广东省监狱中心医院网络安全服务项目需求书（2025年）

**广东省监狱中心医院**

**2025年04月**

**目录**

[第一章 项目背景 7](#_Toc17527)

[第二章 项目现状 7](#_Toc18478)

[2.1 概述 7](#_Toc11812)

[2.2 现状痛点 8](#_Toc29091)

[2.2.1 漏洞修复困难 8](#_Toc11508)

[2.2.2 告警处理不及时 8](#_Toc30661)

[2.2.3 安全设备协同不足 8](#_Toc13935)

[2.2.4 安全管理不够标准规范 8](#_Toc7374)

[2.3 需求分析 9](#_Toc17295)

[2.3.1 网络安全防护能力提升需求 9](#_Toc16099)

[2.3.2 安全管理制度落地需求 9](#_Toc18063)

[2.3.3 安全运营模式构建需求 10](#_Toc10558)

[第三章 服务内容 10](#_Toc8204)

[3.1 资产梳理 10](#_Toc31558)

[3.1.1 服务概述 10](#_Toc5659)

[3.1.2 服务内容 10](#_Toc15808)

[3.1.3 服务方式 11](#_Toc9555)

[3.1.4 服务流程 11](#_Toc15943)

[3.1.5 交付成果 12](#_Toc724)

[3.2 安全检查和运维 12](#_Toc19360)

[3.2.1 服务概述 12](#_Toc8145)

[3.2.2 服务内容 12](#_Toc433)

[3.2.3 服务方式 13](#_Toc16939)

[3.2.4 服务流程 13](#_Toc2589)

[3.2.5 交付成果 13](#_Toc8987)

[3.3 架构安全风险评估 13](#_Toc7891)

[3.3.1 服务概述 13](#_Toc19459)

[3.3.2 服务内容 13](#_Toc17946)

[3.3.3 服务方式 14](#_Toc27348)

[3.3.4 服务流程 14](#_Toc15316)

[3.3.5 交付成果 14](#_Toc25271)

[3.4 安全设备配置适应性调整 14](#_Toc23062)

[3.4.1 服务概述 14](#_Toc17106)

[3.4.2 服务内容 14](#_Toc9031)

[3.4.3 服务方式 15](#_Toc23647)

[3.4.4 服务流程 15](#_Toc25182)

[3.4.5 交付成果 15](#_Toc14972)

[3.5 安全配置备份 15](#_Toc14847)

[3.5.1 服务概述 15](#_Toc4431)

[3.5.2 服务内容 15](#_Toc385)

[3.5.3 服务方式 15](#_Toc10102)

[3.5.4 服务流程 15](#_Toc1829)

[3.5.5 交付成果 16](#_Toc5089)

[3.6 安全事件紧急响应 16](#_Toc18693)

[3.6.1 服务概述 16](#_Toc15233)

[3.6.2 服务内容 16](#_Toc647)

[3.6.3 服务方式 17](#_Toc5493)

[3.6.4 服务流程 17](#_Toc6744)

[3.6.5 交付成果 18](#_Toc12700)

[3.7 失陷终端处置 19](#_Toc7475)

[3.7.1 服务概述 19](#_Toc7349)

[3.7.2 服务内容 19](#_Toc5129)

[3.7.3 服务方式 19](#_Toc22127)

[3.7.4 服务流程 19](#_Toc14405)

[3.7.5 交付成果 19](#_Toc28958)

[3.8 安全设备日志分析 19](#_Toc24376)

[3.8.1 服务概述 20](#_Toc28650)

[3.8.2 服务内容 20](#_Toc32253)

[3.8.3 服务方式 20](#_Toc24508)

[3.8.4 服务流程 20](#_Toc29004)

[3.8.5 交付成果 20](#_Toc18474)

[3.9 配合安全建设 20](#_Toc20757)

[3.9.1 服务概述 20](#_Toc15668)

[3.9.2 服务内容 21](#_Toc5604)

[3.9.3 服务方式 21](#_Toc24476)

[3.9.4 服务流程 21](#_Toc18001)

[3.9.5 交付成果 21](#_Toc18696)

[3.10 系统漏洞扫描与分析 21](#_Toc21775)

[3.10.1 服务概述 22](#_Toc2660)

[3.10.2 服务内容 22](#_Toc23639)

[3.10.3 服务方式 22](#_Toc22039)

[3.10.4 服务流程 22](#_Toc2495)

[3.10.5 交付成果 22](#_Toc32000)

[3.11 主机基线检查 22](#_Toc26049)

[3.11.1 服务概述 23](#_Toc23651)

[3.11.2 服务内容 23](#_Toc15483)

[3.11.3 服务方式 23](#_Toc3112)

[3.11.4 服务流程 23](#_Toc22897)

[3.11.5 交付成果 23](#_Toc22551)

[3.12 安全加固 23](#_Toc5717)

[3.12.1 服务概述 24](#_Toc9209)

[3.12.2 服务内容 24](#_Toc32036)

[3.12.3 服务方式 24](#_Toc6601)

[3.12.4 服务流程 25](#_Toc28)

[3.12.5 风险规避 26](#_Toc14931)

[3.12.6 交付成果 28](#_Toc7754)

[3.13 渗透服务 28](#_Toc27644)

[3.13.1 服务概述 28](#_Toc16850)

[3.13.2 服务内容 28](#_Toc16512)

[3.13.3 服务方式 29](#_Toc19734)

[3.13.4 服务流程 29](#_Toc12777)

[3.13.5 交付成果 30](#_Toc13920)

[3.14 应急演练 30](#_Toc22550)

[3.14.1 服务概述 30](#_Toc19921)

[3.14.2 服务内容 31](#_Toc25471)

[3.14.3 服务方式 31](#_Toc26505)

[3.14.4 服务流程 31](#_Toc20254)

[3.14.5 交付成果 31](#_Toc13427)

[3.15 安全宣贯及培训 31](#_Toc2728)

[3.15.1 服务内容 31](#_Toc9757)

[3.15.2 服务流程 31](#_Toc10101)

[3.15.3 交付成果 32](#_Toc24180)

[3.16 安全制度建设 32](#_Toc9678)

[3.16.1 服务概述 32](#_Toc29295)

[3.16.2 服务内容 32](#_Toc11635)

[3.16.3 服务方式 32](#_Toc16096)

