1. **采购需求一览表**

|  |  |
| --- | --- |
| 项目名称 | 江西旅游商贸职业学院现教中心网络安全服务采购项目 |
| 数量（单位） | 1项 |
| 服务期限 | 详见第五章采购需求 三、商务要求。 |
| 项目实施地点 | 采购人指定地点 |
| 备注 | 1、所有价格均应以人民币报价，全额单位为元。2、投标报价指完成采购内容中所发生的一切费用均应包含在报价总价中。包括服务中发生的监控费、维保费、评估费、检查费、系统调试费、标配工具费用、办公设备及物耗费用、培训费、咨询费、人员工资（包括应交的五险一金等费用）、加班费、风险金和税费、利润、不可预见费等在项目实施过程中的全部费用，响应供应商报价中漏报、少报的费用，视为此项费用已隐含在报价中，成交后不得再向采购人收取任何费用。 |

1. **技术标准及要求**
	1. **服务具体内容及要求**

| **序号** | **总体****建设** | **建设****内容** | **主要功能参数** | **年限** |
| --- | --- | --- | --- | --- |
| 1 | **安全****服务** | **渗透****测试服务** | 模仿黑客的手法远程或本地对重要资产进行模拟攻击，渗透测试内容，应包括数据库系统、中间件、应用系统以及身份认证等安全机制，具体要求内容：根据网络脆弱性检测中发现的脆弱点，模拟黑客对系统中的终端、服务器进行现场滲透性验证、SQL 注入、XSS (跨站脚本)、CRLF 注入、代码执行、目录遍历、文件包含、输入验证、认证、逻辑错误、密码保护匿域猜测、字典攻击、特定的错误页面检测、脆弱权限的目录和危险的 HTTP 方法（如：PUT、DELETE)等。由安全专家进行深入的手工测试和分析，识别弱点扫描工具或者脆弱性扫描工具无法发现的问题。主要分析内容包括逻辑设计缺陷、上传绕过、输入输出校验绕过、数据篡改、功能绕过、异常错误、逻辑漏洞、越权等以及其他专项内容测试与分析，了解应用系统可能存在的潜在漏洞以及发生漏洞利用时可能造成的危害，渗透结束后生成相关报告并提供修复建议。漏洞扫描不限次数。**交付物：《渗透测试报告》****服务频次：不低于20个系统** | 一年 |
| 风险评估服务 | 通过全局的脆弱性评估、威胁评估和风险评估，掌握通过信息摸排、基线核查等手段对信息系统安全风险状况，以更好地满足国家、行业要求，并与信息系统自身安全保护需求结合起来，针对信息系统进行一次完整的风险评估，明确风险实际状况，并提出风险处置建议和风险评估报告。**交付物：《风险评估报告》****服务频次：不低于10个系统** |
| 应急响应服务 | 在出现重要安全事件时（如信息系统遭受攻击、网络病毒爆发等），派遣高级安服人员，通过远程和现场支持的形式协助采购人对遇到的突发性安全事件进行紧急分析和处理。主要工作内容包括：突发事件相关信息的收集、事件的分析、报告提交、问题解决建议等，协助用户解决突发安全事件，并提供应急响应报告。为保证应急响应服务中故障排查的质量，供应商提供的故障排查服务工具需具备一种故障排查方法，可提高应急响应服务过程中故障排查的效率。**交付物：《应急响应技术服务单》，需客户签字****服务频次：4次** |
| 网站监测服务 | 通过对目标站点进行 7×24 小时不间断的页面爬取、分析、匹配，主动实时的发现网站的风险隐患，并及时采取修补措施，对采购人指定网站进行远程安全监测、安全检查、实时告警。网站安全监测服务主要包括以下几方面的内容：* 远程网站漏洞扫描：通过远程网站漏洞扫描服务，由供应商提供的网络安全专家每月 1 次定期进行网站结构分析、漏洞分析，获知网站系统层和应用层的漏洞情况，以及对修补漏洞的安全建议。
* 远程网页木马监测：基于安全云平台，采用智能木马检测技术，高效、准确的识别网站页面中的恶意代码，使网站管理员能够第一时间得知网站的安全状态
* 网页敏感内容监测：实时监测网站是否出现一些敏感关键字，如果发现敏感内容，在第一时间通知采购人。采购人也可以自定义所关心的敏感关键字。
* 网站平稳度检测：对网站进行实时远程访问平稳度的动态监视，跟踪访问平稳度动态变化情况，并根据严重程度及时发出报警信号。
* 网页篡改监测：实时监测网站页面状况，如发现页面被篡改情况，第一时间通知采购人。

