CHIMA

医院网络安全托管服务（MSS）实施指南［2025 版］

中国医院协会信息专业委员会（CHIMA） 编

二〇二五年 四月

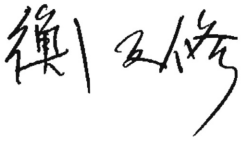
前言

在数字化浪潮的持续推动下，医疗行业信息化建设取得显著进展。医院信息系统已深度融入医疗服务全流程，成为支撑诊疗业务开展、医院管理运营及医学科研创新的核心基础设施，承载着海量患者诊疗数据、医院管理信息等关键资产。然而，新技术应用带来的便利与效率提升，也伴生了复杂多样的网络安全风险。

当前，勒索软件攻击、数据泄露、系统瘫痪等网络安全事件频发，严重威胁医疗行业信息安全与业务连续性。这些安全事件不仅可能导致医院业务中断，影响患者正常就医，更可能造成患者隐私泄露，危及公众生命健康安全与合法权益。作为关键信息基础设施的重要组成部分，医院网络安全防护能力关乎公共卫生体系的稳定运行，构建坚实的网络安全防线已成为医疗行业发展的必然要求。

但从行业调研情况来看，众多医院受限于专业安全人才短缺、安全投入不足、技术更新滞后等因素，难以独立构建全面、高效的网络安全防护体系。在此背景下，网络安全托管服务（Managed Security Service, MSS）作为一种专业化、集约化的安全运营模式，为医院网络安全建设提供了新的解决方案与发展路径。

中国医院协会信息专业委员会立足行业发展需求，联合多家医疗机构、行业专家及专业机构，共同编撰《医院网络安全托管服务（MSS）实施指南》。本指南旨在为各级医疗机构提供科学、系统、可操作的指导，帮助医院在保障患者信息安全和医疗业务连续性的前提下，规范引入网络安全托管服务，充分发挥其在医院网络安全防护体系中的重要支撑作用。指南围绕托管服务的需求分析、服务商选择、技术部署、运营管理及合规要求等关键环节，提出规范性要求与实施建议，助力医院提升网络安全防护能力，推动医疗行业在数字化转型进程中稳健前行，为智慧医疗健康发展筑牢安全屏障。



北京大学肿瘤医院

指南编制说明

中国医院协会信息专业委员会与北京大学肿瘤医院共同编制《医院网络安全托管服务（MSS）实施指南》，旨在为医院实施网络安全托管服务提供系统性建设规范，指南内容覆盖医疗卫生机构网络安全服务的各实施环节。针对当前医院普遍存在的网络安全服务选择能力参差不齐、服务质量缺乏统一标准、服务成本投入产出比低、安全技术应用覆盖面不足等痛点，本指南通过构建标准化的服务框架和可落地的实施方案，为医院提供兼具实用性与参考价值的建设指引。指南发布后，我们将持续关注医院发展，持续监测指南的指导效果，积极收集广大读者的反馈，适时进行更新和修订，以适应医院不断变化的业务安全诉求，详细建议可反馈 CHIMA 官方邮箱：sec@chima.org.cn。

在专委会指导下，以下单位参与本指南的编写和审核：北京大学肿瘤医院、北京协和医院、华中科技大学同济医学院附属同济医院、上海交通大学医学院附属仁济医院、复旦大学附属中山医院、盐城市第一人民医院、华中科技大学同济医学院附属协和医院、浙江大学医学院附属第四医院、中南大学湘雅二医院、中南大学湘雅三医院、四川大学华西天府医院、山西医科大学第一医院、河北医科大学第四医院、江苏省人民医院、中山大学附属第六医院、安徽医科大学第一附属医院、西北妇女儿童医院、海南医科大学第二附属医院、潍坊市人民医院、郑州大学第三附属医院、中国医科大学附属盛京医院、兰州大学第二医院、北京市卫生健康大数据与政策研究中心、浙江医院、杭州市第一人民医院、杭州师范大学附属医院、浙江大学医学院附属口腔医院、杭州市妇产科医院、江苏乾元通信息科技有限公司、深信服科技股份有限公司。

（以上排名不分先后）

指南编写参与人员（按姓氏笔画排序）

主　　编： 衡反修

主　　审： 王才有　薛万国

编委成员： 王安莉　邓　悟　付继刚　白云云　朱洪涛　朱　杰　朱丽艳　伊永菊　刘　华　孙润康
李润平　李金刚　杨剑峰　吴　蘩　沈玉强　张俊钦　张　楠　汪　伟　苏子仁　邵　尉
陈元春　郑　涛　郑　智　郜　勇　郗　群　倪红波　袁　林　陶　敏　蔡雨蒙　翟亚奇

审核专家： 马聿嘉　田　昕　孙国强　张　睿　陈　斌　费科锋　琚文胜

目录

一、背景

1.1 医院网络安全现状与挑战

近年来国家及行业主管单位接连颁布了《中华人民共和国数据安全法》《关于落实卫生健康行业网络信息与数据安全责任的通知》《医疗卫生机构网络安全管理办法》等法律法规文件，明确要求定期开展安全检查，对信息系统安全性进行有效验证，以查促建、以查促管、以查促改、以查促防，促进网络安全能力稳步提升，杜绝网络信息与数据安全事件的发生。

从相关调研数据来看，尽管全国约 75% 的三级医院已开展网络安全等级保护建设，但仍面临较多的安全挑战：

- **关键资产管控难度大**
  多数医院的互联网资产类型复杂、不可视；许多科室自建系统脱离统一管理，形成大量“影子资产”。
- **安全运维效率低**
  当前医院安全建设主要依赖传统安全设备和人工运维，存在漏洞修复滞后、告警处置率低等问题；常见隐患包括弱密码、高危漏洞、非必要开放端口等，但因人力不足、能力差异，难以及时闭环。
- **医院实战能力薄弱**
  大部分医院存在安全人员实战机会少、经验不足以及应急响应流程不完善等问题，难以应对外部专业、频繁的实战攻击。医院的安全运营防护能力还有进一步提升的空间。

1.2 网络安全托管服务的价值

网络安全托管服务可作为医院安全体系建设的补充，医院可通过服务化技术托管方式，获得 7*24 小时不间断的威胁监测、研判分析、快速处置、事件闭环等安全运营能力及服务，能够经济、便捷地帮助医院建立安全监测预警防护体系，对抗网络信息安全威胁。

- **全天候防护能力：**7×24 小时威胁监测、分析、处置，快速阻断攻击；结合 AI 自动化与人工研判，实现分钟级响应，降低业务中断风险。
- **系统性风险管控：**覆盖资产梳理、漏洞修复、事件响应全流程，避免“头痛医头、脚痛医脚”；通过定期安全评估与加固，持续优化防护策略。
- **合规与成本平衡：**帮助医院满足法规要求，减少因违规导致的处罚风险；以服务化模式替代高成本自建团队，帮助医院节约投入成本。

1.3 指南的目标和适用范围

核心目标

- **规范服务选择：**统一托管服务的内容、质量标准和实施流程，解决医院“选不准、用不好”问题。
- **降低实施门槛：**为医院提供可落地的操作模板（如合同条款、验收标准），减少试错成本。
- **推动能力共建：**引导医院借助外部专业力量，逐步培养自身安全团队，实现“授人以渔”。
- **适用范围：**本指南适用于医疗卫生行业网络安全服务供需双方开展网络安全服务内容、操作规范、服务响应能力以及相关合同编制等活动中，都可以在此规范中获取所需要的信息。

1.4 相关术语与定义

- **信息安全漏洞 Information security vulnerability**
  信息安全漏洞（以下简称“漏洞”）是指计算机信息系统在需求、设计、实现、配置、运行等过程中，有意或无意产生的缺陷，这些缺陷以不同形式存在于计算机信息系统的各个层次和环节之中，一旦被恶意主体所利用，就会对计算机信息系统的安全造成损害，从而影响计算机信息系统的正常运行。

- **威胁 Threat**
  可能导致信息系统危害的不期望事件的潜在缘由。

- **威胁情报 Threat Intelligence**
  业内大多数所说的威胁情报可以认为是狭义的威胁情报，其主要内容为用于识别和检测威胁的失陷标识，如文件HASH，IP，域名，程序运行路径，注册表项等，以及相关的归属标签。

- **高级可持续威胁：Advanced Persistent Threat 简称：APT**
  持续攻击是指对特定对象展开的持续有效的攻击活动。

- **事件响应剧本 Playbook**
  事件响应剧本是基于安全专家对各类安全事件的深入理解，以及丰富的实战经验固化出来的一种事件响应最佳实践，并将其固化到平台中，提升安全事件响应的效率及专业程度。

- **黑客 hackers**
  泛指对网络或联网系统进行未授权访问，但无意窃取或造成损坏的人。黑客的动因被认为是想了解系统如何工作，或是想证明或反驳现有安全措施的有效性。

- **信息安全事件 information security incident**
  由单个或一系列意外或有害的信息安全事态所组成的，有可能危害业务运行和威胁信息安全。

- **攻击 attack**
  在信息系统中，对系统或信息进行破坏、泄露、更改或使其丧失功能的行为（包含窃取数据）。

- **服务水平协议 SLA**
  服务水平协议是指通过书面形式对服务交付成果进行明确约定，一般包含一系列可测量的服务指标。一般来说，SLA 是服务提供者与医院之间协商并签订的一个具有法律约束力的合同或协议，规定了服务提供过程中双方所承担的商务条款，简称服务指标。

- **安全编排自动化及响应 SOAR**
  SOAR（Security Orchestration, Automation and Response）技术是指一种可自动防范网络攻击和自动进行响应的服务和工具。这种自动化是通过统一集成、定义任务运行方式和制定满足组织需求的事件响应计划来实现的。

二、医院网络安全托管服务的种类及选择

国际咨询机构 IDC 将安全托管服务（MSS）定义为安全服务提供商（MSSP）通过安全运营中心进行全天候监控和管理的 IT 安全服务。服务范围包括部署在本地、外部数据中心和云上的安全托管服务。

医院网络安全托管服务（MSS）是指医院通过外包托管的方式获取 7*24 小时持续有效、高质量的安全运营能力，实现“合规可达、风险可管、事件可控”的医院网络安全目标。网络安全服务商通过安全托管服务平台和服务团队，围绕资产、脆弱性、威胁、事件四个核心安全风险要素，提供风险预防、威胁监测和事件响应闭环等一系列服务。

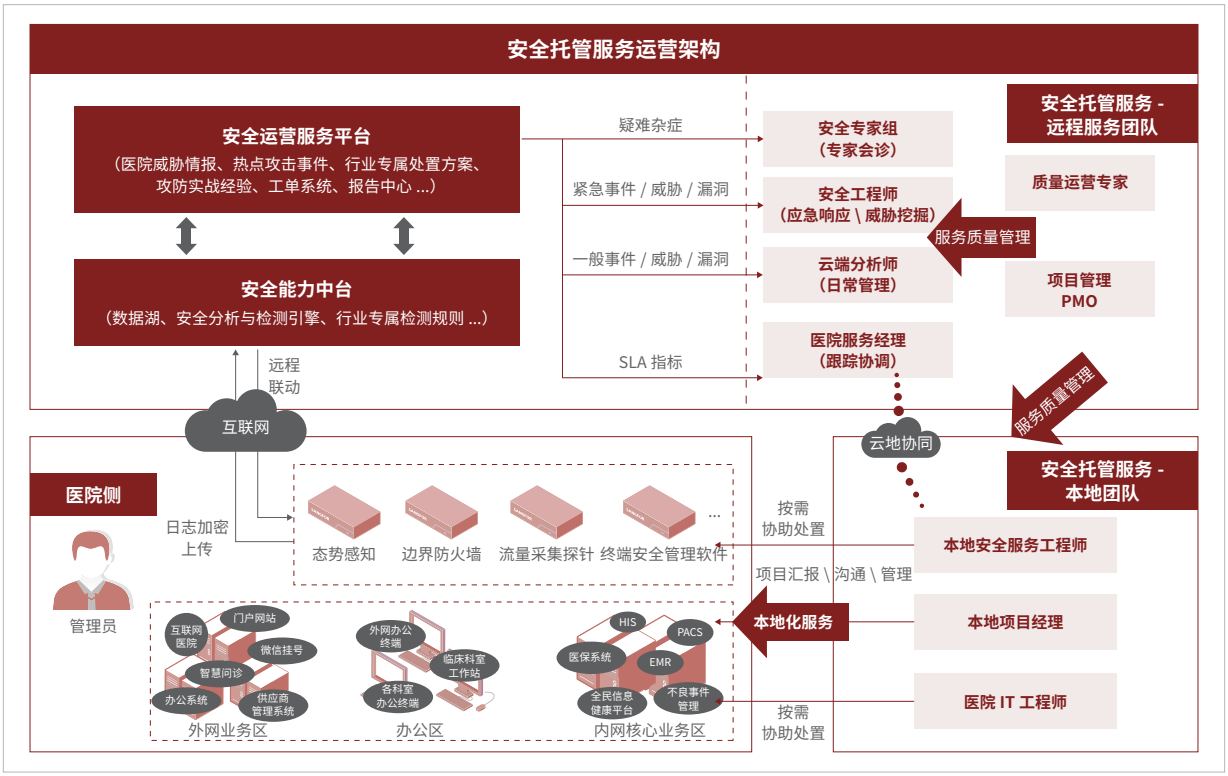


图 2—1 安全托管服务运营框架

2.1 医院网络安全托管服务种类及内容

在当前的安全服务选择中，主要分为两类：本地网络安全托管服务和远程网络安全托管服务。

2.1.1 远程网络安全托管服务

- **特点：**通过云端平台提供7×24小时威胁监测、分析及处置，覆盖安全事件全生命周期管理，具备灵活、经济的特点。
- **运作流程**

  基础配置：医院通过信息安全等级保护建设的安全设备（如防火墙、终端防护系统）建立基础防护。

  日志上传：重要安全设备的日志加密上传至云端运营中心。

  云端分析：结合AI引擎、威胁情报及人工研判，识别真实事件并生成处置方案。

  协同闭环：云端团队与医院本地人员配合完成事件处置。

- **医院安全组件接入说明**

  - **托管服务组件范围**

    平台类：如态势感知平台、扩展检测与响应平台（XDR）。

    流量采集类：如威胁流量探针。

    边界防护类：如防火墙。

    终端管理类：如终端安全管理系统。

  - **接入流程与管理要求**

    接入方式：医院通过服务组件作为接入点，将安全日志加密传输至托管平台。

    授权管理：所有组件接入需经医院明确授权，托管平台需支持异构安全设备的统一管理。

  - **权限与协作**

    服务商安全服务专家与医院安全工程师可通过平台查看已接入设备，并进行策略配置、升级包更新、开展处置动作及对威胁、事件进行分析和溯源。

    托管服务方需配合医院对威胁事件进行联动分析与处置。

- **服务商数据采集内容说明**

  服务商应全面采集相关的事件数据、告警数据、安全日志等。

  - **采集内容**

    - **资产信息：**资产的主要信息和指纹信息，如 IP 地址、物理位置、对应的业务系统、负责人、操作系统版本、开放的端口等。
    - **脆弱性信息：**需采集漏洞扫描器主动发现或安全设备被动发现的系统漏洞、WEB 漏洞和弱口令脆弱性数据，按脆弱性进行优先级排序。
    - **网络攻击日志：**应含 WEB 应用防护日志、漏洞攻击防护日志、DDOS 日志、僵尸网络日志、应用控制日志、文件杀毒日志、邮件安全日志和业务脆弱点日志。
    - **流量审计日志：**应含 TCP/UDP 会话日志、HTTP 日志、DNS 日志、文件审计日志、邮件协议（SMTP/POP3）日志、第三方设备日志（Syslog）。
    - **终端行为日志：**应含 Windows 进程创建日志、进程销毁日志、文件创建日志、文件创建时间修改日志、文件删除日志、远程线程创建日志、注册表创建 / 删除 / 设置日志、DNS 查询日志、网络连接日志、进程调用 API 日志、计划任务创建日志、Windows 主机系统 / 状态日志等；Linux 终端行为日志应含进程创建 / 销毁日志、文件创建 / 时间修改 / 重命名 / 移动 / 删除日志、DNS 查询日志、网络连接日志、进程凭证修改 / 修改日志、内核动态加载信息日志和系统内核交互日志、Linux 系统日志、Linux 主机状态日志等。
    - **终端安全日志：**应含病毒查杀日志、WebShell 查杀日志、暴力破解日志、微隔离日志和异常账号检测日志。
    - **其他安全产品**（SIP、NTA 或其他 SIEM）分析得出的告警数据包括安全事件、威胁事件、脆弱性事件和明文传输信息事件。