[3.16.4 服务流程 33](#_Toc5022)

[3.16.5 交付成果 33](#_Toc25035)

[3.17 新系统上线安全评估 33](#_Toc12458)

[3.17.1 服务概述 33](#_Toc27659)

[3.17.2 服务内容 33](#_Toc10141)

[3.17.3 服务方式 34](#_Toc15026)

[3.17.4 服务流程 34](#_Toc17218)

[3.17.5 交付成果 34](#_Toc27286)

[3.18 服务器资源整合 34](#_Toc24127)

[3.18.1 服务概述 34](#_Toc68)

[3.18.2 服务方式 34](#_Toc13673)

[3.18.3 服务流程 34](#_Toc19917)

[3.18.4 交付成果 35](#_Toc210)

[3.19 服务内容清单 35](#_Toc18467)

[第四章 服务要求 39](#_Toc4677)

[4.1 服务期限 39](#_Toc20498)

[4.2 人员要求 40](#_Toc3264)

[4.3 服务商要求 41](#_Toc21601)

[4.4 保密要求 41](#_Toc9392)

[4.5 专业工具使用要求 42](#_Toc7582)

[4.6 资产权属 42](#_Toc5871)

[4.7 违约处罚 43](#_Toc22944)

# 项目背景

项目名称：广东省监狱中心医院网络安全服务项目

根据监狱中心医院体制机制改革，进一步发展对外医疗业务，医院信息系统与各类院外平台对接，内部网络与外部多类型网络实现互联互通。当前，网络安全威胁日益复杂，监狱中心医院的信息系统面临着严峻的安全挑战。黑客攻击、数据泄露、恶意软件等安全风险时刻威胁着系统的稳定运行。一旦发生安全事件，不仅会影响医院的正常业务，还可能对监狱安全和社会稳定造成严重影响。

为了保障医院信息系统的安全性、可靠性和合规性，依据国家相关法律法规和行业标准，制定本信息安全运维服务方案。该方案旨在通过全面的安全服务，及时发现并解决安全隐患，提升医院信息系统的安全防护能力，确保其稳定运行，为监狱中心医院的管理和安全提供有力支持。

# 项目现状

## 概述

随着信息技术的飞速发展，监狱中心医院对外开放后必然会加强信息化建设，通过建设互联网医院、协同医疗、远程医疗等新兴医疗模式，构建全新的医疗生态。然而，业务边界不断拓展，医院网络安全面临着前所未有的挑战。互联网+医疗的普及打破了医院原有内外网边界，面向患者和机构的各类服务不断涌现，信息共享和业务协同成为常态，这在极大地方便了患者和医疗机构的同时，也扩大了网络威胁的攻击面。从电子处方、远程监护到远程会诊、在线缴费，众多业务延伸至医院外部，使得医院信息系统暴露在更广阔的网络环境中，遭受网络攻击的风险显著增加。此外，医联体、医共体的建设，进一步将医疗服务下沉至基层，药品配送、远程教学等业务的开展，使医院的网络边界更加模糊，攻击范围进一步扩大。在这样的背景下，医院网络安全空间建设面临着一系列亟待解决的问题。

## 现状痛点

### 漏洞修复困难

监狱中心医院当前漏洞修复困难。漏洞修复难度大，技术要求高，在漏洞修复前，需专业研判对业务系统的影响。因专业性要求高，管理人员无法迅速采取措施进行修复，从而增加了系统遭受攻击的风险，难以保障系统的安全性。

### 告警处理不及时

在告警管理上，缺乏有效监控和处理机制，缺乏实时告警机制，难以及时发现和应对潜在安全威胁，导致安全隐患不断积累。可能会遗漏或不及时处理重要告警，从而错失应对安全威胁的最佳时机。

遇到突发安全事件，缺乏专业技能和专业工具，无法快速处置，难以最大程度地减少危害和影响。

### 安全设备协同不足

监狱中心医院的各类安全设备和系统之间缺乏有效的协同和整合。例如，不同品牌、不同类型的设备各自产生告警信息，但这些信息分散在各个设备中，难以进行统一的分析和管理。这种碎片化的工作模式导致安全人员在处理告警时需要在多个设备间频繁切换，增加了工作复杂度和时间成本，降低了告警管理的效率和协同性。

### 安全管理不够标准规范

监狱中心医院虽然已经具备一定的安全管理制度和流程，但在实际执行过程中，由于缺乏有效的技术支持和工具，导致制度难以落地。例如，在任务分配和跟踪方面，缺乏自动化的任务管理系统，导致安全任务的分配、执行和监督难以有效落实，任务执行进度和完成情况难以实时掌握，影响了安全管理的规范化和标准化。

## 需求分析

为全面落实网络安全主体责任，进一步提升我院关键信息基础设施的安全防护水平，提高网络安全事件处置、协同配合能力，加强网络安全实战能力建设，根据实际工作需求，采购专业的信息安全保障服务，实施攻击面梳理及安全性自查，建立有效的安全事件监测、防护及处置机制，以此确保我院关键信息基础设施的安全稳定运行，尤其是重大活动期间对网络安全进行重点保障。

### 网络安全防护能力提升需求

**协同防护需求**

安全策略的统一管理与联动至关重要。面对繁多的安全设备，医院急需建立一套能够实现协同防护的机制，能够集中配置和管理所有安全设备的策略。各类安全设备应能共享威胁情报，如情报共享、漏洞利用方式等，形成统一的防护战线。

**全方位威胁检测需求**

为了应对复杂多变的网络威胁，医院必须构建全方位的威胁检测体系。除了传统的基于特征码的检测方法外，还应引入先进的行为分析技术。通过分析网络流量中的异常行为模式，如突发的大流量数据传输、频繁的端口扫描等，及时发现潜在的未知威胁，如新型恶意软件、高级持续性威胁（APT）攻击等。

### 安全管理制度落地需求

**制度执行与监督机制**

制定详细的网络安全管理制度执行流程，明确各项制度的适用范围、操作步骤和责任人。例如，在网络安全设备的配置和维护方面，规定由信息科负责具体操作，定期进行设备巡检和策略更新。

建立严格的监督机制，对网络安全管理制度的执行情况进行定期检查和考核。不定期抽查各部门的网络安全工作落实情况，对于未按制度执行的部门和个人进行通报批评，并督促其及时整改，确保制度的严肃性和有效性。

