技术参数确认书

项目名称：网络安全分析、等保测评服务与安全设备维保

一、项目概述和使用需求

1.我院开放了大量的互联网业务，且互联网业务逐年递增，这些开放的互联网业务均与内网相连，虽然购买了大量的安全设备，但是否真正安全，是否存在系统漏洞和安全漏洞仍然未知，需要通过安全厂商每月一次的上门安全分析巡检服务，可以迅速发现和解决全网安全问题，彻底保障我院网络信息安全，安全服务持续2年。

2.2023年下半年即将有3台应用防火墙、1台SSLVPN、1套态势感知系统售后维保服务即将到期，为保证安全设备特征库能持续升级保护网络，需要购买此6项设备的维保服务2年。

二、主要技术参数

**①网络安全分析、等保测评服务**

1、服务清单

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **序号** | **产品名称** | **数量** | **单位** | **服务次数** | **服务结果** | **工具说明** |
| 1 | 安全漏洞扫描服务 | 1 | 年 | 4次 | 《数据库漏洞扫描报告》  《网络及安全设备配置扫描报告》  《网站漏洞扫描报告》 | 人工及漏洞扫描工具 |
| 2 | 安全培训服务 | 1 | 年 | 2次 | 《信息安全培训教材》  《信息安全培训记录》 | 自备 |
| 3 | 渗透测试服务 | 1 | 年 | 服务期内按需提供 | 《渗透测试报告》 | 人工及渗透测试工具 |
| 4 | 代码审计服务 | 1 | 年 | 服务期内按需提供 | 《代码审计报告》 | 人工及代码审计工具 |
| 5 | 应急响应服务 | 1 | 年 | 服务期内按需提供 | 《应急响应报告》 | 人工 |
| 6 | 安全咨询服务 | 1 | 年 | 4次 | 《安全咨询报告》 | 人工 |
| 7 | 服务器安全加固服务 | 1 | 年 | 持续使用 | 《安全加固报告》 | 人工及服务器安全加固工具；持续使用 |
| 8 | 人工智能值守服务 | 1 | 年 | 持续使用 | 《人工智能值守报告》 | 人工及人工智能值守工具；持续使用 |
| 9 | 等级保护测评服务 | 2 | 项 | 1次 | 为his系统和互联网医院信息系统出具《信息系统等级保护测评报告》 |  |
| 10 | 智能护网服务 | 1 | 年 | 持续使用 | 《护网服务报告》 | 人工及智能护网工具；持续使用 |
| 11 | 资产梳理 | 1 | 年 | 1次 | 提供《资产清单》 |  |
| 12 | 培训认证 | 1 | 项 | 1次 |  |  |

