**网站安全防御服务要求**

|  |  |
| --- | --- |
| 分类 | 指标要求 |
| 产品形态 | 云防护产品，基于Linux安全操作系统  无需在被防护网站上安装任何软件和代理  采用B/S架构支持通过浏览器远程对产品进行配置  无需对原有网络拓扑进行任何更改，只需将原网站域名指向云防护平台 |
| 产品资质 | 运营厂商具有全国性的增值电信业务经营许可证（ISP）  具备赛可达实验室的东方之星安全认证  需提供近一年内三次以上的国家级大型活动的网站安全保障支持活动的证据（包括感谢信），并不能有保护网站被攻击成功的案例。  需提供近一年内政府网站群防护案例（30个网站以上） |
| 攻击防护 | 支持对SQL注入、XSS跨站、文件注入、代码执行、文件包含、远程命令、恶意扫描等Web攻击的防范  支持对WebShell的防护  支持后台锁-禁止非授权IP访问网站后台管理地址或重要页面  支持在线锁-确保网站永久在线，发现页面不可访问可立即恢复  支持敏感关键词过滤-包括替换敏感信息、反动言论和淫秽内容，可自行添加关键词  支持防盗链-保护网站图片、压缩包等资源文件不被其它站点盗用  支持DDoS攻击和CC攻击防护， 需支持不低于CC攻击峰值不低于10000IP/小时及拒绝服务流量攻击防护不低于500Gbps的防护能力  能防护DNS flood攻击  7\*24小时专业团队防黑人工值守 |
| 智能加速 | 支持DNS负载均衡-根据用户使用的不同运营商链路智能选择DNS进行解析，并支持解析负载功能  支持访问加速-将页面缓存到节点供访客就近访问，提升网页访问速度  支持多域名绑定  支持页面压缩 |
| 服务范围（网站域名） | SMG官网[www.smg.cn](http://www.smg.cn) |
| 网站管理 | 支持IP黑白名单  支持网址黑白名单  支持网站访问情况和网站安全状况统计  支持攻击扫描统计CC攻击统计 |
| 实时防御动态 | 支持攻击统计数据- 包括TOP5攻击来源国家/城市、TOP5攻击来源IP国内、国外等 |
| 支持实时防御和追踪展示-基于世界地图和中国地图两种视角，动态展现攻击源位置对网站发起的各种方式攻击，攻击类型用不同颜色的动态线条来表示 |
|  |  |

**网站安全监测要求**

|  |  |
| --- | --- |
| 分类 | 指标要求 |
| 服务内容 | 网站安全7\*24小时监控  支持网站挂马监控  支持网站暗链监控  支持网站篡改监控  支持网站敏感内容监控  支持网站可用性监控  支持网监控  支持Web漏洞监控 |
| 服务频率 | 网站挂马、网站暗链、网站篡改、网站敏感内容监控每12小时一次  网站可用性监控每30分钟一次  Web漏洞监控每周一次 |
| 服务范围（网站域名） | SMG官网[www.smg.cn](http://www.smg.cn)，看看新闻网[www.kankanews.com](http://www.kankanews.com)，东方卫视[www.dragontv.cn](http://www.dragontv.cn)，第一财经[www.yicai.com](http://www.yicai.com)，东方广播网[www.eastradio.com](http://www.eastradio.com)，纪实[www.docuchina.tv](http://www.docuchina.tv)。 |
| 报警 | 发现网站挂马、网站暗链、网站篡改等问题发送邮件报警  发现网站可用性异常发送邮件报警  发现网站高危Web漏洞发送邮件报警 |
| 服务输出 | 每月提供监控报告，内容包括当月监控网站安全情况  每月对高危风险漏洞进行人工验证  每季度提供安全情况总结 |
| 服务案例 | 平台输出的监测服务，需证明该监控平台要求以下：  具备运营商实际应用案例三个以上  要求具备国家级信息安全监管机构成功案例三个以上  要求具备省级信息安全机构成功案例三个以上  要求具备五台以上的集群化部署能力并提供实际案例 |