**南方医科大学口腔医院年度信息系统安全保障服务及等保测评服务市场调研函**

我院拟了解医院年度信息系统安全保障服务及等保测评服务的市场动态情况，现邀请有意向的单位根据我院对需求进行参与。参与办法如下：

**一、项目编号：** 20230613021（117043）

**二、报名时间：**公告发起之日起至2023年 6月 21日17:00。

三、**报名方式：**请意向参与市场调研公司于截止时间前按报名材料要求提交：**提供纸质资料（加盖公章+密封）。**

**联系人：刘生、陈老师 020-84427043**

**资料递交地址：广州市海珠区江南大道南368-1号三楼总务科**

**四、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，拟开展本年度南方医科大学口腔医院信息系统安全保障服务及等保测评服务。本年度信息系统安全保障服务覆盖南方医科大学口腔医院（含四院区）所有业务系统（含在用及服务期内上线系统）、交换机设备、安全类设备、终端等。本年度等保测评服务覆盖南方医科大学口腔医院已定级备案的信息系统。

**五、项目名称：**南方医科大学口腔医院年度信息系统安全保障服务及等保测评服务。

**六、服务地点：**南方医科大学口腔医院

地址：广州市江南大道南366号。

七、**提供服务保障方案应至少包括如下内容（详见附件一）：**

1、资产发现：互联网资产发现、内网资产发现；

2、风险评估：系统层漏洞扫描、web渗透测试、基线检查、新系统上线安全评估；

3、风险保护：网站安全监测服务、安全意识培训、网络与安全检查专项检查、安全预警通告；

4、风险响应：安全运行机制优化、安全事件应急响应、安全事件应急演练；

5、态势感知安全运营管理检测与响应服务（MSS服务）；

6、重保时期威胁专家研判服务；

7、等级保护测评服务。

**八、安全保障服务资质要求（提供相关证明文件加盖公章）**

1、参加本项目投标的供应商必须是具有独立承担民事责任能力的在中华人民共和国境内注册的法人；

2、中国信息界发展研究院颁发的信息化建设及服务能力评价一级资质；

3、国家计算机网络应急技术处理协调中心CNCERT网络安全应急服务支撑单位（反网络诈骗领域 ）资质；

中国信息安全认证中心颁发的信息安全服务资质认证（安全运维服务类、风险评估服务类、应急处理服务类，信息系统安全集成服务类）；

4、中国信息安全测评中心信息安全服务资质认证（安全开发类、安全工程类、风险评估类、云计算安全类）；

5、国家互联网应急中心发布的CNCERT网络安全应急服务支撑单位；

6、国家互联网应急中心发布的CNCERT 网络安全信息通报单位；

7、国家信息安全漏洞库（CNNVD）技术支撑单位；

8、具备安全漏洞挖掘能力。

9.市级以上政府采购电子平台或具有实时公开征集供应商报价功能的网络采购平台供应商库中的供应商：被邀请投标单位须为市级以上政府采购电子平台或具有实时公开征集供应商报价功能的网络采购平台供应商库中的供应商，包括但不限于广东省政府采购网、广东省电子化采购执行平台、广州公共资源交易中心、广东省政府采购智慧云平台等；

10.本项目不允许联合体投标。

**九、等级保护测评资质要求：**

1、具有国家信息安全测评信息安全服务资质证书（提供相关证书复印件加盖公章）

十、**报名资料（所有资料均需盖公章）：**

注：报名材料需设置封面页及目录页，封面页内容包括项目编号、项目名称、公司名称、项目联系人姓名及手机号码，页面内容按市场调研函序列编排，报价函放置最后。（报价方式：总价包干）