2、服务要求

|  |  |
| --- | --- |
| **服务项目** | **主要技术要求** |
| **第1项**  **安全漏洞扫描服务** | 1．服务内容：  构建一体化合规检查、安全能力、资产侦测及管理服务等能力，实现等保合规检查、安全自查等合规能力，并提供全网漏洞扫描、病毒查杀等安全检测服务。投标人需提供安全合规评估工具。  2．服务要求：  提供安全合规评估服务工具应满足以下需求：  （1）任务管理：支持手动创建重要信息系统检查、行业主管部门检查、备案单位检查、网站检查、专项检查、自定义检查任务；支持接收上级监管部门下发的通知，处置，监察任务。  （2）检查范围：支持行业主管部门、备案单位、重要信息系统、网站四类检查对象；检查内容：支持系统定级情况、岗位设置情况、安全审计情况等检查内容；  （3）检查要点：支持检查对象检查内容具体检查指标项进行检查；  （4）检查结果录入类型：单项判定（支持判定是、否、不适用符合项结果）、检查结果录入（支持录入检查结果记录）、复合型结果录入（支持在选择符合性结果的基础上录入相应记录）。  （5）检查执行：针对每个检查要点应提供相应的检查方法，检查结果判定依据等相关检查知识，以便引导进行现场检查；支持禁用或启用检查要点；支持检查结果录入功能，要求检查结果录入的类型包括选择型、文本型、复合型三种录入类型；支持对检查过程中具体检查对象（例如：主机、网络设备等）进行调整功能，要求可以选择已有的检查对象或录入新的检查对象；支持检查证据录入和管理功能，检查层面、检查内容、检查指标项支持筛选功能，支持检查工具检查结果信息的展现功能；支持一键检查，工具执行支持多任务多工具一键选择，自动执行；支持一键导入，智能自动匹配工具检查结果所对应的信息系统；支持单个工具检查结果快捷导出，根据用户需要求挑选单个工具检测结果导出word、HTML格式，提供简洁明了的单个工具检查报告。 |
| **第2项**  **安全培训服务** | 1.服务内容：  通过开展信息安全培训工作，强化安全意识，理解安全理论，掌握安全技术，获得安全实践经验，甚至通过安全认证，使得信息安全人员能够掌握安全方面必要的专业理论和技能，全面提升从事信息安全工作人员的管理和技术水平，保证其能够胜任相应的岗位，且能够融会贯通并应用于单位的安全建设当中。  2.服务要求：  使用安全供应商自研的信息安全意识培训教材包和素材包； |
| **第3项**  **渗透测试服务** | 1.服务内容:  通过安全扫描，真实模拟黑客使用的工具、攻击方法来对用户指定业务系统进行非破坏性质的安全测试，对采购人网站和信息系统进行渗透测试，找出系统中存在的漏洞进行验证，提供渗透结果及截图，进行深层次漏洞挖掘并提供解决建议，并对网站和系统的安全现状、安全保护程度进行评估。测评过程中，使用专业的安全分析工具（至少包含专业的主机网络安全分析、应用系统安全分析工具）对待测系统进行安全分析。  2.服务要求：  （1）在保证信息系统正常运行前提下，模拟黑客攻击行为通过远程或本地方式  对信息系统进行非破坏性的入侵测试，查找针对应用程序的各种漏洞，帮助采购人理解应用系统当前的安全状况，发现在系统复杂结构中的最脆弱链路并针对安全隐患提出解决办法，切实保证信息系统安全；  供应商应在得到我院授权后方可开始实施渗透工作。  3.服务时限：  （1）每季度来我院执行一次.  （2）当新互联网信息系统上线时执行一次。 |
| **第4项**  **代码审计服务** | 1．服务内容：  为我院指定的业务系统提供代码审计服务。  2．服务要求：  代码审计服务以及报告应满足以下需求：  （1）服务期限内对新上线系统和我院指定的信息系统源代码进行审计分析，需审计的系统数量不少于50个。  （2）每个新上线的系统源代码至少找出3类问题（包括不限于owasp top10类，加密算法类，函数或指针调用后未释放，未使用标准的内置工具，代码运行质量类，程序自身加密弱或加密方式不合规，函数声明后未使用，越权使用，以及其他开源信息等。），并出具相应的报告，在报告中体现有问题的代码原始行号。  （3）应支持主流开发语言的代码审计，如：JAVA、Pythion、C、C++、C#、Ruby、GO。  （4）支持主流动态脚本的审计如：PHP、JSP、ASP等。  3.服务时限：  （1）按需提供服务。  （2）每季度来我院执行一次。  （3）当新互联网信息系统上线时执行一次。  ▲（4）代码审计服务需业务提供商提供源代码后服务商现场执行服务。 |
| **第5项**  **应急响应服务** | 1．服务内容：  （1）在我院遇到重大或突发安全事件后按照要求的服务响应级别采取相关的措施和行动。帮助我院正确应对安全事件，降低安全事件带来的损失和影响，并将业务以及网络恢复到正常状态；  （2）应急响应包含但不限于以下几类安全事件：WEB安全事件、恶意程序事件、网络攻击事件、信息破坏事件等。  2．服务要求：  （1）提供7×24应急响应服务，提供应急响应服务方案；  （2）安全事件要求应急团队在规定的时间，对信息安全事件做出响应，并严格按照采购人信息安全等级要求迅速到达现场并解决问题：  特别重大事件（Ⅰ级），5分钟做出响应，提供远程 7×24 小时响应服务、1小时到达现场进行应急响应服务；  重大事件（Ⅱ级），10分钟做出响应，提供远程 7×24 小时、2小时到达现场进行应急响应服务；  较大突发事件（Ⅲ级），30分钟做出响应，提供远程 7×24 小时响应服务、4小时到达现场进行应急响应服务；  一般性突发事件（Ⅳ级），30分钟做出响应，提供远程 7×24 小时响应服务、远程无法解决时，在4小时到达现场进行应急响应服务；  （3）每次故障处理完毕3个工作日内提供详细的故障处理报告。 |
