**广医附属番禺中心医院网络及数据安全服务**

**用户需求书**

# 项目基本情况

广州医科大学附属番禺中心医院从网络安全运营的全局视角和安全需求出发，按照法律法规、行业标准的要求，从风险识别、纵深防护、安全监测、应急处置、安全加固的维度，构建以数据为核心、技术为手段、服务为支撑、管理为保障的，能为支撑医院数字的持续发展提供资产管理、脆弱性管理、合规管理、指挥决策、联防联控为一体的，从而为医院网络安全空间治理持续赋能，提高整体的网络安全管理效益和治理水平，确保与关键基础设施和应用业务持续稳定运行。

番禺中心医院网络及数据安全服务项目包括以下安全服务：网络安全运营服务、渗透测试服务、新系统上线评估服务、日常巡检、安全策略优化、安全有效性验证服务和协助安全加固服务，同时提供重要时期保障、安全培训、应急响应、应急演练等服务实现医院网络和数据安全的保障。

# 项目采购的具体服务内容要求

## 采购内容及要求

注意：需考虑同时满足本院与分院的网络及数据安全服务建设要求，具体服务内容如下表：

|  |
| --- |
| **网络及数据安全服务要求** |
| **序号** | **服务项** | **服务分项** | **内容** | **数量** | **单位** | **服务年** | **备注** |
| 1 | 安全运营服务 | 全局安全日志采集监测服务 | 1）日志采集探针：提供软件版或者硬件版，安全日志采集探针，采集支持SYSLOG、流量探针等多种数据采集方式，支持多厂商异构设备，流量融合探针将从流量中检测的已知威胁，上报态势感知系统。支持远程连接沙箱实现恶意文件攻击检测。内置的异常行为检测引擎，实时匹配流量，当发现存在异常或违规行为时会将流量片段在采集的流量数据中进行标记，发送给态势感知系统，由安全服务分析平台进行深度关联分析，挖掘潜在的威胁。2）服务器探针：软件部署，可进行资产自动发现和服务器资产脆弱性扫描，发现和扫描信息上传至态势感知平台。3）全局安全服务分析平台：采用先进的大数据采集、建模、分析技术，通过对各种网络资源的多维度信息采集和自动化的关联分析，及时发现网络当中的威胁和异常行为，通过安全编排与自动化联动防火墙、入侵防御、终端安全等安全产品的联动处置，实现对威胁和异常行为的及时有效处置。系统通过图形化、可视化技术将识别到的各种威胁和异常通过图形化方式直观的展现给用户，有利于用户全面掌握网络总体安全态势，并可通过运营中心的工单处理和通报预警系统进行全方位协同管理，让网络安全可感知、易运营、安全事件快速联动闭环。平台通过“能力三要素，四中心一平台”构建网络空间安全治理体系，从顶层架构设计出发，内置基于监管行业的神经网络训练模型，结合自动化编排、人工编排、混合编排等方案；实现技术与管理双驱动，提供综合性网络安全态势感知与协同指挥平台。为监管部门打造网络安全的宏观、中观、微观一体化的综合治理体系，实现战略决策、战役指挥和战技方法能力。支持通过第三方存储备份工具限制超出时间或次数限制的情况下为了确保数据安全，可以强制销毁盘内内容。同时工具可提供安全登录、设置、文件操作等日志进行记录并上报服务分析平台进行安全蒴源。提供工单的新增、编辑、处理、删除、查看工单详情、查看工单处理记录以及工单的导出等功能，内置知识文章、安全专家、事故案例、安全基本要求、应急预案库和应急处置建议等知识，同时提供管理自定义知识的功能。支持镜像流量和服务器探针检测业务系统中的弱密码，检测列表包含账号、密码、服务器、所属分析和业务、弱密码数、弱密码类型、URL、登录状态、类型、最近发现时间等信息。通过打造协同联动的响应机制，让态势感知系统成为智慧的安全大脑，精准分析全网未知威胁和针对性攻击，利用协同联动实现针对性加固防御和精准打击，让全网安全建设具备主动防御的能力。 | 2 | 年 | 2年 | 　 |
| 7\*24小时安全监测分析 | 对全局的安全日志进行7\*24小时全天候、不间断的监控和分析，以发现和处理安全威胁和攻击。在重要告警方面，发现威胁及时通告单位。7\*24小时全天候涵盖但不限于以下范围：工作日、周末节假日重要时期保障：两会、国庆、春节、元旦、五一等，需要重点防护，不能出安全事件HW重保：国家HW、省市HW，需要重点防护，不能出安全事件 |