十一、**如需组织现场市场调研会议，将另行通知已报名企业。**

注：如有虚假资料、企业违规行为，一经发现，将列入我院供应商黑名单。

附件一：

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **服务分类** | **服务名称** | **服务内容描述** |
| 1 | **网络资产发现** | **互联网资产发现** | 通过专用互联网自动化发现平台，结合调研的方式确定互联网资产范围，之后基于IP或域名，采用 WEB扫描技术、操作系统探测技术、端口的探测技术、服务探测技术等各类探测技术，对互联网侧的主机/服务器、安全设备、网络设备、工控设备、WEB应用、中间件、数据库、邮件系统和DNS系统等进行主动发现，并生成资产及应用列表，列表中不仅包括设备类型、域名、IP、端口，更可深入识别运行在资产上的中间件、应用、技术架构的详细情况（类型、版本、服务名称等）。发现的资产能够自动化导入现有态势感知安全运营平台，协助进行资产运营。 |
| 2 | **内网资产发现服务** | 利用工具并结合现场调研，对内网资产进行资产发现，要对服务器资产与web资产进行重点发现，并对资产安全进行风险分析，分析包括服务器端口开放情况、不常见服务开放情况、服务端口风险情况、web资产风险情况等，并提供专业整改建议，帮助医院网络安全管理部门梳理内网资产，使医院网络安全管理部门掌握真实资产状况。 |
| 3 | **风险评估** | **新系统上线安评** | 对新上线系统进行安全评估，发现系统存在的技术风险，防止系统带伤上线，一般由漏洞扫描、配置核查、渗透测试等多个服务组成。漏洞扫描、配置核查、渗透测试服务要与风险识别中的对应服务要求提供专业服务。 |
| 4 | **系统层漏洞扫描** | 采用远程安全扫描系统，通过定制的扫描规则，形成安全扫描策略文档，对服务器、网络设备、安全设备等进行自动化安全扫描，人工验证扫描结果并输出安全扫描报告及修复建议。 |
| 5 | **web渗透测试** | 通过模拟黑客使用的工具、分析方法对网站进行安全测试，并结合渗透测试智能工具（非漏洞扫描工具）扫描结果，由专家研判人员进行深入的手工测试和分析，识别工具弱点扫描无法发现的问题。主要分析内容包括逻辑缺陷、上传绕过、输入输出校验绕过、数据篡改、功能绕过、异常错误以及其他专项内容。 |
| 6 | **基线检查** | 根据既定的检查规范及方法，采用人工检查用表（checklist）、脚本程序或基线扫描工具对评估目标范围内的主机系统安全、数据库安全、中间件安全等进行系统的策略配置、服务配置、保护措施以及系统和软件升级、更新情况，是否存在后门等内容进行检查。 |
| 7 | **风险保护** | **安全预警通告** | 基于服务商自身威胁情报、安全大数据以及攻防能力推出网络安全情报类资讯服务，定期以邮件或当面沟通形式向医院汇总月度的高危漏洞、安全热点，威胁情报解读精华及漏洞分析统计，为用户提供有价值的网络安全态势推送；对于紧急重大类漏洞信息，以最快时间通过邮件或电话向医院告知漏洞危害、影响范围及应对方案等 |
| 8 | **网络与安全检查专项检查服务** | 为配合监管层的检查，依据省卫健委、省网信办《关于开展卫生健康行业个人信息安全保护专项行动的通知》与《省卫生健康系统网络与数据安全工作任务清单》，从组织管理、制度规范、资产管理、合规保障、信息通报、监测预警、应急处置，安全加固、供应链安全管理、教育教训与管理保障11个大项81个小项进行安全自查，并给出加固整改建议。检查方式包括但不限于制度调阅、现场调研、网络架构分析、远程现场各种技术校验等。 |
| 9 | **安全意识培训** | 面向单位全员开展专业的网络与信息安全意识培训，提高受众个人隐私保护、常规攻击防护、信息安全管理等能力，增强个人网络安全防护意识，规避网络攻击风险。培训内容交付包括不限于现场培训、现场演示、安全意味海报、易拉宝、意识手册等。 |
| 10 | **网站安全监测** | 提供专用SAAS平台进行7\*24小时监测服务，主要包括漏洞扫描、木马分析、篡改监测、关键字监测、网站可用性监测，提供全面的事前、事中的安全监测。网站云监测服务活动包括网站状态安全监测、安全事件报警与响应、网站漏洞检测及网站监测报告编制等四项主要任务。 |
| 11 | **风险响应** | **安全运行机制优化** | 根据本次安全保障范围，依据安全事件的不同类别，如网站系统面临的网页篡改、拒绝服务攻击、DNS劫持攻击、病毒与木马攻击、钓鱼攻击等情况，建立应急专项处置预案及操作手册，在发生安全事件时，各保障小组及网络安全值守组可以根据实际情况参考指导。工作内容包括现状调研、预案编制、访谈、检查、分析与编制。 |
| 12 | **应急响应** | 提供专用电话统一对接应急响应事件处理，根据事件类别，通过远程和现场支持的形式协助医院对遇到的突发性安全事件进行紧急分析和处理。主要工作内容包括：突发事件相关信息的收集、事件的分析、报告提交、问题解决建议等。紧急事件主要包括：病毒和蠕虫事件、黑客入侵事件等。 |
| 13 | **应急演练** | 协助医院网络安全管理部门组织策划和开展应急演练，包括制定演练计划、编制演练工作方案、设计演练脚本、配合准备演练环境、动员与培训、演练过程记录和总结等工作。演练场景包括病毒事件应急演练与网络攻击事件应急演练。 |
| 14 | **态势感知安全运营（MSS服务）** | **管理检测与响应服务** | 为医院现在有的NGSOC态势感知产品提供数据中心资产（IP）数量≤50个的安全托管服务：通过云端收集NGSOC平台的威胁告警包括流量设备告警、安全设备的告警、系统告警等数据，进行关联分析和研判，为医院提供资产、威胁、脆弱性等方面的综合分析服务，帮助医院网络安全管理部门精准识别和监测网络中的安全威胁，并对确认的威胁事件及时通知医院网络安全管理部门、主动进行响应，远程协助医院网络安全管理部门完成威胁事件的闭环处置工作，提供专业的运营指导及改进建议。 |
| 15 | **重保专项** | **重保威胁专家研判服务** | 专家研判人员分析研判依托现有流量威胁检测系统或态势感知系统，协助医院网络安全管理部门进行更复杂、更深入的安全威胁和事件研判，并且在失陷情况下结合主机、网络、数据库等各类安全日志、业务日志进行分析，对攻击影响范围、后果进行研判，发现安全防御体系和策略的缺陷，同时配合进行紧急整改。  要求专家研判人员有利用现有流量威胁检测系统或态势感知系统进行重保研判经验。 |
| 16 | **等保测评** | **等保测评服务** | 1.等保辅助服务：安排专人完成业主单位系统调研及等保测评实施前期准备材料，统筹整个等级保护服务工作，交付《项目实施计划》及《被测对象调研表》。备注：年测系统不需重新备案；  2.根据等级保护相关技术标准对系统进行逐项测评和整体测评并出具《整改问题清单》；  2.完成系统的安全漏洞和渗透测试，根据检测情况提交漏洞和渗透测试报告。  3.整改咨询服务：针对《整改问题清单》提供不符合项的答疑解惑，协助指导软件公司开展软件整改，协助审核业主单位提交的整改材料，及时给与整改建议；  4.验收测评服务：待完成系统的整改后，开展验收测评实施，根据测评结果提交符合国家信息安全等级保护主管部门要求的《网络安全等级保护测评报告》。 |