**网络安全运维服务用户需求书**

# 项目概述

随着医院的快速发展，信息化的程度越来越高，对信息系统的运维要求也随着提高，为了综合提升医院网络安全运维水平与应急保障能力，需要采购专业的网络安全运维服务，以保障用于承载医院核心业务的数据库系统和安全系统的正常稳定运行，支撑业务系统稳定运营。加强医院信息系统基础平台等基础设施日常稳定运营，当信息系统基础设施出现故障时，能快速响应，排查故障，恢复业务。

# 服务内容

服务内容列表：

|  |  |  |
| --- | --- | --- |
| **序号** | **项目内容** | **服务期** |
| 1 | 网络安全运维服务 | 两年 |

# 具体内容

## 服务团队人员要求

1. 要求不少于四名固定的安全服务工程师现场驻场服务，工作时间5\*8小时。非驻场服务人员不少于20名技术人员。服务人员具备相应能力，取得以下技术认证，如：网络工程师认证、信息安全工程师认证、系统架构设计师认证、网络规划设计师认证、网络空间安全技术应用高级工程师认证、数据库工程师认证等。
2. 现场驻场人员应熟悉网络安全运维系统情况，具备网络拓扑、主机资产、网络边界安全、安全策略等安全监测、研判分析能力，具有不少于三年的同类项目经验。
3. 现场驻场人员需自带工作电脑，需符合需求方网络安全管控要求。电脑网络前端需自行配置终端安全管理设备，该设备不占用电脑计算资源，能实现有线网络访问控制与身份认证（双因子认证）、网络准入功能，有效管理运维电脑的网络权限管控，实时监控该电脑终端的网络访问行为。设备能实现网络不可见，无需配置IP地址。
4. 驻场人员稳定要求：
5. 项目启动后，现场提供技术服务，签订相关保密协议，未经需求方同意，服务商不得随意更换人员。
6. 在现场服务过程中，服务商必须在需求方指定地点办公，并遵守需求方关于第三方人员管理规定要求，场所管理要求等，对因违反规定而被需求方退回的项目团队成员，服务商需在两周内提供工作资历及经验不低于退回人员的替代者。
7. 安全运维管理服务：
8. 服务期内，服务商提供一套智能化安全运维管理平台作为运维服务工具，能对网络安全维护服务过程中的资产、安全、运维数据进行集中采集和统一管理，包含资产管理、安全管理、运维管理和工单管理四个子系统，同时需要实现各子系统之间的数据互通与流程融合。
9. 资产管理工具结合信息化台账、资产探测扫描、核心交换机ARP数据采集、EDR数据采集、线下排查等手段，从资产类别、位置、属性等多个维度理清资产情况、健全资产台账，提升资产快速定位能力和风险资产管理能力。资产管理系统具备资产登记、资产台账管理、资产模型管理、资产稽核管理、资产定位等能力，实现对IT资产的统一管理。
10. 安全管理运维工具能整合汇聚各类安全设备的安全威胁、安全事件和告警日志，构建网络安全问题集中发现、自动派单、快速处置、验证归档的端到端闭环管控体系，防止因安全风险未及时处置引发安全事件，防止因安全事件未及时遏制引发重大事故。同时能实现安全漏洞管理（漏洞类型、漏洞名称、漏洞级别等）、安全事件管理（事件类型、事件名称、事件级别等）、安全规则管理等能力，以资产为核心，整合汇聚各类安全设备的安全威胁、安全事件和告警日志。
11. 运维管理工具能够将网络设备、服务器、数据库、中间件、链路等纳入统一监控，实现业务故障的提前预警和精准定位，提升自动化运维能力。运维管理系统具备性能监控、告警监控、拓扑监控、自动化巡检、业务拨测等能力，能够将网络设备、服务器、数据库、中间件等纳入统一监控，实现业务故障的提前预警和精准定位。
12. 工单管理系统规范运维故障告警和安全风险处置的流程，做到安全和运维问题发现、派单、处置、审核、归档的闭环管控，支持通过企业微信、钉钉等方式实现移动运维。工单管理系统具备工单概览、工单定义、工单创建、工单派发、工单受理、工单处置、工单审核、工单查询等能力。
13. 安全运维管理工具所收集的所有数据信息归需求方所有，只存放在需求方内网服务器中。

