**关于南京医科大学附属口腔医院防扫描系统项目**

**征集潜在供应商的调研公告**

南京医科大学附属口腔医院拟对以下项目进行摸底、调研，公开征集潜在供应商。欢迎符合要求的供应商前来报名。

**项目名称：防扫描系统**

**数量：2套**

**项目基本情况介绍：**

南京医科大学附属口腔医院拟采购防扫描系统两套，通过多种智能分析技术和联动组件持续对抗各类新型攻击，实现用户Web业务应用安全。

**资质要求：**

供应商应具有独立法人资格，营业执照。提供有效的证书复印件加盖公章

**请仔细阅读本项目技术参数要求，并提供以下书面材料一式四份。**

1. 本公司满足本项目全部技术参数要求，无疑问。

或

本公司对本项目技术参数有正/负偏离，并附下表表述。

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 指标 | 原技术指标 | 正/负偏离 | 原因 |
| 1 |  |  |  |  |
| 2 |  |  |  |  |

2、本公司对本项目技术参数有疑问，并附下表表述，标明原技术参数，建议修改内容并阐明原因。

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 指标 | 原技术指标 | 建议修改 | 原因 |
| 1 |  |  |  |  |
| 2 |  |  |  |  |

1. 质检报告情况汇总表

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 质检报告名称 | CMA或CANS或国际权威检测机构或其他 | 依据标准 | 质检报告结果（合格/不合格） |
| 1 |  |  |  |  |
| 2 |  |  |  |  |

1. 该项目人员配置

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 姓名 | 所属工种 | 证书 |
| 1 |  |  |  |
| 2 |  |  |  |

1. 与本项目类似的成功案例（合同或中标通知书复印件）
2. 与本项目相关的公司资质证书专利等证明材料。
3. 报价一览表

|  |  |
| --- | --- |
| **项目名称** | **南京医科大学附属口腔医院 项目** |
| **序号** | **货物名称** | **品牌规格型号** | **数量** | **单价（元）** | **总价（元）** |
| 1 |  |  |  |  |  |
| 2 |  |  |  |  |  |
|  |  |  |  |  |  |
| **合计金额** | **人民币（大写） 元整****（¥ 元整）** |
| **供货时间** | **签定合同后（ ）日历天内** |
| **实施期** |  |
| **质保期** |  |

**注：如有配件及耗材需同时提供报价**

**单位名称（公章）：**

**法定代表人（授权代表）签名：**

 **联系电话（手机）：**

 **年 月 日**

**七、时 间：**2022年9月8日(星期四)上午9:00

（请各供应商委派技术人员参会）

**地 点：**江苏省口腔医院新综合楼十三楼1301会议室

信息中心： 陈主任 联系方式：69593126

采购中心： 李老师 联系方式：69593106

注： 1. 提供虚假文件一经查实将终止其参与资格。

 2. 资料一式四份，加盖单位公章并装订成册，概不退还。

**附件：防扫描系统具体技术参数要求**

|  |  |
| --- | --- |
| **指标项** | **技术规格要求** |
| 性能要求 | ★2U设备，网络层吞吐量≥20Gbps，HTTP应用层吞吐量≥1Gbps，HTTP新建连接数≥150000，HTTP并发连接数≥2200000，内存大小≥8G，硬盘容量≥128GB SSD，千兆电口≥6个，万兆光口SFP+≥2个，提供3年产品质保，3年软件升级 |
| 部署方式 | 支持虚拟网线部署、透明部署、路由部署、旁路镜像等多种部署方式，适应复杂使用环境的接入要求； |
| 协议解析 | 支持HTTP、HTTPS协议流量检测； |
| 支持伪静态解析； |
| 支持通过X-Forwarded-For、Cdn-Src-Ip、Clientip三种方式识别访问的源IP、并用于日志记录和联动封锁； |
| HTTP异常检测 | ★支持识别HTTP异常，包含HTTP方法过滤、HTTP头部字段Referer、User-Agent等注入检测、Host检测、URL溢出检测、POST实体溢出检测、HTTP头部溢出检测、range字段防护、multipart头部字段异常检测；（需提供产品功能截图证明） |
| Web应用防护 | 支持防护SQL注入、XSS攻击、网页木马、网站扫描、Webshell、跨站请求伪造（CSRF）、系统命令注入、文件包含攻击、目录遍历攻击、信息泄露攻击、Web漏洞攻击等； |
| 支持Cookie攻击防护，支持检测到篡改时将Cookie替换为\*，支持自定义需要防护的Cookie属性范围，包括防护所有Cookie属性、防护指定Cookie属性、不防护指定Cookie属性； |
| ★支持自定义Web应用防护规则，通过基于正则表达式自定义规则匹配方向、动作、字符串、危险等级、动作、攻击影响、描述等；（需提供产品功能截图证明） |
| 防扫描和数据防泄漏 | 支持HTTP应用隐藏，支持过滤如Server、X-powered-by类型的HTTP响应报文头，支持替换服务器出错页面（5XX）和替换服务器出错页面（4XX）； |
| ★支持漏洞防扫描，包括404页面检测、WAF规则拦截频率检测、目录访问频率检测、使用不常见的HTTP请求方法、匹配强弱规则扫描、敏感文件扫描等扫描行为特征，支持自定义封锁扫描IP封锁时间、支持隐藏服务器信息；（需提供产品功能截图证明） |
| 支持数据泄密防护，支持敏感信息自定义命中次数统计方式，支持自定义文件下载类型过滤；支持检测到敏感数据泄露时短信告警，支持自定义数据泄密规则库； |
| 口令防护 | 支持WEB弱口令检测、WEB登录明文传输检测、WEB口令爆破防护； |
| 支持识别和拦截中低频、分布式等高级WEB口令爆破攻击方式； |
| 权限控制 | ★支持基于地域维度配置访问控制策略，地址库包含中国大陆及海外地区；（需提供产品功能截图证明） |
| 支持Web权限控制，支持自定义文件上传类型过滤，防止通过修改文件后缀名绕过检测； |
| 支持用户登录权限防护，支持Web登录和非Web登录方式防护，支持短信验证登入； |
| 支持URL防护，可自定义允许访问的地址和拒绝访问的地址；  |
| 界面展示 | 支持针对业务风险汇总，支持展示业务安全状态分布，包括已失陷业务、正在遭受攻击的业务、存在漏洞但暂时未被攻击的业务，以及最近7天内的漏洞风险分布情况； |
| 支持对业务详情进行展示，包括业务存在关键的风险，可以提供具体的攻击链过程并对攻击进行举证；  |
| 支持针对业务攻击事件汇总，展示攻击事件类型TOP5及当前业务命中的全网实时热点事件，支持通过地图区域颜色深浅展示攻击者的分布及数量，展示攻击次数排名TOP5的国家/地区；  |
| ★支持对检测到的攻击行为按照IP地址的地理位置信息进行威胁信息动态投屏展示，实时监测和展示最新的攻击威胁信息；（需提供产品功能截图证明） |
| 智能联动 | ★支持与安全态势感知产品实现联动，Web应用防火墙支持以专属方式对接同品牌态势感知系统，供态势感知系统进行深度关联分析；（需提供产品功能截图证明）  |
| 产品资质 | ★要求所投产品具备“Web应用防护系统”计算机信息系统安全专用产品销售许可证，提供有效证书复印件 |
| 要求所投产品具备“Web应用防护系统”网络关键设备和网络安全专用产品安全认证证书，提供有效证书复印件 |