| 网页篡改监控 | 对客户的对外服务网站可用性、网页完整性进行7\*24小时实时监测，实时发现网页篡改、服务下线等严重问题，保障客户对外服务安全稳定运行。只送一个站点进行监控，若需监控多个站点，需要额外采购。 |
| 联动处置响应 | 通过工具能力联动客户相关设备进行自动处置动作达成闭环 |
| 新漏洞预警通报 | 新漏洞预警通报是指对新出现的安全漏洞进行预警通报，以提醒用户及时采取措施进行修复。信息安全是动态发展的。面对日益演变的安全攻击手段和系统安全漏洞的不断发现和利用，工作网所面临的风险也在不断变化。每周向各单位提供实时安全动态，帮助各单位了解最新的安全技术和安全理念。服务内容系统漏洞信息：将一段时期内，各操作系统、应用系统、网络设备等的最新安全漏洞进行通告，包括漏洞威胁、影响平台及修补方法等。病毒信息：将一段时期内，最具威胁性的病毒信息进行通告，包括病毒危害、感染原理及防护措施等。安全预警：一旦出现将可能造成大规模网络攻击事件的安全漏洞或病毒木马，进行及时的安全预警，积极进行补丁修复和安全防护。信息安全事件：将一段时期内，相关信息安全事件进行通告，避免客户工作网遭遇同样安全攻击事件，造成严重损失。安全技术研究：专业信息安全团队对最新安全技术进行深入研究，包括信息系统漏洞挖掘、风险分析以及安全防护技术。 |
| 线上协助事件响应 | 提供7＊24小时安全事件线上响应服务，对事件进行分析溯源、并提供事件处置方案建议等。 |
| 半年度汇报 | 半年度汇报，每半年对半年的安全运营整体状况输出年度报告，其中包含半年度安全总结、问题总结、优化建议。 |
| 互联网攻击面梳理 | 发现客户暴露在互联网侧的资产，检测安全风险隐患并进行安全性测试，评估安全防护水平，量化安全风险，针对风险问题给出合理化整改建议。服务范围：1个域名或1个互联网出口IP |
| 2 | 安全监测 | 重要时期保障服务（现场） | 在两会、重大演练等重大活动期间，为医院提供安全值守服务，协助处置医院内部网络安全事件。主要工作内容：1、安全值守日常巡检工作在日常应急安全值守的过程当中，将定时针对重要服务器、网络设备、网站系统进行状态检查，并定时针对各安全设备（包括防火墙、IDS）进行日志分析，及时发现异常和处理安全事件。2、范围控制识别事件的蔓延方式，采取关闭一定的设备或应用程序、停止重要数据的存取、限制用户访问权限、限制网络访问、调整安全策略等有效手段对其进行控制、阻隔，防止危害进一步扩大蔓延，以最小危害原则保障医院利益。对已造成影响的系统要求尽快以最大程度消除影响，恢复系统正常状态，保证系统的连续性和稳定性。3、事件处理提前准备好所需工具和设备，并搭建备份环境，根据应急处理流程对出现的安全事件进行恢复，保证恢复损坏系统的原有配置，观察类似方面是否有同种危害，通过一定时间的检测，恢复用户访问权限，为减少影响尽快使系统进入正常运作。4、分析危害应医院要求可对事件的原因进行调查，追溯攻击危害来源，并在符合司法程序的前提下进行取证提供给医院。5、后期工作协助医院完成相关安全记录，完善相关安全标准和脆弱性报告，提出安全改进建议；与相关人员进行专题交流，保存事件处理报告，为后期处理类似事件提供参考资料。 | 40 | 人天 | 2年 | 　 |
| 3 | 安全威胁评估 | 渗透测试服务 | 通过攻防渗透人员提供人工专业的渗透测试服务，针对Web站点、应用系统等，充分挖掘业务系统潜在的风险，并提供整改建议。对网站或者系统进行渗透测试，重点发现网站应用层业务流程和逻辑上的安全漏洞和敏感信息泄露的风险，输出渗透测试报告。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、异常错误等以及其他专项内容测试与分析。 | 10 | 系统 | 2年 | 标配为5个系统/年。鉴于每年业务系统新增及功能更新的不确定性，建议超出部分按实际需求结算。跟等保系统匹配（5个三级系统） |
| 4 | 新系统上线前评估服务 | 根据应用系统上线安全需求情况，加强新业务系统上线安全验收管理，接入与入网前减少和消除安全隐患，有效预防和规避安全事故的发生。根据“安全三同步”的入网安全及风险评估管理办法要求，对新建系统实施入网上线安全评估，修补新业务系统安全漏洞，落实安全合规配置等要求。对新上线的业务系统开展依照入网安全管理方法开展一次安全评估，一到多次的复查，最终让系统达到入网安全管理办法的基本要求。主要内容包括Web漏洞发现、主机漏洞扫描、基线核查、渗透测试、主机服务探测、弱口令检查、业务系统账户口令调研、webshell查杀等整体全面的风险技术评估。 | 10 | 系统 | 2年 | 标配为5系统/年。鉴于每年业务系统新增及功能更新的不确定性，建议超出部分按实际需求结算。跟等保系统匹配（5个三级系统） |
