**项目需求**

**一、项目背景**

深圳市信息安全测评中心（深圳市网络与信息安全应急处置协调中心）（以下简称“我中心”）承担深圳市网络与信息安全检测、应急处置、技术协调和监测预警相关工作。如今移动应用的安全问题日益严峻，攻击手段复杂多变，攻击工具越来越简单智能，攻击后果具有很强破坏力。现我中心拟购买服务，提升全市党政机关移动应用的安全水平，维护公共移动互联网网络安全。

**二、具体技术要求**

（一）租用两套移动应用安全检测工具

针对我中心指定移动App和微信公众号（以下简称移动应用）进行为期一年的专项安全检测，覆盖移动应用的客户端自身安全、业务动态安全、通讯链路安全、服务器端安全，出具安全检测报告。租用两套不同厂商的移动应用安全检测工具，两套工具及服务应满足如下要求：

|  |  |  |
| --- | --- | --- |
| 基本  要求 | 销售许可 | ▲拥有公安部颁发的销售许可证（移动应用安全风险评估或移动应用安全检测的产品类别） |
| 软件著作权 | 需具有计算机软件著作权登记证书（移动应用安全风险评估或移动应用安全检测的产品类别） |
| 多平台兼容 | ▲全面支持Android/iOS应用和微信公众号的真机检测 |
| 部署方式 | 将检测系统以私有云方式部署在我中心，并提供工具调用接口，以便与我中心现有账号系统对接。 |
| 日志管理 | 检测系统可记录各账号的使用日志，保留至少半年。 |
| 并发要求 | 每套系统检测并发数至少为十个 |
| 报告要求 | 支持自动导出报告，报告格式至少包括.doc、.pdf、.xml。报告内容至少包括所有检测项以及所发现问题的漏洞名称、风险内容、风险级别、检测详情、修复建议等。 |
| 漏洞名称及风险级别 | ▲本次提供服务的两套移动应用安全检测工具扫描结果相同问题的漏洞名称及风险级别必须一致，由工具原厂家提供承诺。 |
| 检测方式 | 应支持自动化静态逆向分析技术与动态化运行验证技术，检测APP静态与动态运行时的安全漏洞。 |
| 更新要求 | 必须要在五个工作日内将业界最新发现的病毒和漏洞更新到检测工具的病毒库和规则库内 |
| 检测范围 | ▲覆盖客户端自身安全、业务动态安全、通讯链路安全、服务器端安全 |
| 检测项 | 基本信息检测 | 包括但不限于移动应用基本信息，应用权限，应用行为，第三方SDK等检测项 |
| 恶意风险检测 | 包括但不限于恶意程序，越权行为，启动隐藏服务风险，动态加载外部代码风险等检测项 |
| 加固安全检测 | 包括但不限于加固分析、加固对抗，如Java代码加壳、加花、混淆，SO文件加固等。 |
| 源码风险检测 | 包括但不限于拒绝服务攻击风险，应用完整性检测，程序签名保护检测，应用二次打包风险，Activity、Sevice、Content Provider、Broadcast Receiver、Intent等组件检测项 |
| 调试风险检测 | 包括但不限于Java代码动态调试风险，C代码动态调试风险，动态注入攻击风险等检测项 |
| 通用风险检测 | 包括但不限于Webview明文存储密码漏洞，WebView远程代码执行漏洞，WebView组件忽略SSL证书验证错误漏洞，数据库注入漏洞等检测 |
| 数据风险检测 | 包括但不限于内存Dump风险，RSA加密算法使用不当风险，密钥硬编码漏洞，动态注册Receiver风险等检测 |
| 务风险检测 | 包括但不限于系统键盘使用风险，关键界面劫持风险，SSL证书有效性风险，HTTP传输通道风险，应用超时链接风险等检测 |
| 技术支持 | 技术支持 | 对检测结果进行解释；检测工具发生技术问题导致无法检测时，支持团队需在30分钟内提供现场支持，4小时内解决问题。 |

（二）渗透测试服务

人工渗透应模拟黑客的攻击方式，针对我中心指定Web、移动应用等信息系统，进行专业的渗透测试，最大程度地挖掘系统中存在的安全隐患，并提供专业的漏洞安全修复建议。

（三）移动应用安全监测预警服务

针对我中心指定移动应用开展安全监测预警服务，定期出具安全监测报告。服务要求如下：

|  |  |  |
| --- | --- | --- |
| 技术要求 | 安全漏洞监测 | 针对目标移动应用进行定期安全监测，监测周期不超过一个月，针对高中危漏洞进行人工验证后出具详细报告 |
| 覆盖客户端自身安全、业务动态安全、通讯链路安全、服务器端安全 |
| 仿冒应用监测 | 需支持获取主流APP推广渠道信息，监控所有APP相关渠道的信息，包括：版本、渠道、下载源、下载量等 |
| 支持对比正版与盗版应用的文件差异，并支持差异文件列表下载。差异文件包括新增文件、缺失文件、更新文件。 |
| 支持通过文件HASH比对的方法，可以发现盗版应用被修改或添加的文件信息。APK的基本信息对比主要包括正、盗版相关包名、版本信息、版本号、签名MD5值进行数据对比与展示。 |
| 数据对接 | 中标方提供数据对接接口，以便在我中心系统中展示。 |
| 服务要求 | 定期发布监测报告 | 每月根据当月监测情况，发布详细监测报告。 |

