# 用户需求书

## 项目背景

中山大学孙逸仙纪念医院（中山大学附属第二医院）为国家卫生健康委属（管）医院，创建于1835年，是我国第一家西医医院，中国西医学和西医教育的发源地，至今已有189年历史。2024年11月1日，广州市花都区人民政府与中山大学孙逸仙纪念医院签署协议，合作建设中山大学孙逸仙纪念医院花都院区。这是首家落地花都区的国家卫健委直管三级甲等综合医院，总用地面积约120亩，总建筑面积170000㎡，按照三级甲等综合医院标准设置1000张床位。目前，该院区即将投入使用。

中山大学孙逸仙纪念医院作为国家卫健委直管三级甲等综合医院，需要满足国家等级保护标准、个人信息保护法、网络安全法、数据安全法等安全要求。网络安全防御体系是一项复杂的系统工程，除了网络安全产品建设以外，更重要的是持续的安全运营。随着黑客技术的日新月异，信息科受限于人力资源、技术工具等因素的制约，难以有效应对各类信息安全威胁。因此，需要针对花都院区采购2024-2025年度网络安全服务项目，补充网络安全运营能力，保障各大业务系统安全稳定运行，提升医院服务的质量和水平，为患者提供更加安全、高效的医疗服务。

## 服务需求清单

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **序号** | **服务名称** | **服务产出物** | **服务频率** | **服务期限** |
|  | 安全运营规范制度修订 | 《网络安全管理制度》  《数据安全管理制度》 | 按需 | 1年 |
|  | 网络资产梳理及常态化更新管理 | 《服务器资产台账》  《应用系统资产台账》  《安全设备资产台账》  《互联网资产台账清单》 | 1次/年 |
|  | 漏洞扫描服务 | 《漏洞扫描报告》 | 4次/年 |
|  | 网络安全与数据安全意识培训服务 | 《安全培训教材》 | 1次/年 |
|  | 应急演练服务 | 《应急演练报告》 | 1次/年 |
|  | 重大活动安全保障 | 《重大活动值守方案》  《重大活动值守报告》 | 5人天/年 |
|  | 安全驻场服务 | 《驻点工作周报》  《驻点工作月报》  《事件处置报告》 | 1年  驻场1人 |
|  | 新系统上线检测服务 | 《新系统入网安评报告》 | 按需，10个系统以内 |
|  | 等保整改服务 | 《等保整改记录报告》 | 1次/年 |
|  | 病毒监控防治服务 | 《病毒监控防治服务报告》 | 12次/年 |

## 技术服务内容

★投标人须对其所提供资料的真实性负责，本项目所提供的货物必须经由合法渠道获得，响应内容必须符合采购人的需求，不得出现引起采购人任何知识产权或者法律纠纷，成交供应商必须提供需求书中的技术参数证明材料，并将上述材料的原件在成交后2个工作日内交付采购人核对。采购人有权要求中标供应商在3天内对参数进行演示，若现场演示无法满足招标参数要求，则视为虚假应标，采购人有权追究相关法律责任。

