网络攻击行为监控和脆弱性评估服务需求

一、服务需求

通过网络攻击行为监控和脆弱性评估服务，对所保障的网站进行实时监测以及不定期的安全漏洞扫描，出具网站安全状态报告，当网站出现安全异常或潜在风险时，及时出具报告并提供解决建议。

（一）网络攻击行为监控

针对保障范围内的网站、互联网业务系统、第三方外联系统提供安全监测服务。应包含网站可用性监控、域名解析监控、内容变更监控、HTTP请求方式监控、网站挂马监控、网站异常链接监控、违规内容监控。并实现对应用系统域名或IP地址进行7x24小时安全监测。当有疑似安全事件发生时及时响应并通知相关责任人，协助排查，定位故障原因。

（二）脆弱性评估

针对保障范围内网站、互联网业务系统、第三方外联系统提供Web应用的不定期漏洞扫描。结合人工风险验证，对网站及应用系统的网络安全风险进行评估，报送检测评估结果。

检测主要采用基于爬虫技术的主动监检测方式，无需在被监控网络部署任何代理或探针程序，不改变被检测方网络的任何配置和安全策略。

提供网站安全的漏洞检测服务，发现网站及应用的安全隐患。需包含但不限于OWASP TOP-2017最新的风险CVE，CWE和CNVVD对应编号及处理意见。

提供网站安全的挂马检测服务，基于挂马行为特征，对页面存在的链接进行检测，分析木马链接跳转，判断链接的跳转区域。由技术人员对检测结果进行人工核实确认，生成检测报告并提供相应的修改建议。

提供网站安全的异常链接检测服务，通过成熟的异常链接检测技术，对网站进行全面的链接检测和行为分析，确定链接的行为，判断链接是否为非法的链接，由技术人员对检测结果进行核实确认，生成报告。

提供对网站安全的挂马检测，异常链接、内容变更、违规内容的人工核实服务，漏洞扫描高风险结果的人工验证服务，确认网站的安全漏洞利用威胁，确保检测结果的有效性、准确性。

通过发现网站及系统存在的安全隐患，提供风险评估报告及整改建议，使相关单位网站的风险得以有效防治，确保重保期间所管辖单位重要网站及系统安全稳定运行。

提供通过对重保期间被监控的网站进行漏洞扫描、异常链接检测、挂马、内容变更、篡改监测、违规内容监测来综合分析网站安全及系统状况，并提供网站的安全评估报告。

对例行检查的网站中含有高危漏洞的网站进行单独呈报。

提供安全资讯，报告最新的安全动态以及与业务系统相关的紧急安全漏洞和事件。

二、具体要求

1、监测服务不得影响网站对外服务的正常运转。

2、对网站安全检测时，中、高危漏洞须人工确认。

3、提供7×24小时不间断提供监测服务，项目期内服务故障时间少于1小时。

4、提供7×24小时安全专家技术支持服务。

5、支持至少同时对50个网站页面进行监控。

6、监控间隔最少为2分钟，可按需配置。

7、支持短信、电话、微信、邮件多途径安全事件告警。

8、如有安全事件发生预警时间不超过10分钟。

9、挂马、篡改、暗链等的监控范围至少包含个站点二级页面，且预警时需定位页面。

10、重保监控期间，每日提供所监测网站的安全监测报告。

11、实时提供安全资讯，通告最新的安全动态以及与业务系统相关的紧急安全漏洞或事件。

12、实时了解监测网站安全检测风险结果，对各管辖区域进行深度的安全状况进行统一的查看按需呈现风险现状及预警。

13、服务团队安全工程师数量在20人以上，二线团队至少1 5 人。其中项目团队有不少于5人具有注册信息安全专业人员(CISP)证书及5年或以上相关行业从业经历及建设维护经验的，为优。

14、响应供应商具有本项目相关的安全风险感知软件著作权或专利专有技术的，为优；响应供应商具有中国信息安全测评中心颁布的国家信息安全测评信息安全服务资质证书、CCRC中国网络安全审查技术与认证中心颁发信息安全服务资质认证证书的，为优。