### 安全运营模式构建需求

**安全服务机制需求**

建立完善的安全服务机制，包括安全监测、预警、应急响应和恢复等全流程服务。引入专业的安全服务提供商，定期对医院信息系统进行安全评估和漏洞扫描，及时发现潜在的安全风险，并提供针对性的解决方案。

加强与外部安全机构的合作与交流，建立应急响应联动机制。当发生重大网络安全事件时，能够迅速获得外部专业力量的支持，共同应对和处置安全事件，最大限度降低事件对医院业务的影响。

# 服务内容

## 资产梳理

### 服务概述

全面识别、分类、评估和管理医院信息系统资产，确保资产信息的准确性和完整性，为后续安全管理提供基础数据支持。基于数字化安全运营服务，系统性解决资产底数不清、责任不明、暴露面不可控等问题，构建动态化、责任化、全生命周期管理的资产治理体系。

**核心价值**

**资产可知：**主动测绘+被动探测识别全网存活资产

**责任可溯：**建立「组织-人员-资产-风险」四维关系图谱

**动态可控：**实时监控资产变更，自动更新台账

**暴露面收敛：**识别僵尸资产/高风险外联端口并预警

### 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、电子屏等，根据资产的类型、用途、重要性等属性对资产进行分类，收集资产信息，信息内容包括但不限于：设备品牌、型号、设备位置、设备性能参数、购买年限、保修状态、备件情况等。

### 服务方式

采用「自动化工具+人工验证+流程治理」三位一体工作模式，构建覆盖物理层、逻辑层、业务层的立体化资产发现体系：

1. 多源数据采集、自动化探测、人工验证机制
2. 资产关联建模
3. 数据治理流程、异常数据处理、全生命周期管理
4. 协同工作平台、数字看板功能

### 服务流程

**阶段一：资产探测与验证**

**1、多维度资产发现**

执行网络主动扫描（IP段/CIDR覆盖）

通过流量分析引擎捕获云主机存活特征

调用API同步安全设备资产数据

**2、资产存活状态判定**

存活资产：进入指纹识别流程

未存活资产：标记为「待回收资产」，推送运维团队确认

**阶段二：资产指纹识别**

**1、资产属性提取**

识别设备类型（服务器/网络设备/终端等）

提取操作系统、开放端口、服务版本信息

关联业务系统标签（如CRM/ERP/OA）

**2、资产唯一性标识**

生成资产指纹码

**阶段三：资产数据治理**

**1、安全设备数据清洗**

比对探测数据与安全设备记录差异

修正错误属性（如错误IP归属部门）

补充缺失字段（如设备维保期限）

**2、未知资产标记**

未登记资产分类：

新增资产：标记「待认领」状态

僵尸资产：标记「高风险-待处置」状态

阶段四：资产责任闭环

**3、责任矩阵构建**

通过生成「组织-人员-资产」映射表

输出《资产责任缺失清单》（含未认领资产明细）

**4、责任人协同**

通过OA推送待认领资产清单

责任人确认后自动更新台账

### 交付成果

《资产清单》

《资产分类清单》

《动态资产台账（含IP/责任人/所属系统）》

《僵尸资产清单》

## 安全检查和运维

### 服务概述

配合医院开展安全检查和运维工作，对现网安全进行全面巡检，及时发现并解决安全隐患，保障系统稳定运行。

### 服务内容

配合医院展开安全检查和运维工作，对现网安全提供全面巡检服务，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。

### 服务方式

定期现场巡检与远程监控相结合，使用专业工具进行自动化检测和人工分析。

### 服务流程

1. 制定巡检计划。
2. 执行检查：记录硬件、软件、策略状态。
3. 日志收集与分析：识别潜在威胁。
4. 生成报告并提交医院。

### 交付成果

《安全设备信息表》

《策略分析报告》

《日志分析报告》

## 架构安全风险评估

### 服务概述

对现网架构进行识别和风险评估，提出风险预防和整改措施，确保系统架构的安全性和可靠性。

### 服务内容

对现网架构进行识别和风险评估，提出风险预防和整改措施。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。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、waf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

### 服务方式

采用专业评估工具与专家团队相结合的方式进行风险评估。

### 服务流程

1. 收集系统相关资料，包括网络拓扑图、设备配置文档、管理制度等；
2. 实施风险评估，运用多种评估方法分析系统架构的安全性；
3. 对评估结果进行汇总和分析，确定风险等级；
4. 提出风险整改建议，制定整改方案。

### 交付成果

《网络拓扑图》

《风险评估报告》

《架构整改建议书》

## 安全设备配置适应性调整

### 服务概述

在相关安全设备配置需要调整时，派遣工程师进行配置风险评估、提出调整方案并实施，确保配置变更的安全性和有效性。

### 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。

### 服务方式

现场工程师操作与远程支持相结合，严格遵循变更管理流程。

### 服务流程

1. 受理配置变更申请，进行初步评估；
2. 制定配置变更方案，包括风险评估和预防措施；
3. 审批通过后，实施配置变更；
4. 对变更后的系统进行测试和验证，确保业务正常运行；
5. 记录变更过程和结果，更新相关文档。

### 交付成果

《安全设备配置调整登记表》

## 安全配置备份

### 服务概述

将现网所有安全设备和核心网络设备的配置文件导出并保存到备份服务器进行统一管理，定期验证备份文件的完整性和可恢复性。

### 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。

### 服务方式

自动化备份工具与人工验证相结合。

### 服务流程

1. 制定备份计划，明确备份周期和备份方式；
2. 实施配置备份，将配置文件上传至备份服务器；
3. 定期对备份文件进行验证，记录验证结果；
4. 根据验证结果，对备份策略进行优化和调整。

### 交付成果

《安全设备备份文件》

《网络设备备份文件》

## 安全事件紧急响应

### 服务概述

当主机或网络正遭到攻击或发现入侵成功的痕迹，而又无法当时解决和追查来源时。以最快的速度赶到现场，协助解决问题，查找后门，保存证据和追查来源。服务商有一整套完整的应急响应机制，具备处理紧急事务经验。