| 5 | 日常巡检服务 | 针对医院网络安全软硬件系统进行深度巡检，数据配置审视，安全设备的策略分析和调优、网络性能分析和架构可靠性分析，发现设备运行中存在问题和潜在风险，进行总结和提出措施建议。 | 4 | 按需 | 2年 | 原则上每半年一次 |
| 6 | 安全策略优化服务 | 安全策略优化是指对安全控制策略是否起到作用、是否合理高效进行检查和改进，可以及时地发现和控制风险。在安全服务的过程中，需要持续地对信息系统各个层面的安全策略进行优化，需要通过工具及人工的方式进行检测、分析、优化。策略信息收集后，结合实际业务安全需求，对现有安全策略进行差距分析，发现策略缺失、策略冗余、策略未废止等问题，并制定相应工作方案开展策略优化工作，内容包括：访问控制策略优化、安全防护策略优化、行为审计策略优化等，通过安全策略优化完善策略可用性，提升防护能力。 | 4 | 次 | 2年 | 原则上每半年一次 |
| 7 | 安全有效性验证服务 | 目的是帮助医院通过一系列的评估和检测流程，确保其安全防护措施能够有效地工作，并发现可能存在的弱点。这种服务通常包括但不限于：对已部署的安全防护措施进行综合评估，以确定它们是否按照既定的规则和策略有效地执行防护和检测任务。服务范围：1次1区域 | 2 | 次 | 2年 | 原则上每年一次 |
| 8 | 安全加固 | 安全培训服务 | 根据不同的用户类型安排有针对性的培训内容。培训人员主要包括：全体员工、安全运维人员等。培训目标：对全体员工的培训，目的是使他们了解网络安全相关法律法规，当前网络安全威胁态势，建立网络安全防护意识。技术人员主要包括：操作人员、维护人员等。培训目标：对技术人员的培训，目的是使他们了解工作网所面临的严峻安全威胁和挑战，以及如何进行全面有效的安全防护措施。 | 2 | 次 | 2年 | 原则上每年一次 |
| 9 | 钓鱼演练 | 网络钓鱼威胁攻防演练服务包括三部分：调研分析、测试实施、结果通报。调研分析为构造具有迷惑性的钓鱼邮件，增加测试的真实性，诱导被测试人员查看并点击钓鱼链接，实施前需进行充分的调研分析，包括客户环境、热点事件、人员安全意识现状等。测试实施根据调研分析结果，确定和制作钓鱼邮件样例，敲定测试时间及目标对象后，实施定性测试；结束后发送风险提示邮件，并对客户行为数据统计分析，形成钓鱼邮件测试报告。结果通报对客户组织内人员安全意识输出评估结果并给出提升建议，同时就邮件系统现状提出安全建议。 | 2 | 次 | 2年 | 原则上每年一次 |
| 10 | 应急演练服务 | 根据医院组织架构，完善现有应急预案，预案包括主流应急事件场景（漏洞、病毒、篡改、入侵等），并按照应急预案，选择对应场景和系统进行一次以桌面推演的方式开展应急演练工作，工作内容包括演练场景制定和实际演练，用以提高医院应急响应和处置能力。 | 2 | 次 | 2年 | 原则上每年一次 |
| 11 | 安全加固服务 | 基线加固：对设备系统进行基线核查后，针对资产基线情况进行加固方案设计，并执行系统安全加固，确保系统的安全性及合规性漏洞加固：提供漏洞校验工具，以及人工识别的方式对漏洞进行验证，确保漏洞被充分识别，避免漏报或误报的漏洞信息。针对发现的漏洞问题，进行加固方案设计，包括系统、数据库、中间件、应用工具、管理工具的版本升级、补丁安装、配置优化、工具替用等方法流程。根据漏洞加固方案内容，逐项对漏洞问题进行修复，针对漏洞修复过程中出现的异常问题进行分析、修复。提供漏洞扫描工具，针对已修复的漏洞进行二次验证，确保漏洞修复工作精准有效。针对漏洞管理情况进行整体分析汇报，确保漏洞管理工作具体有效。 | 4 | 次 | 2年 | 原则上每半年一次 |
| 12 | 应急响应 | 应急响应服务 | 当医院发现外部攻击事件、或被监管单位通报时，提供紧急事件处置支持，对攻击事件进行详细分析，根据实际条件情况提出具有针对性的处置办法，并协助医院加以处置。 | 2 | 按需 | 2年 | 原则上每年一次 |
| **A** | **合计** |  |  |

