附件2

**广元市妇幼保健院**

**网络安全渗透性测试和攻防应急演练服务项目市场询价清单**

**项目清单及技术参数要求**

|  |  |  |
| --- | --- | --- |
| 风险评估及渗透测试 | 资产识别 | 1. 依据相关国家标准或国际标准，对招标方的资产进行全面梳理和识别，识别内容包含但不限于资产类型、IP地址、责任人、用途、操作系统、数据库等。 2. 资产类别应按照相关规范分类，包含但不限于以下几大类：  * 业务应用—业务系统，如OA系统、门户网站等； * 网络结构—网络拓扑结构图； * 数据文档—设计方案、操作手册、业务数据等； * 软硬件资产—操作系统、中间件、数据库、网络设备、安全设备、存储设备等；  1. 依据相关规范，投标方应根据资产识别结果，科学、合理的对资产进行重要性赋值，明确资产价值。 2. 投标方应针对资产识别情况及问题及时汇报。 |
| 脆弱性识别 | 1. 依据相关国家标准或国际标准，通过专业的漏洞扫描工具或平台，针对互联网的网站、网络设备、业务应用系统、中间件、操作系统、网络安全设备等IT资产进行脆弱性扫描评估，漏洞扫描结果通过人工复核确认，出具整体系统漏洞扫描报告及修复建议。 2. 脆弱性分类应至少包括但不限于以下两类：  * 技术性弱点—系统、程序、设备存在的漏洞或缺陷，如网络结构设计问题和代码漏洞； * 操作性弱点—软件和系统配置、操作中存在的缺陷，包括人员在日常工作中的不良习惯，审计和备份的缺乏；  1. 技术性弱点识别应按照以下要求实施：   技术性弱点识别流程：   * 投标方应对技术性弱点识别的目标对象进行全面梳理和识别，识别内容包含但不限于资产类型、IP地址、责任人、用途、操作系统、数据库等。 * 投标方应提交技术性弱点识别工具的情况（包括但不限于：设备厂商、设备型号、漏洞库、销售许可证等）、技术性弱点识别工作方案（包括但不限于：目标对象、扫描时间、风险规避措施等）及技术性弱点识别申请，招标方授权后，方可进行。 * 投标方应对技术性弱点识别结果进行人工验证，保证技术性弱点识别结果的真实性。 * 投标方应提交针对性的解决方案，保证漏洞修复可落地。   技术性弱点识别工具支持对象应包含但不限于：   * 网络设备：路由器、交换机、防火墙等； * 操作系统：windows、linux、UNIX等； * 数据库：Oracle、MS SQL、Mysql等； * 中间件：Apache、Tomcat、weblogic等。   技术性弱点识别参数应包含但不限于：版本漏洞、开放端口、开放服务、空/弱口令账户、安全配置等。   1. 操作性弱点识别应按照以下要求实施：   操作性弱点识别流程：   * 投标方应对操作性弱点识别的资产进行全面梳理和识别，识别内容包含但不限于资产类型、IP地址、责任人、用途、操作系统、数据库等。 * 投标方应提交基线核查的标准，会同招标方各接口人进行沟通确认。 * 依据相关标准或规范，投标方应结合招标方制定的基线核查标准、上级单位的基线核查标准、行业基线核查标准及行业最佳实践等，目标对象进行操作性弱点识别，目标对象包括但不限于：网络设备、操作系统、数据库及中间件等。 * 投标方应组织相关人员对结果进行确认后，分析提交科学、合理的整改建议。   操作性弱点识别应包含但不限于以下内容：   * 网络设备： OS安全、帐号和口令管理、认证和授权策略、网络与服务、访问控制策略、通讯协议、路由协议、日志审核策略、加密管理、设备其他安全配置等； * 操作系统：系统漏洞补丁管理、帐号和口令管理、认证、授权策略、网络与服务、进程和启动、文件系统权限、访问控制、通讯协议、日志审核功能、剩余信息保护、其他安全配置等； * 数据库：漏洞补丁管理、帐号和口令管理、认证、授权策略、访问控制、通讯协议、日志审核功能、其他安全配置等； * 中间件：漏洞补丁管理、帐号和口令管理、认证、授权策略、通讯协议、日志审核功能、其他安全配置等。  1. 投标方应将发现的脆弱性及时向招标方反馈，并在后续提出可落地的整改建议或方案。 |