### 服务内容

服务商应提供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

（1）服务商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。

（2）服务商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：

事件描述：事件的性质、发生时间、地点、影响范围等。

事件分析：初步判断事件的原因、影响及可能存在的风险。

应对措施：建议采取的紧急处理措施及后续处置计划。

2、应急响应与处置

（1）服务商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。

（2）在接到安全事件报告后，服务商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。

（3）服务商应采取有效措施，防止事件扩大化，降低对医院业务的影响。

（4）在事件处置过程中，服务商应定期向医院报告事件处置进展情况，直至事件完全解决。

3、事后评估与总结

（1）事件处置完成后，服务商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。

（2）服务商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。

### 服务方式

当网络发生突发安全事件后，启动应急响应服务，服务商提供安全专家紧急响应服务，包括远程应急响应和现场应急响应，安全专家将尽快的赶到现场，恢复网络的正常工作，并协助检查入侵来源，提供事故分析报告和安全建议及服务，为用户提供及时、全面的安全问题解决方案。

### 服务流程

事件响应必须遵循的流程分为以下步骤：

**第一步：记录日志**

当发生安全事件时，首先需要客户对环境现场进行记录，对事件的影响进行详细的描述。安全事件日志对于安全事件的识别、处理和调查非常重要，安全事件可能在其刚刚发生时就暴露，也可能在发生的过程中或发生以后才被发现，因此所有安全事件都应该有一份书面的经过调查证明足够客观的日志，而且应该把日志妥善保存以免被修改。由于在线日志很容易被修改和删除，所以手工记录是必要的。

应该记录的信息有：

* 相关事件发生（或者发现）的日期和时间；
* 值班人员或事件协调小组通知的人员和与事件相关的人员；
* 受影响的系统名称（或IP地址），受影响的程序和网络；
* 事件发生时对系统、程序或者网络的影响和现象。

记录完安全事件后，应该把安全事件上报给直接主管，同时提交事件响应申请给服务商的事件响应小组，此时开始进入事件响应过程。

**第二步：分析确认**

接到事件响应申请后，服务商事件响应小组会根据情况进行远程和现场的响应。事件响应小组会根据客户记录的安全事件描述，结合前期进行过的漏洞检测与分析结果、实时监控与审计结果等已有客户系统和网络状况，进行分析和判断，如果是典型的已知安全事件，部分案例可以仅通过远程方式就能解决。

如果通过远程指导客户无法进行自行解决，事件响应小组成员会赶往现场进行实际问题解决。这时，事件响应小组可以实地看到安全事件的形态和影响，也可以通过工具直接进行测试，结合当前扫描、探测、实时监控和审计的结果进行分析，可以更容易定位出问题所在。

**第三步：事件处理**

事件响应小组最主要的任务就是维持或恢复组织的运作。因此，一旦发生意外事件，如何防止攻击或损害事件的扩大是其主要的目标，相关人员在现场或者远程依照不同事件类型进行事件处理。

在事件处理过程中有一些重要决策要做：

1. 是否要关闭或重启系统？
2. 是否要中断系统的网络连接？
3. 是否要关闭一些特定的服务，如Telnet、FTP等？
4. 是否要调整网络设备或安全产品的策略配置？
5. 是否需要国家网络安全机构协助处理？

某些处理办法可能会暂时影响到组织的业务运转，但都是为了避免安全事件事态的扩大，这也是在第一步中要把安全事件上报给上级领导的原因，事件处理过程中可能会带来一定的风险，需要和组织主管进行协商，确定风险可以接受才能真正实施事件处理方法。事件处理过程中，要对每个处理的动作进行详细的记录。

**第四步：系统恢复，防御**

在抑制住了攻击或损害事件的扩大以后，就要对系统进行恢复，使客户业务重新运转。如果系统在故障点有备份，被攻击的系统就用备份来恢复；应该从系统中彻底删除诸如受到感染的文件；如果调整了网络或安全产品，要把所有安全上的变更作记录。

**第五步：事后分析与跟踪**

在安全事件处理完毕，所有系统恢复正常以后，应该针对事件进行分析。集中所有相关人员来讨论所发生的事件以及得到的经验教训，并对现有的一些流程进行重新评审，对不适宜的环节进行修改。

在安全事件处理后的一段事件内，应该密切关注系统恢复以后的安全状况，特别是曾经出问题的地方。

### 交付成果

《安全事件处置报告》

## 失陷终端处置

### 服务概述

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。

### 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。在网络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。

### 服务方式

结合态势感知系统和人工排查，快速响应处置。

### 服务流程

1. 发现失陷终端：通过态势感知系统或其他检测手段发现失陷终端；
2. 定位与分析：确定失陷终端的位置和感染情况，分析威胁来源；
3. 遏制与处置：采取隔离、杀毒、修复等措施，遏制安全事件扩散；
4. 证据保存与追查：保存相关日志和数据，协助追查攻击来源。

### 交付成果

《失陷终端处置报告》

## 安全设备日志分析

### 服务概述

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，通过分析找到当前系统及网络设备中存在的隐患和被攻击痕迹。

### 服务内容

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。

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。

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。

### 服务方式

自动化日志收集工具与专业分析师人工分析相结合。

### 服务流程

1. 制定日志收集计划，明确收集周期和范围；
2. 实施日志收集，将日志上传至分析平台；
3. 对日志进行分析，识别潜在安全隐患和攻击痕迹；
4. 生成日志分析报告，提出整改建议。

### 交付成果

《安全设备日志分析报告》

## 配合安全建设

### 服务概述

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建设相关工作。

### 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，服务商派遣专业安全技术人员指导配合进行安全建设相关工作，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，重保期间，按预案组织人员实施，增派人手及延长驻场服务时间，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。

### 服务方式

根据客户的需要，服务商将提供在重大节假日活动期间提供增强的安全运维服务，至少派一名专业安全专家进行现场守。在值守期间，服务商将安排专业工程师，协助客户的运维保障人员对各重要信息系统进行不间断监控，定时对监控内容总结。

### 服务流程

1. 接收医院安全建设任务通知，明确任务要求和时间节点；
2. 制定服务计划，安排专业人员；
3. 实施服务，定期向医院汇报进展；
4. 任务完成后，提交工作总结报告。

