附件一

梅州市中医医院网络安全项目需求书

一、项目背景

随着医疗信息化进程加速，医院网络面临多重安全挑战：一是患者隐私数据激增，电子病历、影像资料等核心信息存在泄露风险；二是医疗机构之间共享信息日益增多，网络安全风险随之而来；三是勒索病毒攻击频发，医疗行业网络攻击剧增，业务连续性面临严重威胁。本项目旨在通过专业的网络安全技术团队运维，构建完善的网络安全运维体系，满足《网络安全法》、《数据安全法》、《个人信息保护法》、《国家卫生健康委办公厅关于加强医疗卫生机构信息系统与网络数据安全防护的通知》合规要求，抵御网络攻击和内部渗透风险，切实保障医疗服务质量与患者生命安全，维护医院数字化转型升级的可持续发展。

二、项目目标

本项目旨在通过以下措施，全面提升梅州市中医医院的网络安全水平：

（一）依托云端网络安全运营平台，持续监控、检测、分析并响应网络威胁，结合自动化工具与线上安全专家团队及驻场服务，提升整体网络安全防护水平

（二）建立常态化的网络安全运维机制，确保日常网络安全运维工作的高效、有序进行。

（三）在重要保障期间（如重大节日、网络安全攻防演练等）提供全天候的安全值守，确保医院信息系统不受安全攻击影响。

（四）提升全院职工的网络安全意识，减少因人为因素导致的安全事件。

（五）通过定期的网络安全应急演练，完善应急预案，提高医院应对网络安全突发事件的能力。

（六）确保新系统上线的安全性，对新系统进行全面的入网评测。

（七）加强服务器、网络关键设备、操作系统、中间件、数据库的安全防护，确保医院关键业务系统的稳定运行。

三、项目服务清单

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **服务内容** | **数量** | **备注** |
| 1 | 安全云托管服务 | 1套 | 7\*24小时 |
| 2 | 驻点运维人员服务 | 1人 | 8\*6小时 |
| 3 | 重保期间网络安全监控防守 | 按需 | 含重要会议、节日及网络安全攻防演练期间7\*24小时值守 |
| 4 | 网络安全意识培训 | 按需 | 1年2次以上 |
| 5 | 网络安全应急演练 | 1年1次 |  |
| 6 | 新系统上线安全评估 | 按需 |  |
| 7 | 服务器防病毒软件授权 | 200个 |  |

四、商务要求

（一）资质要求

运维公司需具备CCRC（信息安全服务资质）认证的安全服务资质，包含信息安全风险评估、信息系统安全运维服务资质证书，且证书在有效期内。

（二）相关项目案例要求

1.提供2022年-2025年期间同类型网络安全服务相关业绩证明。

2.提供2022年-2025年期间参加市级或更高级别实战攻防演练证明。

五、技术要求

（一）安全云托管服务

依托云端安全运营平台，提供7\*24小时不间断的威胁检测、研判、处置、溯源分析等服务，并结合线上安全专家团队服务，监测网络环境所面临威胁事件同时，能够及时发现并协同处置闭环网络安全威胁。

1.云端安全运营平台需通过网络安全等级保护三级测评，需提供相关证明。

2.7\*24小时监测与研判

实时监测网络安全状态，对安全告警和威胁进行分析研判，对分析结果提供对应的处置或加固建议（如封锁攻击源、设置安全策略防护等措施），并协助驻点运维人员闭环。

3.云端安全运营平台需具备接入网络威胁检测组件，主机威胁检测组件的接入能力，并具备接入服务商自身品牌之外其他品牌组件的能力。

（二）驻点运维人员服务

提供具备网络安全知识和技能的运维人员8\*6小时驻点服务。

1.人员资质与岗位要求

驻点运维人员需熟悉网络协议、操作系统和数据库安全，掌握防火墙、IDS/IPS、WAF、VPN等安全设备配置与管理，具备网络安全相关认证（如CISP注册信息安全专业人员、CISAW信息安全保障人员认证、NSACE国家信息安全水平考试认证等其一），同时需具备网络安全攻防实战经验（提供参加攻防演练证明）。

2.日常网络安全运维与预警

（1）驻点运维人员需每日对医院网络进行安全监测，包括但不限于入侵检测、漏洞扫描、流量分析等，及时发现并预警潜在的安全风险。

（2）定期（如每日）提交网络安全运维报告，详细记录网络安全状况、已发现的风险点、已采取的措施及建议等。

（3）定期对安全设备的系统配置和策略配置进行完整备份，在设备发生故障后提供配置快速导入等恢复措施，对安全设备的系统版本、特征库、病毒库、威胁情报库和漏洞库等进行更新升级。

3.风险排查与加固

（1）根据安全监测结果，及时对发现的安全漏洞、弱密码、不合规配置等问题进行排查和加固。

（2）定期对医院信息系统进行安全审计，确保系统符合相关安全标准和规范要求。

4.重要系统的数据安全风险评估

（1）基于业务逻辑评估数据泄露风险，重点发现可能导致数据泄露的业务逻辑漏洞，比如“数据接口未授权访问”、“越权访问漏洞”、“越权操作漏洞”。

（2）数据接口未授权访问：评估系统中是否存在未进行身份验证或授权即可访问的数据接口。检查接口的安全性设置，包括身份验证机制、访问控制策略等。

（3）越权访问漏洞：评估系统中是否存在用户能够访问或操作其权限范围之外的数据或功能的漏洞。检查系统的权限分配、身份验证机制等方面，确保用户只能访问其权限范围内的数据。