| 威胁识别 | 1. 依据相关国家标准或国际标准，对存在脆弱性的资产进行威胁的全面识别，及时发现潜在威胁的原因，避免或降低威胁发生的几率。 2. 威胁来源应至少包括但不限于以下四类：  * 人员威胁——包括故意破坏和无意失误； * 系统威胁——系统、网络或服务的故障； * 环境威胁——电源故障、污染、液体泄漏、火灾等； * 自然威胁——洪水、地震、台风、滑坡、雷电等。  1. 威胁可以通过威胁主体、资源、动机、途径等多种属性来描述。造成威胁的因素可分为人为因素和环境因素。根据威胁的动机，人为因素又可分为恶意和非恶意两种。环境因素包括自然界不可抗的因素和其它物理因素。威胁作用形式可以是对信息系统直接或间接的攻击，在保密性、完整性和可用性等方面造成损害：也可能是偶发的、或蓄意的事件。 |
| 人工渗透测试 | 1. 针对服务范围内的目标信息系统，进行专业人工渗透测试，内容包括：   SQL注入检测：检测网站是否存在SQL注入漏洞；  XSS跨站脚本检测：检测网站是否存在XSS跨站脚本漏洞；  缓冲区溢出检测：检测网站服务器和服务器软件，是否存在缓冲区溢出漏洞；  上传漏洞检测：检测网站的上传功能是否存在上传漏洞；  源代码泄露检测：检测网络是否存在源代码泄露漏洞；  隐藏目录泄露检测：检测网站的某些隐藏目录是否存在泄露漏洞；  数据库泄露检测：检测网站是否在数据库泄露的漏洞；  弱口令检测：检测网站的后台管理用户，以及前台用户，是否存在使用弱口令的情况；  管理地址泄露检测：检测网站是否存在管理地址泄露功能。 |
| 风险分析 | 1. 依据相关国家标准或国际标准，对招标方已部署的安全设备、已制定管理体系及其他控制措施进行识别。 2. 根据识别结果的现状，提出建设性意见，避免重复采购相关设备或服务。 3. 投标方应组织专家团队，对存在和潜在的风险进行全面分析，保证风险分析的科学性、合理性及风险处置的可操作性。 4. 投标方应在风险分析完成后，组织召开相关会议，将风险评估实施过程全生命周期发现的情况或问题统一反馈，并提出可落地的建议或方案。 |
| 服务交付文档 | 《资产评估报告》  《脆弱性评估报告》  《威胁评估报告》  《渗透测试报告》  《风险分析报告》  《安全风险分析综合报告》 |

|  |  |  |
| --- | --- | --- |
| 攻防演练 | 服务内容 | 1. 攻防演练应按照以下要求实施： 2. 投标方应确定目标对象后提供攻防演练服务方案和服务申请，内容必须包括但不限于：  * 攻防演练方法和流程； * 攻防演练工具； * 攻防演练面临的风险和规避措施； * 攻防演练时间和地点； * 攻防演练人员（资质、经验等其他证明）。  1. 安全意识培训   安全意识培训为针对的是最一般性的工作所需，目的是提高整个组织普遍的安全意识和人员安全防护能力，使信息口人员充分了解既定的安全策略。培训中强调分析典型案例、记取经验教训、培养安全习惯、提升整体的安全认知水平。供应商在攻防演练结束后，针对各医院在演练中暴露出的网络信息安全问题，对相关医院进行统一的安全培训。  通过网络攻防演练，检验各单位网络安全应急预案制定和实施情况，进一步促进各单位完善自身应急预案。 |
| 服务交付物 | 《攻防演练报告》  《安全意识培训》 |