**上海海事大学24小时网站值班监测告警服务需求**

1. **参数说明**

|  |  |  |
| --- | --- | --- |
| **服务类别** | **服务名称** | **详细参数** |
| **定期风险评估** | 暴露面检测 | 支持关键资产系统域名发现，自动发现客户所填入域名相关的所有子域名； |
| 支持检测网站服务器端口开放情况，比如数据库端口、Ftp服务端口等； |
| 漏洞脆弱性检测 | 支持对Web漏洞进行扫描，覆盖通用漏洞和常规漏洞。支持SQL注入、XSS、安全配置错误、已知漏洞组件包含、敏感信息泄露等常见漏洞的检测； |
| 专家漏洞验证服务 | 对风险评估报告中的高危漏洞进行专家验证，确保高危事件的准确性，并定期给用户推送云扫描报告。 |
|  | 高危0day事件告警 | ▲支持高危0day实时检测出现0Day漏洞时，主动对所监控用户业务做扫描发现，重要网络安全事件和安全漏洞快速预警通告和检测，检测结果第一时间定向推送到客户，能够支持微信端实时推送告警信息（提供截图证明）； |
| **实时异常监测** | 敏感词监测 | 支持对目标站点提供7×24小时网页敏感词检测能力。发现网页敏感词事件第一时间通过微信通知用户，监测内容能够在报告中进行呈现； |
| 业务可用性监测 | 支持页面响应监测，通过固定的频率模拟用户请求访问被监控站点，实时获取站点的响应状态和请求详情，精准的探测出网站的各种异常3分钟检测一次，当连续3次访问失败时判断为业务不可用； |
| 支持网站存活监测，通过固定的频率探测被监控站点存活状态 |
| 篡改监测 | ▲对目标站点的关键页面进行实时篡改监测，分钟级篡改发现，第一时间通过微信进行实时告警，并提供主动电话告警（提截图证明）； |
| ▲支持整站内容进行篡改监测，梳理并在首页展示站点结构图，显示网站各节点是否存在被篡改事件（提供界面截图证明）； |
| 黑链监测 | 支持对目标站点提供7×24小时网页黑链监测能力。发现网页黑链事件第一时间通过微信通知用户，监测内容能够在报告中进行呈现。 |
| **及时告警** | 微信告警 | 支持以微信的方式对篡改、挂马、网站不可用等安全事件进行实时告警，支持微信端内容的及时推送； |
| 邮件告警 | 支持邮件的方式推送安全事件报告、月报运营报告，便于站点安全的管理 |
| **可视化展示** | 风险管理可视 | ▲平台展示包括web业务系统的风险统计、风险分布、潜在风险篡改TOP5和风险等级统计；风险列表中包括已被篡改风险、潜在篡改风险、非篡改风险；风险状态包含未解决状态、平台自动已解决状态、人工标记已解决状态，便于快速了解风险处理进度；支持根据单位名称风险；（提供截图证明） |
| 篡改监测过程可视化 | 支持提供可视化的篡改监测界面，首页可直观展示篡改监测过程和监测结果，如正在监测哪一个页面，历史监测页面的安全状况等，便于实时掌握业务风险情况；  |
| ▲网站篡改事件应支持查看“举证图片”， 管理人员可通过微信及web登录界面，直观查看被篡改内容，便于第一时间掌握被篡改的情况（提供微信及web界面截图证明）； |
| 交付报告 | 支持每月定期进行网站安全评估，并生成安全评估报告，报告应至少包含扫描站点信息、风险分布情况、漏洞的风险描述、影响范围、解决方案和具体的攻击举证进行详细的展示； |
| 平台可自动生成以下报告：《安全事件报告》、《内网扫描报告》、《云扫描报告》、《每日值守报告》、《安全运营报告》、《重大活动值守报告》；支持手动按时间范围导出《值守报告》。 |
| **服务期限** |  | 服务期为1年，服务期满后若甲方对中标单位提供的服务满意且服务价格保持不变，经双方商定后，可与中标单位续约一年服务合同，最多可续约两次。 |
| **网站数量** |  | 监测校内网站数量不少于90个。 |