  - **采集原则**

    支持多种方式采集第三方安全设备日志，确保威胁检测准确性。
    仅收集与安全防护相关的必要数据，避免非必要信息外发。

- **托管服务数据存储要求**
  - **存储架构：**安全日志数据需分层存储，以满足威胁狩猎、事件分析、溯源调查、报表生成等场景需求。
  - **合规要求：**所有数据必须存储在中华人民共和国境内的服务器；存储时长需符合《网络安全法》等规定，以便更好地对安全事件进行分析研判和调查溯源。

- **网络安全托管服务界面能力要求**
  - **平台架构**
    - **安全能力中台：**支持风险检测、分析、响应全流程管理，聚合网络侧与终端侧数据，辅助云端专家精准威胁分析、调查、响应及能力赋能。
    - **托管服务平台 ：**为医院全服务周期内各项服务工作提供支撑，整合服务流程、专家经验、知识库等模块，持续优化服务质量。
      为方便医院了解服务内容、进展、效果等，托管服务方应提供可展示的服务界面并具备以下能力：
    - **安全态势展示：**实时显示威胁事件统计、漏洞分布及风险趋势，支持按资产类别、威胁类型筛选查看。
    - **工单管理**

      a) 工单类型：威胁工单、脆弱性工单、应急工单等。
    - **功能要求**

      b) 平台应展示当前工单数量和处置状态，便于双方查看服务处置过程和闭环效果，掌握当前专家服务进度，监督服务质量。

      c) 安全告警工单管理：展示威胁告警信息，包括威胁类型、威胁发生时间、攻击者 IP、被攻击者 IP、威胁描述、攻击趋势等信息，也应包括安全专家确认告警的记录。

      d) 安全事件工单管理：若判断为有效威胁，服务人员应将该威胁转化为威胁事件，并转给更高级人员处理。威胁事件的分析过程应详细记录到对应工单里，便于工单流转和过程回溯。处置完成后，威胁事件进行关闭。
    - **流程管理 :**提供流程编排引擎，支持服务流程的编排与持续优化，确保达成量化的服务指标。
    - **报告中心**

      a) 自动生成并导出《威胁处置报告》《安全运营月报》等；

      b) 支持按事件管理、攻击威胁、脆弱性管理等模块定制报告。

  - **规则管理**

    支持检测规则配置及自定义规则，增强关联分析能力。
  - **知识库**

    积累安全事件处置方案、策略优化经验，提供工具库以提升服务效率。
  - **重保中心**

    a) 覆盖重大活动保障时期的备战、实战、结束三个阶段的指导性工作流程。

    b) 支持重大活动保障时期特殊的安全要求，如生成每日值守日报、根据重保攻击频率和重点业务关注度而自定义检测规则和告警等级等。

- **服务可视化要求**

  为便于医院实时掌握服务进展与安全态势，托管服务平台需提供以下可视化功能：

图 2—2 医院门户功能模块

- **总览看板**

  展示整体资产安全风险评级、服务前后防护效果对比；
  可视化呈现风险趋势、工单处置进度及当前负责专家。

- **事件管理模块**

  应支持服务周期内所有服务资产发现的事件，经过专家侧人工研判，确定为真实有效的事件后，推送至医院门户，医院可实时跟踪每个事件的分析处置闭环过程。

- **威胁管理模块**

  应支持服务周期内，所有外部攻击以及全网爆发的最新情报，经专家侧人工研判，确定为真实攻击后，推送至医院门户，医院可实时跟踪每个威胁的闭环过程。

- **脆弱性管理模块**

  应支持服务周期内，通过漏洞扫描设备扫描和流量探测上报的漏洞和弱口令数据，经人工研判以后推送至医院门户，方便医院进行跟踪管理。

- **资产管理模块**

  展示托管资产清单（IP、开放端口、存活状态等），支持轻量化管理。

- **质量监控模块**

  实时展示服务指标（漏洞修复率、平均响应时间、事件闭环率等）。

- **报告管理模块**

  归档《安全运营月报》《威胁处置报告》等服务交付物，支持分类检索与下载。

- **设备管理模块**

  实时监控接入安全设备（防火墙、探针等）的在线状态及运行日志。

2.1.2 本地网络安全托管服务

- **特点：**需安全工程师驻场服务，服务周期通常为 1 年、3 年或 5 年。对驻场人员专业性、网络安全经验要求较高，适合具备驻场条件的医院。

- **服务内容：**驻场工程师负责日常安全运维，结合定期的现场安全服务（如漏洞修复、应急响应等）。

  本地托管服务核心流程与远程托管服务一致，区别在于人员驻场执行。

2.1.3 医院网络安全托管服务主要内容

医院网络安全托管服务的核心目标是通过对关键信息资产的持续监测与值守，降低安全事件发生风险。服务内容涵盖以下方面：

- **资产梳理**
  范围：全面识别服务器、网络设备、业务系统等关键资产，记录操作系统版本、IP 地址、开放端口、网络拓扑等信息，并录入安全运营平台动态管理。
  更新机制：资产变更时，通过标准化流程与安全专家协同更新台账，确保数据准确性。

- **安全评估**
  方法：通过漏洞扫描、基线核查等工具，评估医院网络面临的威胁、脆弱性及防护措施有效性。
  范围：涵盖网络架构、现有安全设备、管理制度及流程。

- **脆弱性管理**
  检测服务器、网络设备、小程序 /APP 等系统的漏洞、弱密码问题；通过漏洞管理平台关联资产与漏洞信息，实现全生命周期跟踪（发现、修复、复测）。

- **安全加固**
  根据专业安全评估结果，制定加固方案，涵盖操作系统、数据库、网络设备等。

- **应急响应**
  针对医院突发的安全事件，应包含以下处置流程：

  1. 负责安全事件的取证、分析、修复、加固等应急处置工作；

  2. 包括病毒的查杀、网络攻击行为分析、封堵与溯源等，并协助相关部门处理安全问题。

  3. 提供应急响应报告，对安全风险、安全事件描述、危害性、原因、排查过程、处置加固方法等进行详细说明，进行根因分析，优化应急响应流程。

  通过建立安全事件处置知识库，提升医院安全能力，协助医院闭环处置安全事件，并且通过对安全威胁的趋势分析，提供长期的安全规划及改进建议。

- **重要时期保障**
  在医院的重要时期，例如国家两会、重大活动、国庆、春节等重要节日，以及医院关键业务测评时期，如医院等级评定、互联互通测评、电子病历评级等期间，做好保障和值守，避免恶意攻击对医院关键信息资产造成影响。

- **其他服务事项**
  日常运维：安全设备维护、策略优化、威胁通报；
  体系建设：协助完善安全架构、合规审计支持；
  流程优化：定期总结问题，改进工作流程。

2.2 医院服务种类选择指引

- **选择原则**
  医院需根据资源投入、安全现状、人员配置等综合条件，选择适配的服务模式：
- **本地托管服务**
  适用场景：安全预算充足、已自建安全运营平台的大型三甲医院。
  特点：驻场工程师提供日常运维及定期的现场服务。

- **远程托管服务**
  适用场景：各级医院，尤其是缺乏专职安全团队的单位。
  优势：7×24 小时监测、效果有保障、灵活低成本、快速补齐安全能力。
- **混合模式**
  方案：本地团队负责日常运维（5×8 小时），云端团队提供应急响应等专家能力以及非工作时间的监测与处置。
  趋势：逐渐成为主流，兼顾效率与成本。
  远程网络安全托管服务适用性较广，性价比高、更能满足大多数医院的实际需求，因此本指南围绕该模式重点展开介绍，详细服务清单见附录 C。

三、医院实施网络安全托管服务的基础条件

3.1 医院网络技术条件

医院具备互联网出口，且允许安全设备内相关数据连通到线上的托管服务平台。外网互联网出口的带宽应不低于5Mbps。

3.2 医院基础防护技术条件

医院如果不具备以下相关设备，可通过采购或租赁等方式进行补充，完善基础的防护技术条件。

- **网络流量采集设备（必需）**
  针对医院关键网络处，部署流量采集设备，一般在内网核心交换和外网核心交换处旁路部署镜像模式，网络流量采集设备完成初始化流量采集、分析、上传到托管服务平台，以便线上托管团队分析、研判和定位具体威胁和事件。
- **网络边界防护设备（必需）**
  边界防护设备可与托管服务平台进行有效联动，通过提供边界安全隔离、流量检测、入侵防护和外联管控等防护能力，提升威胁分析、事件定位、联动处置和策略加固等效率与效果。
- **端点防护采集软件（必需）**
  在关键信息资产主机上安装防护软件，实现主机安全防护能力，同时采集主机必要的安全日志并上传至托管服务平台。网端数据聚合有助于安全团队更加精确的定位和处置。
- **漏洞扫描工具（必需）**
  有效识别业务系统、操作系统、中间件、数据库、安全设备的漏洞以及弱口令、高危端口等脆弱性问题，为网络安全托管服务的脆弱性管理提供必要的基础数据。
- **安全运营平台（可选）**
  安全运营类平台（包括态势感知类平台等）可有效加强全方位告警分析、研判和调查溯源能力，增强第三方安全设备的接入与联动能力，从而提升安全运营的效率。

3.3 人员及管理要求

医院本地需要有对接远程网络安全托管服务的接口工程师（医院安全工程师或驻场运维人员），配合远程安全服务团队完成网络安全托管服务的现场配合工作，例如非联网系统的问题处置等，该人员应具备网络安全、设备操作等基础知识与能力。

四、网络安全托管服务提供商的资质要求及选择

4.1 服务技术资质

为保障网络安全托管服务的安全性和可靠性，医院在选择服务商时应重点关注以下资质要求：

- **等级保护测评**
  托管服务平台应当做好严格的安全防护，并严格按照《信息安全技术——网络安全等级保护基本要求》完成等级保护测评工作，服务平台至少应通过等级保护三级测评。
- **安全运营服务资质**
  托管服务平台应具备中国信息安全测评中心开展的安全运营类服务资质认证，证明其服务能力及可靠性。
- **云计算安全能力认证**
  可信云安全运营中心评估：通过中国信息通信研究院的评估，确保云服务能力符合行业标准。
  云计算服务安全评估：通过中央网信办等四部委联合评估，验证云平台安全性与可控性。
- **其他信息安全资质**
  服务商宜具备《信息安全服务资质认证证书（风险评估）》、《信息安全服务资质认证证书（应急处理）》等补充资质，以提升服务全面性。

4.2 服务团队要求

4.2.1 组织架构

- **安全运营团队**
  采用“人机共智”模式（人工与自动化协同），为医院提供 7×24 小时安全运营服务。
- **安全专家团队**
  负责安全威胁研判、事件处置等核心工作，解决复杂疑难问题。
- **攻防研究团队**
  由高级专家组成，研究前沿攻防技术，持续提升平台检测与响应能力。
- **质量管理团队**
  监督服务全流程，通过数据分析和满意度调查优化服务质量。

在实际服务交付中，网络安全托管服务通过云地协同的方式为医院提供闭环服务：本地安全服务工程师负责网络安全托管服务的上线准备、资产梳理、设备策略调优以及首次威胁线下处置等工作，并对线上无法覆盖的问题进行持续跟踪和闭环处理。

4.2.2 职责分工

图 4—1 网络安全托管服务团队职责分工

网络安全托管服务团队的具体分工应至少包含如下表所示。

团队名称	专家角色	职责分工
安全运营团队	云端分析师	负责服务项目的告警审核、告警诊断、告警白名单管理等工作。
	应急响应工程师	负责协同服务经理，通过应急响应对威胁事件处置闭环，提升安全风险响应速度和能力。
	医院服务经理	主要负责项目的全生命周期管理和日常运营服务工作，包含资产管理、脆弱性管理、威胁管理、事件管理、项目问题跟进、运营报告编写、定期汇报等工作。
	威胁挖掘工程师	负责对升级的威胁工单进行研判和主动挖掘服务内资产的隐藏威胁风险，并将其沉淀为平台技术能力。
安全专家组	云端业务专家	负责协助服务经理解决疑难业务问题，根据服务落地情况，不断优化迭代业务流程和规划设计新业务，提升整体安全服务质量。
	高级威胁分析专家	负责通过多维度长期深度分析，挖掘高级威胁，并将其威胁特征沉淀为平台技术能力。

安全专家组	应急响应专家	负责协助应急响应工程师处理威胁事件，对应急响应情况进行审核复盘，优化提升响应速度。
攻防研究部	安全攻防专家	负责参与实战攻防工作，并将实战经验进行人员赋能和沉淀为平台能力。
	渗透测试专家	负责对服务资产进行授权模拟攻击，对安全性进行评估，查找和展示系统安全隐患问题。
	威胁情报专家	负责管理威胁情报，跟踪情报 POC、EXP，审核和验证漏洞真实性情况。
质量管理团队	质量运营专家	负责医院满意度调研，医院质量数据分析及质量报告输出。
	PMO	负责项目的交付质量标准定义、项目质量管理推进，达标情况监督和质量问题整改工作。

4.2.3 安全托管服务人员资质

网络安全托管项目管理人员需具备“项目管理资质认证（PMP）”或“信息系统项目管理师（高级）”资质证书。网络安全托管技术人员需具备“注册信息安全专业人员认证”或“信息安全保障人员认证”。

4.3 服务管理资质

为确保服务质量与规范性，医院应选择通过以下国际管理体系认证的服务商：

- **ISO 27001 认证**
  服务商的信息安全管理体系（Information Security Management System, ISMS）需通过 ISO 27001 认证，且认证范围涵盖网络安全托管服务。
- **ISO 20000 认证**
  服务商应通过 ISO 20000 信息技术服务管理体系认证，且范围应该涵盖网络安全托管服务。