## 服务交付物要求

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **服务项** | **服务分项** | **交付物** |
| 1 | 安全运营服务 | 全局安全日志采集监测服务 | 《MSS运营周报》《MSS运营月报》《MSS运营年报》 |
| 硬件流量采集组件服务（按需） |
| 7\*24小时安全监测分析 |
| 网页篡改监控 |
| 联动处置响应 |
| 新漏洞预警通报 |
| 线上协助事件响应 |
| 半年度汇报 |
| 互联网攻击面梳理 |
| 2 | 安全监测 | 重要时期保障服务（现场） | 《重要时期保障总结报告》 |
| 3 | 安全威胁评估 | 渗透测试服务 | 《业务系统渗透测试报告》《业务系统渗透复测报告》 |
| 4 | 新系统上线前评估服务 | 《业务系统入网安全评估报告》 |
| 5 | 日常巡检服务 | 《安全巡检报告》 |
| 6 | 安全策略优化服务 | 《安全策略优化报告》 |
| 7 | 安全有效性验证服务 | 《安全防护有效性分析报告》 |
| 8 | 安全加固 | 安全培训服务 | 《安全意识培训教材》《安全专项技能培训教材》 |
| 9 | 钓鱼演练 | 《钓鱼演练报告》 |
| 10 | 应急演练服务 | 《安全应急演练报告》 |
| 11 | 安全加固服务 | 《网络安全漏洞整改报告》《安全加固报告》 |
| 12 | 应急响应 | 应急响应服务 | 《应急处置报告》 |

## 响应公司要求

1、供应商必须具有独立法人资格，能独立承担民事责任和合同义务。

2、供应商必须具有有效的中华人民共和国企业法人营业执照。

3、具有良好的商业信誉和健全的财务会计制度。

4、供应商须具备履行合同的设备和专业技术能力。

5、供应商须未被列入“信用中国”网站(www.creditchina.gov.cn)以下任何记录名单之一：①失信被执行人；②重大税收违法案件当事人名单；③政府采购严重违法失信行为。

6、供应商应遵纪守法、诚信经营，近三年内（自本公告发布之日起往前推三年）无违规违法行为或采购活动中无不良记录。

7、本项目不接受联合体参与，中标项目不允许转包。

# 商务要求

## 服务期限和服务地点

### 服务期限

（1）合同签订后2年。

### 服务地点

采购人指定地点，中标人负责将产品运送至采购人指定地点并完成系统软件安装调试，并通过验收合格才可交付采购人使用，中标人须承担由此产生的全部费用。

## 质量、安装及验收标准要求

1、中标人承诺提供原装的、全新的、功能、性能及指标符合或优于国家及招标文件提出的有关技术、质量、安全标准及要求。

2、中标人所提供用于提供服务的产品应具有较高的可靠性和稳定性，满足7×24小时连续不间断运行需要。

3、验收按国家有关的规定、规范进行。国家有强制性规定的项目验收，按国家规定执行，本项目必须严格遵循国家及相关部门的要求，达到招标文件所要求的所有功能。

4、采购人签署的项目验收报告，作为项目款支付的依据。其中硬件验收依据合项目合同相关要求。

## 付款方式（样例，以最终招标为准）

（1）项目签订合同后15个工作日内支付合同总额的30%；

（2）项目签订合同满1年，支付合同总额的50%；

（3）当全部服务内容完成时，支付剩下的20%的费用。

（5）支付方式采用银行电子转账支付。

（6）如涉及硬件，设备到货验收合格后，采购人向中标人支付硬件部分合同金额的余下款项。