网络安全服务招标公告

为堵塞网络安全漏洞，确保学院网络安全稳定运行，我院拟购买网络安全服务。

1. 报名日期：2020年8月 日至8月 日
2. 报名地点：吉林警察学院图书馆四楼网络中心机房
3. 联系人：陈高阳。联系电话：18043139258。
4. 投标人须知
5. 投标人应具备投标本次招标项目的能力。
6. 投标企业需提供企业的营业执照、税务登记证、机构代码证、企业法人有效证件。
7. 开标日期：2020年8月 日
8. 开标地点：吉林警察学院行政楼一楼会议室
9. 评标原则：评标小组将以招标文件、投标文件、报价为依据，在同等条件下最低价中标的原则。
10. 服务期：自2020年9月20日至2021年9月20日
11. 付款方式：合同签订后一次性付款。
12. 本次招标不接受超过10万元的报价。
13. 质保金5000元，中标后以保函方式提交。
14. 技术要求

|  |  |  |
| --- | --- | --- |
| **指标项** | **指标子项** | **技术要求** |
| 安全服务 | 资产梳理服务 | 提供全面详细的网络设备使用情况统计，包含设备类型、型号、部署位置、端口、服务使用情况等信息，以帮助客户实时了解设备情况，并形成相关资产梳理表。利用铱迅网络资产情报系统主动探测用户在互联网上暴露的资产，可以形成明确的资产清单，帮助客户发现自己的未知资产。需要满足以下技术：1. 网站资产梳理（域名信息、特征信息、端口全称、网站标题、网站指纹、网站状态、探测时间等）；
2. 主机资产梳理（IP信息、端口信息、端口服务名、端口全称，主机系统、端口状态、主机状态）;
3. 输出《资产梳理报告》、《资产梳理表（网站资产）》、《资产梳理表（主机资产）》
 |
| 漏洞扫描服务 | 对关键业务系统进行漏洞扫描，发现当前网络中的安全配置和运行的应用程序存在的漏洞风险，评估网络风险。需要满足以下技术：1. Web漏洞扫描（SQL注入、跨站脚本、木马上传、代码执行、远程本地包含、信息泄露等各种类型的web漏洞）；
2. 主机漏洞扫描（缓冲区溢出漏洞、网络设备漏洞、web服务器漏洞、数据库服务器漏洞、邮件服务器漏洞、DNS服务器漏洞、操作系统漏洞）
3. 弱密码扫描（3389远程桌面、FTP、SSH、Telnet、Mssql、 Mysql、Oracle、SMB、VNC等弱密码扫描）；
4. 输出《漏洞扫描报告》（报告中包含漏洞修复建议）；
 |
| 漏洞验证服务 | 利用存在的漏洞及黑客攻击技术，对网站应用进行全局、深度、颗粒的安全检测服务，从信息系统的外部发现信息系统对外所呈现出的安全脆弱性并验证这些安全脆弱性的真实存在性。为客户提供详细的渗透测试报告及修复建议。需要满足以下技术：1. 对系统中发现的漏洞进行验证；
2. 实施人员严格按照漏洞验证准则进行验证，确保目标系统的正常运行；
3. 输出《漏洞验证报告》并提供漏洞修复建议；
 |
| 网站监控服务 | 提供网站入侵攻击检测、网页篡改检测、敏感关键字内容检测、网站实时流量监测、网站备案监测，并能够对严重安全攻击提供邮件报警功能，以及可以定期出具安全监测报告。需要满足以下技术：1. 网站可用性监测；
2. 敏感词监测；
3. 暗链、死链监测；
4. 网页篡改监测；
5. 信息泄漏监测；
6. 定期输出《网站安全监测报告》。
 |
| 安全通报服务 | 定期通过邮件或短信方式向客户提供本信息系统相关的安全通报，为客户实时提供最新出现的安全漏洞和安全警告、安全升级通告和厂商安全通告（包括Windows、AIX、Linux、Oracle、Sybase、Cisco等），并说明各种通告对客户信息系统的影响程度。 |
| 应急响应服务 | 对客户IT基础设施和信息系统提供7X24小时的紧急响应服务，包括受到非法网络攻击、蠕虫病毒爆发、数据受到窃取和破坏的调查取证等方面的应急服务支持。需要满足以下技术:1、支持网站被植入后门的快速响应; 2、支持数据被篡改、窃取的快速响应;3、支持安全漏洞被通报的快速响应处理;4、支持网站被植入恶意代码、广告的快速响应;5、支持服务器被木马远程控制的快速响应;6、其他的网络安全紧急事件快速响应; |
| 重要期间安全保护服务 | 针对国家重大会议、校园大型活动等重点保障时期，为学校提供专项保障服务。为学校提供7\*24h网站监控和技术人员值守，全程协助学校进行安全事件排查及调研取证工作。 |
| 软件 | Web应用安全发布平台 | 针对学校门户网站提供Web应用安全发布软件及服务，实现网站数据安全，具有网页防篡改功能，日志管理功能，告警功能，并提供防篡改相关配置技术服务。需要满足以下技术:1. 网站篡改防护，服务器无需安装任何客户端，无需采用FTP同步，支持源站被篡改情况下，提供正常网站服务；
2. 网站保持在线，即防护网站宕机或者掉线的情况下，可以使用设备中备份的网站内容继续提供服务；
3. 首页锁定，开启后将锁定首页，并且只允许访问首页；
4. 一键断网，开启后将不允许访问网站，或者返回特定的页面；
5. 访问控制，包括基于IP，域名，URL，地理位置，UA的访问控制；
6. 网站升级，不改动源站配置，支持网站ipv4升级ipv6，http升级https，支持网站进行强制https跳转；
7. 智能防扫描，防端口扫描、主机漏洞扫描，防Web漏洞扫描，发现异常端口扫描行为，诱捕攻击源IP，加入黑名单，重保期间自动封堵；
8. 网站监测，支持敏感词监测、网站可用性监测、暗链死链监测、网站篡改监测、信息泄露监测；
9. 统计和日志，支持多种日志类型，满足安全审计需求，攻击日志，网站监测日志，操作日志，同时可开启邮件告警，支持日志导出；
 |
| 硬件设备 | Web应用防护系统 | 电口\*6,2对电口Bypass，支持防护无限个IP,HTTP，请求速率9200，并发连接数50万，总吞吐1000Mbps，web清洗流量230Mbps，1U。需要满足以下技术:1. 部署能力（透明部署、策略路由、反向代理、透明代理部署）；
2. 安全特性（高性能攻击引擎，智能阻断，URL自学习，支持IPv6,HTTP RFC符合性，支持HTTPS，真实来源IP解析，内置规则，WEB应用漏洞扫描，碎片组包，编码还原，WEB基础架构防护，防扫描，WEB应用安全防护，智能木马检测，网页篡改防护，数据库防篡改，支持虚拟化功能，内容安全，弱密码记录，备案检查，访问控制，主动阻断方式，防CC攻击防护，抗拒绝服务攻击）；
3. 网络自适应能力（支持802.1Q，端口汇聚（Trunk），路由配置）；
4. 统计功能（网站统计，URL统计，网站详情）；
5. 报表功能（安全事件报表，webshell提示，报表查询，输出格式HTML、Word等通用格式）；
6. 日志系统（系统日志、审计日志、安全防护日志，日志查询，日志管理）；
7. 系统诊断调试功能（维护工具抓原始报文用于分析，配置备份与导入）；
8. 高可用性（HA双机，硬件BYPASS）。
 |