**中山市中医院网络信息安全运维服务服务项目采购需求**

**一、项目概况**

1、项目名称：中山市中医院网络信息安全运维服务服务项目

2、项目内容：医院拟委托一家服务公司，提供线上线下结合的专业信息安全服务团队，协助完善技术防护体系，强化运营流程，确保在潜在漏洞被利用前完成修复，或在遭受攻击时实现及时的响应处置，从而将业务中断风险降至最低，为医院构建覆盖事前预防、事中监测、事后响应的闭环安全运营体系以加固网络安全。

3、预算金额：315000元

4、服务期：一年

**二、服务内容**

（一）**信息安全运营服务**

1. 服务内容

对医院30个服务器资产提供信息安全运营服务，通过7×24小时全面的安全监测、分析和响应机制，提供暴露面梳理，快速识别和处置违规暴露资产，降低安全风险，提供直观的安全态势展示和定期安全报告，帮助我院构建主动、闭环的安全运营架构，同时满足合规要求。

2. 安全策略与配置核查

每季度对医院网络安全策略和配置进行全面核查，确保其有效性和合理性，及时发现并修正潜在的安全隐患，使医院的安全防护措施始终处于最佳状态。

3. 安全漏洞管理

3.1 每季度进行全面清查服务内网络资产，做好每一个高危可利用漏洞的防护工作，包括但不限于提供漏洞修复方案和安全设备防护策略，以及帮助医院配置防护规则。

3.2 及时更新安全设备防护策略，配置防护规则，防止因漏洞被利用而导致重大安全事件，避免医院遭受损失。

4. 威胁监测与处置

4.1 监测医院服务资产内的网络和系统安全状况，运用先进的监测技术，对异常流量、恶意代码和钓鱼邮件等威胁进行精准检测和分析，一旦发现可疑迹象，立即着手处理。

4.2 发现高风险威胁时，在获得医院授权后，通过迅速联动安全设备，下发阻断命令，快速阻断恶意流量和攻击行为，防止威胁扩散，最大程度降低安全事件对医院业务的影响。

5. 暴露面管理

5.1 每季度开展互联网暴露面梳理工作，精准识别暴露在互联网上的服务器、数据库、端口、数据资源等资产，全面了解暴露面情况，并对其进行有效管理，降低暴露面资产带来的安全风险。

5.2 通过专业的服务工具收集暴露资产信息，暴露面信息至少包括域名、域名标题、IP 地址、开放端口、移动端暴露面等，并能采集对应暴露资产的访问截图向医院举证，同时分析暴露资产存在的漏洞，为后续的安全防护提供有力依据。

6. 安全分析、事件管理及可视化交付物

6.1 对脆弱性、异常流量、攻击日志、病毒日志等数据进行采集和实时分析研判，通过先进的分析技术，准确识别各类安全威胁和潜在风险，为安全决策提供有力支持。

6.2 将同一资产的多个告警进行聚合分析，高效发现各类安全事件并及时生成工单，工单详细记录告警的基本信息，涉及的业务信息、攻击趋势、威胁详情、攻击原理、处置建议等内容，并支持根据医院实际情况提供备注，便于医院跟踪和处理安全事件。

7. 服务期间首月提供《中山市中医院首次安全风险分析报告》、《中山市中医院威胁情报》，每月提供《中山市中医院安全运营月报》，每季度提供《中山市中医院安全运营季报》，年末提供《中山市中医院年度总结汇报》等可视化交付物，帮助医院全面了解安全状况和改进方向。

**（二）本地化安全应急及驻点安全运维服务**

1. 服务内容

提供1年的本地技术应急与现场安全驻点服务，旨在通过现场驻点+技术支撑团队共同协助医院构建一套完善的本地化安全应急及驻点安全运维服务体系。通过专业的技术团队、先进的技术手段和规范化的管理流程，实现对医院网络安全的全方位监测、主动响应、安全加固、应急处置及人员培训，确保医院在日常运营及重大时期的信息安全，为医院的信息化建设与发展提供坚实的安全保障。

2. 网络安全服务需求

2.1 日常运维：负责网络安全设备运维检测，日志收集分析，隐患排查及策略整改；漏洞扫描及基线核查，提供检测报告；持续对接日志审计，保存日志 6 个月；定期查看日志，高风险及时反馈加固；协助设备调试运维，完善相关网络安全设备部署；针对病毒事件提供整改建议及加固，定期升级安全设备及病毒特征库。

