**上海海事大学服务器漏洞风险检测服务技术要求**

1. **参数要求：**

|  |  |  |
| --- | --- | --- |
| **序号** | **功能参数** | **服务内容描述** |
| 1 | 漏洞检测 | 支持以饼图、柱状图、趋势图等形式展示资产风险综合状况，支持从漏洞类型、服务类型等角度展示 |
| 支持风险监控配置，包括自定义监控周期及检测时间（支持按照日/周/月/自定义形式设置），规则配置 |
| 漏洞检测方式：采用高精度检测脚本，识别准确率95%，同时漏报率也控制在可接受范围以内 |
| 系统漏洞库能够覆盖了常见的操作系统漏洞、软件漏洞、最新的网站框架应用漏洞等。能够针对操作系统以及web漏洞进行检测 |
| 漏洞标准兼容：CNNVD、CWE  漏洞库兼容：CNVD、CVE、CNNVD |
| 基础漏洞检测：支持常见CMS应用漏洞，支持常见第三方框架和组件近8年高危漏洞和部分中低危漏洞，运维类漏洞如敏感文件泄露，目录穿越等漏洞的扫描 |
| 主机合规检测：基于服务版本对主机资产进行合规检测 |
| 弱口令检测：支持MySQL,SSH,FTP,SQLServer,Redis等常见服务的弱口令扫描，支持弱口令字典自定义 |
| 网站WEB漏扫：支持按照URL地址、周期、设置监控选项、并进行cookies、配出页面、爬虫深度、爬取URL数、扫描频率的设定进行扫描，支持SQL注入，XSS跨站脚本，命令执行等35种常见通用漏洞类型扫描，包括1500+通用漏洞规则。 |
| 支持主机漏洞检测 |
| 网站内容检测：支持违规内容检测（涉黄/涉赌/涉政/虚假证件）、篡改检测， |
| 基线检测：支持禁止端口及服务开放基线设定，确认是否已开放 |
| 2 | 漏洞管理 | 支持漏洞检测频率设置，可自定义扫描周期及检测时间 |
| 支持漏洞自动复测时间设置（关闭、自定义开始时间点） |
| 支持漏洞信息检索功能，可快速定位不同漏洞类型，不同资产漏洞 |
| 支持通过资产指纹进行漏洞分析，并从资产的类型、服务版本、漏洞类、漏洞严重程度等多个维度进行关联保存 |
| 支持按照漏洞名称、地址、资产IP、资产域名、漏洞状态、处理状态、发现时间进行展示 |
| 支持漏洞查看、重新检测、漏洞处理 |
| 支持漏洞一键导出Excel查看、一键分享给相关人员查看 |
| 支持漏洞确认、忽略操作 |
| 支持风险自定义检测：对资产临时进行风险检测，检测内容包括应急插件、基础风险检测、WEB风险检测，检测结果包括漏洞风险数、合规风险数 |
| 支持应急检测，能够有针对性对单、多个指定的漏洞进行指定范围的检测，快速精准定位 |
| 支持网站可用性监控、主机可用性监控 |
| 3 | 外部资产风险监测 | 支持GitHub代码泄露监测，支持自定义关键词及敏感代码设置 |
| 支持查看泄露的代码仓库、相关联的资产、上传代码的作者、发现时间 |
| 支持对于代码泄露进行确认和忽略操作 |
| 4 | 安全大屏 | 提供资产、风险的可视化大屏展示，包括资产地图、风险分析、监控分析、风险分布信息 |
| 5 | 系统管理 | 支持漏洞告警（站内信、邮件、短信） |
| 支持日报定时推送：掌握资产分布状况以及风险态势 |
| 支持在线升级、离线升级（包括系统版本更新和漏洞库更新） |
| 严重高危漏洞48小时内可出检测插件以及修补补丁，常规普通漏洞两周内更新一次 |
| 支持对账号信息进行管理，包含账户名称、注册邮箱、联系手机、密码强度、企业名称、所属行业 |
| 支持帮助中心：对系统使用过程进行详细指导 |
| 支持自定义logo，可以一键更换产品界面logo |
| 支持操作日志查看及下载，基于用户名/IP/事件的关键字搜索 |
| 支持资产报表、漏洞风险报表生成，支持在线查看，并以Word ,Excel形式导出 |
| 运营后台：支持多管理员使用产品，管理员用户支持添加、删除子用户（默认不给用户开放，除非特殊情况） |
| 支持白名单添加，对白名单资产不进行漏洞巡检检测 |
| 6 | API开放 | 支持API接口开放，可通过API接口实现创建扫描任务、获取扫描任务进度、启停扫描任务等动作 |
| 认证方式：支持token |
| API格式：RESTful |
| 开发者文档：包括接口规范、接口描述、测试用例 |
| 技术支持：在线培训、联调测试、接口升级 |
| 7 | 部署方式 | 设备支持虚拟化模式部署 |

**二、项目服务范畴和要求：**

（一）中标的公司须对上述风险监测管理服务内容提供根据上海海事大学情况针对资产的上线、下线、漏洞验证、修复等方面要做到实时监控，建立有效的资产和漏洞监控体系，实时掌握情况，及时做出响应；鉴于学校资产的复杂性和庞大性，方案需要具备从已知资产的特征入手，智能关联和发掘未知资产的能力，能够对未知及边缘资产进行有效管控，降低资产风险性。

（二）定期巡检

及时响应并处理系统出现的各类问题。对上述系统在维保期内提供每周1天现场技术支持，并提供每季度巡检一次学校系统环境，巡检结束后出具相应巡检报告。通过该巡检服务了解学校各资源使用情况和可能存在的潜在问题，提早预防，避免故障发生。其服务内容包括：

1. 包括漏洞告警、漏洞列表、漏洞操作、漏洞检索、漏洞导出、漏洞查看、漏洞处理；
2. 包括基础漏洞扫描、弱口令扫描、网站安全漏洞扫描、漏洞自动化巡检、基线检测；
3. 包括代码泄露监测、代码泄露详情查看、代码泄露处理；
4. 对资产进行风险分析，包括资产地图、风险分析模块、监控分析模块、风险分布模块等；
5. 包括账号及权限管理，报表管理，日志管理等；
6. 校方其他关于系统需求配置或调整。
7. 主机数量：不少于1000资产（主机资产+网站资产）

**三、服务期限**

服务期限为合同签订后3年。

**四、服务类型**

现场服务、远程服务

**五、付款方式**

合同签订并提供发票后 7 个工作日内，支付合同额 100% 款项。

**六、系统服务考评办法**

上述系统在出现故障遇紧急情况时，联系不上中标方、或者中标方没有在2小时之内到现场以及没有在必要时得到校方允许下通过VPN等方式远程连接到学校环境提供服务及故障排除支持的，视为服务不合格。