## 资产梳理

**服务频次：不小于一年两次**

**服务内容：**资产梳理是全面识别、分类、评估和管理组织内部信息系统资产的过程，信息系统资产梳理范围包括服务器、网络设备、应用系统、终端、电子叫号屏，根据资产的类型、用途、重要性等属性对资产进行分类，建立资产清单。

## 定期安全检查

**服务频次：每季度一次**

**服务内容：**

对现网安全提供全面巡检服务并输出季度巡检报告，巡检的内容包括但不限于：

1. 安全设备硬件信息：安全设备品牌、设备型号、设备放置、设备性能参数、设备内存大小、设备槽位、设备序列号、设备购买年限、设备保修状态、设备备件状况、设备风扇及电源状况、设备标签完善程度。
2. 安全设备软件信息：设备当前系统版本信息、最新系统版本信息、设备持续运行时间、设备CPU利用率、设备内存利用率、设备模块运行状态、设备端口使用数量。
3. 安全设备策略：安全设备连通性、冗余协议运行状态、VLAN信息、设备配置信息分析、多余配置信息分析、配置精简建议、策略变更分析。
4. 安全设备日志分析：对设备性能、告警信息、被攻击和入侵情况（如入侵事件、入侵源、前十位攻击对象等）、安全威胁进行动态评估。

## 架构改动安全风险评估

**服务频次：一年内不限次数**

**服务内容：**

在现网架构变动带来的风险进行识别和评估，提出风险预防和必要的整改措施。风险评估的内容包括但不限于以下内容：

1. 整个系统的网络拓扑结构；
2. 安全设备，包括防火墙、上网行为管理、堡垒机、主机安全等；
3. 网络设备，包括路由器、核心交换机、汇聚交换机以及认证网关等；
4. 涉及到信息系统安全的所有管理制度和记录；
5. 第三方机构系统接入医院信息系统安全评估。

风险评估的方式包括人工访谈、工具检测、登录系统检测、文档分析、渗透测试等。

## 安全事件紧急响应

**服务频次：一年内不限次数**

**服务内容：**

服务方应提供24小时安全事件紧急响应服务，确保在发生任何安全事件时能够迅速、精准地定位风险点、深入分析潜在威胁、全面报告事件详情，并高效执行相应的处置措施，以保障业务系统的持续安全与稳定运行。

1. **事件识别与报告**
2. 服务方应提供有效的安全事件识别机制，包括但不限于：通过日志分析、入侵检测、网络监控等手段发现潜在的安全事件。
3. 服务方应在发现安全事件后的第一时间向医院提交详细的安全事件报告，报告应包含但不限于以下内容：
4. 事件描述：事件的性质、发生时间、地点、影响范围等。
5. 事件分析：初步判断事件的原因、影响及可能存在的风险。
6. 应对措施：建议采取的紧急处理措施及后续处置计划。
7. **应急响应与处置**
8. 服务方须提供专业的安全应急响应团队，具备处理各类安全事件的能力和经验。
9. 在接到安全事件报告后，服务方应立即启动应急响应流程，组织相关人员进行事件分析、处置和恢复工作。
10. 服务方应采取有效措施，防止事件扩大化，降低对医院业务的影响。
11. 在事件处置过程中，服务方应定期向医院报告事件处置进展情况，直至事件完全解决。
12. **事后评估与总结**
13. 事件处置完成后，服务方应对整个事件进行事后评估，总结经验教训，并提出改进建议。
14. 服务方应协助医院完善安全策略、更新安全系统或进行必要的培训，以提高医院的整体安全防护能力。

## 安全配置备份

**服务频次：不小于一个月一次**

**服务内容：**

服务商须将现网所有安全设备和核心网络设备通过设备的命令行界面或网页界面导出配置文件，保存到配置备份服务器进行统一管理；在备份完成后，定期验证备份文件的完整性和可恢复性，确保备份的可靠性和有效性。

## 安全设备日志分析

**服务频次：一年内不限次数**

**服务内容：服务商须在工作日内对关键服务器和安全设备告警日志进行分析处置，生成定制化工作日报和月报，服务内容如下：**

1. 日志收集：定期统一收集各个安全设备的日志和报表进行存档以便分析。
2. 分析日志：根据需求方设备的具体情况，分析关键服务器、安全设备等设备的日志, 采取人工加工具的审计分析方法对日志信息进行综合分析,找到当前的系统及网络设备中存在的隐患和被攻击痕迹。
3. 生成报告：根据以上评估，生成具体的日志分析报告，为需求方量身定制出专业又极具可读性的报告，并会针对报告中的各项问题，为需求方提供修补建议，使发现的问题能尽可能早的得到解决，避免引起更大范围的影响和损失。

