**广东省妇幼保健院信息安全服务项目用户需求书**

1. **项目概况：**依据《中华人民共和国网络安全法》、《医疗卫生机构网络安全管理办法》等相关文件要求，拟开展信息安全服务，覆盖番禺、越秀和天河三个院区所有业务系统、交换机设备、安全类设备、终端等。

**二、项目详细需求：**

| **编号** | **服务类** | **安全服务项** | **安全服务内容概述** | **备注** |
| --- | --- | --- | --- | --- |
| **1** | 技术检测类 | 漏洞扫描服务 | 对系统进行安全扫描评估，及时发现系统中存在的安全漏洞，出具安全扫描评估报告和加固建议，并指导进行安全加固等操作。 | 每季度不少于4次 |
| **2** | 基线核查服务 | 采用最佳配置核查实践对操作系统、数据库、中间件、网络设备、网络安全设备、网络边界进行分析和配置核查。 | 服务期内开展不少于1次 |
| **3** | 渗透测试服务 | 通过模拟黑客对目标系统进行渗透测试，发现分析并验证其存在的安全漏洞并提出安全加固建议。 | 核心系统，一年不少于1次 |
| **4** | 外网攻击面管理 | 通过IP扫描、子域名扫描、IP反查域名等技术手段对客户单位的”开放IP、开放端口、域名、网站资产“等互联网资产进行识别和梳理，发现未知资产、不必要开放端口。  对网站的“漏洞、篡改、黑链、敏感文件、敏感词、可用性、域名劫持”等6个维度开展实时监测，并通过邮件/微信告警等形式提供网站风险预警服务。输出《外网攻击面监测报告》 | 服务期1年 |
| **5** | 安全事件监测与处置 | 通过全网部署蜜罐，基于欺骗防御技术，诱骗攻击者、病毒主机攻击蜜罐陷阱，实时零误报定位攻击威胁。  针对重要系统服务器部署主机安全监测软件，针对webshell、后门以及异常行为实时监测。  针对事件监测结果，提供处置办法：  1、失陷主机病毒、木马查杀；  2、被入侵网站的webshell网马查杀；  3、针对高频攻击目标进行溯源分析，甄别是否封堵。  输出《安全事件监测报告》 | 服务期1年 |
| **6** | 威胁情报分析服务 | 提供威胁情报分析平台，对医院网络安全状态开展24小时分析服务，发现安全隐患及时提供安全整改建议，协助医院开展整改措施。 | 服务期1年 |
| **7** | 移动APP安全检测 | 通过对移动APP系统的网络通讯、服务器端、客户端(包含安卓和IOS版本)、数据和业务逻辑等多个层面进行细致的梳理、测试和分析 | 重要系统，一年不于少1次 |
| **8** | 日志分析 | 通过对医院的关键设备，包括网络及安全设备、服务器等进行日志分析、溯源、取证。判定是否有入侵痕迹的现象存在。 | 服务期1年 |
| **9** | 安全运维类 | 资产梳理服务 | 对数据中心区资产进行梳理，并形成资产台账。（资产类型包含但不限于：拓扑、资产的IP地址、系统类型/版本、系统账户/密码、开放服务类型/端口、服务组件名称/版本等） | 服务期1年 |
| **10** | 安全驻点服务 | 安排1名中级或以上能力的安全工程师（CISP）驻点医院现场，协助信息科开展网络安全相关工作。 | 服务期1年 |
| **11** | 安全巡检服务 | 对现有网络及安全设备进行巡检，及时发现风险信息，消除安全隐患，巡检完成后提交巡检报告。 | 服务期1年 |
| **12** | 安全加固服务 | 对全院网络设备、安全产品、操作系统、应用系统、数据库等信息资产的安全配置策略和漏洞实施安全加固。针对使用技术检测手段及等级保护测评发现的安全问题，协助医院对存在安全问题的对象进行实施加固整改工作。 | 服务期1年 |
| **13** | 重要时期安全值守 | 在重大活动或迎检等特殊时期，以“事前准备、事中保障（值守、监控、应急、处置）、事后总结（复盘、提升）”的思路来保障用户信息系统的安全。 | 不少于30人天 |
| **14** | 安全管理类 | 体系建设及应急演练服务 | 对现有应急制度进行梳理和完善，满足合规要求，并开展一次应急演练服务。（应急演练场景根据开展时定，应急演练场景有：模拟服务器遭黑客攻击等情况的应急处理、遭遇病毒攻击时的应急处理、系统崩溃和网络故障等信息系统突发情况的应急处理等。） | 服务期内开展至少1次 |
| **15** | 应急响应服务 | 在服务期内，当发生安全事件时，提供应快速应急响应，协助进行安全事件处理及溯源。 | 服务期1年 |
| **16** | 安全培训服务 | 对医院全院人员及信息技术人员进行安全意识培训和安全技能培训，内容包括个人信息保护，日常终端的安全使用，安全事件的引发注意事项等，主要目的提高医院人员的安全意识。 | 不于少1次 |
| **17** | 安全咨询服务 | 根据上级下达任务和其它专项安全需求（迎检），配合完成规范研究、制度落地、方案设计等工作。包括新系统第三方安全评估报告的评审。 | 服务期1年 |
| **18** | 安全事件通告服务 | 在对于紧急重大类漏洞信息，以最直接方式向客户告知漏洞在客户应用系统危害、影响范围及修补方案等信息。 | 服务期1年 |