网络安全服务项目2024

用户初步需求书

# 项目概况

为继续深化并认真落实我院网络安全各项规划工作，结合我院现有信息化现状，本次项目主要以优化网络架构、补强网络安全防护能力、建立长效的安全服务机制为主要目标，通过此次项目建设进一步提升我院网络安全整体防护能力。

|  |  |  |
| --- | --- | --- |
| **拟调研项目** | **最高限价（人民币）** | **交付时间** |
| 信息安全服务2024 | 200万元 | 自合同签订之日起3个月内完成软硬件产品的部署实施交付，1年内完成相关安全服务。 |

# 二、 拟调研内容

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **序号** | **项目** | **技术参数** | **数量** | **单位** | **备注** |
| 1 | 安全服务1：渗透测试 | 以主流渗透工具模拟黑客攻击为主要手段，发现常见的高中危漏洞为主要目标，将发现的安全漏洞进行整理，给出详细说明，并针对每一安全漏洞提供相应的解决方法。并结合医院修复情况，协助医院针对修复后的漏洞进行复测验证。 | 1 | 项 | 目前医院对外映射的各类api、web+门户等共计90余个  1年，2次 |
| 2 | 安全服务2：红队测试 | 以APT攻击者视角对医院目前现有防御措施进行深度渗透测试，对目标系统、人员、软硬件设备、基础架构，进行多维度、多手段、对抗性模拟攻击，旨在发现可能被入侵的薄弱点，并以此为跳板将攻击渗透结果最大化（包括系统提权、控制业务、获取信息），进而检验现有防御体系的短板。 | 1 | 项 | 1年，2次 |
| 3 | 安全服务3：漏洞扫描 | 使用系统漏洞扫描工具对 数据库、操作系统、中间件等进行漏洞、端口、弱口令扫描，扫描完成后由技术人员对漏洞进行确认测试，提出整改建议，协助开发人员整改。 | 1 | 项 | 1年，2次 |
| 4 | 安全服务4：外部攻击面管理 | 敏感数据泄漏排查加上  1）互联网暴露面梳理（根据医院的公网ip、根域名、ICP备案号、业务系统名称等在互联网上做资产梳理，发现影子资产或僵尸资产）  2）攻击面分析（识别暴露的攻击路径和资产风险等级，确定关键风险的优先级，并给出关键风险的处置建议）  敏感数据泄漏检测（覆盖全网（含暗网、深网）范围数据泄露监测和分析） | 1 | 项 | 1年，每季度一次 |
| 5 | 安全服务5：日常安服 | 每年20人天的重保现场值守；每周1人天的现场安服、应急响应、安全巡检、态势感知月度季度报告等。长期驻场安全工程师1名。 | 1 | 项 | 1年 |
| 6 | 零信任系统 | 700并发，3年软件升级+服务 | 1 | 套 | 3年 |
| 7 | 内网探针 | 配合威胁检测与响应平台及MSS使用，部署于内网区域 | 1 | 台 |  |
| 8 | 出口上网行为管理AC | 性能参数：网络层吞吐量（大包）≥20Gb，应用层吞吐量≥6Gb，带宽性能≥4Gb，实配准入终端数≥10000，每秒新建连接数≥60000，最大并发连接数≥2000000。 硬件参数：规格：2U，内存大小≥32G，硬盘容量≥960G SSD，电源：冗余电源，接口≥4千兆电口+4千兆光口SFP+2万兆光口SFP+。  全模块开启，软件升级(\*5年);  产品质保(原厂5年);  **要求满足信创** | 2 | 台 |  |
| 9 | 出口边界防火墙 | 性能参数：网络层吞吐量≥40G，应用层吞吐量≥25G，防病毒吞吐量≥5G，IPS吞吐量≥5G，全威胁吞吐量≥3G，并发连接数≥800万，HTTP新建连接数≥20万  硬件参数：规格：2U，内存大小≥16G，硬盘容量：≥480G SSD，电源：冗余电源，接口≥4千兆电口+4千兆光口SFP+4万兆光口SFP+。  全模块开启，软件升级(\*5年);  产品质保(原厂5年);  **要求满足信创** | 2 | 台 |  |
| 10 | Api网关平台 | 包含数据开放服务资产、数据开放服务授权管理、数据开放服务安全态势、数据开放服务问题追踪、数据服务路由、网关服务、解析/调用服务等功能模块 **请自行选型并描述具体功能** | 1 | 套 | 质保1年 |
| 11 | 云端安全网关平台 | 改变目前医院业务直接映射至公网的架构，web类、api类端口映射由云端安全网关首先进行清洗和过滤，通过技术手段阻拦扫描、漏洞利用、爬虫、CC、ddos等多种攻击手段；过滤之后再转发至真实业务出口地址。  **请自行选型并描述具体功能** | 1 | 年 |  |
| 12 | 堡垒机授权扩容 | 医院在用的2台堡垒1000个点授权已满  扩到1300点 | 2 | 套 |  |
| 13 | 零信任沙箱 | 在目前aturst上实现安全访问，比如敏感文件的编辑管理，不可远程打开不可截图 | 1 | 套 |  |
| 14 | 集成技术服务 | 详见下文服务要求、商务要求 | 1 | 套 |  |