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **服务名称** | **要求项** | **技术指标** |
|  | 安全运营规范制度修订 | 服务频率 | 提供1年按需提供的安全运营规范制定修订服务，服务期限为1年。 |
|  | 服务内容 | 建立网络规划、建设、运维与数据收集、存储、传输、处理、使用、交换、销毁全过程安全管理工作操作规程。 |
|  | 建立完善包括但不限于机构人员、物理环境、网络通信、数据管理、安全建设和安全运维等管理制度。 |
|  | 网络资产梳理及常态化更新管理 | 服务频率 | 提供1年1次的网络资产梳理及常态化更新管理服务，服务期限为1年。 |
|  | 服务内容 | 内部资产识别与梳理：借助安全工具对用户资产进行全面发现和深度识别，梳理医院内部资产，并在后续服务过程中触发资产变更等相关服务流程，确保安全运营中心中资产信息的准确性和全面性，满足落实关键信息基础设施保护资产梳理要求。 |
|  | 资产台账表常态化更新管理：根据医院实际业务发展需要，协助医院定期更新资产台账表，针对资产管理流程包括资产上线和下线的登记、资产负责人或者资产信息变更等内容的登记。 |
|  | 漏洞扫描服务 | 服务频率 | 提供1年4次的漏洞扫描服务，服务期限为1年。 |
|  | 服务内容 | 采用业界主流的漏洞扫描器，针对服务范围内的资产的系统漏洞和Web漏洞进行全量扫描，针对漏洞扫描结果进行漏洞验证与分析，给出漏洞整改建议，最终提交漏洞扫描报告。 |
|  | 服务工具要求 | ▲支持对漏洞进行单个或批量复测，且支持查看复测结果（需提供工具界面截图并加盖厂家公章） |
|  | ▲内置扫描任务报表、基线检查报表、资产报表、漏洞报表、对比报表和自定义报表模板；自定义的维度包括且不限于资产（主机存活性、主机指纹、端口、web指纹等）、漏洞（修复方案、CVSS评分、漏洞细节、漏洞描述、漏洞危害、影响范围等）进行筛选（需提供工具界面截图并加盖厂家公章） |
|  | ▲支持按需自定义漏洞POC检测插件，包括漏洞名称、漏洞类型、漏洞危害、CVSS信息、检测脚本等，用于日常突发漏洞应急。（需提供工具界面截图并加盖厂家公章） |
|  | 支持通过图标的方式展示不同单位的资产漏洞风险情况；包括且不限于漏洞总数、修复漏洞数、新增漏洞数、漏洞变化趋势、漏洞修复状态统计、修复漏洞耗费时间分布、漏洞类型统计。弱口令统计等。 |
|  | 网络安全与数据安全意识培训服务 | 服务频率 | 提供1年1次的网络安全与数据安全意识培训服务，服务期限为1年。 |
|  | 服务内容 | 针对医院相关员工提供网络安全与数据安全相关知识培训，根据不同的用户类型安排有针对性的培训内容（包括管理培训、意识培训）。 |
|  | 应急演练服务 | 服务频率 | 提供1年1次的应急演练服务，服务期限为1年。 |
|  | 服务内容 | 建立网络安全应急机制。根据医院目前应急管理现状和应急资产现状进行评估,协助医院进行应急管理组织与人员结构设计、应急预案设计以及开展应急演练，从整体业务出发完善优化应急管理体系。当信息安全事件发生时，及时，准确的解决事件，将安全事件的影响及损失降到最低。 |
|  | 重大活动安全保障 | 服务频率 | 提供1年按需提供的重大活动安全保障服务，服务期限为1年，全年5人天保障。 |
|  | 服务内容 | 提供重大活动保障，提供现场服务或远程值守服务，包括“粤盾”“粤网安”等年度“护网”专项行动、国家重大会议（两会）、国庆、春节等重要时期，为医院提供包括安全设备检查、安全监控保障、安全事件应急处置等安全保障服务。 |