2.2 设备调整优化：针对不同网络安全设备，根据院方实际场景需求进行临时调整或策略优化，满足信息部门日常运维需求。

2.3 应急响应：提供应急故障现场增援服务，确保及时处理。

3. 日常监测与运维服务

每天针对监测类的安全产品进行巡检、包括但不局限防火墙、WAF、入侵防御、入侵检测、防病毒系统、态势感知等网络安全设备，通过日志分析，每天为医院信息系统内防病毒系统、安全设备和态势感知系统产生的海量日志进行深度挖掘和分析，从IP分布、时间分布、事件分布，行为分布、告警趋势这五个维度对用户信息系统内安全设备和态势感知平台产生的日志进行梳理，发现潜在的风险点，并及时进行处置，每周针对安全情况，汇聚成一份运维监测报告，进行安全汇报。

4. 主动响应与安全日志巡检服务

4.1 提供每月1次的安全日志巡检分析服务，主要由安全服务工程师对医院数据中心的网络安全设备、防病毒系统、态势感知平台分析等进行安全巡检、安全日志分析及安全告警事件处理，主要包含以下三块内容：

4.1.1 医院数据中心的安全设备进行安全巡检：包括设备的运行状态、设备负载是否正常，设备授权是否到期，系统版本是否需要更新等，通过每月的安全巡检可以保障设备的正常运行。

4.1.2 医院的防病毒系统日志分析：针对医院的防病毒系统进行日志分析时，需配套提供防病毒运维工具，可以配合医院快速进行病毒分析并出具巡检报告，输出《中山市中医院防病毒巡检报告报告》。服务期间提供的防病毒运维服务系统，导入病毒日志数据后，自动生成病毒分析报告，全网安全治理服务频率和病毒分析报告内容包括如下：

4.1.2.1 周期内全网病毒感染趋势图，需要对大量重复数据进行降噪去重，整理出实际可用的潜在病毒风险实时数据。

4.1.2.2 提供当期、历史前十位感染病毒的机器清单，直观了解全网病毒感染分布，迅速定位高危计算机。

4.1.2.3 提供病毒传播及感染方向分析，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、局域网横向传播病毒数，直观判断病毒传播渠道风险。

4.1.2.4 提供前十病毒全网扩散情况分析，并且进行相关处置事件闭环动作，确保病毒得以控制。

4.1.2.5 提供覆盖“事前防御-事中阻断-事后处置”的全生命周期勒索病毒防护体系，包括基于攻击链的入侵防御、行为拦截及数据恢复能力，并实时生成攻击事件工单，联动防火墙快速隔离恶意文件。服务承诺攻击响应≤15分钟、勒索变种防御率≥99%，且基线配置符合等保2.0要求。

4.1.2.6 提供全网感染黑客工具的计算机分析，直观发现网内是否存在黑客入侵风险。

4.1.2.7 可自定义防病毒运维考核KPI指标，并通过防病毒日志分析周期内KPI指标达成情况。

4.1.2.8 安全态势感知系统巡检分析。

4.1.3 巡检结束后，结合巡检目标的具体安全内容编写解决方案和相关的安全建议，为管理员的维护和修补工作提供参考。输出如下报告：《中山市中医院月度安全监测运维报告》

5. 安全加固服务

根据安全服务团队进行漏洞扫描和渗透测试过程中发现的弱点和安全隐患，配合协助医院对信息系统的服务器、网络设备、信息安全设备进行安全加固服务，提高系统与服务器平台运行的安全性、可靠性。配合漏扫中查出的问题对应实施安全加固，对软件系统补丁的安装指导，输出安全加固报告。

5.1 系统安全加固

主要完成根据漏扫报告，对操作系统、应用中间件、数据库增打补丁的需求，使打完补丁后的系统环境能够正常运作，发挥系统软件应有的功能。至少应完成以下工作内容：

5.1.1 分析补丁的可用性及风险；

5.1.2 制定升级计划及应急回退计划；

5.1.3 做好各项系统备份准备；

5.1.4 安装软件升级包；

5.1.5 检测升级的有效性；

5.1.6 升级失败，做系统回退；

5.2 应用程序漏洞加固

协助对除操作系统、应用中间件、数据库以外的业务系统应用程序的漏洞，出具安全整改报告，及时通知相关业务系统管理员，并协同各管理员、第三方软件开发商、第三方维护人员等共同制定整改计划，在整改过程中提供相应的技术指导。