| **第6项**  **安全咨询服务** | 1.服务内容：  基于我院在用的态势感知系统发现的终端威胁信息进行安全排查，并判断是否存在误报，对有问题的终端进行相应的处理，提供相关的安全解决方案。  2.服务要求：  每个季度到现场配合并帮助我方人员排查有安全隐患的终端，提出解决方案。最后给出《安全咨询报告》。 |
| **第7项**  **服务器加固服务** | 1．服务内容：  在内网服务器（含虚拟服务器）中部署服务器安全加固工具，有效提升内网服务器的整体安全性。  2．服务要求：  对内网服务器提供安全加固工具应满足以下需求：  ★（1）国产品牌，安全加固工具授权的服务器数量不低于100台（提供加固工具的计算机软件著作权登记证书复印件并加盖投标人公章）。  （2）拥有SQL防注入功能,并能准确记录被攻击的页面和攻击者的信息,如IP地址、机器MAC地址以及物理位置。  （3）拥有XSS跨站攻击过滤功能，能对常见的跨站攻击进行过滤  （4）拥有针对WEB的入侵检测功能，能对来自网路层的攻击进行有效防御，比如：远程溢出攻击、数据库溢出攻击、DZ论坛漏洞攻击、暴力口令猜测攻击等。  （5）拥有过滤WEB错误页面,对404 403 505等网页错误过滤。  （6）能针对第三方的WEB应用扫描进行阻断，如Acunetix Web Vulnerability Scanner等  （7）有WEB应用虚拟补丁功能，能对存在公开漏洞且未安装补丁的WEB应用进行防护；  ★（8）Web恶意脚本的查杀识别准确率不低于测试样本总数的95%；能对常见的网页木马文件进行脱壳解密；有主动防御技术，能对系统全方位监控，对于文件的复制、移动、修改、重命名以及下载上传等都能做到监控；支持文件防篡改功能；支持系统账户保护功能，防止操作系统账户被修改或增加。（提供第三方检测机构针对该指标的检测报告复印件，并加盖投标人公章）。  （9）支持对Web服务器进行加固，依据设定的规则对特定的项进行执行限制，包括但不限于支持IIS、Apache、Nginx等Web服务软件禁止执行某个程序；  （10）支持对数据库进行加固，依据设定的规则对特定的项进行执行限制，包括但不限于支持MongoDB 命令行进程、MongoDB 共享服务进程、MongoDB 核心进程、Oracle 监听服务进程、Oracle 核心进程、Mysql数据库客户端、Mysql数据库核心进程、Mssql数据库核心进程等禁止执行某个程序；  （11）支持对应用运行环境进行加固，依据设定的规则对特定的项进行执行限制，包括但不限于支持Node.js、Java、PHP FastCGI、PHP等运行环境禁止执行某个程序；  （12）支持对Windows、Linux服务器其它特定进程进行加固：特定进程将受到限制，具体行为依据设定的规则；  （13）允许在应用加固规则中设置白名单，支持设置程序名或全路径等信息。 |
| **第8项**  **人工智能值守服务** | 1．服务内容：  提供7\*24小时计算机AI（人工智能，非人工）值守服务工具，智能研判黑客攻击概率后，由该工具自动拨打报警电话或发送APP信息调度护网工程师进行相关应急处理。  2．服务要求：  提供AI值守服务工具应满足以下需求：  （1）▲AI值守服务工具的AI综合风险度分析引擎支持接入第7项的内网服务器安全加固工具，经数据融合处理后实现综合研判。  （2）名单设置：允许部署工具时预设人员相关信息，包括但不限于姓名、部门、通信权重、电话、通信时间等；当网络安全出现紧急情况时，工具会根据预设权重，从优先级别高到低自动循环拨打联系人电话，直至名单内人员接听电话为止。  （3）排班管理：可在工具中预设应急人员的排班计划，排班信息包括但不限于姓名、通信优先级、通信时间等；当网络安全出现紧急情况时，工具会自动按照当日预设的排班表按优先级循环拨打值班人员电话，通过AI语音告知出现的风险。 |
| **第9项**  **等级保护测评服务** | 1.服务内容：  为我方的《his系统》和《互联网医院信息系统》2个系统提供信息安全等级保护三级测评服务；测评机构能够利用测评、评估、漏洞扫描等方法发现系统安全隐患并提出合理的整改建议，对系统漏洞能够及时定位，并对后续修复的情况进行验证，最终出具信息系统等级保护测评报告。同时在项目服务周期内，服务方应提供相关的安全咨询服务，提供的安全咨询建议、策略、规范和整改建议要切合我方实际情况，满足GB/T22239-2019《信息安全技术-网络安全等级保护基本要求》等标准、规范的相关要求。  2.服务要求：  （1）网络安全通用测评  安全物理环境测评：依次对信息系统重要非涉密系统所在位置进行检查：物理位置的选择、是否有物理访问控制、是否有防盗窃和防破坏、是否有防雷击、是否有防火设施设计、是否有防水和防潮、是否有防静电、是否有温湿度控制、是否有电力供应UPS、是否有电磁防护等防护项目进行检查测评。  安全通信网络测评：安全通信涉及的测评对象包括：系统网络结构，通信传输完整性，可信验证的检测和防范。网络安全测评所对应生成的检查记录表包括：系统网络结构安全核查记录、通信传输完整性安全核查记录、可信验证安全核查记录。  安全区域边界测评：测评对象包括接入边界防护情况，访问控制情况，入侵防范情况，恶意代码防范情况，安全审计情况，可信验证情况。  