## 采购项目商务和技术要求

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 需求名称 | 技术参数和需求内容 | 备注 |
| （**此项为实质性响应，不允许负偏离**） | 服务要求 | \*1.互联网评估服务项目，根据甲方需求对总医院全年全部互联网资产进行风险检测（每个月进行一次），包含互联网全量资产的资产识别服务、风险识别服务、敏感信息识别服务、管控与闭环服务、应急保障服务等，并按时提交资产识别报告、风险识别报告、敏感信息识别报告、应急响应报告、管控闭环分析报告等。 \*2.根据甲方需求对指定的一个院区开展互联网应急保障服务，保障服务的内容由甲方根据当前互联网安全状况指定，全年保障次数没有上限。 \*3.提供安全技术培训服务，每个月开展一轮安全攻防培训、安全开发培训、CTF竞赛培训、安全意识培训等 | **提供承诺函** |
| 人员资格 | 1、项目经理不少于1人。 2、实施团队人员不少于6人。 |  |
| 企业资格 | 符合《中华人民共和国政府采购法》第22条资格。 |  |
| 1 | 项目经理具备资质 | •1.项目经理应具备10年以上网络安全行业工作经验 •2.项目经理应掌握项目管理体系知识，具备项目管理PMP证书或国际项目管理师PRINCE2证书 •3.项目经理应掌握网络安全和数据安全知识，具备信息安全专业人员CISP证书或数据安全治理专业人员CISP-DSG证书 •4.项目经理应掌握国际云安全和信息系统审计能力，具备云安全系统认证专家CCSSP证书或信息系统审计专家CISA证书 •5.项目经理应掌握安全运维和风险管理能力，具备ITIL4 Foundation证书或ISO27001 Foundation证书 |  |
| 2 | 团队其他人员具备资质 | 项目团队成员技术能力与人员投入（除项目经理外），实施团队人员不少于6人，提供相应人员在投标公司3个月社保证明（截止投标之日前）。 |  |
|
| 2.1 | 安全咨询顾问 | 1、安全咨询顾问不少于1人且具备10年以上网络安全行业工作经验 2、安全咨询顾问应同时具备高级信息系统项目管理师证书 |  |
| 2.2 | 安全服务人员 | 1、安全服务工程师不少于2人，需具备CISP、CCSK 2、渗透测试工程师不少于2人，需具备CISP-PTE，并在CNVD或CNNVD上提交过原创漏洞 |  |
| 2.3 | 应急保障人员 | •1、应急保障工程师不少于1位，每人同时具备CISAW-应急服务（专业级）认证，CISSP认证或CISP认证 |  |
| 3 | 服务方案 | 服务方案应包括资产识别、风险识别、敏感信息识别、管控与闭环、应急保障、安全培训 |  |
| 3.1 | 资产识别 | 1、提供专业的安全服务人员，利用主动识别技术对网络空间资产进行识别，实现资产识别、资产变更维护、资产废弃，全生命周期监测，协助完成摸清家底工作，主动掌控资产动态。基于端口与服务识别技术对资产进行指纹识别（IP、端口、操作系统、服务、系统名称、中间件及版本等），对资产进行标签化管理，建立清晰全面的资产档案 •2、服务过程中需自行提供检测工具，可对各类资产进行自动发现，可检测在线资产的IP、MAC、操作系统、设备类型、设备厂商、设备型号、软件版本等，并支持基于A/B/C段的检测目标的任务创建 |  |
| 3.2 | 风险识别 | 1、提供专业的安全服务人员，进行资产测绘。基于资产测绘结果，以攻击者视图对互联网资产暴露面进行统计梳理，对僵死资产、无主系统、高危端口服务、老旧web资产、边缘系统等进行识别，提供暴露面收敛方案，协助指导收敛工作 2、提供基线检查工具，配合专业安全服务人员，进行基线合规检查。根据最佳配置核查实践经验，对互联网重要操作系统、数据库、中间件、网络设备、网络安全设备等进行配置核查，发现安全基线配置存在的问题，为后续基线加固提供依据 3、提供漏洞扫描工具，配合专业安全服务人员，进行漏洞扫描。对互联网Web应用和主机系统进行自动化扫描，发现应用系统、操作系统、数据库、中间件、网络设备、安全设备等存在的高危、中危、低危漏洞情况。可根据资产重要性权重定制不同的漏洞深度扫描策略，深度挖掘存在的漏洞，并提供漏洞详情解读和漏洞修复建议 4、提供专业的渗透测试人员，进行渗透测试。在授权和监督下，通过模拟黑客，使用业界可靠的攻击手段、攻击技术、攻击工具和自编脚本，对目标的安全漏洞、安全隐患进行全面检测，对发现的安全漏洞提供修复建议，并协助用户进行复测验证修复情况 5、服务过程中需自行提供检测工具，能针对现网的非法外联主机进行有效检测和定位，可检测出目标设备连接智能手机热点、通过智能手机 USB 共享网络等违规双网卡共享外联行为、能对Web应用和主机系统进行自动化扫描、能进行基线合规检查 •6、服务过程中需自行提供检测工具，具备漏洞验证能力，可对高危漏洞提供自动化验证功能。自动化验证不需要任何人进行参与，平台自动对漏洞进行验证、判断，并可在安全检测报表中体现。 |  |