6. 安全迎检服务

提供信息安全迎检服务，为积极迎接网监、卫健局等上级单位的安全检查，确保安全检查工作能够顺利开展，医院需要做好相关的安全准备工作，因此通过安全检查迎检服务能够有效帮助医院开展检查前的准备工作、检查过程中的密切配合及检查后的问题跟进。迎检结束后，提供《中山市中医院安全迎检检查计划》、《中山市中医院安全问题跟进清单》。

7. 重大时期安全保障服务

提供重大节假日安全保障，由安全运维团队提供重保期间线上或现场的值守服务，例如年度“护网“专项行动、国家重大会议（两会）、国庆、春节、五一劳动节等重要时期，配合医院进行相关安全准备与监控工作，工作主要包括如下方面工作：

7.1 安全设备检查

7.1.1 安全设备健康情况实时监控，包含：CPU使用率、内存占用率、接口流量、接口工作状态、硬盘使用情况等设备健康相关的基本参数监控。

7.1.2 安全设备告警事件实时监控，包含：拒绝服务攻击，网络病毒爆发，漏洞远程利用、恶意代码传递等高危事件告警信息。

7.2 安全事件协助处理

当安全设备产生高危事件报警时，积极协助用户相关人员对报警事件进行确定、排查，对于真实存在的事件第一时间进行上报，并做好后期的分析和处理。服务结束后，提交不限于以下报告：《中山市中医院重保值守安全巡检报告》、《中山市中医院重保值守安全注意事项》

8. 应急事件分析与处置服务

8.1 安全响应：对医院上报的安全事件进行及时响应。

8.2 安全分析：针对分析得到的勒索病毒、挖矿病毒、篡改事件、webshell、僵尸网络等安全事件，通过工具和方法对恶意文件、代码进行根除，配合医院快速恢复业务，消除或减轻影响。

8.3 加固建议指导：结合现有安全防御体系，指导医院进行安全加固、提供整改建议、防止再次入侵。

8.4 根据每次事件分析与处置的结果，输出《中山市中医院安全事件分析与处置报告》。

9. 安全事件管理服务

配合医院针对前期的渗透和漏洞扫描过程中发现的问题并整合近期遇到的安全事件，每季度进行时间跟踪和维护，提供安全事件的通知、整改进度跟踪、复核服务。每半年提交1份《中山市中医院安全事件的通知》、《中山市中医院整改进度跟踪》以及《中山市中医院复核报告》等相关标准交付文件。

10. 应急安全服务需求

10.1 由本地专业网络安全服务商提供全方位技术支持应急服务，包括但不局限以下技术支撑服务：当医院系统或者网络出现紧急故障或其他不可抗力因素需要技术支撑时，服务商安排专业的技术工程师对接现场驻场服务人员提供7\*24小时应急支撑服务，由专门负责应急服务经理15分钟内响应技术团队支撑现场驻场服务人员，并30分钟内提供远程技术支撑服务，若故障事件升级可提供1小时内快速上门应急服务，并与现场驻场服务人员联动处理，若机器出现故障需返厂维修，配合院方提供备机服务保障医院系统正常运行。

10.2 网络架构分析:梳理当前数据流向网络架构，绘制并优化网络拓扑，按照等级保护要求初步评估网络架构的安全问题，例如链路防护、区域隔离、节点冗余等。

10.3 资产识别与梳理:通过安全工具、人工访谈、现场收集等方式，对院方资产进行识别梳理，输出完善院方的资产信息管理表；每季度对当前医疗系统进行漏扫服务，梳理所有医疗系统存在的漏洞隐患，并协助院方进行修复加固。

10.4 安全管理体系建设:通过访谈交流、文档分析、日常工作处置与观察，了解院方现有的信息安全管理体系运行情况，包括安全组织部门、应急处置流程、人员岗位设置、职责人工、联系方式等，建设完善的安全管理体系:

10.5 日常巡检工作，输出《中山市中医院日常巡检分析报告》，包括安全设备运行状态记录、安全日志分析、访问日志;分析异常IP攻击源、访问链路等;日常问题处理工作包含:安全预警检测预警与威胁处置服务、漏洞管理总结等。

10.6 协助院内制定网络安全策略，针对网络安全防护以及合规设备进行配置策略优化，根据院内实际使用场景对相关设备进行策略加固和调整；若现场发生网络安全事件时，协助院方进行相关系统和终端进行全盘查杀以及漏洞修复，必要时可提供病毒事件溯源服务；