## 安全建设配合响应

**服务频次：一年内不限次数**

**服务内容：**

在医院相关或上级部门提出安全建设、安全整改、安全加固等任务时，派遣专业安全技术人员指导配合进行安全相关工作，工作内容包括但不限于以下内容：

1. 医院网络安全通报处置；
2. 公安部门递送的安全检查或安全漏洞通知；
3. 上级部门递送的安全检查或安全漏洞通知；
4. 国家重大事件的安全保障检查；
5. 突发性事件的检查通知或现场检查；
6. 医院相关定级评审配合
7. 重大节假日（五一、十一、春节等）安全保障
8. 医院相关或上级部门组织的攻防演练活动防护

在上述事件发生的时候，服务商需根据医院指定时间安排专业安全工程师提供安全相关服务，配合医院开展安全方面相关工作，具体服务内容由医院和服务商根据具体要求商议决定。

## 安全设备配置适应性调整

**服务频次：一年内不限次数**

**服务内容：**

在相关安全设备配置需要调整时，服务商必须派遣工程师进行配置风险评估、提出调整方案并实施。安全相关设备配置包括但不限于以下情况：

1. 网络出口新增加，评估新网络出口的风险和安全防护措施；
2. 防火墙、路由器等边界类设备的配置变更，详细记录变更内容，包括IP策略、端口策略、放通/禁止策略等；
3. 态势感知、网络行为分析等旁路安全设备配置变更，包括协议监控、端口监控、联动策略等；
4. 杀毒软件、准入控制等终端管理类软件的配置变更，包括扫描策略、准入方式、控制范围等；

服务商在协助医院进行安全设备配置变更时，要充分考虑到配置变更过程中和变更后带来的安全风险，采取一定的预防措施，将风险降低到最小，最小化对医院正常业务开展的带来的影响。

## 系统漏洞扫描与分析

**服务频次：每季度一次**

**服务内容：**

服务商定期利用专业的技术工具对系统进行测试，包括基于网络探测和基于主机检测的漏洞扫描、数据库漏洞扫描等，扫描相关使用的专业工具由服务商提供，医院无需为该工具支持额外费用。

服务商对服务器主机、业务终端设备发现的问题或安全漏洞提出整改建议，并协助医院做好整改工作。包括服务器高危漏洞在不影响业务的情况下协商修复。

## 主机基线检查

**服务频次：一年轮询检查服务器现有及新增IP（不小于800个），每个检查一次**

**服务内容：**

安全基线检查是对服务器系统进行评估和检查，以验证系统是否符合最低安全要求，确定系统中存在的安全风险，并提供相应的改进建议。安全基线检查包括以下几个方面

1. 确定系统是否按照安全要求进行配置。这涉及到检查系统的各种安全设置，如身份鉴别、访问控制、安全审计和入侵防范、恶意代码防范等。
2. 发现系统中存在的漏洞和弱点。通过采用安全检查设备以及人工检查两种方法，从对应目标的安全合规性等方面开展对系统的全量安全基线检查，从而发现其基线的不合规项。
3. 确保系统的基本安全设置和策略是否得到正确实施。这包括检查系统的日志记录和审计功能是否符合最低要求，以及评估系统的访问控制和权限管理是否得到有效的实施。

## ▲安全加固

**服务频次：根据服务器现有及新增IP（不小于800个）漏洞扫描结果和主机基线检查，修复高危漏洞和配置主机基线**

**服务内容：**

安全加固对象是漏洞扫描和基线核查中发现的问题，包括核心网络设备、安全设备、主机操作系统。安全整改加固建议主要关注身份鉴别、访问控制、安全审计、入侵防范、恶意代码防范等问题。