# 三、 详细技术要求：略，请报名单位自行选型描述

# 四、 安全要求

（一）应用安全管理建设

所建应用包括用户管理、用户访问安全和应用操作安全，满足国家及我院对应用安全管理相关规定。

（二）数据安全管理要求

数据安全管理包括数据传输安全、数据加工存储安全、数据备份等，信息系统在建设的过程中应该有具体的数据安全管理方案和措施，满足国家及我院对数据安全管理的相关规定。

（三）实施安全管理建设

根据我院对医院信息系统实施安全管理相关文件的基本要求，做好实施安全管理建设，配合好信息系统等级保护测评及整改相关工作。

# 五、 商务要求

（一）供货要求

1. 产品均应为原厂全新的原装产品，无侵权行为、无任何缺陷隐患，在中国境内可依常规安全合法使用；
2. 产品必须得到制造商认证，符合国家或国际的质量标准；
3. 浙江省肿瘤医院有权对产品进行第三方的检测，如产品未能达到调研内容的性能参数，可要求无偿更换或单方面终止合同。
4. 本项目的所有软、硬件(如线缆、软件、硬件模块等，包括未列出而系统实施又必需的软件、硬件)需配齐以构成一套完整实用系统，所有辅材采用原装配套产品，没有原装配套的产品的，由供应商提供相应产品并保证其质量安全。
5. 完成设备的安装调试，电源、相关缆线（网线、光纤线）必须齐全并满足机房实际布局连接要求；新增设备后如涉及到机房布局需要进行调整。
6. 本次拟调研内容内容除包括上述设备外，还应包括随机的辅助设备、专用电线电缆、随机软件、技术资料（包括操作手册、使用指南、维修指南和含维修网点在内的服务手册等）、设备运行所必需的随机消耗材料，相应的技术服务与质量保证。
7. 产品的应详细列明设备的所有技术指标（包括所投产品的品牌、规格型号、详细配置、主要技术参数、随机软件等），明确表示该项指标所涉及的软硬件是标准配置还是选择配置。同时还须包括产品说明书或产品主要技术资料和性能的详细描述，产品制造、安装、验收标准，详细的交货时所配文件清单、主要部件明细表（包括品牌、制造厂名和主要技术参数）等。
8. 产品相关所有预装和为本项目安装的软件均为具有合法版权或使用权的正版软件且无质量瑕疵。
9. 如遇软件产品升级、改版，应免费提供更新、升级服务。
10. 注：报名单位可对于供货要求提供更细化的内容。

（二）交付时间

自合同签订之日起3个月内完成软硬件产品的部署实施交付，1年内完成相关安全服务。

（三）交付地点

由浙江省肿瘤医院指定地点，免费送货上门，免费安装调试合格。

（四）实施服务

为保证项目质量，保证措施、服务响应及时、项目管理（包括项目组织管理、人员管理、技术管理、进度管理、资料管理等），在项目各项内容实施期内，提供不少于3人的项目组成员现场支持。

注：报名单位可根据拟定拟调研内容提出更细化的实施方案内容。

（五）验收要求

1. 项目完成软硬件部分安装、调试、测试后正式移交浙江省肿瘤医院，试运行30个日历日后，如系统运行正常，由供应商提出初验申请并出具项目实施情况初验报告。
2. 项目完成剩余服务部分内容后，如服务内容根据要求实施完毕，由供应商提出终验申请并出具项目实施情况终验报告。
3. 交付验收标准依次序对照适用标准为：①符合中华人民共和国国家安全质量标准、环保标准或行业标准；②符合招标文件、投标文件及浙江省肿瘤医院认可的合理最佳配置、参数及各项要求。

# 六、 服务要求

（一）售后服务

1. 保修期自项目验收合格之日起计算，软硬件产品质保详见清单要求，服务类内容服务1年，报名单位应对保修期的具体期限做出承诺，保修期内对所供产品提供免费上门保修保用服务。
2. 保修期内负责对所供产品实行包退、包维护保养，所有产品的维修、版本升级均为免费。
3. 报名单位须提供不少于四次/年的巡检服务，巡检对象须包括医院现有的核心网络安全设备的巡检服务。
4. 提供详细的实施方案，若在实施过程中造成医院业务非计划性停机或者数据丢失，由中标方负全部责任并赔偿院方因此造成的全部损失。
5. 报名单位需充分考虑医院现有的软、硬件的利旧方案，并免费提供设备搬迁服务、机柜搬移服务和数据迁移服务，所产生的第三方费用由中标方承担。
6. 报名单位须具备全专业技术团队服务能力并针对本项目组建专门的实施团队，且实施团队不少于5人，要求投标时提供相关工程师社保证明以及证书复印件，后续实施的工程师必须与投标文件中的工程师一一对应。
7. **报名单位须提供7\*24小时技术支持，全年不少于40个工作日的现场技术支持。**
8. 报名单位须提供现场技术保障服务，协调原厂人员实行网络安全检查和加固，并向用户汇报各项工作情况。
9. 报名单位应提供系统扩充、升级方面的技术支持服务。

注：报名单位可对于售后服务提供更细化的内容。

（二）培训要求

1. 基本培训要求：针对系统管理人员提供产品的配置、操作及维护培训，主要内容为平台系统的基本结构、功能与特性，日常使用操作、维护与管理，常见故障的排除，紧急情况的处理等，直到业主工程师熟悉使用。培训时间不少于1天。
2. 用户使用培训：针对业务人员使用操作培训，主要内容为平台系统基本情况与功能介绍、实践操作，技术指导等。培训时间不少于3天。
3. 培训地点：平台系统安装所在地，具体由浙江省肿瘤医院确定，人数不限。
4. 维保期内提供不少于6次的集中培训服务。

注：报名单位可根据上述需求提供更细化的培训内容。

# 七、调研要求

1、面向集成商、服务商进行本次项目方案征集。

2、请对拟调研内容中各项各准备至少3个设备/系统/服务商选型（12-14项只需1个选型），详细描述参数及功能，分别进行分项报价。

3、综合出具针对我院的信息安全改造优化方案，提出合理化建议，进行短期和长期的安全建设规划。

4、报价包含达到项目实施条件的一切内容，不再增加额外费用。