### 交付成果

《安全建设情况报告》

《安全检查报告》

## 系统漏洞扫描与分析

### 服务概述

漏洞管理在整个信息安全运维服务中起着至关重要的作用，它全面整合了漏洞管理的各个环节，从漏洞的发现、统计分析到处置修复以及相关流程的审批与闭环管理，涵盖了主机、WEB、弱口令及基线问题等多方面内容。通过各子模块的协同运作，确保系统漏洞得到及时有效的处理，提升整体系统的安全性与稳定性，为企业的安全运营提供坚实保障。

### 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、业务终端设备发现安全漏洞或上级部门发现的安全漏洞提出整改建议，整改方案经医院审核同意后进行漏洞修复。对无法修复的漏洞或修复漏洞会影响业务系统运行的，应提出替代防护措施和方案，并说明情况。

### 服务方式

自动化漏洞扫描工具与人工验证相结合，同时从漏洞扫描、漏洞列表、漏洞修复、漏洞工单等多方面建议漏洞管理制度，实现漏洞成发现到修复的全流程闭环管理。

### 服务流程

1. 制定漏洞扫描计划，明确扫描范围和周期，并引入漏洞管理制度；
2. 实施漏洞扫描，记录扫描结果；
3. 对扫描结果进行分析，确定漏洞风险等级，针对高中危漏洞建立处置工单；
4. 提出整改建议，经医院审核同意后进行漏洞修复。

### 交付成果

《系统漏洞扫描分析与整改情况报告》

## 主机基线检查

### 服务概述

对服务器系统进行评估和检查，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。

### 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、数据库等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。

### 服务方式

安全检查设备检测与人工检查相结合。

### 服务流程

1. 制定基线检查计划，明确检查标准和范围；
2. 实施基线检查，记录检查结果；
3. 对检查结果进行分析，确定不合规项和安全风险；
4. 提出改进建议，经医院审核同意后进行整改。

### 交付成果

《主机基线检查及整改情况报告》

## 安全加固

### 服务概述

安全加固是基于安全评估发现的系统脆弱性，对服务器、终端、数据库及应用中间件等存在的安全漏洞，通过打补丁、强化帐号安全、修改安全配置、优化访问控制策略、增加安全机制等方法，提高系统健壮性和安全性。

本次安全加固的范围主要是客户系统中的主机系统、网络设备以及相关的数据库系统，包括服务器、数据库、网络设备和安全设备。

### 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。

### 服务方式

安全加固服务主要以人工的方式实现，主要有：

基于网络层的加固：主要包括传输链路安全加固和网络拓扑结构的合理性检查。

服务器加固：主要包括对Windows服务器和Unix服务器的评估加固，其中还包括对服务器操作系统层面的评估和数据库层面的评估加固。

网络设备加固：主要包括对路由器，交换机的评估加固。

安全防护系统加固：主要包括防火墙系统、入侵检测系统、防病毒系统等的加固

应用系统开发优化：主要包括应用系统的开发优化、应用服务加固及数据系统加固。

其他需要安全加固的系统等。

### 服务流程

安全加固流程如下图所示：



**图：安全加固流程图**

### 风险规避

表：网络层加固过程中风险控制

| **项目** | **可能的影响和方式** | **等级** | **控制方式（措施）** | **备注** |
| --- | --- | --- | --- | --- |
| 基础设施加固 | 误操作引起设备崩溃或数据丢失、损坏 | 高 | 制定备份和恢复策略  规范审计流程；  严格选择审计人员；  用户进行全程监控；  制定可能的恢复计划； |  |
| 网络/安全设备资源占用 | 中 | 避开业务高峰；  控制扫描策略（线程数量、强度） |  |

表：操作系统层加固过程中风险控制

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **项目** | **可能的影响和方式** | **等级** | **控制方式（措施）** | **备注** |
| 操作系统平台加固 | 系统信息泄漏 | 高 | 合同、协议、规章、制度、法律、法规 |  |
| 误操作引起系统崩溃或数据丢失、损坏 | 高 | 规范加固流程；  严格选择操作人员；  用户进行全程监控；  制定可行的恢复计划； |  |

表：安全防护系统加固过程中风险控制

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **项目** | **可能的影响和方式** | **等级** | **控制方式（措施）** | **备注** |
| 防火墙 | 增加应用响应时间  不当的策略导致网络不可用 | 高 | 部署时避开业务高峰  准备备用设备 |  |
| 入侵检测系统 | 产生的网络流量 | 低 | 制定合适的策略 |  |
| 防病毒系统 | 安装时占用系统资源 | 低 | 部署时避开业务高峰时间 |  |

表：数据库加固过程中风险控制

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **项目** | **可能的影响和方式** | **等级** | **控制方式（措施）** | **备注** |
| 数据库加固 | 产生非法数据，致使系统不能正常工作 | 中 | 和DBA、SA、NA协同工作  做好系统备份和恢复措施 |  |
| 异常输入（畸形数据、极限测试）导致系统崩溃 | 高 | 和DBA、SA、NA协同工作  做好系统备份和恢复措施 |  |

表：应用服务加固过程中风险控制

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **项目** | **可能的影响和方式** | **等级** | **控制方式（措施）** | **备注** |
| 应用服务系统 | 误操作引起系统崩溃或服务不可用 | 高 | 规范加固流程；  严格选择操作人员；  用户进行全程监控；  制定可能的恢复计划； |  |
| 部分业务暂时中断 | 中 | 尽量避开用户正常业务时间或在非业务高峰期操作操作 |  |

### 交付成果

《安全加固报告》

## 渗透服务

### 服务概述

渗透服务主要依据已经发现的安全漏洞，模拟黑客的攻击方法对系统和网络进行非破坏性质的攻击性测试，更加需求对客户的指定系统进行全面的渗透测试，从而从深层次发现客户应用系统存在的安全问题。

### 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。

3、将模拟攻击的过程和技术细节生成报告，并根据渗透测试所提及的问题和修复建议对安全漏洞进行修复。

4、在完成渗透测试并发现安全漏洞后，服务商需要积极配合客户进行整改工作。首先，与客户的安全部门和技术团队进行详细沟通，确保他们充分理解测试报告中的问题和建议。然后，协助客户制定整改计划，明确整改的时间表和责任人。在整改过程中，提供必要的技术支持和指导，帮助客户解决遇到的技术难题。定期跟进整改进度，确保整改措施得到有效执行。最后，对整改结果进行验证，确保漏洞得到有效修复，安全防御能力得到提升。