| 3.3 | 敏感信息识别 | 1、提供专业的安全服务人员，对公开渠道的敏感信息进行检索，如员工信息、账户、口令、系统文档、源代码等，为后续安全加固提供依据 2、提供专业安全服务人员，通过工具和自编脚本，对互联网Web应用和主机开展敏感信息专项检查工作 |  |
| 3.4 | 管控与闭环 | •1、服务过程中需自行提供检测工具，能够对两次检测任务进行对比分析，能够对比分析出两次检测任务的资产漏洞变更情况，可导出漏洞对比报告，查看新增漏洞和遗留问题 •2、服务过程中需自行提供检测工具，具备风险闭环管理能力，包括资产整改、漏洞整改，其中漏洞整改包括：待通报、待处置、待审核、已闭环四个维度，通报的内容需包括：资产名称、资产地址、资产类型、组织机构、问题描述、漏洞类别、端口、责任人、修复优先级、首次发现时间、最近检测时间等。支持邮件通知、通报期限、整改说明填写。支持通报漏洞的跟踪，能记录从首次发现到最终修复处置的全过程 3、服务过程中需自行提供检测工具，能够对资产台账进行管理，详细列举所有可信资产、可疑资产，展示内容包括但不限于IP地址、mac地址、资产名称、机构、操作系统、资产类型、资产子类、生产厂商、安全等级、业务系统、安全区域、在网状态、资产价值、服务、端口、重要组件、集成厂商、软件版本、设备序列号、设备型号等。并支持点击跳转到独立界面查看单一资产详情。支持资产台账的手动添加修改、批量编辑、导入、导出备份。 |  |
| 3.5 | 应急保障 | 提供专业的应急保障人员，对突发安全事件进行应急响应。根据安全评估、分析研判、事件溯源等提供的数据，开展响应处置工作，包括：病毒事件、失陷事件、主机临时加固、安全策略增改等威胁处置工作。服务人员到现场时间≤2小时。 |  |
| 4 | 技术支持 | 1.投标人具有中国网络安全审查技术与认证中心CCRC信息安全应急处理一级资质（提供证书资质复印件，并加盖公章） 2.投标人具有中国网络安全审查技术与认证中心CCRC信息安全风险评估一级资质（提供证书资质复印件，并加盖公章） 3.投标人具有中国信息安全测评中心颁发的信息安全服务资质（工程类）资质二级或以上（提供证书资质复印件，并加盖公章） |  |
| **商务要求（不接受负偏离）** | | | |
| 5 | 质量控制 | 1、投标人应按照招标人评审意见对项目工作及交付物进行改进和完善。 2、投标人应在项目服务期内按时开展安全服务工作，并每月月底前按时提交报告，包含资产识别报告、风险识别报告、敏感信息识别报告、应急响应报告、管控闭环分析报告。 3、服务期内，投标人保证所提供的技术服务为7\*24小时，投标人的安全应急响应切实解决了信息安全事件，降低了潜在损失。 4、投标人在其所提供的技术服务执行过程中应保证所有操作的可靠性和安全性。 |  |
| **\***6 | 验收考核办法 | 1、工作质量：投标人对于甲方提出的服务工作联系（电话、邮件或书面函）在两个工作日内明确回复，并按照甲方工作联系中的计划和要求按时完成工作任务，对于不属于投标人职责范围或暂无条件完成的任务，投标人需说明原因并提出建议方案。 2、现场服务：投标人提供的现场服务人员应严格遵守医院及各医学中心各项规章制度，按时提供月报，对招标人各项工作要求执行到位，不得出现在正常工作日缺岗、故意懈怠工作等情况。 3、紧急（突发）事件报告与处理：投标人对于紧急（突发）事件原则应在事件知晓第一时间答复甲方，原则不超过10分钟。到场时间不超过1小时，处理时长不超过4小时。 4、造成非技术重大事故的（因投标人工程师工作疏忽造成招标人经济损失或名誉损失，导致特别严重后果的），不予验收。 | **提供承诺函** |
| 7 | 服务时间 | 从签订合同之日起满365天 |  |
| 8 | 付款方式 | 从签订合同之日起服务满半年支付50%，服务满一年验收合格后再支付50%。 |  |