |  |
| 信息安全管理咨询服务 | 协助甲方对网络与信息安全内部管理建议、制度建立。 |  |
| 应急响应服务 | 派遣工程师到现场协助甲方开展信息安全应急方案演练工作，在国家召开重大会议、举办重大活动或节假日、发生相关安全事件及相关部门安全检查时，为甲方提供远程或现场信息安全应急服务支持，并由专人（至少1人）对日常应急情况提供响应，设立7\*24小时应急服务支持电话。 | 1小时内到达故障现场，并在到达后4小时内解决 |  |
| 培训服务 | 提供安全意识和技能培训服务包含：网络架构知识培训、安全意识培训、信息和信息安全、风险管理和风险评估、网络及安全技术培训、网络及安全产品培训等项目。 | 每半年进行一次全院安全培训，信息科专业培训按需进行 |  |
| ★等保测评 | 等级保护  测评 | 1.根据国家相关法律法规的要求，设计甲方的等级保护所需方案，提供等级保护相关咨询、进行等级划分、等级保护策略的部署及等级保护相关的其他工作，同时配合各个相关部门的检查。  2.配合完成甲方信息系统的等级保护测评服务，包括：1个三级系统。 | 1次 |  |
| 网站安全监测与防护 | 资质 | 知名品牌网站监测与防护系统，原厂商注册资金不少于5000万，需提供经年检合格的营业执照副本复印件  原厂商产品开发、生产、服务等管理体系符合ISO27001:2013要求，提供相关认证证书的复印件，并加盖单位公章  原厂商应为国家级网络安全应急服务支撑单位，应提供相关证书或CNCERT网站截图的复印件，并加盖单位公章  原厂商作为中国国家信息安全漏洞库（CNNVD）一级技术支撑单位, ，应提供相关证书的复印件，并加盖单位公章 |  |  |
| 平台要求 | 全国范围内具备至少20个云防护和CDN加速节点  支持不小于300Gbps拒绝服务攻击流量防护能力，并提供证明文件  要求安全防御平台为一体化平台，应同时具备网站漏洞监测、可用性监测、攻击防御状态、防护报表、页面防篡改等功能,要求所有的功能集成在同一产品上实现。所要求的功能需要提供可视化界面配置。 |  |  |
| 部署方式 | 无需在网站前端安装任何安全设备、软件，通过DNS流量指向到云端进行安全防护 |  |  |
| 支持将防护网站NS解析到云防护DNS服务器，支持将防护网站CNAME别名指向云防护 |  |  |
| 防御功能 | 支持检查提交的报文是否符合HTTP协议框架，如异常的请求方法、特殊字符、重点字段的缺失、超长报文造成的溢出攻击以及对高危文件的访问等 |  |  |
| 支持识别恶意请求含：跨站脚本(XSS)、注入式攻击（包括SQL注入、命令注入 、Cookie 注入等）、跨站请求伪造等应用攻击行为 |  |  |
| 支持识别服务端响应内容导致的缺陷：敏感信息泄露、已有的网页后门、错误配置、目录浏览等缺陷 |  |  |
| 支持基于访问行为特征进行分析，能识别盗链、爬虫攻击的能力 |  |  |
| 支持识别网站中的网页木马程序，通过策略可防止木马网页被用户访问 |  |  |
| 支持对用户上传的文件后缀名和文件内容进行全方面检查，杜绝Webshell的上传和访问 |  |  |
| 支持对WEB服务器容器、应用中间件、CMS系统等第三方组件漏洞进行有效防护 |  |  |
| 支持页面缓存，通过水印匹配算法防止页面被篡改 |  |  |
| ★支持智能识别攻击者，对网站连接发起攻击的IP地址进行自动锁定禁止访问被攻击的网站，提供界面截图并加盖公司公章 |  |  |
| ★支持一键虚拟补丁功能，网站出现0day漏洞时能快速完成修复，提供界面截图并加盖公司公章 |  |  |
| ★支持按地理区域对攻击次数等进行统计，通过地图展示，用户可在地图上可以指定某一地理区域进行访问控制，阻断此区域 IP的访问，提供界面截图并加盖公司公章 |  |  |
| 安全审计 | 能详细记录攻击事件的HTTP请求头信息，含请求的URL、UserAgent、POST内容，cookie等所有的请求头内容 |  |  |
| 能详细记录服务器响应头信息，包括状态码、服务器类型等信息 |  |  |
| 报表 | 提供全面、详细的统计报表功能，能够提供图形界面进行查询 |  |  |
| 可查看安全防护报告，包含攻击者区域统计、攻击者IP统计、被攻击页面统计、被攻击域名统计、攻击事件统计、攻击威胁等级统计等报告。 |  |  |
| 可查看可用性监测报告，包括各省的延时数据、可用性、故障次数和故障时长等信息。 |  |  |
| 告警方式 | 支持Syslog、手机短信、邮件、密信等多种告警方式 |  |  |
| 网页防篡改 | ★提供专业防篡改软件，部署于网站服务器中，支持主流的web服务器和操作系统，实现网页防篡改功能 |  |  |
| CDN内容加速 | 全国范围内具备至少20个CDN加速节点支持页面缓存和压缩 |  |  |
| 云监测 | 支持服务质量监测，支持全国多省服务是否中断或报错告警、访问延时分析、域名劫持监测、页面加载质量分析、CDN服务质量监测 |  |  |
| 支持钓鱼监测，通过大数据监测网络中是否存在与防护对象相匹配的钓鱼网站，发现钓鱼网站后及时与用户沟通并协助上报处置 |  |  |
| ★支持漏洞检测，对网站存在的脆弱性进行探查，包括SQL注入漏洞、跨站脚本漏洞、开放服务漏洞、网站第三方应用漏洞等，及时发现漏洞 |  |  |
| ★支持篡改监测，监测出网站是否被嵌入暗链地址、监测网站是否存在非法外部链接、监测网站内容是否存在敏感内容、监测网站是否篡改为黑页 |  |  |