评分标准

对通过符合性审查的投标文件，采用综合评分法：具体分为三个部分（技术分、商务分、价格分），上述分项都按百分制打分，在最终的综合分中按一定的比例进计算。按综合得分由高往低进行排名，综合得分最高者为第一预中标候选人，根据各投标单位综合得分由高至低排出名次，如果综合总分相同，则以报价低的为优先中标的原则确定排名，以此类推，推荐预中标候选人一到三名：

一、本次评标采用综合评分法。

|  |  |  |  |
| --- | --- | --- | --- |
| **内容** | **技术部分** | **商务部分** | **价格部分** |
| 权重 | 60% | 20% | 20% |
| 分值 | 60分 | 20分 | 20分 |

二、量化评审内容如下：

#### 1.技术评分标准（60分）

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 具体项目 | | 评分要求 | 分值 |
| 1 | 安全服务工具和系统技术参数要求（允许多系统组合） | 1)支持面向集团主体及其下属分子公司的自动化资产发现，并将各资产自动归类至对应分子公司； | 需要提供盖章确认的产品界面截图证明。分项评分； | 2 |
| 2)支持资产梳理识别，资产识别内容包含不限于：IP、子域名、URL、开放端口、协议、服务应用、HTTP响应码、网站标题、IP地理位置、网站证书、域名备案单位、数据更新时间等，提供IP域名资产清单； | 2 |
| 3)支持发现互联网侧资产上高危端口的暴露情况，如3389、1521、3306等高危敏感端口、telnet、rdp等高危敏感服务等，同时支持高危端口自定义，支持一键快捷筛选高危端口； | 2 |
| 4）支持不少于20种协议弱口令检测，包含但不限于：ZooKeeper弱口令、ApacheTomcat弱口令、Openssh弱口令、Spark弱口令、Solr弱口令、Smb弱口令、WindowsRdp弱口令、Cassandra弱口令、SqlServer弱口令、MongoDB弱口令、Memcached弱口、JBoss弱口令、InfluxDB弱口令、Hadoop弱口令、ElasticSearch弱口令、ClickHouse弱口令； | 2 |
| 5）包含丰富的攻防工具集， 包括但不限于漏洞探测、漏洞扫描、渗透测试、反编译、图片隐写、逆向工程、SQL注入、密码破解、编码转换、溢出提权等类型； | 2 |
| 6)支持钓鱼邮件模拟攻击功能，包括钓鱼邮件模板、发送目标、发送策略等参数，以执行模拟钓鱼攻击演练； | 4 |
| 7）提供攻防演练平台产品支撑本次应急预案检测演练，功能包含资源配置、报告递交、裁判评审、管理后台等模块，通过界面进行展示。检测队通过平台授权相关攻击出口IP资源，及攻击跳板机资源进行攻击,所有攻击队员需通过Web页面的方式进行操作,在获得攻击成果后，进行平台报告递交。防守方通过自行监测手段,对攻击方的攻击行为开展监测,将监测数据上报至平台。裁判及专家将对报告进行审核研判管理等相关工作。确保所有流程可控，所有行为可追溯； | 6 |
| 2 | 获奖情况 | 投标单位或者安全服务团队（投标单位代理的安全服务厂商指定服务团队）最近3年参与国家/省级网络攻防演习活动，获得优秀或最佳攻击队伍，每次加2分；  最近3年参加国家/省级攻防大赛，获得前十名次，每次加2分；  总分不得超过10分。 注：需提供人员有效的获奖证明材料，包括但不限于证书复印件（加盖公章）、相关新闻报道截图等。 | 分项评分 | 10 |
| 3 | 安全服务方案 | 对南财集团环境了解、需求清晰，提供的技术服务方案中的各项服务方案（包括应急预案安全检测、漏洞扫描、渗透测试、重保时期安全监控、应急响应服务等），方案思想先进，方案内容详细、保障、响应机制完善。各项内容交付的报告模板逻辑清晰、编写规整、内容充实、建议切实可行；优秀得10分，良好得6分，一般得3分，差得0分。 | 分项评分 | 10 |
| 4 | 项目经理能力 | 投标单位或者安全服务团队（投标单位代理的安全服务厂商指定服务团队）为本项目配备1名10年以上工作经验的项目经理。具有国家认可的高级技术工程师证书、项目管理专业人员资格认证证书（PMP）、注册信息系统安全专家证书（CISSP）、信息安全工程师资格证书（CISP）、注册信息系统审计师认证证书（CISA）、注册信息安全经理认证（CISM），注册渗透测试工程师(CISP-PTE) 、网络安全攻防实战演习专家聘书，每个证书得2分，本项最高得8分，不提供不得分；  注：需提供人员有效的资质证书、项目经理工作经验年限的有效证明（工资流水、社保缴费记录、劳动合同、单位工作证明等材料之一）、投标单位或投标单位代理的安全服务厂商为其缴纳近1年的社保证明材料（截止至2025年6月）。 | 分项评分 | 8 |
| 5 | 项目团队成员能力 | 投标单位或者安全服务团队（投标单位代理的安全服务厂商指定服务团队）配备的项目技术服务团队人员应不少于6人（不包括项目经理）：  1）团队技术负责人1名：工作年限10年及以上，具备国家认可的高级技术工程师证书、国家注册渗透测试专家（CISP-PTS）、注册信息系统安全专家证书（CISSP）、注册信息安全专业人员证书（CISAW）、信息安全工程师资格证书（CISP）、注册信息系统审计师认证证书（CISA），每个证书得1分，本项最高得4分，不提供不得分。  2）团队其他成员5名：工作年限3年及以上，具备国家认可的高级技术工程师证书，CISP（注册信息安全工程师证书）、CISP-PTE（国家注册渗透测试工程师）、CISAW(信息安全保障人员认证证书，认证方向：风险管理)，每个证书得1分，本项最高得4分，不提供不得分；  注：需提供人员有效的资质证书、人员工作经验年限的有效证明（工资流水、社保缴费记录、劳动合同、单位工作证明等材料之一）、投标单位或投标单位代理的安全服务厂商为其缴纳近1年的社保证明材料（截止至2025年6月）。 | 分项评分 | 8 |
| 6 | 企业本地化支持 | 投标单位或者投标单位代理的安全服务厂商是在广州拥有核心团队（人数不少于10人）得4分；  注：需提供广州办公场地租赁合同复印件、团队成员在广州缴纳社会保险的证明文件或者其他可以证明此项要求的材料。 | 分项评分 | 4 |