10.7 如遇启动安全应急服务，交付成果包括但不限于：

《中山市中医院应急事件处理报告》

《中山市中医院信息安全应急预案》

《中山市中医院服务实施计划》

《中山市中医院服务实施方案》

《中山市中医院信息化资产信息表》

《中山市中医院业务系统流程梳理表》

《中山市中医院网络拓扑图》

《中山市中医院网络和安全设备巡检报告》

《中山市中医院驻场安全运维服务日/周报》

《中山市中医院驻场安全运维服务月度总结》

《中山市中医院驻场安全运维服务半年度总结》

《中山市中医院驻场安全运维服务年度总结》

11. 应急演练服务

协助医院建立网络安全应急机制，进行每年1次的安全应急演练，进行安全应急演练，完善监测预警能力、防御能力、响应能力。应急演练结束后，应急演练服务结束后在一周之内交付《中山市中医院应急演练服务方案》、《中山市中医院应急演练场景脚本设计》、《中山市中医院应急演练总结》等报告。

12. 网络安全培训服务

提供每年2次的安全培训服务，为医院的相关人员在不同岗位和知识层次，建立安全进阶培训体系，针对不同岗位的管理人员和技术人员进行安全方面的意识和方法论的培训，提供信息安全知识普及培训及信息安全技能培训，以提高用户管理员的安全知识和技能，进一步提高相关人员的安全意识和安全处理水平，协助医院逐步建立一支综合素质强的安全维护队伍。

12.1 《中山市中医院网络安全意识培训》：通过案例强调安全意识的重要程度，可作为医院全体员工进行安全合规和信息安全标准以及风险管理培训的基础课程。

12.2 《中山市中医院技术管理人员培训》：提供技术管理人员培训，培训信息管理人员掌握必备的基本安全技能，可作为医院信息安全管理人员进行安全管理和信息安全技术加强的培训课程，保证医院信息管理人员更加有效的对信息系统进行管理，能了解市场上大部分安全产品，能够有效的使用现有的安全设备。

12.3 安全讲师在进行安全培训服务前，需出具一份《中山市中医院安全培训计划》、《中山市中医院安全培训教材》，文档中会详细的列出本次培训的课件和培训的计划，以便有针对性的进行本次培训，达到培训的效果。

**三、服务要求**

**1、人员配置及岗位职责**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 岗位 | 数量 | 是否驻场 | 职责 |
| 1 | 项目经理 | 1人 | 非驻场 | 3年以上同类项目经验，具备项目管理能力，负责项目整体规划、实施、沟通及投诉处理 |
| 2 | 安全运维工程师 | 1人 | 完全驻场 | 5\*8小时工作制，负责设备软硬件维护、巡检、文档填写、与后台技术团队实时沟通协调及其他各项现场驻点任务 |
| 3 | 安全运维工程师 | 2 人 | 非驻场 | 负责安全事件分析、处理、巡检及应急响应 |
| 4 | 应急工程师 | 不少于1 人 | 非驻场 | 作为后备力量，协助处理复杂故障 |
| 5 | 云上运营安全服务团队 | 不少于2 人 | 非驻场 | 应对应急或大范围故障 |

**2、人员要求**

2.1 驻场服务人员要求具有计算机相关专业大专及以上学历或同类项目一年以上驻场服务经验。

2.2 服务人员衣着要整洁，佩戴胸卡，使用礼貌用语，待人接物诚恳有耐心。

2.3 严格遵守医院内部各项规章制度，遵守医院信息和网络安全保密要求，尊重个人隐私，保守医院商业秘密。

2.4 驻场服务人员须在医院主管部门进行备案，并签订保密协议。

2.5 驻场服务人员上岗前须到医院信息科接受培训，并通过考核。达不到考核要求或服务过程中不能胜任工作的，服务商需配合更换符合要求的人员。

2.6 因服务商问题需更换人员的，需提前1个月告知采购人，做好人员更换方案，并得到医院同意。

**3、服务时间要求**

3.1 工作日，驻场服务时间为上午8:00-12:00，下午14:30-17：30。

3.2 非工作日，驻场工程师与应急响应团队保持24小时通讯联络通畅且具备远程处理能力。

3.3 应急响应支持：服务商应有完善的应急响应机制，服务期间，如发生重大故障，能够及时组织后备专业技术团队，制定紧急预案，与驻场工程师一起以最快速度进行问题解决，包含但不限于根据采购人的需求和实际情况增派人手、增加驻守时间、增加分巡检频率和人员、非工作时间的应急服务支持、临时性驻场服务等。