4.4 服务能力要求

4.4.1 数据采集与存储安全要求

- **加密传输**
  安全日志数据需通过加密方式采集，防止被网络嗅探泄露。
- **数据隔离与脱敏**
  不同医院的日志数据隔离存储；
  对敏感信息进行脱敏处理，确保不可还原。
- **存储与删除**
  支持医院在存储期内取回或删除数据；
  数据存储期限需符合《中华人民共和国网络安全法》要求，到期后应自动删除。

4.4.2 人员安全管控要求

- **设备管理**
  服务人员办公计算机禁止接入互联网；

  部署防泄密措施（如禁用数据拷贝、添加水印）。
- **访问控制**
  服务人员需通过 VPN 或零信任加密方式访问平台；

  访问源 IP 需限制为白名单地址。
- **保密协议**
  服务人员上岗前需与医院签订保密协议。

4.4.3 平台安全管控要求

- **访问限制**
  平台禁止直接对互联网开放访问。
- **身份验证**
  服务平台和加密隧道登录需多因素认证（账号密码 + 短信验证码 / 硬件特征码）。
- **权限管理**
  遵循最小授权原则，仅向直接服务专家开放医院数据；

  数据操作全程审计，分析人员与处置人员权限分离。
- **容灾与开发安全**
  核心数据异地备份，确保 7×24 小时可用性；

  平台开发需遵循 SDL 流程，代码通过严格安全测试。
- **漏洞管理**
  定期开展风险评估、渗透测试、漏洞扫描，及时修复问题。
- **医院门户安全**
  医院查看服务成果的门户需多因素认证登录。

4.4.4 服务商技术能力要求

医院网络安全托管服务商需具备以下技术能力，以确保防护效果与实战能力：

- **AI 驱动的防护能力**
  - **技术应用：**结合 AI 技术提升高隐蔽攻击的监测与防御能力，优化资产梳理、漏洞修复、威胁监测等流程自动化水平。
  - **持续迭代：**基于医院实际场景，持续改进自动化处置流程，提升防护效率。
- **安全编排自动化及响应技术实现告警闭环**

  应通过安全编排自动化及响应技术，整合多源威胁数据，利用专家与机器的组合执行事件分析和分类，定义标准工作流；进而根据医院标准工作流来定义、确定优先级并推动标准化事件的响应活动，实现医院安全问题的闭环工作。

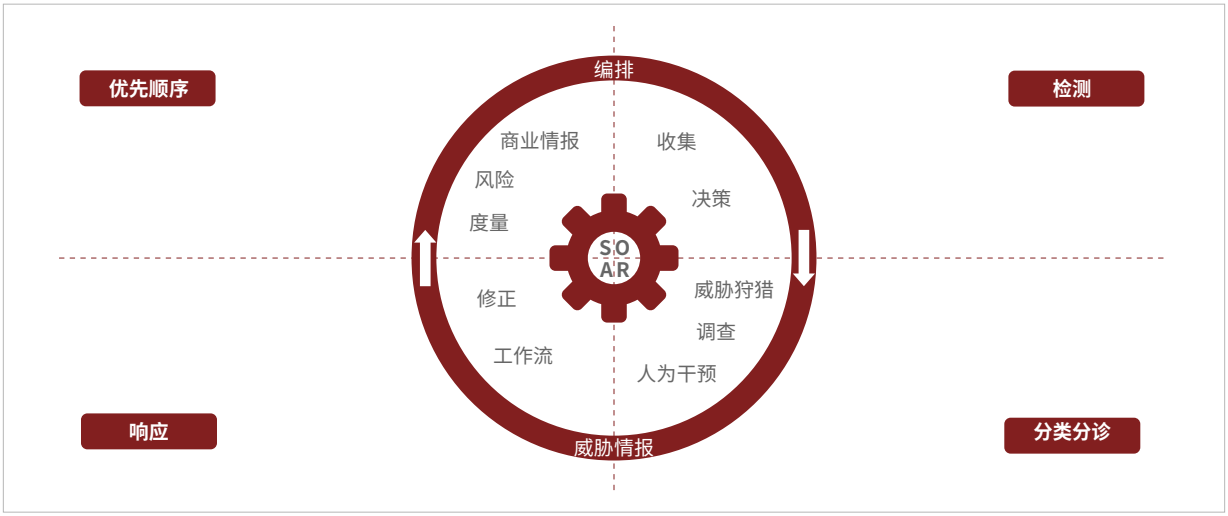


图 4—2 SOAR 技术典型框架

应将安全专家和技术通过 SOAR 技术编入医院安全服务的业务处理流程中，确保安全事件响应的及时性、标准性和专业性。

- **国际主流威胁检测架构**
  - **技术框架：**采用 ATT&CK 等国际标准框架，覆盖全球常见攻击方式。
  - **定制能力：**支持根据医院业务特点定制检测策略（Usecase），满足个性化检测告警需求。

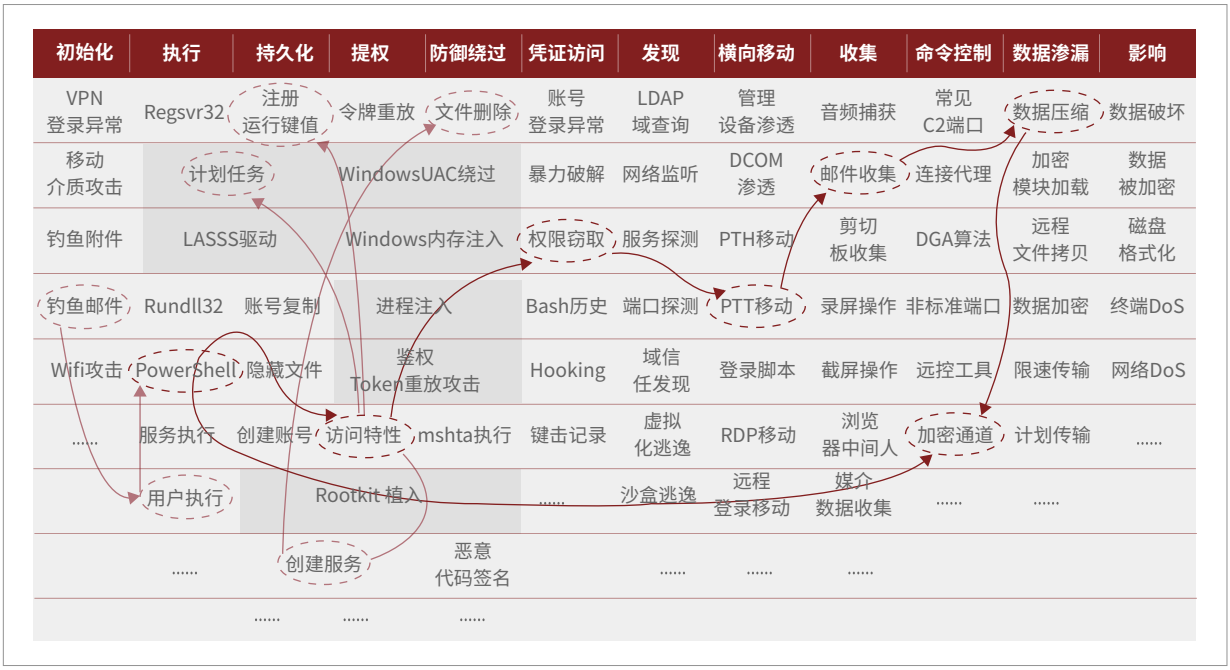
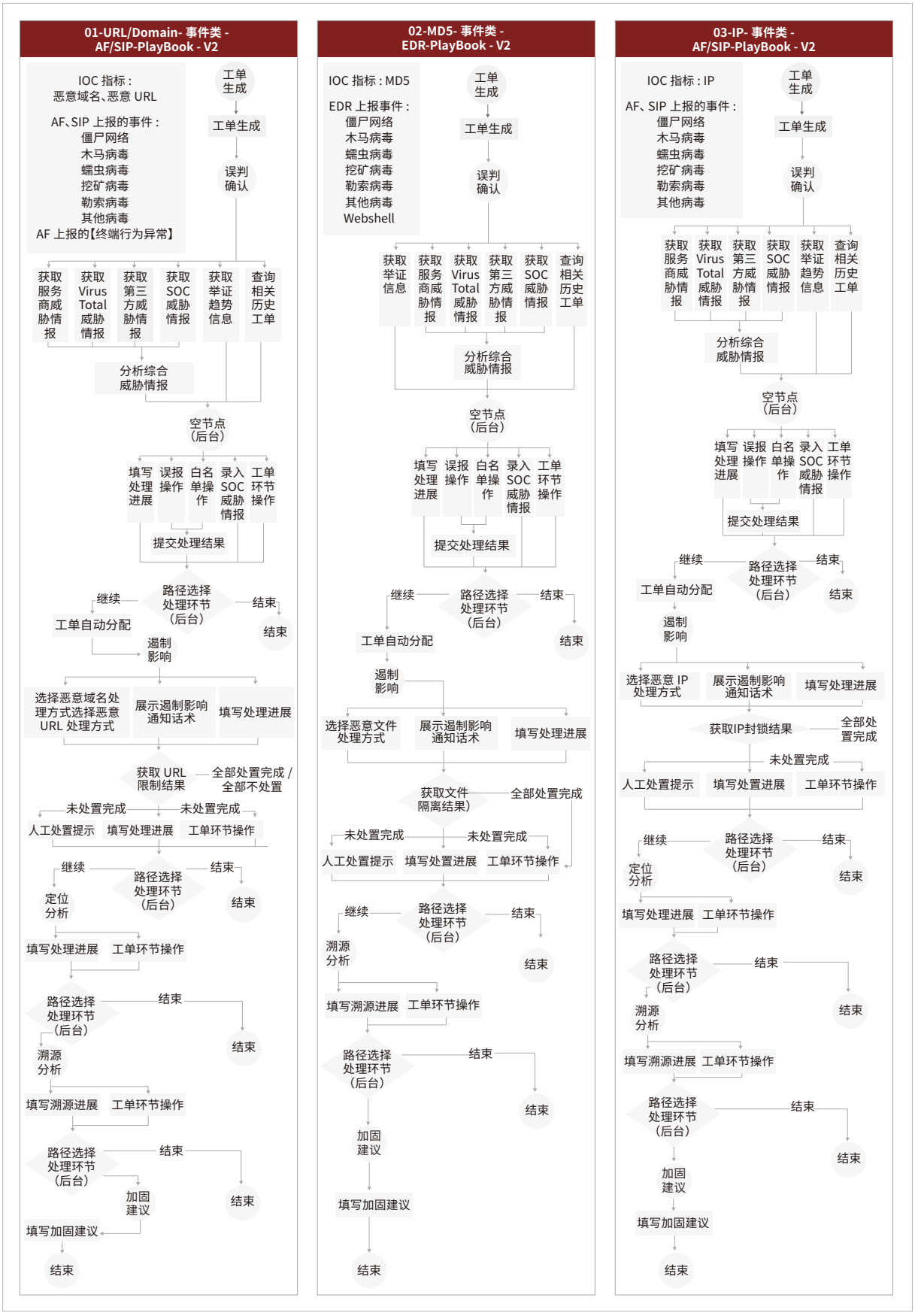


图 4—3 基于 ATT&CK 框架的典型攻击路径示例

- **面向医疗实战的闭环处置流程**

  经验沉淀：基于医疗行业攻防经验，形成标准化事件响应流程（Playbook），内置处置剧本。

  闭环管理：通过 SOAR 技术将流程固化至平台，确保每类事件均按专业方案闭环。


01-URL/Domain- 事件类 - AF/SIP-PlayBook - V2
IOC 指标：恶意域名、恶意 URL
AF、SIP 上报的事件：僵尸网络 木马病毒 蠕虫病毒 挖矿病毒 勒索病毒 其他病毒
AF 上报的【终端行为异常】
工单生成
工单生成
误判确认
获取服务商威胁情报
获取 Virus Total 威胁情报
获取第三方威胁情报
获取 SOC 威胁情报
获取举证趋势信息
查询相关历史工单
分析综合威胁情报
空节点（后台）
填写处理进展
误报操作
白名单操作
录入 SOC 威胁情报
工单环节操作
提交处理结果
路径选择处理环节（后台）
继续
结束
工单自动分配
遏制影响
选择恶意域名处理方式选择恶意 URL 处理方式
展示遏制影响通知话术
填写处理进展
获取 URL 限制结果
全部处置完成 / 全部不处置
未处置完成
人工处置提示
定位分析
溯源分析
填写溯源进展
加固建议
填写加固建议
02-MD5- 事件类 - EDR-PlayBook - V2
IOC 指标：MD5
EDR 上报事件：僵尸网络 木马病毒 蠕虫病毒 挖矿病毒 勒索病毒 其他病毒 Webshell
工单生成
工单生成
误判确认
获取举证信息
获取服务商威胁情报
获取 Virus Total 威胁情报
获取第三方威胁情报
获取 SOC 威胁情报
查询相关历史工单
分析综合威胁情报
空节点（后台）
填写处理进展
误报操作
白名单操作
录入 SOC 威胁情报
工单环节操作
提交处理结果
路径选择处理环节（后台）
继续
结束
工单自动分配
遏制影响
选择恶意文件处理方式
展示遏制影响通知话术
填写处理进展
获取文件隔离结果）
全部处置完成
未处置完成
人工处置提示
填写处置进展
工单环节操作
溯源分析
填写溯源进展
加固建议
填写加固建议
03-IP- 事件类 - AF/SIP-PlayBook - V2
IOC 指标：IP
AF、SIP 上报的事件：僵尸网络 木马病毒 蠕虫病毒 挖矿病毒 勒索病毒 其他病毒
工单生成
工单生成
误判确认
获取服务商威胁情报
获取 Virus Total 威胁情报
获取第三方威胁情报
获取 SOC 威胁情报
获取举证趋势信息
查询相关历史工单
分析综合威胁情报
空节点（后台）
填写处理进展
误报操作
白名单操作
录入 SOC 威胁情报
工单环节操作
提交处理结果
路径选择处理环节（后台）
继续
结束
工单自动分配
遏制影响
选择恶意 IP 处理方式
展示遏制影响通知话术
填写处理进展
获取IP封锁结果
全部处置完成
未处置完成
人工处置提示
填写处置进展
工单环节操作
定位分析
填写处理进展
工单环节操作
溯源分析
填写溯源进展
加固建议
填写加固建议