**交付物：《网站监测报告》-每周一次****服务频次：不低于个20个站点** |
| 安全运营服务 | * 服务方具备云端检测和分析平台，通过采集学校安全设备和本次提供的组件工具的安全告警和安全日志，结合大数据分析、人工智能等技术手段，为学校提供核心10个资产的7\*24小时持续不间断的安全威胁分析鉴定，同时在平台界面进行展示；分析研判包括但不限于对脆弱性、异常流量、攻击日志、病毒日志等数据进行采集和实时分析研判，支持将同一资产的多个告警进行聚合分析发现各类安全事件并生成工单，并在告警详情中展示告警的基本信息，涉及的业务信息、攻击趋势、威胁详情、攻击原理、处置建议等内容。
* 提供的服务监控门户（或用户portal）应具备服务质量可视化展示，服务方能通过可视化的数据，清晰的了解安全专家的服务水平，包括漏洞闭环率、漏洞平均响应时长、漏洞平均闭环时长、威胁闭环率、威胁平均响应时长、威胁平均闭环时长、事件闭环率、事件平均闭环时长。（***响应文件中须提供所投产品符合以上技术功能参数的产品功能界面相关截图加盖服务方公章。***）
* 云端服务平台应当具备丰富的策略检查工具（要求不少于40种策略检查的工具），支持排查安全设备防护策略配置的合理性。***（响应文件中须提供所投产品符合以上技术功能参数的产品功能界面相关截图加盖服务方公章）。***

**交付物：《特殊时期值守报告》、《运营周报》、《运营月报》、《运营季报》、《威胁情报》、《年度汇报》、《事件总结报告》****服务频次：一年** |  |
| 外部攻击面管理服务 | * 支持基于给定一级域名/组织名称对互联网资产进行探测，主动获取互联网侧所能解析的子域名，基于资产探测任务的结果，深度识别并记录资产下各种资产属性，包含但不限于：子域名、IP、开放端口服务应用、资产变动情况、HTTP响应码、端口banner、组件、归属地、SSL证书等；
* 服务方支持根据招标方定义的特定关键字或关键字组合，发现并监测微信公众号、微信服务号、微信小程序、APP的资产及变化情况；支持识别资产内容包括但不限于：账号主体、资产类型、微信号、简介等；
* 服务方支持基于指纹从网络侧发起主动扫描识别漏洞，漏洞类型包括但不限于：Web/应用漏洞、中间件/常用软件漏洞、数据库漏洞、系统漏洞、云类型（容器、虚拟化、云原生等）、设备型漏洞等；
* 服务方支持基于暴露面检测的结果，针对互联网资产进行PoC漏洞扫描；PoC漏洞类型包含但不限于：未授权访问漏洞、数据库弱口令、远程登录协议弱口令、远程代码执行漏洞、SQL注入、敏感信息泄露漏洞、文件上传漏洞等；
* 服务方兼容CNNVD、NVD、CVE等国内外漏洞库，支持对基于资产探测到的组件、应用、中间件的版本进行漏洞检测；
* 服务方能够根据招标方定义的关键字或关键字组合，对Telegram等黑客活跃的即时通讯软件进行监测，用于发现服务方相关的黑产舆情事件。
* 服务方能够根据招标方定义的关键字或关键字组合，对GitHub、Gitee等国内外主要开源社区、代码托管平台进行监测，并分析判断是否存在招标方相关敏感信息，如代码/证书文件/测试数据/通讯录等；
* 暗网泄露事件：支持面向招标方检出暗网事件的展示，主要从暗网交易标题、暗网卖家ID、发帖事件、交易链接、交易内容等维度展示出当前招标方泄露的暗网事件信息，使得招标方能直观了解到当前泄露的暗网事件情况。
* 代码泄露事件：支持面向招标方检出代码泄露事件的展示，主要从代码项目名称、代码链接、命中关键字、关键字代码片段等维度精准定位到当前招标方泄露的代码信息，使得招标方能直观了解到当前泄露的代码事件情况
* 黑产舆情事件：支持面向招标方检出黑产舆情事件的展示，主要从黑产论坛网站、涉及舆情群组、发布时间、黑产舆情内容等维度精准定位到当前涉及招标方黑产舆情相关信息，使得招标方能直观了解到当前存在的黑产舆情事件的情况。

交**付物：《外部攻击面管理服务报告》。****服务频次：1次。** |

**注:以上技术要求全部为实质性要求，供应商须全部响应或优于。**