**四、考核**

**维保服务考核评分表**

年 月

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **序号** | **分类** | **分项** | **详细描述** | **扣分分值** | **扣分说明** |
| 1 | 安全运维人员管理 | 驻场人员资质 | 服务商需按照合同、需求文件以及响应文件要求，提供符合资质要求的驻场服务人员。如提供人员与要求不符的，扣5分。 |  |  |
| 项目经理资质与工作能力 | 服务商需按照合同、需求文件以及响应文件要求为此项目配备符合要求的项目经理，项目经理应具备良好的沟通协调能力，如发现项目经理与要求不符、常无法联系、不能胜任工作的情况，扣5分。 |  |  |
| 人员管理规范性 | 1、驻场人员轮换需提前报信息科，人员变动必须经过信息科批准。违反规定扣2分。2、驻场人员不得有串岗、脱岗、迟到和早退行为，发现一次扣1分；若因此造成严重后果者，每发现一次扣2分。3、服务人员应加强服务意识，积极做好安全运维工作。如发生运维人员不服从信息科工作安排的，扣2分/次。情节严重的扣8分/次。 |  |  |
| 驻场人员行为规范 | 1、若有疫情，严格配合医院的疫情防控要求，未按信息科传达的要求执行的，扣1分/人次。如有出市出省的，提前跟信息科报备，如发生未报备导致影响后续驻场工作的，扣3分/次。2、遵守信息科的卫生及消防要求，严禁科室内吸烟，如有发现，扣0.5分/次。 |  |  |
| 2 | 运维服务质量 | 运维服务及时性 | 对于医院日常安全问题及风险，发现或处理不及时的（按合同或需求文件的及时性要求），扣1分/次。由于处理不及时而造成严重影响的，扣3分/次。 |  |  |
| 运维服务影响 | 如日常巡查中发现安全问题及隐患应及时向信息科报备并评估影响，盲目处理安全问题导致系统或网络故障的，每次扣0.5分，造成严重影响的扣2分。 |  |  |
| 3 | 安全管理 | 系统安全 | 1、按要求积极配合医院的信息安全审查及整改，无法在规定时间内完成的扣2分/次。不配合整改的，扣5分/次。2、因信息安全等原因，被上级部门通报且不积极配合整改的，每次扣3分。 |  |  |
| 信息安全 | 1、驻场人员如需出入机房的，需严格按照信息科的机房出入管理和安全管理要求，未按要求执行的，扣2分/次。如因违规操作，造成严重影响的，扣10分/次。2、加强系统的数据安全管理。因驻场人员工作失误导致数据丢失的，经核实，每次扣2分。3、加强驻场人员的信息保密教育，如发生利用工作之便，窃取系统数据的，经核实扣40分/次，并移交司法机关处置。 |  |  |
| 4 | 日常巡检管理 | 日常巡检 | 1、项目经理按合同或需求文件的规定对驻场人员负监督责任，并每月至少一次进行现场巡检，检查驻场人员工作情况并填写巡检记录，未执行的扣1分/次。2、由于项目经理督导、巡检不到位，造成驻场人员工作未达标或未及时发现潜在安全隐患的，扣3分/次。 |  |  |
| 5 | 应急备件管理 | 备品备件 | 服务商应按照合同或需求文件的要求，根据医院的实际情况准备充足的应急备件，如发生应急备件不足的，扣2分/次。如因应急备件不足，造成严重影响的，扣4分/次。 |  |  |
| 6 | 文档管理 | 文档规范 | 按照合同或需求文件的要求，按时提交安全运维文档，如日报、周报、月报、巡检记录、整改报告等资料，如有缺失，每次扣0.5分。 |  |  |

说明：

1、此表每季度考核一次，跟随发票作为每期的结算依据，根据评分情况按以下比例扣除相应的服务费作为处罚；

2、考核分为A、B、C、D四级，A≥95分，90分≤B＜95分，85分≤C＜90分，D＜85分；

3、以每季度的服务费为基数，扣罚比例如下：A级不扣罚；B级扣罚当期5%服务费，C级扣罚当期10％服务费，D级扣罚当期20％服务费，连续两个季度考核为D级的，采购人有权单方面无条件终止本服务合同。

采购人考核人员 服务商代表

签名及盖章： 签名及盖章：

 年 月 日

**五、结算方式**

1、每季度结算一次。

2、凭每期合同相应金额的正规发票、月度维保服务质量考核表、月度维护保养工作单，采购人于60个自然日内支付该期服务费用。