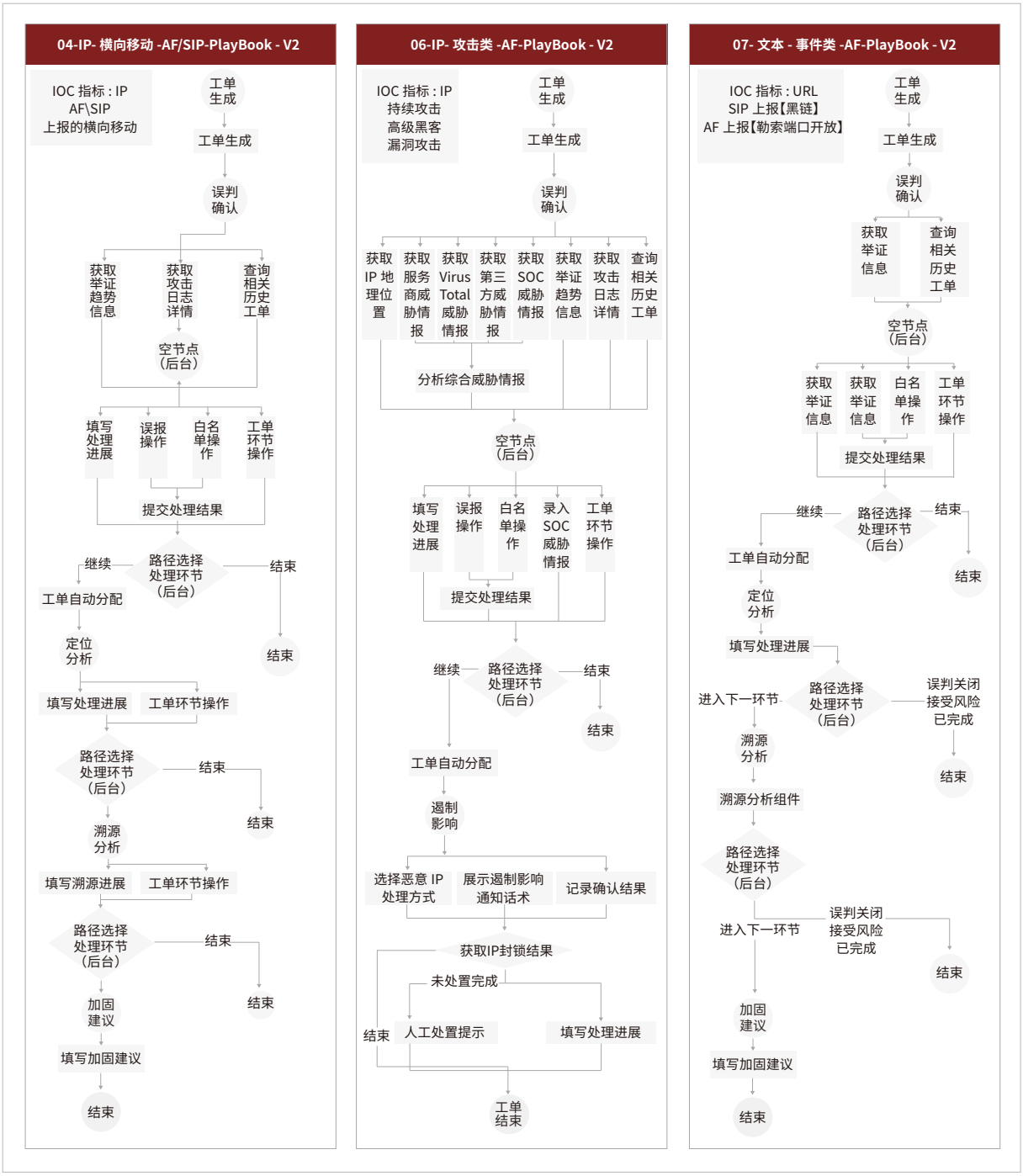


图 4—4 网络安全托管内置的事件响应剧本示例

- **威胁情报联防联控**
  情报整合：聚合医疗行业漏洞、暗网监控等情报，建立高质量威胁情报库。
  精准匹配：通过云端共享与下发，实现情报与医院资产关联，支撑风险预警与响应。
- **威胁调查与溯源能力**
  攻击链分析：提供攻击路径还原、网端数据关联分析，自动化定位根因及影响范围。
  加固支持：通过攻击链回溯漏洞、配置缺陷等入口，协助医院及时修复脆弱点。

4.5 服务效果要求

医院需与服务商明确约定可量化的服务指标，以评估服务效果并保障安全目标达成，具体要求如下：

- **服务指标分类分级**
  围绕安全事件、威胁、漏洞三个维度定义分级标准，事件级别需符合国家标准。
- **关键指标定义**
  需包含检测准确率、平均检测时间、平均响应时间、事件闭环率、高危漏洞修复率等核心指标。
- **重大事故要求**
  对重大安全事故（如数据泄露、勒索攻击）需设定更严格的服务指标，包括响应时间、现场处置时效等。
- **职责与协作说明**
  明确服务指标达成所需的医院配合事项（如授权、资源支持）及双方责任边界。
- **未达标的处理措施**
  约定服务指标未达成时的具体惩罚条款（如延长服务时间等）。
- **法律约束力**
  服务指标需明确写入合同，具备法律效力，确保安全目标的达成。
- **服务承诺管理**
  服务过程中，医院可基于实际需求要求服务商补充书面效果承诺。以下供参考：

面向安全服务的服务指标要求：

威胁等级 / 服务指标	一般威胁	重大威胁
分析研判通知时效 MTTA	从安全日志上传分析研判到通告，用时 <60mins	从安全日志上传分析研判到通告，用时 <30mins
遏制影响时效 MTTC	联动防火墙 / 终端防护软件 遏制影响时间 <30mins	联动防火墙 / 终端防护软件 遏制影响时间 <15mins
准确率	经专家确认后，准确率达 >99%	经专家确认后，准确率达 >99%
闭环率	100%	100%

面向安全事件提供的服务指标要求：

事件等级 / 服务指标	一般事件	重大事件
分析研判通知时效 MTTA	从安全日志上传分析研判到通告，用时 <30mins	从安全日志上传分析研判到通告，用时 <15mins
遏制影响时效 MTTC	联动防火墙 / 终端防护软件遏制影响时间 <30min	联动防火墙 / 终端防护软件遏制影响时间 <15mins
准确率	经专家确认后，准确率达 >99%	经专家确认后，准确率达 >99%
漏报率	攻击成功事件 0 漏报；至少发现攻击链路上的一个攻击行为	
事件闭环时间 MTTR	经医院授权后协助医院闭环安全事件的时间 <8 小时	经医院授权后协助医院闭环安全事件的时间 <24 小时
闭环率	100%	100%
重大事故应急响应承诺：工作时间 15 分钟内、非工作时间 30 分钟之内云端专家响应，默认由专家团队远程协助处置，如远程无法解决的则安排安全专家上门处置，省会（含北京、上海、深圳、重庆、天津等一线城市和直辖市）2 小时内上门处置，省内 8 小时内上门处置。		

面向高危可利用漏洞提供的服务指标要求：

漏洞级别	漏洞通知	准确率	防护率
高危可利用漏洞	云端专家使用服务商漏扫工具完成漏扫后 2 个工作日内推送漏洞报告。	漏洞经专家确认后，准确率达到 99%。	联动防火墙配置规则后，防护率 99%。

网络安全托管服务应提供多种增值服务，如网络安全保险、网站监测、攻击面管理等，以满足医院的个性化需求和应用场景，充分保障医院的实际安全效果。

4.6 服务体验要求

为保障医院对服务进展及安全态势的透明感知，托管服务需满足以下要求：

- **专属服务经理**
  服务商应为医院配置专属服务经理，负责服务全周期管理（计划制定、沟通协调、定期汇报等），深化对医院业务特性及安全需求的理解，提升服务精准性。
- **多样化沟通渠道**
  日常沟通：通过即时通讯群组推送安全事件通告；
  进展跟踪：移动端门户实时展示工单处置进度；
  紧急响应：电话授权关键操作；
  文档交付：邮件发送服务报告、处置方案等。
- **7×24 小时服务保障**
  非工作时间仍按服务指标要求提供持续监测与响应，并推送夜间 / 节假日安全态势简报。

- **服务可视化与反馈**
  通过可视化界面实时展示服务进展、风险趋势及闭环效果；
  定期输出总结报告，辅助医院安全管理决策。

4.7 服务成本要求

- **高性价比投入**
  推荐采用远程托管服务，利用云端资源共享机制，减少自建安全团队及平台的初期投入，降低运维成本。
- **灵活扩展策略**
  初期阶段：优先将核心业务资产（如患者数据系统、电子病历平台）纳入托管范围；
  后续阶段：根据安全预算及实际需求，逐步扩大托管资产覆盖范围，最终实现全资产统一管理。

五、网络安全托管服务协议约定

5.1 责任声明

医院是网络安全的第一责任主体，托管服务仅为辅助手段，不可替代医院自身管理职责，医院自身仍需高度重视网络安全工作。医院可借助安全托管服务公司的力量优化自身人员、流程、技术能力，强化网络安全运营能力。

5.2 服务协议主要条款

- **协议内容范围**
  需明确服务时间、内容、清单、范围、方式及交付物等核心要素。
- **服务指标约定**
  协议需包含可量化的服务指标（如响应时间、漏洞修复率等），并说明承诺条件与考核方式，便于医院监督。
- **责任与义务划分**
  明确医院与服务商的责任边界，包括服务授权、协作方式、保密义务及知识产权归属。
- **违约处理机制**
  约定未达成服务指标或服务缺失时的惩罚措施（如整改、赔偿），细化责任划分、生效条件及免责条款。
  相关安全托管服务合同或协议模板可参考附录 D。

5.3 安全托管责任界定

- **主体原则**
  根据《中华人民共和国网络安全法》及《医疗卫生机构网络安全管理办法》,医院作为网络运营者始终是安全第一责任人，服务托管部分安全工作内容，第一责任人不因网络安全托管服务的实施而变化。
- **服务边界确定**
  责任范围以协议约定的服务内容、服务指标和资产覆盖范围为准，双方需在服务边界内明确分工。
- **医院工作内容和要求**
  - 服务保障：确保医院网络环境可以正常访问，避免托管服务平台与医院本地安全设备的连接中断；
    授权与配合：提供必要权限、网络环境及第三方设备策略优化支持

- 设备维护：保障托管接入设备的在线状态及监测能力。
- 日常运营支持：为服务商提供必要的支持和协助，如协调医院内部各部门之间的工作，确保服务商的工作能够顺利进行。
- 服务质量：按照服务指标的要求，对服务商的服务质量进行监督和评估，定期检查服务指标的完成情况，及时提出改进意见和建议。
- 其他：除网络安全托管服务范围外的其他安全工作，包括但不限于及时修复漏洞等。

- **服务商工作内容和要求**
  - 按服务清单完整交付服务内容；
  - 对于影响服务正常开展的风险进行及时预警，并明确告知医院所需的配合动作；
  - 避免服务人员出现操作失误，造成不良影响；
  - 服务人员应在得到授权后进行具体操作；
  - 服务人员应严格遵守保密要求，不得泄露医院数据；
  - 服务过程中应监控并确保服务指标承诺达标，如及时通知风险与响应闭环等。

  若服务商未按照约定的服务指标完成既定工作，应承担相应责任；

- **争议处理**

  若发生重大安全事件或监管通报，服务商需优先采取补救措施，双方按协议协商界定责任。

六、医院网络安全托管服务流程

安全托管服务（MSS）是提升医院网络安全防护能力、保障患者隐私和业务连续性的重要举措。从服务全生命周期角度，安全托管服务流程一般可分为四大阶段，即服务启动阶段、服务上线阶段、服务持续运营阶段和服务终止阶段。

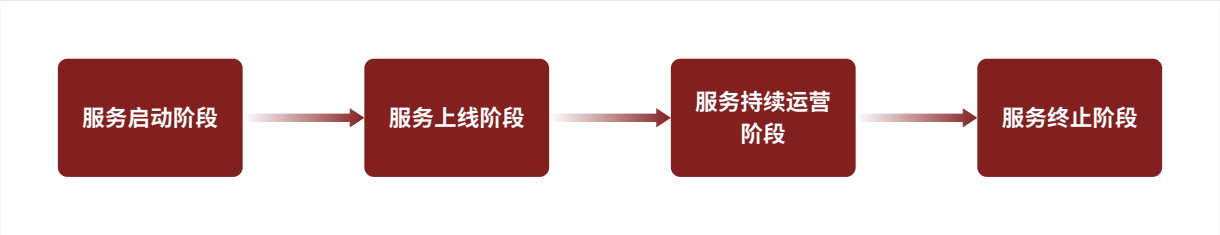


图 6—1 网络安全托管服务流程的四个阶段

6.1 服务启动阶段

服务启动阶段，通过召开内外部服务启动会，明确服务预期，对沟通机制和交付内容达成一致，并针对安全托管服务进行授权、完成保密协议的签署。

6.2 服务上线阶段

服务上线阶段，聚焦于对现有业务安全问题进行综合评估及问题处置，主要包括服务资产确认和首次分析与处置流程。

6.2.1 服务资产确认流程

借助安全工具对当前信息资产进行全面发现和深度识别，并结合人工确认，梳理成真实、可用的资产台账，具体步骤如下：

- 资产探测工具部署：部署资产探测工具并配置安全策略，主动发现网络中的资产信息。
- 资产梳理：首次全面扫描服务内资产，记录关键信息，形成资产台账并录入托管平台。
- 建立台账：与医院核对资产责任人、重要性等信息，建立可信资产数据库。

6.2.2 首次分析与处置流程

服务初期需对服务资产现状从脆弱性评估、病毒类事件评估、攻击行为评估、失陷类事件评估等方面对现有安全问题进行客观评估，对评估发现的安全问题进行处置。具体流程如下：

- **脆弱性分析与处置**

  漏洞扫描：检测操作系统、数据库、常见应用等存在的系统漏洞和 Web 漏洞。

  弱口令核查：对 SMB、MySQL、SSH 等服务的弱密码进行自动化猜解检测。

  安全基线检查：核查主机操作系统、数据库、中间件的账号管理、访问控制、服务配置等是否符合安全基线要求。

  修复建议：根据漏洞风险等级提供修复方案（如补丁更新、配置优化）。

- **病毒类事件分析与处置**

  勒索病毒分析：分析主机是否感染勒索病毒文件；根据漏洞攻击行为分析是否存在勒索病毒攻击等。

  挖矿分析：分析主机是否感染了挖矿病毒 / 木马；是否处于挖矿状态；根据漏洞攻击行为分析是否存在以植入挖矿木马为目的的漏洞攻击等。

  蠕虫病毒事件：确认文件是否被感染，定位失陷的代码。

  针对病毒类事件，提供病毒处置工具和有效处置措施建议，协助医院进行病毒查杀。

- **攻击行为评估**

  - **攻击行为检测：**
    工具和人工相结合，分析 SQL 注入、WebShell 上传、暴力破解等攻击痕迹，判断是否攻击成功，发现风险点。
  - **策略调优：**
    根据攻击特征调整防火墙、入侵检测系统（IDS）等防护策略。