|  | 安全驻场服务 | 服务频率 | 提供1年的安全驻场服务，服务期限为1年。 |
|  | 服务内容 | 提供1人专人驻场，驻场人员须具备3年以上安全工作经验。负责日常性运维工作，同时按照医院的实际需求，保障非工作时间段的现场运维支持和突发事件处理，协助医院解决各类安全事件。当发生突发任务驻场工程师无法及时有效处理时，安排二线工程师临时现场协助解决问题，保障服务质量。 运维工作内容如下：  1、网络安全监控：  1）负责院内态势感知平台、各边界防火墙、应用安全防火墙、网络准入设备等安全设备系统监控、安全日志分析、安全攻击研判处理、防火墙访问控制策略梳理及优化配置，策略新增及过期策略回收等；  2）负责态势感知平台高危事件研判处置，失陷主机处理；  3）负责新上线网络安全设备纳入常态安全监控、上报与处理。  2、系统安全监控：  1）终端防病毒日志分析，病毒传播态势分析，高危病毒及高危机器分析，病毒源头定位及处理，全院部署率分析，未覆盖终端处理等。  2）院内服务器主机安全监控，日志分析，问题处理，漏洞修复，配置优化等。  3）新上线安全软件纳入常态安全监控、上报与处理。 |
|  | 定期安全巡检服务 | 服务频率 | 每月一次，服务期限为1年。 |
|  | 服务内容 | 每月度对医院态势感知平台、各区防火墙、安全审计、网络准入、防病毒软件、日志平台等安全设备进行深度安全检查和安全日志分析，分析全院整体安全态势，深挖安全隐患，评估整体安全措施的完善性，发现问题及时进行处理，服务内容如下：  设备健康评估：基于历史CPU使用率、内存使用率、硬盘可用空间等，评估设备健康情况，预判设备资源使用的合理性，设备性能负荷的合理性，检查发现的问题并提供有效的解决建议，并如实记录评估结果；  系统运行检查：检查各设备或系统服务是否正常运行，数据库文件大小是否过大或存在碎片文件，各项功能模块是否生效，安全策略是否成功应用，安全防护规则是否更新至最新；  安全日志分析：检查安全设备及系统日志、分析安全设备防护状况，对安全日志进行风险分析，排除内外部安全威胁源及传播渠道，及时进行风险分析、趋势分析及予以有效处置。每次巡检后提交巡检报告材料。  安全策略优化：针对设备安全防护态势，评估安全策略的有效性，针对无效策略、未启用的重要功能、未全面覆盖保护对象等问题进行策略优化，充分发挥安全设备防护效能。 |
|  | 新系统上线检测服务 | 服务频率 | 1年按需提供的新系统上线检测服务，服务期限为1年。全年10个系统以内。 |
|  | 服务内容 | 提供新系统上线前的入网安评服务，采用渗透测试、基线检查、漏洞扫描、弱口令扫描等技术手段，对新上线系统进行全面的安全评估，针对发现的问题提供专业的整改建议，并在整改完成后，进行复测，保障系统上线的安全性。 |
|  | 等保整改服务 | 服务频率 | 提供1年1次的等保整改服务，针对医院定级系统提供等保测评与整改服务。 |
|  | 服务内容 | 等保整改：根据等保测评报告，通过等保测评报告中安全防护级别与业务系统所定级级别要求，进行安全整改与安全加固，包括安全管理制度整改与安全技术整改，落实医院完成等保整改工作，配合院方通过等保复审，最终提升业务系统的安全防护能力。开展等保整改工作期间，提供漏洞安全隐藏服务，对经评估整改后影响业务运行的高危漏洞进行隐藏，达到等保整改要求。 |
|  | 服务工具要求 | ▲网络安全防护能力检测服务工具支持对纵深防御体系做整体验证，支持对各类攻击向量、攻击场景和攻击过程的编排，验证范围覆盖边界突破、权限提升、权限维持、横向移动完整过程。（需提供工具界面截图并加盖厂家公章） |