（4）业务流程逻辑漏洞：评估系统中业务流程是否存在逻辑缺陷，可能导致数据泄露或被篡改。对业务流程进行详细分析，确保每个操作都经过必要的验证。

5.完善网络安全策略

（1）根据医院业务发展和安全需求变化，动态调整和优化网络安全策略，包括但不限于访问控制策略、防火墙规则、安全审计策略等。

（2）定期对网络安全策略进行评审和更新，确保其有效性和适应性。

6.处理网络安全事件

（1）发生网络安全事件时，能够根据事件活动为相关单位及部门依法提供技术支持和协助。

（2）建立网络安全事件快速响应机制，确保在发生安全事件时能够迅速定位、隔离和处置。

（3）对安全事件进行深入分析，找出根本原因，提出改进措施，防止类似事件再次发生。

7.整理网络安全资产与应急预案

（1）对医院网络资产进行全面梳理和登记，建立详细的网络资产清单。

（2）制定和完善各类网络安全应急预案，包括但不限于数据泄露应急预案、网络瘫痪应急预案等，确保在突发事件发生时能够迅速启动应急响应流程。

8.协助进行等保测评

包括但不限于漏洞修复、文档制修订、管理制度制定和发布、配置管理、指导建议等，保障顺利通过等保测评。

9.协助进行医院三甲复审

协助补充和准备复审所需的文档资料，如网络安全管理制度、安全事件报告制度、应急管理制度和应用预案等。

（三）重保期间网络安全监控防守

1.全天候安全监测与值守

（1）在重保期间（如重大会议、节日、网络安全攻防演练等），需提供7\*24小时不间断的安全监测和值守服务。

（2）实时监控网络流量、系统日志等关键信息，及时发现并处理异常行为。

2.排查网络安全攻击并处理

（1）一旦发现网络安全攻击行为，立即启动应急响应流程，对攻击进行快速排查和处置。

（2）采取必要的技术手段（如IP封锁、流量清洗等）阻断攻击行为，确保医院信息系统正常运行。

3.溯源攻击对象

（1）对攻击行为进行深入分析，尝试溯源攻击对象的真实身份和动机。

（2）将溯源结果及时上报给医院相关部门和领导，为后续的处置和防范工作提供依据。

（四）网络安全意识培训

1.培训内容与对象

（1）培训内容应包括网络安全基础知识、常见安全威胁及防范措施、个人信息保护等。

（2）培训对象应包括全院职工，特别是信息部门、临床科室等重点部门的工作人员。

2.培训方式与频率

（1）采用线上与线下相结合的方式开展培训，确保培训内容的广泛覆盖和深入传播。

（2）每年至少开展两次网络安全意识培训，提高全院职工的网络安全意识和防范能力。

3.培训效果评估

能够通过问卷调查、模拟攻击等方式评估培训效果，确保培训内容能够有效提升员工的安全意识。

（五）网络安全应急演练

1.演练内容与目标

（1）演练内容应涵盖医院可能面临的各类网络安全突发事件，如数据泄露、网络瘫痪、恶意软件感染等。

（2）演练目标是通过模拟真实场景，检验应急预案的有效性和可操作性，提高医院应对网络安全突发事件的能力。

2.演练流程与总结

（1）制定详细的演练计划和流程，明确各参与部门的职责和任务。

（2）在演练结束后，及时组织总结会议，对演练过程进行全面评估和分析，找出存在的问题和不足，提出改进措施和建议。

（3）根据演练总结结果，完善应急预案和应急响应流程，确保在真实突发事件发生时能够迅速、有效地应对。

（六）新系统上线安全评估

1.评估内容

（1）对目标系统进行入网安全测评，包括但不限于代码审计、漏洞扫描、渗透测试。

（2）对系统的合规性进行审查，确保符合《网络安全法》《数据安全法》等相关法律法规。

2.评估流程

（1）提交新系统上线申请，并提供相关文档和资料。

（2）驻点运维人员对新系统进行初步审查，确定评估范围和重点。

（3）制定详细的评估计划和方案，明确评估方法和步骤。

（4）实施评估工作，记录评估结果和发现的问题。

（5）提交评估报告，提出改进建议和措施。

3.评估工具与方法

（1）使用专业的安全评估工具进行漏洞扫描和安全测试。

（2）采用渗透测试、代码审查等方法，全面评估系统的安全性。

（七）服务器安全防病毒软件授权

1.授权数量与范围

（1）为医院服务器提供不少于200个防病毒软件授权，确保医院关键业务系统能够得到有效防护。

（2）授权范围应包括病毒查杀、恶意软件防护、漏洞修复等功能。

2.软件选型与部署

（1）选择业界知名、技术成熟、兼容性好的防病毒软件产品。

（2）根据服务器的实际情况，制定合理的软件部署方案，确保软件能够正常运行并发挥最大防护效果。

3.软件维护与升级

（1）定期对软件进行维护和升级，确保其能够及时识别和防御最新的安全威胁。

**以上需求可向上响应。**