安全计算环境测评：安全计算环境是针对身份鉴别、访问控制、安全审计、入侵防范、恶意代码防范、可信验证、数据完整性、数据保密性、数据备份恢复、剩余信息保护、个人信息保护的情况进行检查。安全管理中心测评：安全管理中心员是检测是否进行进行身份鉴别，是否只允许其通过特定的命令或操作界面进行系统管理操作，是否对这些操作进行审计。测评对象为：系统管理、审计管理、安全管理、集中管控。  安全管理制度测评：安全管理制度的测评将采用访谈、检查文档的方式测评该信息系统的管理制度方面的安全保障情况。安全管理制度的测评对象为：安全策略、管理制度 、制定和发布、评审和修订文档记录等。  安全管理机构测评：安全管理机构的测评将采用访谈、检查文档的方式测评该信息系统在安全管理机构方面的安全保障情况。安全管理机构的测评对象为：岗位设置、人员配备、授权和审批、沟通和合作 、审核和检查。  安全管理人员测评：安全管理人员的测评将采用访谈、检查文档的方式测评该信息系统在人员安全管理方面的安全保障情况。人员安全管理的测评对象为：人员录用、人员离岗、安全意识教育和培训、外部人员访问管理。  安全建设管理测评：安全建设管理的测评将采用访谈、检查文档的方式测评该信息系统在系统建设管理方面的安全保障情况。系统建设管理的测评对象为：定级和备案、安全方案设计、产品采购和使用、自行软件开发、外包软件开发、工程实施、测试验收、系统交付、等级测评、服务供应商选择。  安全运维管理测评：安全运维管理的测评将采用访谈、检查文档的方式测评该信息系统在系统运维管理方面的安全保障情况。系统运维管理的测评对象为：环境管理、资产管理、介质管理、设备维护管理、漏洞和风险管理、网络和系统安全管理、恶意代码防范管理、配置管理、密码管理、变更管理、备份与恢复管理、安全事件处置、应急预案管理 、外包运维管理。  （2）安全扫描与测试  对信息系统设备进行安全测试与扫描。  （3）分析与报告  通过测评信息收集分析，形成《差距评估报告》、《评测报告》等。  （4）可委托具有等保测评资质的第三方公司进行此项服务，提供该项服务前需和我院签订现场测评授权书。 |
| **第10项智能护网服务** | 一、服务概述：  在服务期内，安全服务商需提供并部署一套智能护网工具，对现有系统进行7\*24小时日常安全监测及风险处置。 二、要求：  ★1、护网工具应拥有微隔离、内核加固、网络防御、文件主动防御、防篡改、防勒索、应用伪装、态势感知等安全护网功能，为了保证安全运营闭环需求，所有功能需在同一后台界面、统一账号登录管理并进行综合日志分析（提供软件截图证明并加盖投标人公章）。  2、拥有风险发现能力，能根据检查项对不同的服务进行弱口令检查，包括但不限于： windows、Linux、MySql、MSSQL、Ftp、Telnet、RDP 等。  3、护网工具需提供黑客攻击服务器态势感知功能，支持采集和展示网络防御、文件主动防御、防篡改、防勒索、微隔离、风险发现、应用伪装模块及安全日志，以安全大数据为基础进行研判分析，从全局视角提升对安全威胁的发现识别、理解分析、响应处置等能力；支持轮播模式。   1. 护网工具管理端底层具备独立安全的操作系统。 2. 护网工具支持对访问IP设置白名单，限制对系统的访问时间。 3. 防勒索模块拥有系统防勒索功能，基于驱动级拦截技术实现针对勒索病毒及恶意代码的防护，不依赖于特征库识别方式防御勒索病毒攻击，开启防御后保护目录只拥有防勒索策略中的权限和可读权限。能自行设定防勒索规则，如：特定进程、特定范围、特定文件、特定格式等。 4. 防勒索模块堡垒模式：支持对特定终端实现强安全保护模式，禁止任何新应用程序的运行，有效防止包括勒索软件、已知勒索病毒、未知勒索病毒、挖矿病毒等恶意攻击。 5. 微隔离模块拥有自学习功能，能在设定的时间范围内，按流量方向（出站/入站/双向）和流量类型（外网/内网/双向）自主学习整个网络的访问情况并自动生成规则，学习结果支持融合入站或出站规则，使用者可以根据学习结果自行下发规则。 6. 应用伪装模块拥有应用伪装功能，能根据设定的规则（如端口号、描述、协议等）自动开启端口。允许设置连接次数阈值、数据包数阈值和间隔时间等。。   10、▲智能护网工具应兼容鲲鹏等国产处理器（出具相关证明材料并加盖投标人公章）。 |
| **第11项 资产梳理** | 对核心网络设备、业务主机配置的系统版本和安全策略梳理并形成资产管理表格；对安全设备性能、配置、策略等梳理形成资产管理表格。 |
| **第12项 培训认证** | 1．服务内容：  通过开展信息安全培训工作，强化安全意识，理解安全理论，掌握安全技术，获得安全实践经验，甚至通过安全认证，使得信息安全人员能够掌握安全方面必要的专业理论和技能，全面提升从事信息安全工作人员的管理和技术水平，保证其能够胜任相应的岗位，且能够融会贯通并应用于单位的安全建设当中。  2．服务要求：  使用安全供应商自研的信息安全培训教材包和素材包。 |
| **安全服务资质** | ▲投标人资质：须提供ISO9001质量管理体系认证证书；ISO20000信息技术服务管理体系认证证书；ISO27001信息安全管理体系认证证书的复印件并加盖投标人公章。  ▲工程师资质：安服人员需具备CISP（注册信息安全专业人员证书）、CISAW（信息安全保障人员认证证书）、CIW（认证网络安全技术工程师证书）三种证书的其中一种，提供相关证书复印件和在投标人单位近三个月缴纳社保的证明文件复印件并加盖投标人公章。 |
| **备注** | ★以上所有服务技术要求，所包含的软件系统和硬件都必须为国产品牌。投标人响应无偏离和正偏离的，需提供一份对应的《服务可实现承诺书》并加盖投标人公章。 |