|  | ▲网络安全防护能力检测服务工具支持对黑客工具进行模拟仿真，包括但不限于MSF、哥斯拉、冰蝎、Empire、Cobalt Strike、frp等，数量不少于30种。（需提供工具界面截图并加盖厂家公章） |
|  | ▲网络安全防护能力检测服务工具支持模拟涉及2台以上服务器的完整攻击路径模拟，可模拟横向移动过程。（需提供工具界面截图并加盖厂家公章） |
|  | 网络安全防护能力检测服务工具支持以攻击方视角展示样本对应的请求包、响应包、攻击工具等信息；支持以防守方视角展示验证样本所属的攻击阶段、技术点、涉及安全设备等信息。 |
|  | 网络安全防护能力检测服务工具支持以图表形式展示验证结果，并在结果中给出综合打分。验证指标包括但不限于产品的阻断率、检测率、穿透率等。 |
|  | ▲漏洞安全隐藏服务工具支持对导入的高危漏洞信息进行智能分析，生成漏洞分析结果和屏蔽建议。（需提供工具界面截图并加盖厂家公章） |
|  | ▲漏洞安全隐藏服务工具支持一键开启漏洞屏蔽策略，支持针对不同主机范围应用不同的屏蔽策略，并支持灵活调整屏蔽的策略，设置是否拦截漏洞攻击，也可对应设置屏蔽白名单，放行正常业务。（需提供工具界面截图并加盖厂家公章） |
|  | 病毒监控防治服务 | 服务频率 | 提供1年12次的病毒监控防治服务，服务期限为1年。 |
|  | 服务内容 | 提供防病毒系统巡检、病毒查杀服务、防病毒管理软件的安装管理和协助安装。旨在提升防病毒系统的使用效果，实现防病毒安全预警，提升病毒安全事件应对能力。针对防病毒系统提供防病毒运维工具进行病毒日志深度分析，结合人工研判，通过人机共治方式，对周期性病毒数据进行自动化分析，保障病毒巡检报告的准确性与可靠性。 |
|  | 服务工具要求 | 防病毒运维工具支持病毒感染情况分析，可展示数据包括网络内前十位病毒感染情况和前十位计算机感染情况，直接呈现病毒名、病毒感染次数、前十病毒感染总数占记录总数的比例、计算机名、计算机被感染次数数据、前十计算机感染总数占总记录的比例，使网络病毒感染现状可视化。 |
|  | ▲防病毒运维工具支持病毒传播及感染方向分析，可展示数据包括本机内横向扩散病毒数、通过移动存储感染病毒数、通过互联网感染病毒数、引导区病毒数、局域网横向传播病毒数，辅助安全管理人员直观判断病毒传播渠道风险。（需提供工具界面截图及病毒分析报告证明） |
|  | 防病毒运维工具支持前十病毒全网扩散情况分析，可展示数据包括病毒扩散情况排名前十的病毒名称、被感染计算机数量与具体被感染的计算机名称。（需提供工具界面截图及病毒分析报告证明） |
|  | ▲防病毒运维工具支持勒索病毒感染情况、挖矿病毒感染情况分析，可展示数据包括病毒名、受感染文件路径、感染计算机名称、感染计算机数量，帮助安全管理人员梳理勒索病毒、挖矿病毒感染情况，有效闭环病毒处置工作。（需提供工具界面截图及病毒分析报告证明） |
|  | ▲防病毒运维工具支持全网感染黑客工具的计算机分析，可展示数据包括黑客工具名称、感染计算机名称和感染计算机数量。基于全网感染黑客工具的计算机分析数据，可以直观发现网内是否存在黑客入侵风险与被入侵的计算机名称及数量。（需提供工具界面截图及病毒分析报告证明） |
|  | ▲防病毒运维工具支持自定义防病毒运维考核KPI指标包括病毒码更新率、客户端部署率、病毒感染率、病毒接触率。通过防病毒日志分析周期内运维考核KPI指标完成情况，直观呈现出单位当前防病毒运维效率。（提供工具界面截图及病毒分析报告证明） |
|  | 防病毒运维工具支持病毒扫描方式数量及占比情况分析，可展示数据包括病毒扫描方式如实时扫描、预设扫描、手动扫描、其它扫描类型以及扫描数量占比情况，帮助用户了解单位工作周期内的防病毒运维工作情况。 |