- **失陷类事件分析与处置**

  失陷主机分析：对失陷主机进行分析研判，并给出修复建议。

  潜伏威胁分析：分析内网主机的非法外联威胁行为，判断是否存在潜伏威胁，如对外攻击、C&C 通道、隐藏外联通道等外联威胁行为，并给出解决建议。

  针对勒索、挖矿类事件：应主导处置工作，并进行最大程度溯源；定位恶意文件路径并提供查杀指导；并分析有无异常进程与服务，发现异常及时通知医院，并协助处置。

  针对后门脚本类事件：高级专家主导处置工作，提供专杀工具对感染服务器进行全面后门脚本查杀，并进行最大程度溯源。

  针对隐藏通信通道、可疑外发行为：提供实际佐证材料，进行最大范围溯源，并给出修复建议；配合定位异常进程以及恶意文件，并提供查杀建议。

6.3 服务持续运营阶段

持续运营阶段，是指围绕脆弱性、威胁、事件三个核心要素帮助医院开展持续化的安全保障工作，主要分为脆弱性管理、威胁管理、事件管理、安全通告以及定期总结汇报五个环节。

6.3.1 服务资产定期梳理流程

服务资产定期梳理，核心是医院配合服务商进行服务内的资产梳理，包括资产再识别、录入以及资产全生命周期的追踪管理，具体步骤如下：

- 变更监控：定期探测资产可用性及变更状态（如设备指纹变化），识别新增或异常资产。
- 变更响应流程：发现变更后自动触发工单，通知医院确认并更新台账，确保信息准确。
- 台账维护：定期与医院核对资产责任人、重要性等信息，动态维护可信资产数据库。

6.3.2 脆弱性管理流程

通过以下流程实现脆弱性（系统漏洞、弱密码等）的全生命周期管理：

图 6—2 脆弱性管理执行准则框架

- **漏洞扫描与数据同步**

  工具部署：部署脆弱性扫描工具，定期对服务器、网络设备、Web 业务系统等进行漏洞扫描，结果同步至托管服务平台。

  扫描策略：根据医院网络环境配置扫描频率与范围，避免影响业务运行。

- **优先级排序**

  工单确认：安全团队需确认漏洞工单，结合漏洞危害程度、资产价值及利用难度划分优先级。

  风险评级：高危漏洞（如可被直接利用的远程代码执行漏洞）需优先处置。

- **制定修复方案**

  方案输出：安全团队提供修复建议（如补丁下载链接、配置修改步骤），并通知医院责任人员。

- **安全加固实施**

  医院自主修复：常规漏洞由医院按方案自行修复；

高危漏洞联动防护：对无法及时修复的高危漏洞，通过防火墙规则、入侵防御策略临时阻断攻击路径。

现场支持：必要时协调服务商工程师协助处置，并将结果同步至平台。

- **修复验证与闭环**

进度跟踪：通过工单系统监控修复进度，逾期未处理时自动提醒。

复测确认：修复完成后重新扫描验证，确保漏洞彻底消除。

6.3.3 威胁管理流程

通过以下流程实现威胁的持续监测与闭环处置：

医院应要求服务商基于网络安全托管服务界面 + 云端专家托管模式，综合运用行业经验和威胁情报知识库，对不同安全组件设备的安全日志、流量进行聚合、关联分析，并通过对安全威胁的分析及定位，全面检测网络和主机中的安全告警 / 威胁。同时，托管服务团队应对识别到的威胁进行主动响应，采取措施降低威胁可能造成的影响，协助医院闭环处置安全威胁，并且通过对安全威胁的趋势分析，提供长期的安全改进建议。

图 6—3 威胁管理执行准则框架

在网络中部署网络侧、终端侧的安全组件，应配置安全策略收集安全日志，汇聚并同步到云端网络安全托管安全运营中心平台，触发相关流程，具体流程如下：

- **安全组件部署与日志聚合**

组件接入：在网络侧（如防火墙）和终端侧部署安全组件，加密传输日志至云端安全运营中心。

日志整合：聚合多源安全日志（攻击告警、流量记录等），为关联分析提供数据基础。

- **持续监测与告警生成**

自动化分析：平台基于规则引擎 7×24 小时分析日志，生成威胁告警及事件工单。

初步分类：按攻击类型（如 DDoS、WebShell 上传）自动划分工单优先级。

- **威胁分析与研判**

人工确认：安全团队结合威胁情报和响应剧本，验证告警真实性并评估影响范围。

处置建议：向医院推送威胁详情及处置方案（如封禁攻击 IP、隔离受感染主机）。

- **联动处置与闭环**

快速响应：联动防火墙、终端防护系统等设备自动阻断攻击，提升处置效率。

状态更新：处置结果实时同步至平台，更新威胁状态（如“已处置”“待复查”）。

- **策略优化与防护升级**

  策略检查：定期审查安全组件的防护规则（如 WAF 策略、入侵检测规则），确保有效性。

  动态调优：根据威胁趋势调整策略，例如新增针对高频攻击的阻断规则。

6.3.4 事件管理流程

通过以下流程实现安全事件的全生命周期管理，确保事件闭环处置与防护能力提升：

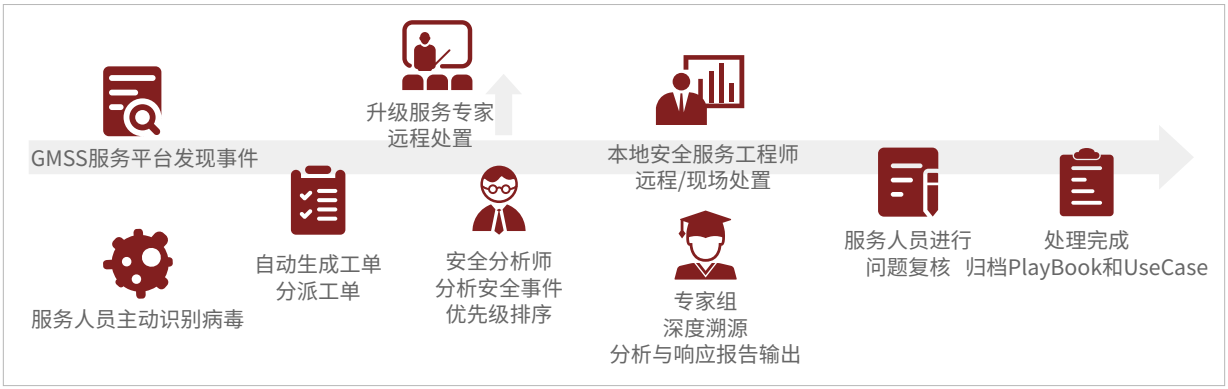


图 6—4 事件管理流程执行准则示例

- **事件调查与分析**

  7×24 小时响应：安全团队需提供全天候在线支持，对安全事件进行人工研判、影响范围分析及证据采集。

- **事件处置与闭环**

  快速联动处置：通过医院现有安全设备（如防火墙、终端防护系统）自动阻断攻击，或人工操作清除威胁。

  工单闭环：处置完成后标记事件工单状态，并将结果同步至托管平台。

- **影响抑制与恢复**

  业务恢复优先：通过隔离受感染主机、暂停高危服务等措施，快速降低事件对业务的影响。

- **威胁清除与根因分析**

  恶意文件清除：使用专用工具清除木马、后门脚本等恶意文件。

  攻击链还原：基于日志与流量数据，还原攻击路径并定位入侵入口（如漏洞、弱密码），生成溯源结果。

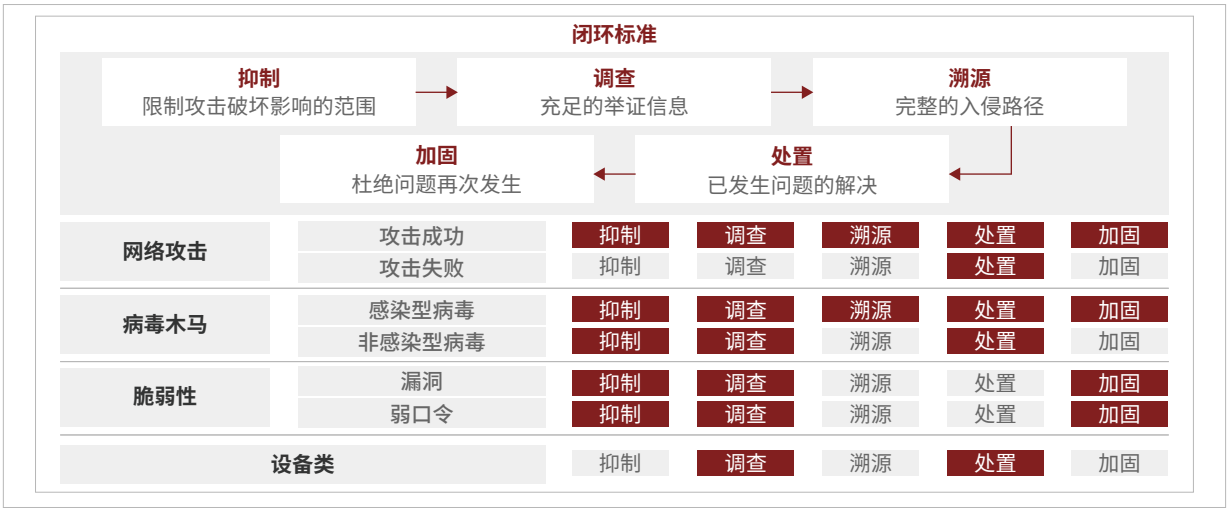
- **安全加固与防护优化**

  修复建议：提供漏洞修复、配置优化等加固方案，指导医院实施。

  策略调优：根据事件分析结果更新防护规则，防止同类事件复发。

- **知识库沉淀与复用**

  经验积累：将事件处置过程及方案录入知识库，为后续事件响应提供参考。



网络攻击	攻击成功	抑制	调查	溯源	处置	加固
	攻击失败	抑制	调查	溯源	处置	加固
病毒木马	感染型病毒	抑制	调查	溯源	处置	加固
	非感染型病毒	抑制	调查	溯源	处置	加固
脆弱性	漏洞	抑制	调查	溯源	处置	加固
	弱口令	抑制	调查	溯源	处置	加固
设备类		抑制	调查	溯源	处置	加固

图 6—5 网络安全托管服务事件闭环执行标准

八大闭环流程	
闭环方案对齐	基于实际业务环境，就典型类型事件后续协作机制达成一致
抑制	封锁 IP/ 封锁域名 / 隔离文件 / 隔离主机
调查	全局扫描 / 调查进程 / 调查启动项 / 调查计划任务 ..
溯源	分析设备日志 / 分析系统日志 / 分析 Web 日志 ...
处置	封锁 IP/ 查杀病毒 / 结束进程 / 清除异常项 ...
加固	策略调优 / 指导打补丁 / 指导修复漏洞 ...
跟进	主动跟进并提供帮助直至彻底闭环 ...
同步	同步处置进展、根因结论及最终的闭环结果 ...

图 6—6 网络安全托管服务闭环执行流程

6.3.5 安全通告流程

可通过以下流程实现威胁情报驱动的主动防护：

- **威胁情报预警**

  情报推送：实时同步云端最新威胁情报（如高危漏洞、行业安全事件），结合医院资产信息（操作系统、中间件版本等）进行精准匹配，推送风险预警。

  影响预判：通过资产指纹库判断潜在受影响范围，避免重复漏洞利用或攻击。

- **受影响资产排查**

  工具辅助检测：利用扫描工具验证威胁情报关联的资产是否受影响，并通知医院具体风险点。

- **漏洞处置指导**

  修复方案输出：提供补丁安装指南及临时规避措施（如防火墙规则调整），协助医院快速加固。

6.3.6 安全汇报流程

- **服务成果可视化**
  通过专属 WEB 门户及交付报告（如《安全运营月报》），以图表等形式展示资产风险趋势、漏洞修复率、威胁处置时效等核心指标。
- **周期性复盘与改进建议**
  每季度 / 年度对服务效果全面复盘，针对遗留问题（如未修复漏洞、防御短板）提出优化方案。
- **定期汇报机制**
  在关键节点（如季度末、年度总结）向医院汇报服务成效、风险态势及下一步计划。

6.4 服务终止阶段

6.4.1 服务验收

- **验收标准制定**
  医院需在服务开始前明确验收标准及通过条件，并与服务商达成一致。
- **验收会议**
  服务终止前召开验收会议，服务商汇报服务成果并形成会议纪要。
- **验收确认**
  医院签署《网络安全托管服务验收报告》，双方存档备查。

6.4.2 终止交接

- **材料交接**
  服务商需通过加密方式移交服务交付物及过程文档。
- **遗留问题与建议**
  服务商应整理需要持续跟进的安全问题及后续改进建议，提交医院备案。
- **工具与文件处理**
  删除医院本地部署的安全工具，或在不违反知识产权协议的前提下移交工具手册及使用权限。

6.4.3 权限回收

- **权限清理**
  服务商需移交或删除所有服务期间获取的账号权限（如设备账号、VPN 权限）。
- **设备配置还原**
  关闭日志上传通道，断开设备连接，还原防火墙策略、IP 白名单等配置。
- **组件回收**
  回收因服务期结束的而下线的安全设备组件，必要时应现场操作。
- **沟通群组处理**
  服务商备份即时通讯群组文件并保存 6 个月，双方备份后方可解散群组。

6.4.4 数据处置

- **数据迁移或删除**
  服务终止时，医院可要求将平台数据迁移至本地或立即删除。
- **默认清理规则**
  若无明确要求，服务商需在终止 6 个月后自动删除医院所有数据。

七、医院网络安全托管服务的监管

医院对网络安全托管服务的监管应以“合规导向、量化评估与实效验证、动态改进”为原则，建立多维度监督机制，对安全托管服务商的质量保障措施进行考察，对服务成果和效果进行全程监督考核，确保 MSS 服务商能力与医院安全需求精准匹配，并持续满足医院业务变化对应的安全要求，实现医院既定的安全目标。

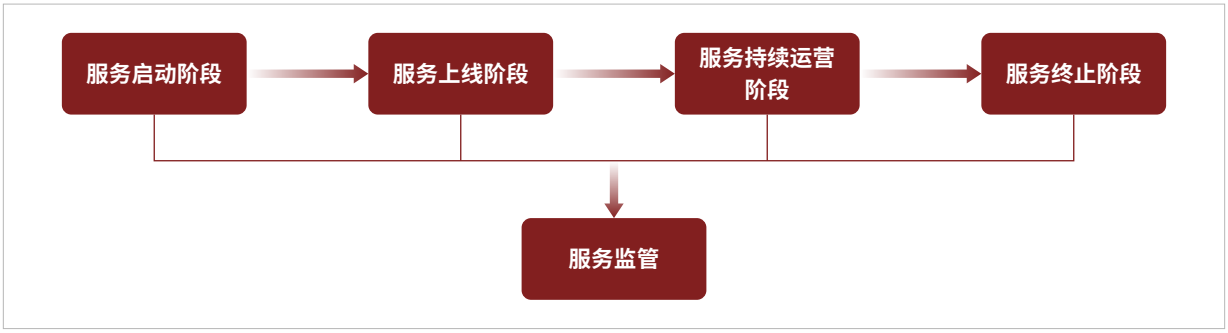


图 7—1 医院网络安全托管服务监管

7.1 监管原则

- **合规导向原则**
  以国家法律法规、行业标准及医院安全管理制度为基准，通过定期检查服务商交付成果、交付物文档完整性、服务流程，确保安全托管服务全生命周期符合合同约定与要求。
- **量化评估与实效验证原则**
  采用量化指标（如高危漏洞防护率、平均确认时间、平均遏制时间、平均闭环时间、安全事件闭环率等）评估安全运营效果，并结合医院对安全实战效果的总结梳理，重点考核服务商在威胁监测、漏洞治理、应急响应等环节的实际成效，确保安全投入转化为实质性风险管控能力。
- **动态改进原则**
  实施服务质量的动态跟踪管理，通过阶段性复盘、年度验收考核等机制持续评估服务商更新迭代的能力，并通过制定服务计划等方式，推动服务商不断改进服务，促进双方安全能力的协同进化与可持续发展。