（四）移动应用安全威胁情报

威胁情报体系对实施移动应用安全监测预警非常重要，购买移动应用的安全情报可解决我市缺少威胁情报来源和情报难以甄别的问题，要求如下：

|  |  |
| --- | --- |
| 安全动态 | 每周提供深圳属地的移动应用相关的威胁情报及安全动态，包含但不限于恶意/攻击行为鉴别（IP、域名、文件、最新漏洞）、行为定性（目的、动机、组织）、 事件溯源（历史事件、事件关联）、 安全监控（监控变化、异常），覆盖业界移动应用新型高危风险及0day安全漏洞。 |
| 安全态势 | 每月、每季度、每年提供深圳属地及在深圳发布的移动应用安全态势报告及在全省、全国的各类（恶意应用、高危应用、仿冒应用等）占比情况，安全态势报告内容应包含对安全动态中所有内容的梳理及统计分析。 |
| 专项威胁分析 | 依据威胁情报出现的最新安全漏洞对深圳属地及在深圳发布的移动应用输出安全专项态势报告。 |
| 安全应急 | 针对涉及移动应用的重大安全事件协助我中心进行应急处置。 |

（五）驻场技术人员服务

两名移动应用安全检测工具原厂检测人员，提供社保或劳动合同证明。每名技术人员均需具备CISP或CISAW资质，并参与过至少3个移动应用安全检测项目经验（提供相关证明），能胜任本项目提出的各项技术服务要求。

两名专家级技术人员负责驻场渗透测试工作，每名技术人员均需参与过不少于三个渗透测试项目（需提供相关证明），并拥有国家或省部级CTF相关网络安全大赛及获奖经验（需提供相关证明），能充分胜任本项目提出的各项技术服务要求。

一名移动应用安全监测工具原厂监测人员，提供社保或劳动合同证明。人员参与过移动应用安全监测项目（提供相关证明），能胜任本项目提出的各项技术服务要求。

以上五名驻场技术人员均需提供个人简历及无犯罪证明。

在服务期内，中标方不得擅自更换派驻的服务团队中的任何人员。对于不合格的人员，招标方有权要求更换。中标方须在收到招标方通知后一周内完成技术人员更换工作。

**本项目中标单位在预中标公示期间，采购方有权要求中标人到使用单位做全套产品演示。不能提供产品测试或演示内容达不到招标要求的，采购单位有权拒绝签订合同并追究中标单位虚假应标责任。**

**三、商务需求**

1.投标人资质：见招标公告。

2.服务期限：本项目服务期为一年,从合同签订之日起算起。服务期满如采购方评价满意可直接续签合同（最多续签两次）。

3.服务质量要求：在服务期间，投标方应保证先于上级部门发现服务范围内的信息安全事件或漏洞。投标方和每个工具原厂商都需在深圳本地具备一定的技术服务能力，至少都要有拥有20人以上的技术团队（需提供社保证明），并保证发生重大技术问题后技术团队可在30分钟内提供现场支持。

4.培训

（1）提供本项目所涉及的工具功能培训，并提供用户手册；

（2）提供一次本项目所涉及的工具功能培训（含场地及教材费用），人数不超过200人；

（3）提供一次移动应用安全技术培训（不少于两个工作日），培训讲师需具备编写地市及以上移动应用安全标准经历。

5.保密要求：服务期间及服务期结束十年内，中标方必须对服务过程中接触的招标方以及相关方系统中所有信息和数据、服务过程中产生的所有信息和数据等进行严格的保密。不得以任何方式向外界传递或泄露任何相关信息或数据，一旦发现，将追究中标方的法律责任。服务过程中所产生所有文档资料和数据均为招标方所有。

6.违约承诺：投标方违反投标书或合同的承诺（包含但不限于承诺的服务质量、保密要求等），需支付相应的违约金。

7.系统部署时间要求：中标方须在2018年12月1日之前完成所有平台工具的部署、配置和调试，确保所有组件都可以投入运行。

8.付款要求：合同签订且项目所有服务人员到位后，招标方向中标方支付首付款，付款金额为合同总金额的70%。本服务项目经招标方验收合格后，招标方向中标方支付尾款，付款金额为合同总金额的30%。