1. 身份鉴别：设置口令复杂度检查策略、设置登录失败处理功能、配置合理登录连接超时时间、采取HTTPS、SSH、VPN等加密措施保证系统和设备远程管理时用户鉴别信息的传输安全
2. 访问控制：对登录的用户分配账户和权限；重命名或删除默认账户，修改默认账户的默认口令；删除或停用多余的、过期的账户；
3. 安全审计：启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。
4. 入侵防范：关闭不需要的系统服务、默认共享和高危端口；设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；
5. 恶意代码防范：统一部署防病毒软件，并及时更新病毒库，设置告警策略，抵挡外部恶意代码攻击。
6. 漏洞修复：当发现高危紧急的漏洞时，提供漏洞分析和加固建议，及时对操作系统进行加固，并协助应用厂商修复应用中间件的漏洞。

## ▲渗透服务

**服务频次：一年两次，不小于24个业务系统**

**服务内容：**

服务商提供评估计算机系统、网络或应用程序安全性的方法，发现系统中的漏洞和安全弱点、评估安全防御的有效性。

1. 发现未知的安全漏洞：渗透测试模拟真实攻击者的行为，通过专业的方法和工具来寻找网络、系统或应用程序中的安全漏洞。这些漏洞可能是未知的、未被修复的，或者是已经被发现但尚未被组织识别出的。
2. 评估安全防御的有效性：渗透测试不仅关注漏洞的发现，还关注安全防御措施的有效性。它可以帮助组织评估其防火墙、入侵检测系统（IDS/IPS）、安全策略等是否能够有效地阻止或检测潜在的安全威胁。

## 应急演练

**服务频次：不小于一年一次**

**服务内容：**

制定信息系统的应急预案，定期举行应急演练，及时发现安全问题，准确分析和查找产生问题的原因。通过应急演练，全面检验应急预案的可行性、有效性和针对性，发现预案中存在的问题和不足，并及时进行修订和完善。提高预案的实用性和可操作性，确保在突发事件发生时能够迅速、有效地启动应急响应。

## 安全培训服务

**服务频次：不小于一年两次**

**服务内容：**

配合医院展开安全建设和运维的工作，定期对医院信息科相关人员提供信息安全技术培训，提升医院信息安全意识和技术知识水平。

培训对象：医院系统管理员、网络管理员、数据库管理员、安全审计员等专业技术人员。

培训内容包括但不限于以下内容：国家等级保护流程与相关内容、医疗行业等级保护建设案例分享、医疗行业网站建设和漏洞防范介绍。

## 安全制度建设

**服务频次：不小于一年一次**

**服务内容：**

结合需求方信息安全的实际情况，为需求方提供信息安全制度建设服务，服务内容包括但不限定于：

1. 网络安全工作总体方针和安全策略；
2. 安全管理组织规范；
3. 外部人员访问管理制度；
4. 移动存储设备的使用管理制度；
5. 安全事件报告和处置制度；
6. 恶意代码防范管理制度。

## 失陷终端处置

**服务频次：不小于一周一次**

**服务内容：**

针对检查中发现的失陷终端进行及时、准确的发现和定位，化解安全危机、处置隐患和问题，将安全事件的发生的风险概率降到最低。在需求方现网终端遇到安全告警的时候，采取适当的措施及时遏制安全事件发生，确保业务正常运作不受到影响，保存证据和追查来源等。例如：勒索病毒、信息窃取、拒绝服务攻击、网络流量异常等。。

针对杀毒软件未能捕捉到潜在威胁，而态势感知系统成功预警的失陷终端，服务商应快速启动终端响应处置流程，确保网络环境的安全与稳定。

## ▲新系统上线安全评估

**服务频次：一年不限次数**

**服务内容：**服务商需提供新系统上线安全评估服务，确保新系统能够安全、稳定地运行，防止潜在的安全风险。

1. 收集信息：收集系统相关信息，如系统架构、设计文档、安全策略等。这些信息将作为评估的基础，帮助评估人员更好地了解系统的特点和安全需求。
2. 漏洞扫描和渗透测试：使用工具对系统进行漏洞扫描，发现系统存在的漏洞。同时，进行渗透测试，模拟攻击者对系统进行攻击，评估系统的抵抗能力。
3. 安全配置检查：检查服务器的安全配置，确保系统已经按照最佳实践和等保基线标准进行配置。
4. 出具安全评估报告：将渗透测试、漏扫、安全配置检查相关检查结果整理成安全评估报告，报告应详细记录评估过程、发现的问题、风险等级以及建议的修复措施等。
5. 漏洞修复验证：使用与发现漏洞时相同的工具和方法，对修复后的系统进行测试，确保漏洞已被成功修复。