**上海海事大学校园网络资产管理服务技术需求**

上海海事大学经历了多期的信息化工程建设，导致内部网络和信息化资产种类繁多、数量庞大，但是对资产的管理工作目前还普遍停留在手动登记的方式上。传统的资产管理方式无法实时和准确的掌握资产的变更情况，比如新资产上线、未处理违规资产，这些风险点往往是黑客和病毒发动攻击的有力支点。为了更好的管理校园网络资产，特提出本服务需求。

1. **参数要求：**

|  |  |  |
| --- | --- | --- |
| **序号** | **功能参数** | **功能描述明细** |
| 1 | 资产发现 | 支持资产导入功能，包括域名资产、IP资产、URL资产，实时查看导入进度（共手工导入/Excel导入两种） |
| 支持对主机的名称、存活状态、端口、服务指纹、物理位置等基础信息识别 |
| 支持资产存活状态自动发现，支持自定义端口存活探测 |
| 支持资产来源识别，区分是人工导入还是系统发现 |
| 支持资产状态检测，资产自动收集、识别资产上线、下线和更新状态 |
| 支持以饼图、柱状图、趋势图等形式展示资产综合状况，支持从资产类型、漏洞类型、主机存活状态、服务类型等角度展示 |
| 能集合丰富的服务版本指纹库，可对主机端口服务进行精准识别，判断主机类型，系统版本，以及系统运行的组件类型、组件版本等指纹信息，能够收集和展示资产主机名 |
| 支持大数据分类算法，能够建立精准的资产识别模型，提高了识别的精准度。能够识别的服务类型包括但不限于CMS网站应用、数据库服务应用、服务中间件、开源框架、商用软件，识别数量不低于500种 |
| 支持识别设备指纹共计45类：如华为、海康，思科，松下等厂商摄像头，打印机、路由器、防火墙 |
| 支持框架指纹49类：如spark、Hadoop、struts2、springMVC等框架 |
| 支持服务指纹20+类：如weblogic、F5、tomcat等企业常见web应用 |
| 支持操作系统指纹240+类：如Microsoft windows系列、linux等 |
| 支持主机服务指纹1200+类：如http、ssh、mysql等 |
| 支持IP地理位置库可以自动关联主机所属的省份，自动识别IP所属的运营商信息，精确识别IP网络信息 |
| 支持对网站的名称、服务、网站状态、截图快照等基础信息识别 |
| 支持资产监控配置，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 |
| 支持对子域名的发现，支持多级域名自动发现 |
| 支持IP反查域名：根据当前IP，根据DNS历史记录等信息自动化发现互联网中指向该服务器的域名信息 |
| 支持IP/域名矫正，IP与域名关系绑定 |
| 支持主机拓扑，域名、端口、主机、服务关联显示 |
| 2 | 资产管理 | 支持资产按照负责人、分组、标签为基本属性进行管理（添加、编辑、删除） |
| 支持资产详情查看、批量删除、批量监控管理 |
| 展示资产主机地址、主机名称、操作系统、服务信息、主机状态、风险等级、负责人、负责人手机、邮箱、标签、资产更新时间等信息 |
| 支持批量Excel格式导出，导出内容包括资产地址、资产风险等级、资产分组、负责人、负责人手机、邮箱、标签、资产更新时间等信息 |
| 支持基于高危、中危、低危、安全的资产风险等级标识 |
| 支持对资产基于风险等级、导入时间范围、资产来源、资产分组、负责人的检索 |
|  支持从多个维度对资产进行聚合保存，通过设置资产特征值的方式对资产进行识别和过滤 |
| 3 | 自定义检测 | 支持资产自定义更新检测：对资产临时检测，观察资产变动情况（检测结果包括主机更新数、网站更新数） |
| 支持网站可用性监控、主机可用性监控  |
| 4 | 外部资产监测 | 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 |
| 5 | 安全大屏 | 支持资产、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 |
| 6 | 系统管理 | 支持资产状态变更站通知（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） |
| 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 |
| 7 | 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 |
| 8 | 部署方式 | 设备支持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网络资产管理服务提供根据上海海事大学情况针对性的校园网络资产管理部署方案，需要通过对上海海事大学多个业务子网段，多业务区域保护的实现从而达成全网的保护。监控节点分布在不同的网络环境中，控制台进行统一管理。

（二）其他服务

及时响应并处理系统出现的各类问题。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. 配置服务：包括资产导入、删除、分组及导出管理，资产归属及负责人管理、资产检索及监控管理；多级域名资产、网段存活IP、主机开放服务、服务版本及指纹的发现；资产状态Ping包监测、异常状态告警；校方其他关于系统需求配置或调整。
2. 软件升级与服务响应：包括版本升级、漏洞库升级，7\*24小时售后服务响应，必要时在校方允许下通过VPN等方式远程连接到学校环境提供服务及故障排除支持。遇紧急情况，接到校方通知后10分钟内响应，并派遣工程师2小时内赶赴现场进行故障修复。
3. 技术咨询服务：校方在系统使用过程中，可以通过电话、邮件、微信、QQ等方式提出问题，我公司工程师给出必要回答，并为系统日后使用和规划、管理等提供咨询服务。
4. 信息资料服务：对于系统运行环境的变更或配置工作，以文档形式提供给校方相关技术资料、培训资料、服务报告、配置文档等。每项工作实施完成后提供规划、实施、维护等全套文档。

**三、服务期限**

服务期限为合同签署后3年。

**四、服务类型**

现场服务