## 技术服务要求

为保障服务质量，服务团队以项目组形式驻场医院，提供全年实时现场响应服务，具体安排如下：

（一）服务范围

驻场于采购方花都院区；

（二）人员要求

1.中标人需按要求安排1名项目经理、1名现场驻场工程师、5名二线技术专家组成项目团队，提供7\*24小时保障服务，项目团队具备网络安全、数据安全、渗透测试等方面的安全能力。并提供参与本项目的全部人员名单，名单内容包括但不限于姓名、项目角色、服务方式（现场或远程支持）、获得认证证书、工作经验（即参与类似安全服务项目案例情况及项目角色）。

2.在项目实施过程中，招标人有权要求对不符合项目服务要求的成员进行更换。

3.如项目关键阶段需补充人员，投标人要及时保障人力资源补充，确保项目按计划交付。

4.投标人的团队应具备以下资质：

**（1）项目经理**

职责：负责项目的总体计划安排和协调工作，负责与招标方项目负责人对接，项目运维体系建立、制度编写、工程师管理、组织项目沟通会等管理运营工作，即服务工作的衔接和协调，确保项目整体成功。

人员要求：

1. 要求本科以上学历，拥有5年或以上网络安全服务或相关领域的管理实施经验；
2. 具有政府部门或事业单位批准颁发网络安全相关认证证书。

**（2）团队人员配置（驻场安全服务工程师**）

职责：

1. 驻场人员要按照采购人各相关部门负责老师的安排，完成各项工作；
2. 故障受理率要求达到100%，并按照服务级别对事件进行响应；
3. 驻场人员的能力水平，要达到标书上对各个系统的维护指标要求；包括工程师技术水平、故障诊断的准确性、沟通能力、准备工作、遵守服务方和用户规范等；
4. 驻场人员要求具备专业网络安全运维服务经验，能够独立开展网络安全检测、网络安全日志分析、安全事件处置的能力，同时具备沟通技巧和和独立思考能力，对医院业务流程有深入理解。
5. 要求本科以上学历，拥有5年或以上网络安全服务或相关领域的管理实施经验；
6. 驻场人员存在工作态度、责任心、技术能力、协调能力等方面的问题时，用户有权要求更换驻场人员，中标供应商须在收到用户方书面通知之日起7个工作日内更换。

人员变更要求：

满足招标文件中项目经理及项目团队人员要求；如有人员更换，中标方需提前1个月向采购方报备。

（三）服务报告

1.《服务周报》：每周提供一份周运维简报，内容包含设备维护数据、工作任务执行、重大事项、待办事件跟进、下周工作计划。

2.《月度服务报告》：内容包含设备维护数据、总结分析月度服务统计等内容，并提出合理化的改进意见。

3.《季度服务报告》：总结分析每季度内设备运行情况、服务统计等内容，并提出合理化的改进意见。

4.《年度服务报告》：总结分析全年设备运行情况、服务统计等内容，并提出合理化改进建议，并向医院进行正式的总结性汇报。报告及全年服务记录装订成册后于每年合同结束前 10 天内提交。

（四）出勤机制

中标方须为采购方提供全天候驻场运维服务，根据医院出勤时间要求安排出勤。

（五）服务响应

中标方为采购方提供7\*24小时热线响应、技术支持服务。运维人员接到故障请求后不能通过远程指导解决时，要15分钟抵达现场处理，故障处理时间控制在20分钟内；重点部门（如急诊、门诊、收费处、手术室等）有特殊的响应机制，要做到随叫随到。

（六）应急处理

中标方应建立应急处理机制，当故障评估在1小时内无法解决时，需要及时调动公司级别资源开展应急处置，保障医院业务不间断运行。

（七）沟通管理

1.日常沟通：中标方驻场工程师可以采用电话、微信、书面、面对面交流等方式与采购方进行沟通，保障沟通效率与质量；

2.定期沟通会：中标方每月或季度安排项目经理向采购方进行工作汇报，汇报内容包含但不限于工作计划完成情况、工作存在问题、建议与意见等。