7.2 质量保障

为规范服务交付并保障效果，托管服务需建立以下质量保障机制：

- **独立质量管理团队**
  设立独立于交付团队的质量管理团队，负责服务全流程监督与检视。
- **质量规范与考核**
  制定服务交付规范、分级问题管理措施及考核机制，并对交付团队定期培训。
- **质量评估指标**
  设计科学指标（如服务指标达成率、漏洞修复时效）客观评估服务质量。
- **定期检视与改进**
  质量管理团队需定期检查服务指标执行情况，优化服务流程，提升安全能力。
- **质量红线与处罚**
  明确服务质量红线标准及违规处罚措施。

7.3 监督考核

医院需建立监督考核机制，涵盖以下内容：

- **服务指标监督**
  医院监督服务商通过 WEB 门户、移动端等实时展示的服务指标达标情况（如响应时间、闭环率）。
- **服务评价与反馈**
  服务商主动提供便捷渠道（如工单系统、线上评分）供医院对具体服务项进行评价。
- **满意度调查**
  医院定期开展满意度评估，及时对服务效果、体验及人员进行效果反馈。
- **安全资质监督**
  医院可要求服务商提供有效等级保护测评报告、资质续证证明，服务商在更新安全资质时应主动向医院提供最新资质文件。

八、安全托管典型应用场景

8.1 典型应用场景介绍

- **常态化安全运营**
  通过线下网络侧设备具备入侵防御、网关杀毒、WEB 应用防护，终端侧防护软件的勒索、挖矿等顽固病毒木马的专项查杀、策略调优及其他安全功能，结合网络安全托管服务的线上可持续生长的安全能力与安全运营整体情况可视化展示，以及线上安全专家 7*24 小时值守主动评估风险、监测与响应事件等服务内容，覆盖医院常态化安全运营场景，实现对医疗卫生行业常见安全事件的有效防御，如层出不穷的变种勒索病毒与挖矿木马等，保障医疗服务正常运行。为避免包括勒索病毒在内的安全事件造成经济损失，可结合网络安全保险方式增加常态化的损失兜底能力，进一步强化安全运营效果。
- **安全通报预防与响应**
  随着各单位均在积极履行网络安全通报职责，通报工作呈现通报检查方式更多样、通报内容更广泛、通报频率更高、处罚更严厉等特点。医院应加强重视，化被动为主动，了解自身安全风险、弥补安全短板、建设常态化通报应对能力，有效配合好监管单位和主管单位的通报工作，进一步提升医院网络安全保障水平。
- **勒索预防与响应**
  医院的业务系统涉及大量患者、医药等敏感数据，容易成为勒索团队的重点攻击对象。通过网络安全托管服务覆盖勒索病毒防御及响应的场景，做好 7*24 小时的持续监测和值守，避免勒索团队攻击医院关键信息资产带来的重大影响和损失。
- **攻防实战演练及重要时期保障**
  医院往往会被列为攻防演练重点检验目标，因此需要积极部署、主动应对，在实战演练前、中、后均有完善的工作流程进行安全保障，具备快速监测与响应各种安全攻击和事件的能力。同时，医院应以实战攻防演练为契机，实现实战攻防能力由“战时”向“平时”的转化，全面提升常态化的安全防护能力。
  在医院的重要时期，例如国家两会、重大活动、国庆、春节等重要节日，以及医院关键业务测评时期，如医院等级评定、互联互通测评、电子病历评级等期间，通过网络安全托管服务做好 7*24 小时安全保障和值守，避免黑客对医院关键信息资产造成影响。

8.2 医院最佳实践介绍

华中科技大学同济医学院附属同济医院

- **背景介绍**

华中科技大学同济医学院附属同济医院（以下简称“武汉同济医院”）始建于 1900 年，是一所集医疗、教学、科研为一体的三级甲等医院，综合实力居国内医院前列。

- **需求描述**

1、安全设备“上架配置即终生”：医院信息人员没有精力频繁更新防护策略和规则库，导致无法检测出新型病毒和威胁，也无法防护新业务资产。

2、安全风险不断累积：没有对信息资产进行全生命周期的追踪管理，导致隐形资产、“老、隐蔽、难修复”的漏洞越积越多。

3、安全工作繁杂耗费人员精力：医院信息人员不仅要大力投入信息化建设，也要经常处理设备巡检、日志分析等安全工作，无暇对不同设备产生的告警进行联动分析。

4、事件通报较多且响应不及时：面对真实攻击时缺乏相应的流程和应急机制，导致医院信息人员处置滞后，容易被通报批评。

- **解决方案**

在长期探索中，武汉同济医院将网络安全“常态化运营”作为其新一代安全建设的理念，大胆尝试，稳步推进安全运营建设工作，以“平台 + 组件 + 服务 + 流程“四位一体的建设模式，最终搭建起了 7*24 小时实时守护的“网络安全运营体系”。

1、提前预防：定期清除业务系统安全风险

医院的业务系统数量多且交互复杂，日常由云端安全专家对医院资产的脆弱性、威胁持续管理和追踪。信息中心根据云端安全专家定期扫描出的资产变动、弱口令、漏洞、威胁，及时进行设备策略优化、资产指纹库更新、老旧系统风险清除等工作。云端专家持续复测进一步确保了风险清除工作的有效。

2、加强了对勒索病毒的提前预防

基于合作的安全厂家多年来对勒索病毒家族和勒索行为的大数据分析，总结出百余项勒索检查项 Checklist，并由云端专家定期按照 Checklist 展开深度排查，助力武汉同济医院提前排查勒索病毒，排除勒索病毒隐患。

正是武汉同济医院在安全运营中对“资产、脆弱性、威胁、事件”的持续管理，早于攻击者发现并处置了数个安全风险，避免“带病运行”，才在大型攻防演练中多次获得最佳防守单位的殊荣。

3、持续有效：提高安全事件闭环效率

在多个重要活动时期，面对几十万的网络攻击下，打通平台、组件、服务，打造出一套高效的事件管理流程——7*24 小时监测、分钟级响应、溯源分析、启动应急预案进行闭环处置。在云端专家全天候的监测值守下，不再滞后于监管通报。AI 安全感知平台和云端专家的线上快速研判、通告攻击、溯源分析，辅助信息中心快速利用安全组件进行攻击阻断和防御，根据提前制定的应急预案快速拉通医院内部人员处置、决策。实现 10 分钟内响应、2 小时内 100% 闭环处置攻击！

4、实时可视：随时掌握安全态势

安全需要持续有效，也需要可视可控。同济医院利用安全感知平台和安全运营专家做到了省心掌握安全态势，在日常运营中不断优化安全防护策略、提高安全管理效率，为全院的信息化布控和决策助力。

- **上线效果**

如今，武汉同济医院的常态化安全运营已经结出累累硕果：零重大安全事故、零监管通报，并多次获得省实网攻防演习“最佳防守单位”，对于武汉同济医院来说，这个结果绝不是“临阵磨枪”。在过往的春节、国庆假期、二十大等网络攻击密集时期，频频有医院失守。武汉同济医院作为全国排名靠前的三级甲等医院，往往遭受着黑客最猛烈的火力，却始终以“零网络安全事故”保障着医院业务稳定运行。

未来，武汉同济医院会打造更多的安全实践，并依托数字化安全底座，让智慧医疗更稳定、更安全！

复旦大学附属中山医院

- **背景介绍**

复旦大学附属中山医院，始建于 1936 年，为纪念中国民主革命先驱孙中山先生而命名，是三十年代由国人自己创办的一所规模较大的综合性医院，是一所三级甲等综合医院，医院在心脏、肝脏、肾脏、肺脏、消化道、泛血管等领域的临床能力处于国内顶尖、世界先进水平，拥有众多国家临床重点专科建设项目和上海市“重中之重”临床医学中心。

近年来，组织机构面临的监管侧实战化、常态化安全检查越来越严格。与此同时，我国承办的国内外重大会议越来越多。医院作为民生组织，重大活动期间的网络安全保障成为了安全建设工作的重中之重，中山医院作为国家重点医院，网络安全的保障成为所有业务开展的基石。

- **需求描述**

在当前数字化时代，医院的信息系统承载着患者数据、医疗记录、财务信息等众多敏感数据，其安全性直接关系到患者隐私保护、医疗服务的连续性和医院的整体声誉。

1）漏洞与威胁管理深入挑战：对资产现存的漏洞、面临的威胁无法做到 100% 识别处置，如在重要节日、活动期间被人利用，将造成无法挽回的损失。

2）黑客攻击手段的日新月异：外部黑客技术的快速更迭、复杂多变的攻击手段、智能化的攻击工具都不断增大防守难度，对防守人员的安全知识和处置经验提出了更高的要求。

3）跨院区安全管理需求：医院有东西两个院区，各院区资产众多，缺少整体的安全监控中心，难以形成有效的安全管理机制。

- **解决方案**

通过可扩展检测与响应平台 XDR+ 端点安全管理 aES+ 网络安全托管服务的整体解决方案，中山医院在重保时期，通过对运营中心流量日志以及外部威胁进行 7*24 小时监测，缓解中山医院运维人员的值守压力。在有外部攻击时，安全运营平台及时响应，通知云端高级专家进行深度分析研判，联合中山医院运维人员根据前期制定的应急预案那进行快速响应、实时攻击对抗、实时策略调优，以高阶专家的安全能力 + 平台的经验弥补医院的安全“短板”。

- **上线效果**

  - **云地协同助力医院安全闭环**

  服务上线后，云端服务经理实时在线，基于云端大量实战经验积累，提供准确分析能力，微信群中实时通告，一定程度上缓解了医院 IT 人员的工作负荷。医院只需要做好人员的管理，通过“云地协同”机制，由云端提供专业的分析、研判，输出可落地处置建议，由本地驻场根据云端输出的结果进行落地闭环，形成良好配合，高效闭环日常安全事件。

  - **夜间紧急通知应急，真 7*24 小时守护**

  云端监测到安全事件存在异常行为，夜间紧急通知医院安全负责人，院方安全负责人迅速赶赴现场协助配合。云端第一时间对威胁进行遏制，防止其进一步扩散，本地做好风险面管理及横向扩散排查，避免造成更大损失。保障医院第二天正常医疗业务的开展。

- **跨院区统一安全管理**

  通过整合两院区的安全资源，建立统一的安全运营中心，实现对全院资产的安全情况集中监控和管理，打破信息孤岛，提升安全管理效率；并通过自动化编排工具 SOAR 将日常安全事件流程化标准化，做好事件留存沉淀安全知识。

盐城市第一人民医院

- **背景介绍**

  盐城市第一人民医院创建于 1948 年，历经七十余年的发展，现已成为一所集医疗、教学、科研、康复、急救为一体的国家三级甲等综合性医院。

  随着智慧医院建设不断推进，盐城市第一人民医院近年陆续上线了不少互联网医院的业务系统，内网生产业务不得不与外网业务进行打通，实现数据互访。面向公众的互联网诊疗服务暴露在公网，频繁遭受网络扫描攻击，医院十分担心互联网业务的安全防护效果，希望以最小的成本提升整体的网络安全防护效果。

- **需求描述**

  医院的互联网业务不仅面临来自公网的扫描攻击，还会定期接受网络安全主管单位的人工渗透式的安全检查，导致医院承受较大的安全运维压力，尤其是缺少安全专业人才，缺失夜间和节假日的安全值守，导致医院安全运维较为被动，往往投入较多工作精力，但各类安全问题时有发生。

  - **内外业务打通以往静态防御被打破**

    盐城市第一人民医院此前按照等级保护的基本要求，对医院内网业务系统进行了比较完善的安全建设。随着医院不断上线互联网医院等业务系统，导致越来越多的互联网业务与内网业务、数据库进行打通，原本相对稳定的内部安全环境被打破，需要在互联网侧补齐安全建设能力，并伴随外网业务的变化，不断调整安全策略，优化安全防护效果。

  - **安全运维考验人的技术能力和时间精力**

    医院前期按照等级保护三级进行采购了各类安全设备。不同品牌、不同类型、不同部署位置的安全防护设备往往对同一安全事件有不同的安全告警，导致人工溯源分析难度大大增加。另外，医院的业务需要 7×24 小时稳定运行，而复杂的安全攻击往往发生在夜间和节假日。在控制预算的大背景下，医院面临如何通过高性价比方式实现 7×24 小时的安全效果。

  - **终端安全问题反复出现难根治**

    医院的医护工作站和行政办公终端数量众多，安全运维人员经常通过流量分析设备、网关防护设备发现特定终端存在安全风险，通过杀毒软件的管理平台下发查杀策略。虽然杀毒软件能够发现并查杀病毒，但其他安全设备仍提示安全风险存在，多次反复操作仍无法确定具体的安全问题，导致安全运维工作耗费大量精力。

- **解决方案**

  建设面向医院整体的安全运营平台，分区部署流量分析探针持续监控医院内网、外网的流量行为，并汇集分析边界防火墙、终端杀毒软件、合规审计设备的安全告警日志，进一步汇集分析形成安全事件，自动化实现溯源与联动处置能力。结合第三方的远程网络安全托管服务，实现对夜间、节假日以及重大活动时期的网络安全值守，并通过规范的协同机制，协助医院持续改进安全防护策略，使得漏洞利用、病毒感染等安全问题持续改进，高效提升医院整体的安全防护效果。

  基于互联网区业务的安全风险评估结果，建设互联网的安全防护技术体系，包括借助应用交付设备实现对 SSL 业务的流量解密，便于其他安全设备进行流量监测分析。考虑到互联网业务面临较大的安全风险，医院在互联网业务主机上部署终端检测响应 EDR，对操作系统的进程、文件操作、网络外联、注册表修改、服务运行等行为信息进行全方位采集，从而实现对 WebShell 上传、勒索病毒攻击等高级威胁的防护效果。

- **上线效果**
  - **风险驱动，持续提升整体安全建设效果**
    远程托管服务平台通过对现网安全告警、流量行为、外部最新漏洞、恶意攻击威胁进行持续评估，给出当前医院整体安全建设存在的防护短板，并提出整改建议，并通过工单等方式，确保在服务期内整改落地。
  - **云地协同，更低成本实现 7×24 小时持续运营**
    本地驻场工程师与云端线上专家协同配合，实现对本地安全运营平台的各类安全告警进行统一分析，并结合全球海量威胁情报，发现内部隐藏的安全风险，有效弥补了医院本地在夜间、节假日和重大活动时期技术人才短缺的问题。
  - **精准联动，彻底根治终端安全威胁**
    主机上安装的 EDR 软件采集了各类信息，使得安全运营平台可以将网络侧发现的恶意流量和终端上的恶意文件、恶意进程以及其他操作行为进行关联，实现恶意文件精准定位，恶意进程阻断遏制以及主机安全攻击故事线自动还原等高级能力。同时，安全运维平台为运维人员提供自动化编排能力，通过预先配置不同安全事件处置的场景化剧本，即可实现自动化处置效果，大大提升安全运维效率。