#### 2.商务评分标准（20分）

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 具体项目 | | 评分要求 | 分值 |
| 1 | 企业资质 | 投标单位或者投标单位代理的安全服务厂商是否具有以下资质证书：  1） 信息安全管理体系认证证书（ISO27001）认证证书；  2） 质量管理体系认证证书（ISO9001）认证证书；  3）中国通信企业协会颁发的通信网络安全服务能力评定证书风险评估资质；(CESSCN)  4）中国信息安全测评中心颁发的信息安全服务资质安全工程类资质证书；  5）中国信息安全测评中心颁发的信息安全服务资质风险评估类资质证书； | 全满足5分，一项不满足扣1分； | 5 |
| 2 | 同类业绩 | 投标单位或者投标单位代理的安全服务厂商提供2022年至今完成的同类攻防演练、网络安全服务项目业绩数量进行计分：每份1分 ，最高6分。  注：提供合同（包括但不限于合同首页、数量页、金额页和签章页等）作为证明材料，否则相关业绩不得分。 | 全满足6分，少一个扣1分，没案例得0分； | 6 |
| 3 | 标书响应质量 | 标书应答内容完整详实准确，制作格式规范，装订整齐并提供文件索引速查表得5分；标书应答一般，制作简单得2分；标书应答存在错漏，不符合招标要求得0分； | 分项评分 | 5 |
| 4 | 企业实力 | 投标单位或者投标单位代理的安全服务厂商在广州技术人员超过30人及以上得4分，低于得2分，没有不得分（提供社保及毕业证书复印件） | 分项评分 | 4 |

#### 3.价格评分标准（20分）

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 具体项目 | 评分要求 | 分值 |
| 1 | 价格评分 | 1）以各有效投标单位的最低报价作为基准价。  2）评审价等于基准价，得分为20分；评审价每高于基准价1%，报价得分扣减0.1分；不足1%按实际比例计算，减至0分为止。  3）计算公式：价格得分=20-[(报价/基准价-1)×100×0.1]；  4）分数出现小数点，保留小数点后二位，第三位小数四舍五入。 | 20 |