5、对于测试中发现的每一个漏洞，服务商应在报告中详细列出整改方案，包括具体的修复步骤、所需的技术资源和时间估算等。当遇到无法直接整改的漏洞时，服务商应提出替代的修复措施，如通过调整系统配置、加强访问控制、部署临时补丁等方式来降低安全风险。同时，向客户提供详细的解释和建议，帮助他们理解为什么无法直接整改以及替代措施的有效性和局限性，以便客户能够做出明智的决策，确保系统的安全性。

### 服务方式

渗透测试可以分为黑盒和白盒渗透。黑盒渗透是客户只告诉被渗透目标的域名（或IP），然后由渗透测试方去进行安全渗透测试，白盒渗透是客户提供被渗透目标的域名、IP、系统版本、数据库版本、测试帐号等一系列信息，然后由渗透测试方去进行安全渗透测试。

渗透测试也可以分为外部渗透和内部渗透。外部渗透是渗透测试方在互联网上模拟入侵者对客户指定系统进行安全渗透测试，内部渗透是渗透测试方在中客户内部网模拟入侵者和内部人员进行渗透测试。

### 服务流程

渗透测试流程如下图所示：



**图：渗透测试流程图**

### 交付成果

《渗透测试报告》

## 应急演练

### 服务概述

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，分析原因，检验应急预案的可行性、有效性和针对性，提高预案的实用性和可操作性。

### 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。

### 服务方式

桌面推演与实际演练相结合，邀请医院相关人员参与。

### 服务流程

1. 制定演练计划，明确演练目标、时间、地点和参与人员；
2. 实施演练，模拟安全事件发生和处置过程；
3. 对演练过程进行记录和评估，收集参演人员反馈；
4. 根据评估结果，修订和完善应急预案。

### 交付成果

《医疗信息系统的应急预案》

《应急演练报告》

## 安全宣贯及培训

### 服务内容

以多形式开展网络安全知识宣传，并贯彻落实。在国家网络安全宣传周开展内容丰富、形式多样的主题活动。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。

### 服务流程

根据服务商信息安全培训体系的设计思想，培训课程分为三类：

（一）安全意识培训：面向客户的一般工作人员、非技术人员以及所有信息系统的用户，目的是提高整个组织普遍的安全意识和人员安全防护能力，使组织员工充分了解既定的安全策略，并能够切实执行。

（二）安全技术培训：面向客户的网络和系统管理员、安全专职人员、技术开发人员等，目的是让其掌握基本的安全攻防技术，提升其安全技术操作水平，培养解决安全问题和杜绝安全隐患的技能。

（三）安全管理培训：面向客户的管理职能和信息系统、信息安全管理人员，目的是提升客户整体的信息安全管理水平和能力，帮助客户有效建立信息安全管理体系。

除此之外，还可以根据用户的特殊需求，制定符合客户自身特点的培训方案，定制培训内容，编写培训计划。

### 交付成果

《培训报告》

## 安全制度建设

### 服务概述

结合院方信息安全的实际情况，为院方提供信息安全制度建设服务，完善医院信息安全管理体系。

### 服务内容

结合院方信息安全的实际情况，为院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。

### 服务方式

调研访谈、参考行业标准和最佳实践，结合医院实际修订制度。

### 服务流程

1. 收集医院现有安全制度和相关资料；
2. 分析医院信息安全管理现状，识别制度缺失和不足；
3. 制定信息安全制度框架和具体内容；
4. 组织医院相关人员对制度进行评审和修订；
5. 发布实施信息安全制度，并提供培训和宣贯。

### 交付成果

《网络安全制度建设总结报告》

## 新系统上线安全评估

### 服务概述

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。

### 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。

### 服务方式

专业评估工具与人工评估相结合，严格遵循评估流程。

### 服务流程

1. 制定评估计划，明确评估范围和标准；
2. 实施评估，包括信息收集、漏洞扫描、渗透测试、安全配置检查等；
3. 分析评估结果，生成安全评估报告；
4. 跟踪漏洞修复情况，进行修复验证。

### 交付成果

《新系统上线安全评估报告》

## 服务器资源整合

### 服务概述

服务器资源整合服务主要针对监狱中心医院的服务器使用率进行资源整合，包括但不限于网站、终端管理、防病毒系统、FTP服务、人事管理系统、监管系统、财务管理等业务系统服务器资源整合。服务商将根据用户的要求，负责完成资产梳理、思路梳理、方案出具，提前做好系统和数据备份，配置运行环境，配合厂家实施整合工作，确保各系统能够平稳、高效地整合到新的环境，保障业务的连续性和数据的安全性。