场景最佳实践——北京大学肿瘤医院

- **医院介绍**

  北京大学肿瘤医院（北京肿瘤医院、北京大学临床肿瘤学院、北京市肿瘤防治研究所）始建于 1976 年，是一所由北京大学、北京市医院管理中心共管的三级甲等肿瘤专科医院。被国家卫健委授予首批肿瘤多学科诊疗试点医院、国家首批肿瘤高通量基因测序临床试点单位；是唯一承担北京地区癌症发病登记与生存统计，并向政府及 WHO 提供数据的中心。全年门诊量达 75 万人次，年收治病人 9.6 万人次，手术 1.7 万例; 在这里，每天都进行着生与死的抗争，很多人不远万里，来这里寻求生命的希望。

- **现状描述**

  癌症的治疗是一场持久战，很多患者需要进行多轮的放疗、化疗，治疗结束后也要定期复查，需要频繁地来回复诊。2019 年，北京大学肿瘤医院日均门诊量约为 3000 人次，其中 70% 的患者来自外地。再加上疫情的爆发，上线互联网诊疗成为了必然的选择。

  打开“北肿云病历”APP，患者就来到了“线上门诊”。绑定个人信息，点击“在线复诊”，完成预约申请后，患者即可排队候诊。通过视频，患者与医生的问诊过程被搬到了线上。互联网诊疗破解了空间限制的问题，同时让广大患者在频繁的复诊就医过程中享受更大的便利。

  但互联网诊疗给广大患者打开一扇门的同时，也给黑客攻击打开了一扇窗。过去，医院的核心业务系统都运行在内网中，随着互联网诊疗的重要性日益提升，外网已然成为医院的重要生产系统。

  但网络攻击无孔不入，尤其是近年来勒索病毒、数据泄露等恶性事件频发，网络安全问题成为了悬在医院头上的“达摩克里斯之剑”。

- **需求描述**

  对于国内不少医院而言，网络安全能力要求高、专业人员不足一直以来都是一个棘手的难题，尤其是专职的安全专家，对很多医院来说都是“奢侈品”。北京大学肿瘤医院也不例外。

  - 1）由于专职安全人员的缺乏，北京大学肿瘤医院此前采用的是定期安全运维服务模式，即每个月针对院内安全产品做巡检，有问题时通过第三方运维人员远程服务 + 现场服务的模式进行解决。医院发现这个运维过程中存在很多漏洞点，技术人员和第三方运维需要下班休息，黑客的攻击却是 7*24 小时的，且专挑防护薄弱的时间下手。

- 2）此外，由于缺少长期的、统一的安全运营机制，整体安全建设的效果并不理想。医院存在各种异构品牌的安全设备，导致日志分散、割裂且告警量巨大，这也对驻场人员的安全专业度提出了非常高的要求。面向大量的告警日志，现有技术人员很难对真实事件进行高效、准确的研判，整体防护过程中较为被动。
- 3）信息科衡主任说“网络安全事件往往发生得非常快，需要我们马上能够应对，对安全人员的要求很高。我们也在寻找一种办法帮助我们实现 7*24 小时值守”，面对网络安全的重重压力，北京大学肿瘤医院也在思考，有没有一种方式能够快速补齐专业安全能力的短板，并且在此基础之上实现 7*24 小时的不间断的值守。

解决方案

这时候，网络安全托管服务进入了北京大学肿瘤医院的视野。在深入沟通了解之后，医院果断进行了尝试，最终效果也达到了医院的预期。

简而言之，网络安全托管服务是以保障风险管控效果为目标，以“人机共智”模式为手段，以 7*24 小时持续在线守护为主线，以【资产、脆弱性、威胁、事件】四个核心安全风险要素为抓手，帮助北京大学肿瘤医院提升安全风险管控能力和安全工作效果。

通过 7*24 小时的“人机共智”安全运营服务，联动云端安全专家和线下驻场服务人员配合共同处置安全问题，很好的完善了北京大学肿瘤医院整体的安全运营闭环机制。

上线效果

在网络安全托管服务的助力下，北京大学肿瘤医院网络安全防护压力得到了一定程度的缓解，这让医院信息部门在宵衣旰食的数字化建设中解除了“后顾之忧”，也让医信工作者有更多精力投入到直面临床、直面业务、直面患者服务的工作中。主要体现在以下几个方面：

7X24 小时主动防御，让安全风险无处遁形

网络安全托管平台能够 7×24 小时不间断收集医院网、端两侧上传的告警日志，并借助机器学习引擎与异常行为分析引擎，在海量的日志中准确识别勒索病毒、APT、钓鱼等高级威胁及异常行为，并自动发出预警。
此外，借助网络安全托管服务 400+ 云端实时在线的高级安全专家，还能在平台告警基础上进一步分析研判，确保攻击威胁和事件是真实发生的。云端安全专家还能利用平台提供的各类工具，协助医院线下运维人员一道加速事件的闭环处置，帮助医院提升和完善现有安全体系建设能力，有效解决了医院专业安全人员不足的难题。在网络安全托管服务的加持下，不管是医院内网还是外网的重要资产，都实现了安全主动监测；不管是白天还是深夜，平日还是节假日，都实现了持续检测与快速响应，实现平均 5 分钟响应、10 分钟遏制、事件闭环率 100%。

实战见真章，安全防护能力实现质的飞升

近年来，国家对于网络安全重视程度与日俱增，对医院的安全防护要求日渐严格。每年，各个相关单位都会面向医院组织多轮的网络安全“大考”。
借助网络安全托管服务，北京大学肿瘤医院迅速补齐了在弱口令等方面的短板，实现了安全防护能力的常态化提升。此外，在“大考”来临之前，医院也将实施开展针对性的专项排查，再次筛查风险并进行安全加固，确保各个业务系统已充分满足安全基线。实战见真章，在使用了网络安全托管服务之后，医院的安全防线在当年的网络安全攻防演练中经受住了重重考验，取得了非常不错的成绩，从过去的倒数第五名上升到了第二名。这也侧面体现了医院在实战防护能力上已取得质的飞升。

持续赋能安全人员，铸造网络安全更强防线

“人”往往是网络安全防护中最薄弱的一环。北京大学肿瘤医院在重视安全服务质量的同时，更重视自身医院安全能力的沉淀，安排多名医院工程师参加安全能力培训，不断提升安全专业能力，并取得了 CISP（ 注册信息安全专业人员）的资质，不断提升安全人员专业水平，让整体安全运营水平趋于无懈可击。

九、附录

附录 A
网络安全托管服务保密协议示例

以下是网络安全托管服务人员与医院在服务期间，签署的安全服务保密协议的典型示例：

安全服务保密协议

甲方（服务接受方）：

乙方（服务提供方）：

甲乙双方经友好协商，根据《中华人民共和国民法典》及相关法律法规的规定，就乙方在为甲方提供安全服务的过程中可能获悉的甲方保密信息及为甲方保密事宜，达成如下协议：

1. 本协议所称“保密信息”是指：乙方基于为甲方提供安全服务所获取的甲方域名、业务系统等虚拟资产中所附带的或甲方安全设备上报的网络安全信息、以及医院数据和业务相关信息等。

2. 未经甲方书面同意，乙方不得以任何形式或任何方式将保密信息和 / 或其中的任何部分，披露或透露给任何第三方。乙方有义务妥善保管保密信息，不得擅自复制备份，并应避免泄露或遗失。乙方亦不得依据保密信息，就任何问题，向任何与甲方所需安全服务无关的第三方做出任何建议。

3. 甲方同意乙方有权因提供服务的必要，而向其安全服务人员透露或允许其接触保密信息和 / 或其中的任何部分，同时，乙方承诺该等服务人员在提供服务的过程中将对其所接触的保密信息承担与本协议同等的保密义务。

4. 甲方有权在服务终止时要求乙方将所获悉的保密信息归还给甲方，不能归还的，应进行销毁处理。

5. 凡因执行本协议所发生的或与本协议有关的一切争议，双方应通过友好协商解决。如果协商不能解决时，任何一方可向被告所在法院提请诉讼。

6. 本协议保密期限为整个安全服务期间及服务期限截止后两年。

7. 本协议一式两份，自双方盖章之日起生效。

甲方： **乙方：**
（印章） **（印章）**

附录 B
网络安全托管服务对医院日志数据的使用和保护说明示例

由于网络安全托管服务需要采集部署在医院本地的安全组件的安全告警日志，因此需出具对医院安全日志数据所采取的严格保护措施的详细说明。

以下是一个典型的安全日志数据的使用和保护说明示例。

关于网络安全托管服务对医院日志数据的使用和保护说明

尊敬的医院：

网络安全托管服务（以下简称“MSS 服务”）需以服务组件的安全日志数据为基础，通过整合技术、专家和流程开展持续化的网络安全保障工作。本着对医院负责的态度和原则，为更好地保障医院的知情权以及同时确认医院授权同意，本文件再次对 MSS 服务期间可能涉及使用的日志数据信息以及对数据信息的保护进行说明。

一、网络安全托管服务所需数据类型及用途

- 以下说明的数据均仅用于为医院提供网络安全托管服务，不用于其他任何目的。
- 为提升安全事件检出率，以更好地对安全事件进行溯源分析，MSS 需要搜集网络攻击日志、流量审计日志、Windows 终端行为日志、终端安全日志、Windows 主机系统日志、Windows 主机状态日志以及其他安全产品分析得出的告警数据。
- 为实现事前预防，需要搜集漏洞扫描组件主动发现或安全设备被动发现的系统漏洞、WEB 漏洞和弱口令脆弱性数据，按照脆弱性危害进行优先级排序以及生命周期管理。
- 为实现安全事件深度溯源和未知威胁分析，需要搜集安全组件识别到的可执行文件样本以识别未知文件的安全性，检测其是否为恶意程序文件，文件样本会用于人工分析或沙箱自动化分析。

二、网络安全托管服务数据信息存储措施

- 网络安全托管服务仅在中华人民共和国境内收集日志数据，产生的数据信息将存储于中华人民共和国境内的服务器上。
- 针对不同医院使用网络安全托管服务期间提交的数据，网络安全托管平台将进行隔离存储，确保数据保密性。
- 针对网络安全托管涉及使用的安全类数据（如安全日志、告警数据、脆弱性数据等），为确保在发生安全事件时的溯源调查效果，网络安全托管将在医院提交该部分数据后存储 6 个月。前述设置的存储期限届满后相关数据会被自动删除。在存储期内，贵单位也可以根据自身实际需求通知网络安全托管服务人员取回或删除贵单位的数据信息。

三、网络安全托管服务的数据信息保护措施

3.1 网络安全托管服务的平台系统已通过公安部等级保护三级认证和 ISO 27001 认证。
安全认证将严格按照认证标准落实等级保护和安全要求，以切实保障贵单位的信息安全。

3.2 物理及网络安全

- 业务划分 DMZ 区和内网隔离区，网络入口及区域之间部署防火墙防护，并做严格的 ACL 访问及上网白名单控制，保证内外网安全。
- 生产网络与研发网络物理隔离，研发人员采用 VDI 方案，无外网访问权限。

- 生产内网部署安全流量检测平台，及时发现异常行为并处置。

3.3 主机及业务安全

- 主机上部署终端杀毒软件进行本地防护，并开启微隔离策略实现内网不同主机之间的隔离，保证主机安全。
- 网络安全托管服务平台基于 SDL 流程开发，对应用代码进行严格的安全测试，上线前会通过渗透测试，确保上线代码无新漏洞引入。线上系统定期进行漏洞扫描和外部渗透测试，及时发现新的漏洞并修复。
- 网络安全托管服务平台不对公网发布，通过登录 VPN 进行线上运营，并且 VPN 配置源 IP 白名单只对服务团队开放；VPN 和服务平台采用账号、短信验证码、硬件特征码等多重校验机制，确保账号安全。
- 服务人员使用云桌面办公，确保数据不外泄。
- 核心业务数据异地机房备份，确保发生事故时能够快速恢复。

3.4 数据传输及访问安全

- 网络安全托管服务采用 SSL 加密的方式采集日志数据，确保数据在传输过程中不因网络嗅探而泄露。
- 对医院的账号信息、电话号码、邮箱等敏感信息进行加密存储。
- 网络安全托管服务平台采用严格的权限控制策略，医院数据只对服务专家开放，数据使用范围仅限于安全事件分析和响应溯源。数据相关的操作过程也将被全程审计。

由于网络安全托管服务涉及使用的数据信息均来自于前述已说明的基础服务组件设备，在向贵单位提供设备使用时也已就相关医院信息保护政策进行说明并获取贵单位的明示同意，如对使用和保护贵单位的数据信息仍有其他疑问，贵单位可以具体查看设备后台的医院信息保护政策说明，或联系业务人员为贵单位解答。

感谢贵单位对网络安全托管服务的信赖与支持！

服务提供商
年 月 日

附录 C
网络安全托管服务内容清单示例

服务项	服务细则	详细描述	交付方式	交付物
服务上线	组件部署与接入	安全专家对需要接入MSS的组件（如漏扫工具/态势感知平台/边界防护设备/终端安全防护软件等）进行部署并接入至安全托管运营平台。	安全专家	/
	资产收集与录入	安全专家在上线前对服务资产进行收集，并将资产信息录入到安全运营平台中进行管理。	安全专家	《资产信息确认表》《项目启动会 PPT》
安全现状评估	策略检查	上线前安全专家对安全组件上的安全策略进行统一检查，确保安全组件上的安全策略始终处于最优水平，针对威胁能起到最好的防护效果。	安全专家	《首次安全风险分析报告》
	脆弱性评估	对操作系统、数据库、常见应用/协议、系统与Web漏洞进行漏洞扫描，弱口令扫描可实现信息化资产不同应用弱口令猜解检测，如：SMB、Mssql、Mysql、Oracle、smtp、VNC、ftp、telnet、ssh、mysql、tomcat等。	安全专家 + 安全组件	
	资产暴露面梳理	安全专家在上线前使用扫描组件对资产开展暴露面探测，以梳理资产面向互联网的开放情况，快速发现违规暴露在互联网中的资产及存在的风险并进行协助处置，实现对暴露面资产可管可控，降低暴露面资产的风险。	安全专家 + 安全组件	
	失陷类事件评估	勒索病毒事件分析：安服专家分析判断主机是否感染了勒索病毒，是否已感染勒索病毒文件，根据已发生的漏洞攻击行为分析判断是否存在勒索病毒攻击等。	安全专家	
		挖矿病毒事件分析：安服专家分析是否感染了挖矿病毒/木马，是否处于挖矿状态，根据已发生的漏洞攻击行为分析判断是否存在以植入挖矿木马为目的的漏洞攻击等。		
		蠕虫病毒事件：安服专家确认文件是否被感染，定位失陷的代码并进行修复。		
		失陷主机分析：安全专家对失陷主机进行分析研判（如恶意程序及后门脚本类事件），并给出处置及加固建议。		
		潜伏威胁分析：安全专家分析内网主机的非法外联威胁行为，判断是否存在潜伏威胁，并给出处置及加固建议。含：对外攻击、APT 、C&C通道、隐藏外联通道等外联威胁行为。		
	攻击行为评估	针对漏洞利用攻击行为、Webshell上传行为、Web系统目录遍历攻击行为、SQL注入攻击行为、信息泄露攻击行为、口令暴力破解攻击行为、僵尸网络攻击行为、系统命令注入攻击行为及僵尸网络攻击行为进行分析评估，判断攻击行为是否成功以及业务风险点。	安全专家	
安全问题处置	安全策略调优	安全专家根据安全威胁/事件分析的结果以及处置方式，对安全组件上的安全策略进行调整工作。	安全专家	《首次安全威胁分析问题记录表》《安全问题整改指导》
	脆弱性问题修复指导	针对资产脆弱性，安全专家分析研判后提供实际佐证材料，并给出修复建议。	安全专家	
	失陷类事件处置	针对服务资产的勒索、挖矿类事件。安全专家主导处置工作，并提供最大程度溯源服务（如涉及到重装业务系统，服务商提供重装指导）；安全专家定位恶意文件路径并提供查杀指导（授权情况下，可由服务商直接操作）；并分析有无异常进程与服务，发现异常进行通告（授权情况下，可由服务商直接对异常情况进行操作）。	安全专家 + 安全组件	