**②安全设备维保**

1、维保硬件:三台防火墙型号分别为AF-1000-D420-VG、AF-2000-H642-VR、AF-2000-B2150。1台SSLVPN型号为VPN-1000-A400。

态势感知探针和态势感知系统型号为STA-100-B440和SIP-1000-B400。

维保内容：1、AF-1000-D420-VG：2年网关杀毒升级，2年规则库升级，2年产品质保，2年软件升级。

2、AF-2000-H642-VR：2年网关杀毒升级，2年规则库升级，2年产品质保，2年软件升级。

3、AF-2000-B2150：2年规则库升级许可，2年产品质保，2年软件升级。

4、VPN-1000-A400：2年产品质保，2年软件升级。

5、STA-100-B440：2年探针特征库软件升级，2年产品质保，2年软件升级。

6、SIP-1000-B400：2年安全感知系统平台特征库软件升级，2年产品质保，2年软件升级。

7、产品质保包含以上所有硬件的免费保修。

三、交货期与安装实施要求

★1.交货时间与服务时间

(1)中标人应在采购合同签订后之日起开始对安全设备进行维保服务，为期两年；网络安全服务时间从2024年5月1日起至2026年4月30日止。

★2.交货地点与交货方式

（1）交货地点：申请科室指定地点。

（2）交货方式：在签定正式合同前，中标人须针对招标文件“二、技术要求”中响应无偏离和正偏离的重要参数、核心参数，向采购人提供相对应的招标文件要求的相关资质（或证明材料）原件。同时，采购人可要求拟成交供应商在采购人现场按照招标文件技术要求对所提供的产品功能逐条进行POC验证性测试，并填写POC测试报告。若无法满足技术指标要求或未能通过测试，院方可以不签订合同，并将其列入供应商黑名单。