### 服务方式

现场服务：驻点技术人员进行资产梳理、环境评估、方案设计等工作，确保服务的准确性和针对性。及时响应并解决医院在整合过程中遇到的问题，提高服务效率。

厂家协作：对于涉及具体IT资源整合工作，与相应厂家紧密协作。负责具体的技术实施，确保整合工作的专业性和高质量完成。

### 服务流程

前期调研与准备：开展需求调研和资产梳理工作，形成详细的调研报告和资产清单。进行环境评估，制定初步的整合思路和计划。

方案设计与审核：根据调研结果，设计详细的整合方案，包括技术方案、实施计划、风险评估与应对措施等。

整合实施：按照整合方案，搭建目标环境，进行整合、系统配置与部署。在实施过程中，严格遵守操作规范，进行详细的操作记录和日志记录，确保整合过程的可追溯性。

测试与验证：完成整合后，进行全面的测试工作，包括功能测试、性能测试、安全测试等，确保目标系统的稳定性和可靠性。

### 交付成果

《服务器资源整合报告》

## 服务内容清单

表：服务内容清单

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **序号** | **任务名称** | **实施时间** | **服务频次** | **任务内容描述** |
| 1 | 资产梳理 | 项目启动后的第1个月内完成 | 一年2次 | 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、电子屏等，根据资产的类型、用途、重要性等属性对资产进行分类，收集资产信息，信息内容包括但不限于：设备品牌、型号、设备位置、设备性能参数、购买年限、保修状态、备件情况等。 |
| 2 | 安全检查和运维 | 项目启动后的第1个月内完成，之后每季度首月的下旬 | 每季度一次 | 配合医院展开安全检查和运维工作，对现网安全提供全面巡检服务，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。 |
| 3 | 架构安全风险评估 | 项目启动后的第2个月，隔离6个月 | 一年不少于两次 | 对现网架构进行识别和风险评估，提出风险预防和整改措施。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。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、waf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 |
| 4 | 安全设备配置适应性调整 | 按需及时响应，在配置变更需求提出后的3个工作日内 | 不限次数 | 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。 |
| 5 | 安全配置备份 | 每月的前3个工作日 | 每月一次 | 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，并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。 |
| 6 | 安全事件紧急响应 | 发生安全事件立即响应 | 不限次数 | 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  （1）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。  （2）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：  a. 事件描述：事件的性质、发生时间、地点、影响范围等。  b. 事件分析：初步判断事件的原因、影响及可能存在的风险。  c. 应对措施：建议采取的紧急处理措施及后续处置计划。  2、应急响应与处置  （1）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。  （2）在接到安全事件报告后，服务商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。  （3）采取有效措施，防止事件扩大化，降低对医院业务的影响。  （4）在事件处置过程中，服务商应定期向医院报告事件处置进展情况，直至事件完全解决。  3、事后评估与总结  （1）事件处置完成后，服务商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。  （2）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。 |
| 7 | 失陷终端处置 | 发生失陷事件立即响应 | 不限次数 | 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。 |
| 8 | 安全设备日志分析 | 项目启动后的第3个月，之后每个季度第2月的中旬 | 一季度不少一次 | 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。 |
| 9 | 配合安全建设 | 按需服务 | 不限次数 | 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，包括医院网络安全通报处置、公安部门递送的安全检查或安全漏洞通知、上级部门递送的安全检查或安全漏洞通知、国家重大事件的安全保障检查、突发性事件的检查通知或现场检查、医院相关定级评审配合、重大节假日安全保障、医院相关或上级部门组织的攻防演练活动防护等，在重保期间，按预案组织人员实施，增派人手及延长驻场服务时间，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。 |
| 10 | 系统漏洞扫描与分析 | 项目启动后的第2个月，每季度首月的上旬 | 每季度一次 | 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，发现服务器主机、业务终端设备等存在的问题或安全漏洞，并提出整改建议，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。 |
| 11 | 主机基线检查 | 项目启动后的第3个月，每个季度第二个月的下旬 | 每季度一次 | 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、数据库等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。 |
| 12 | 安全加固 | 项目启动后的第3个月，根据漏洞扫描和主机基线检查结果，修复高危漏洞 | 根据漏洞扫描和主机基线检查结果，修复高危漏洞 | 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。 |
| 13 | 渗透服务 | 项目启动后的第4个月，间隔6个月 | 每半年一次，每次不小于12个业务系统 | 通过模拟黑客的攻击方法对系统和网络进行非破坏性质的攻击性测试，更加需求对客户的指定系统进行全面的渗透测试，从而从深层次发现客户应用系统存在的安全问题，发现未知的安全漏洞，评估安全防御的有效性，并将模拟攻击的过程和技术细节生成报告，根据渗透测试所提及的问题和修复建议对安全漏洞进行修复。 |
| 14 | 应急演练 | 11月前完成 | 不少于2个预案演练 | 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。 |
| 15 | 安全宣贯及培训 | 12月前完成 | 一年两次 | 以多形式开展网络安全知识宣传，并贯彻落实，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，培训对象包括医院系统管理员、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等。 |
| 16 | 安全制度建设 | 项目启动后的第5个月内完成 | 不少于一次 | 结合院方信息安全的实际情况，为院方提供信息安全制度建设服务，服务内容包括但不限于网络安全工作总体方针和安全策略、安全管理组织规范、外部人员访问管理制度、移动存储设备的使用管理制度、安全事件报告和处置制度、恶意代码防范管理制度等。 |
| 17 | 新系统上线安全评估 | 按需服务 | 不限次数 | 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。 |
| 18 | 服务器资源整合 | 项目启动后的第3个月 | 不限次数 | 服务器资源整合服务主要针对监狱中心医院的服务器使用率进行资源整合，包括但不限于网站、终端管理、防病毒系统、FTP服务、人事管理系统、监管系统、财务管理等业务系统服务器资源整合。服务商将根据用户的要求，负责完成资产梳理、思路梳理、方案出具，提前做好系统和数据备份，配置运行环境，配合厂家实施整合工作，确保各系统能够平稳、高效地整合到新的环境，保障业务的连续性和数据的安全性。 |

# 服务要求

## 服务期限

本项目服务期限为1年。

## 人员要求

1．服务商需派驻1名人员（至少拥有3年以上网络安全项目维护经验，提供无犯罪证明）于全年度工作日、法定节假日以及重大活动期间8：30-17：30驻场，提供现场渗透测试、漏洞扫描、基线检查、例行检查、年度检查、安全策略优化、安全培训、应急演练、攻防演练等服务，以及远程值守、远程监控等服务。在相关事件处置时，按院方要求增派人手及延长驻场服务时间。非驻场时间，接院方通知处置相关事件时，服务商必须在2小时内到达现场处置。

## 服务商要求

1．项目服务过程中，所需专业工具由服务商免费提供。

2．服务使用的工具需满足可控性原则，服务时提前3个工作日通知院方，服务时如发现对院方系统产生影响的应立即停止服务并及时通知和协助院方完成系统修复。

3．服务商在合同签订之后10个工作日内以书面形式提供该项目每个阶段的工作人员清单、项目服务方案和项目总体实施计划。项目服务方案与提交的服务报告必须满足采购文件相关要求。

4．项目实施过程中需要院方组织人员进行配合的内容，需要提前3个工作日与院方负责人进行沟通，对院方的项目服务需求需要在8小时内现场响应。

5．经上述标准化服务发现的风险，服务商有义务协助院方进行风险处置，并在处置后对风险降低程度进行评估，涉及院方原始硬件或老旧业务系统迭代才能解决的，应在院方解决前采用其他方式进行必要的加固。

6．安全事件处置兜底：A、来源无论是自发或经其它部门通报，发生网络安全事件Ⅲ级以上时（含Ⅲ级），服务商对院方名下所有网络信息系统，服务商均无条件响应，在院方调动处置资源前予以先期介入，阻止事态扩大，降低损失。B、发生网络安全事件Ⅲ级以下时，服务商应提供直接处置建议及督导服务，必要时协助院方上机开展处置工作。