安全问题处置	失陷类事件处置	针对后门脚本类事件。安全专家主导处置工作，提供专杀工具对感染服务器进行全面后门脚本查杀，并提供最大程度溯源服务。	安全专家 + 安全组件	《首次安全威胁分析问题记录表》《安全问题整改指导》
		针对隐藏通信通道、可疑外发行为。安全专家提供实际佐证材料，并给出修复建议，提供最大范围的溯源服务。配合定位异常进程以及恶意文件，并提供查杀建议。		
	攻击行为处置	针对分析研判确认的入侵行为，安全专家给出策略调整建议。如果有可联动处置的边界防护设备等，在获得授权后，在服务时间内安全专家调整安全策略进行封禁。		
资产管理	资产指纹探测	持续服务过程中安全专家每季度对资产进行指纹（操作系统、中间件、软件厂商等信息）探测，并对指纹信息进行确认与更新，确保安全托管服务安全运营中心中资产指纹信息的准确性和全面性。	安全专家 + 安全组件	《资产信息确认表》
	资产变更管理	持续服务过程中安全专家每季度对资产进行存活性探测，当发现未存活资产或资产发生变更时，安全专家对变更信息进行确认与更新，确保安全托管服务安全运营中心中资产信息的准确性和全面性。	安全专家 + 安全组件	
脆弱性管理	漏洞扫描与验证	每月对服务资产的系统漏洞和Web漏洞进行全量扫描，并针对发现的WEB漏洞进行验证，验证WEB漏洞在已有的安全体系发生的风险及分析发生后可造成的危害。	安全专家 + 安全组件	《漏洞清单》
	漏洞修复优先级排序与通告	基于漏洞扫描结果、资产重要性及漏洞的威胁情报，对漏洞进行重要性排序，确定修复的优先级；并将最终结果通告给医院接口管理员。	安全专家 + 安全组件	
	漏洞可落地修复方案	对漏洞进行分析并输出可落地的修复方案，通过工单系统跟踪修复情况。	安全专家	
	漏洞复测与状态追踪	对修复的漏洞进行复测，及时更新漏洞工单的漏洞修复状态。	安全专家 + 安全组件	
	弱口令分析与管理	实现信息化资产不同应用弱口令猜解检测，如：SMB、Mssql、Mysql、Oracle、smtp、VNC、ftp、telnet、ssh、mysql、tomcat等。针对医院提供行业密码字典，有针对性的进行弱口令检测。并将检测发现的问题通过工单系统跟踪修复状态。	安全专家 + 安全组件	
	高利用漏洞防护	对于配备有可联动处置防火墙的医院单位，支持一键防护扫描组件发现的高可利用漏洞。	安全专家 + 安全组件	
威胁管理	7*24 小时威胁分析研判	基于云端安全能力平台，云端专家提供 7*24 小时的威胁监测：依托于安全防护组件、检测响应组件和安全平台，将海量安全数据脱敏，包括漏洞信息、共享威胁情报、异常流量、攻击日志等数据，经由大数据处理平台结合人工智能和云端安全专家使用多种数据分析算法模型进行数据归因关联分析，实时监测网络安全状态，对安全告警和威胁进行分析研判，并生成工单。	安全专家	/
	7*24 小时威胁通告	安全专家将云端分析确认后的真实威胁、事件实时通过微信、邮件等方式向医院接口管理员通告，并提供处置建议。	安全专家	
	威胁影响面分析	安全专家针对每一个真实的威胁和告警，进行深度分析验证，分析判断受影响范围及是否攻击成功，将深度关联分析的结果通过服务群 / 邮件等方式告知医院。	安全专家	《威胁情报通告》
	威胁协助处置	安全专家针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），并协助医院闭环。	安全专家	/

威胁管理	威胁情报管理	实时抓取互联网最新威胁情报与详细资产信息进行匹配，对最新威胁情报进行通告与排查，结合威胁情报，安全专家排查是否对服务资产造成影响并通知医院，及时协助进行安全加固。	安全专家	《威胁情报》
	高级威胁狩猎	安全专家每年可按需开展2次针对内/外网或特定业务系统及特定漏洞，基于医院业务定制检测逻辑，尽可能快地发现漏洞或攻击痕迹，发现潜在的安全隐患和已失陷的主机/被钓鱼成功的员工/账密信息泄露等，最大限度地降低攻击者造成的危害，评估造成的损失等内容，最终帮助医院验证风险并推动发现的问题和隐患进行闭环处理。	安全专家	《威胁狩猎报告》
	策略检查	每月安全专家对安全组件上的安全策略进行统一检查，确保安全组件上的安全策略始终处于最优水平，针对威胁能起到最好的防护效果。	安全专家	/
	策略调优	每月安全专家根据安全威胁/事件分析的结果以及处置方式，按需对安全组件上的安全策略进行调整工作。	安全专家	
事件管理	安全事件调查与分析	安全专家7*24小时在线服务，针对主机发生的安全事件开展调查分析和影响面分析，对发生的安全事件进行人工鉴定和举证分析。	安全专家	/
	安全事件处置与闭环	对医院网络内服务资产爆发勒索病毒、挖矿病毒、篡改事件、webshell、僵尸网络等安全事件，利用一些工具和脚本对恶意文件、代码进行根除，帮助医院快速恢复业务，消除或减轻影响，闭环事件工单。	安全专家	
	重大事件应急响应	事件影响抑制：通过事件检测分析，提供抑制手段，降低入侵影响，协助快速恢复业务。 入侵威胁清除：排查攻击路径、恶意文件，并清除。 入侵原因分析：还原攻击路径，分析入侵事件原因，提供安全事件溯源结果。 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。	安全专家 + 安全组件	《应急响应报告》
7*24 小时服务团队	专属服务经理	为医院配置一名经验丰富的安全专家作为专属服务经理	安全专家	/
	实时专家咨询	安全专家对医院咨询或上报的安全问题进行及时响应并给出建议，如主机加固建议咨询、安全事件处置建议咨询等。	安全专家	/
	节假日值守	安全值守专家进行7*24小时安全监测，对发生的安全事件进行及时响应并在节假日期间每日进行值守总结，在服务群发送值守总结快报	安全专家	节假日值守快报（微信群）
运营成果可视	安全运营周报	安全专家每周对服务资产进行安全运营情况的分析总结并输出《安全运营周报》。	安全专家	《安全运营周报》
	安全运营月报	安全专家每月对服务资产及整体安全状况进行分析总结并输出《安全运营月报》。	安全专家	《安全运营月报》
	安全运营季度汇报	安全专家每季度总结阶段性安全运营情况并输出《安全运营季报》发送给医院，向医院进行远程或线下总结汇报。	安全专家	《安全运营季报》
	安全运营年度汇报	安全专家总结年度安全运营情况并输出《年度总结报告》发送给医院，向医院进行总结汇报。	安全专家	《年度总结汇报》
	医院 portal	可视化Portal支持随时查看服务范围内业务资产安全状态。	医院 portal	/
		支持在线展示所有脆弱性、威胁、事件工单的处置进程和结果		
		支持医院在线对服务SLA进行查阅和监督。		

附录 D

附录 D 为《医院网络安全托管服务合同》的部分内容示例，对应第五章的主要内容，仅供医院参考，详细内容请结合实际情况补充修订。注释内容（斜体）仅供参考，正式签署前请删除。

医院网络安全托管服务合同（示例）

合同编号：

签约日期：

甲方： _____

地址： _____

电话： _____

传真： _____

邮编： _____

乙方： _____

地址： _____

电话： _____

传真： _____

邮编： _____

鉴于甲方有意采购安全托管服务，用于自身网络系统建设或安全维护，经与乙方协商一致，同意按照中华人民共和国有关法律法规的规定签订本合同。

第一条 合同标的

1. 甲方向乙方采购本合同项下安全托管服务的具体清单及服务内容详见附件《服务采购清单》。（注：《服务采购清单》内容可参考本指南附录 C）

2. 甲方所购买之服务提供完毕后，需要乙方继续提供服务的，双方可另行签订服务合同。

3. 服务内容要求中如有关于 SLA 的约定，以附件《SLA 协议》内容或双方书面约定为准。（注：《SLA 协议》内容可参考本指南第 4 章第 5 小节）

第二条 支付条款

1. 本合同项下的服务费用金额（含税）总计￥ _____ 元（大写：人民币 _____ ）。

2. 本合同签订后，甲方须在___个工作日内向乙方支付全部款项，乙方应向甲方开具相应金额的合规增值税发票（税率 6%）。

第三条 双方保证

（一）甲方：

1. 甲方保证其有能力及资格签署本合同并授权乙方提供本合同项下安全托管服务，并保证向乙方提供的授权 / 声明文件及所有相关数据资料在整个授权服务期间均真实、合法和有效。

2. 甲方保证签署本合同时已充分理解乙方提供的服务内容，知悉相关可能性风险，并同意授权乙方为提供服务之必要收集及处理相关信息。

3. 甲方应在服务的各个阶段配合乙方进行协调和管理，包括但不限于及时向乙方提供必要的工作环境、资料信息及其他必要协助。

4. 对服务账户和验证码进行有效的管理和保护，避免无权限人员对服务账户进行非正常操作。

5. 为实现服务目的，乙方有可能为甲方提供安全服务期间所需的配套硬件设备，此设备由乙方运用专业技术手段方可使用，并构成乙方提供服务所使用的工具；硬件设备虽然安装在甲方所在地，但硬件设备的所有权和使用权均归乙方所有。甲方应于服务期届满时配合乙方拆除并回收该设备。如因甲方原因造成乙方设备损坏或灭失，甲方应按乙方设备公开报价予以赔偿。

（二）乙方：

1. 乙方保证所提供的安全服务符合相关技术规范要求，所指派的专业人员均有能力按照本合同约定完成服务交付相关事项。

2. 乙方应严格按照本合同约定或甲方授权或知情同意的范围提供服务，服务过程中应注意保护相关信息系统及数据的安全。

3. 乙方应按约定交付相应的服务文档，如合同终止或解除，乙方应配合进行相关文档资料的移交。

第四条 知识产权条款及保密条款

1. 甲乙双方应互相尊重对方的知识产权和商业秘密。如甲方对于项目保密有特别要求的，甲乙双方均应严格按照特别要求执行。

2. 乙方为甲方提供服务及交付相关服务成果并不意味着乙方向甲方转让或授权许可使用任何乙方自主拥有或已获第三方许可的知识产权；甲方应注意保护乙方交付的相关文档中可能包含的乙方的商业秘密或技术方案等内容，未经乙方同意不应向其他任何第三方披露。

3. 乙方应对提供服务过程中获取或知悉的甲方保密信息履行严格的保密义务，非经甲方同意不得向第三方披露，并不得用于提供服务以外的其他任何目的。

4. 一方可仅为本合同目的向其确有知悉必要的雇员披露对方提供的保密资料，但同时须指示其雇员遵守本条规定的保密义务。一方因法律法规的强制性规定或政策要求须披露相关信息的，应尽可能提前通知披露方，使其得以采取其认为必要的保护措施。

5. 本合同所述应予以保密的信息不包含属于以下情形的内容：

(1) 并非因接收方的过错而已经进入公有领域的；

(2) 已通过接收方的有关记录证明是由其独立开发的；

(3) 由接收方从没有违反对披露方的保密义务的一方取得的。

第五条 违约责任

1. 乙方应依约履行合同义务。乙方所交付安全服务不符合本合同约定的，乙方应予以补救。如因乙方原因给甲方造成损失的，乙方应按甲方的直接经济损失进行赔偿。

2. 甲方应按本合同约定的时间付款，甲方逾期付款应每日按未支付款项金额的_____的标准向乙方支付违约金。如延迟付款时间超过 15 日，乙方有权终止对甲方的服务承诺。

3. 甲方违背本合同第三条所述保证，乙方有权自发现甲方违背保证情形之时起中止服务（服务期限不予顺延）。若甲方在约定期限内仍未履行相关保证义务，乙方有权单方解除合同。乙方因此解除合同、终止服务的，不免除甲方的付款义务；乙方因甲方违约事由受到第三方追责的，由甲方承担全部损失的赔偿责任。

4. 甲乙双方均一致同意，因境内外基础电信运营商的通讯线路故障或其他各种不可抗力原因而导致的任何损失，双方均无需向对方承担违约或损害赔偿责任。

5. 如乙方所交付的安全服务不符合附件《SLA 协议》（如有）相关要求时，应按照《SLA 协议》承担相应责任。

第六条 通知与送达

1. 为方便开展工作，提高双方的工作效率，甲方安排 _____（联系方式：_____）负责与乙方保持日常联系，乙方安排 _____（联系方式：_____）负责与甲方保持日常联系。

2. 任何一方的联系人或联系方式如需变更，应以书面形式提前通知对方，因未及时通知而造成的损失由责任方自行承担。

第七条 争议解决

与本合同有关的一切争议，双方应首先通过友好协商解决，如协商不成，任何一方可向 _____（原告方 / 被告方）所在地人民法院诉请解决。

第八条 合同生效及其它

1. 本合同自双方盖章之日起生效，一式贰份，双方各持壹份，每份具有同等法律效力。

2. 如有相关未尽事宜，或需对合同内容作任何修改或补充的，双方可在协商一致后签署书面的补充协议进行约定，补充协议生效后即成为本合同不可分割的组成部分。

3. 除双方另行协商一致外，因非乙方原因导致服务提前终止的，乙方有权不予退还服务费用。

4. 双方同意并认可：一方或双方在签约时使用电子签章的，与实体签章具有同等法律效力。同时，传真件、打印件、复印件、扫描件与原件亦具有同等法律效力。

5. 附件：《服务采购清单》《SLA 协议》（如有）。

（以下为签署页，无正文）

甲方（盖章）：

法定代表人 / 授权代表（签字）：

乙方（盖章）：

法定代表人 / 授权代表（签字）：