## 保密要求

1．服务商应签订保密协议，对其因身份、职务、职业或技术关系而知悉的院方商业秘密和党政机关保密信息应严格保守，保证不被披露或使用，包括意外或过失。

2．服务商不得以竞争为目的、或出于私利、或为第三人谋利而擅自保存、披露、使用院方商业秘密和党政机关保密信息；不得直接或间接地向无关人员泄露院方的商业秘密和党政机关保密信息；不得向不承担保密义务的任何第三人披露院方的商业秘密和党政机关保密信息。服务商在从事政府项目时，不得擅自记录、复制、拍摄、摘抄、收藏在工作中涉及的保密信息，严禁将涉及政府项目的任何资料、数据透露或以其他方式提供给项目以外的其他方或服务商内部与该项目无关的任何人员。

3．服务商对于工作期间知悉院方的商业秘密和党政机关保密信息（包括业务信息在内）或工作过程中接触到的政府机关文件（包括内部发文、各类通知及会议记录等）的内容，同样承担保密责任，严禁将政府机关内部会议、谈话内容泄露给无关人员；不得翻阅与工作无关的文件和资料。

4．严禁泄露在工作中接触到的政府机关科技研究、发明、装备器材及其技术资料和政府工作信息。

5．须保证对本项目实施中所获得任何资料和信息严格保密，并与院方签订保密责任书。

6．服务期满后，服务商对部署在院方地点的设备所有存储介质（含内置、外接）进行数据清除（抹零）处理，经院方或第三方检测机构确认后方可随原设备撤出，否则应将存储介质留存于院方处，待保密期满后取回。

## 专业工具使用要求

为确保服务的合法性和合规性，保障服务的质量和稳定性，避免因使用盗版或未经授权的软件而导致的安全风险和服务中断。服务商承诺在提供信息安全服务的过程中，所有使用的工具都必须是正版软件，并且服务商需要明确承诺这些工具不涉及任何版权纠纷或知识产权侵权问题。

## 资产权属

1．本采购项目不会引起任何已申请、登记的知识产权所有权的转移。服务商需承诺，本采购项目所涉服务成果的知识产权归属按下列方式处理：院方基于本采购项目约定委托服务商定制开发的产品、程序、服务，以及定制的方案、规划、规范性文件等的知识产权归院方、服务商共同所有，服务商应按院方书面要求交付该共有部分的成果；服务商在共有部分的基础上进行二次研究的及对二次研究形成的产品、程序等财产进行处置的，需经院方书面同意，二次研究所形成的产品、程序、服务，以及方案、规划、规范性文件等的知识产权归服务商所有，共有部分仍归院方、服务商共同所有。

2．服务商承诺向院方提供的服务成果不存在任何侵犯第三方专利权、商标权、著作权等合法权益。如因服务商提供的服务成果侵犯任何第三方的合法权益，导致该第三方追究院方责任的，服务商应负责解决并赔偿因此给院方造成的全部损失。

3．在整个服务过程中产出的服务成果，在服务期结束前应将服务成果以纸质和电子版格式全部移交给院方，包括但不限于资产清单、安全设备配置文件、漏洞扫描结果、安全日志、应急响应记录等，要确保其完整性和可用性。在移交院方时，数据的格式要规范、内容要清晰，便于院方后续的使用和管理。服务成果移交清单作为项目验收的重要文档资料。

4．工具数据清除。对所有专业化工具使用过程中产生的日志和数据全面清除后方可撤场。

## 违约处罚

1．因服务商未严格履行需求文件及合同的约定导致出现网络安全事故，如出现一般网络安全事件网络事件，每次扣合同款项的1%；出现较大网络事件，每次扣合同款项3%，出现特别重大、重大事件网络安全事件，每次扣合同款项5%。造成经济损失的应当承担赔偿责任。

2．未出现网络安全事故，但因服务商未严格履行需求文件及合同的约定被有关部门通报网络安全存在问题的，每次扣合同款的0.3%。造成经济损失的应当承担赔偿责任。

3．对于院方已按服务商所出具相关报告的建议进行整改，仍出现同样问题的，每次扣合同款的0.3%。

4．未按服务清单时间和质量完成服务任务的，每项任务每超时5个工作日扣合同款的0.3%。

表：网络安全事故分级与响应时间

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **事故级别** | **影响范围** | **危害程度** | **数据破坏程度** | **响应时间** |
| **特别重大事故（I级）** | 影响整个医院的信息系统，导致关键业务全面中断，如全院网络瘫痪、核心业务系统无法使用等。 | 对医院的医疗秩序、监管安全造成极其严重的负面影响，可能危及人身安全或导致重大财产损失。 | 大量敏感数据遭受严重破坏、泄露或丢失，恢复难度极大。 | 在事故发生后，相关人员必须在15分钟内向信息科主任报告，信息科主任在知晓情况后，立即向领导小组报告，并在1小时内组织开展应急处置工作，必要时协调外部技术专家参与。 |
| **重大事故（II级）** | 影响医院部分重要信息系统，导致主要业务受到严重影响，如部分科室业务系统无法正常运行。 | 对医院的医疗秩序、监管安全造成严重负面影响，可能对人身安全或财产安全构成较大威胁。 | 重要数据遭受严重破坏、泄露或丢失，恢复难度较大。 | 在事故发生后，相关人员必须在15分钟内向信息科主任报告，30分钟内向领导小组报告，并在2小时内组织开展应急处置工作。 |
| **较大事故（III级）** | 影响医院个别信息系统或局部网络，导致部分业务受到一定程度的影响，如个别科室的网络故障。 | 对医院的医疗秩序、监管安全造成一定负面影响，但不直接危及人身安全或财产安全。 | 部分数据遭受一定程度的破坏、泄露或丢失，恢复难度适中。 | 在事故发生后，相关人员必须在1小时内向信息科主任报告，2小时内向领导小组报告，并在4小时内组织开展应急处置工作。 |
| **一般事故（IV级）** | 影响医院少量信息系统或局部设备，对业务的影响较小，如个别终端设备出现故障。 | 对医院的医疗秩序、监管安全造成轻微负面影响。 | 少量数据遭受轻微破坏、泄露或丢失，恢复难度较小。 | 在事故发生后，相关人员应在发现事故的当天向信息科主任报告， 24小时内组织相关人员进行应急处置工作。 |