## 附件二、招标参数

## 一、安全服务需求

## 1.1 安全运维服务

常规的安全服务工作应该形成一个巡检、加固、应急的安全闭环。通过定期的加固和巡检不断增强安全防护能力，消除新的安全隐患。在安全事件发生时，通过有效的应急处理机制，最快速恢复系统的保密性、完整性和可用性，阻止和降低安全威胁事件带来的严重性影响，建立立体化防护体系。

### 1.1.1 安全巡检服务

可根据用户需求定制巡检周期，一般巡检的周期每季度一次。设备巡检的目标是通过该项工作，了解信息系统的运行健康状态，使IT管理人员清楚信息系统的运行情况，信息系统稳定性。技术人员进行设备巡检有三项主要工作：

检查各项IT基础设施（云服务器、安全设备、网站应用、数据库等），查看设备的各项运行指标是不是正常，查看各项设备硬件运行状态是否正常。

查看各项安全设备的软件版本（如操作系统补丁、防病毒系统病毒库等）是否升级，并在得到IT管理人员同意的情况下协助对各项内容进行升级。

利用现有的运维管理系统记录各项基础设备的历史数据，对信息系统的运行规律进行分析。分析信息系统在各周期各项IT基础设施的运行基线，使IT管理人员能了解信息系统运行的各种情况，及时合理的调整各项IT资源分配，保障信息系统稳定运行。

一年提供4次安全巡检服务，每季度巡检一次。

巡检完成后需在一周内提供安全巡检服务报告。

### 1.1.2 安全加固服务

系统安全加固（SystemSecurityHardening，SSH）是专门针对由各类服务器及主机统构成的混合型信息网络环境的安全性而提供的一项专业服务。为了消除现有的安全漏洞，安全加固服务主要包括以下主要内容：

审核系统当前及实施加固之后的安全性；

安装最新的系统安全补丁；

禁止不必要的应用和服务；

审核并加强文件系统的安全性；

禁止不必要的账号，并加强账号及口令管理策略；

去除后门，内核参数及配置调整；

启动日志审计功能。

中间件及常见网络服务安全加固包含以下内容：

漏洞补丁管理，为业主方信息系统（含网站）的中间件及其他应用软件的漏洞补丁加固或版本更新提供修复建议，并在加固的前后提供漏洞验证。

帐号和口令管理

认证、授权策略调整

通讯协议加固

日志审核功能增强

其他安全配置增强通过以下途径来实施系统加固服务：

通过人员访谈、现场调查等途径来了解客户对欲加固系统的技术要求；

实施必要的安全扫描，确认安全加固前目标系统问题所在，提取加固需求；

为系统安全加固做好准备（环境、工具、资料、人员等）；

通过系统加固测试来确认加固方案的可行性；

借助预先准备好的Checklist及工具来实施正式的系统安全加固；

通过后期安全扫描及审计来验证加固结果的有效性。

一年提供4次安全巡检服务，每季度巡检一次。

安全加固完成后需在一周内提供安全加固报告。

### 1.1.3 应急响应服务

安全事件应急响应是指当安全威胁事件发生后迅速采取的措施和行动，其目的是最快速恢复系统的保密性、完整性和可用性，阻止和降低安全威胁事件带来的严重性影响。

安全事件应急响应是指当安全威胁事件发生后迅速采取的措施和行动，其目的是最快速恢复系统的保密性、完整性和可用性，阻止和降低安全威胁事件带来的严重性影响。安全事件主要包括：病毒和蠕虫事件、黑客入侵事件、误操作或设备故障事件等。

针对基础网络系统、主机系统、安全系统等重要信息化设施可能出现的信息安全事件制定详细的应急响应流程和策略，提供及时的信息安全应急响应服务。要求在1小时内排查与解决相关安全问题，保护关键信息系统免受重大故障或灾难的影响，并提供应急响应分析报告。

### 1.1.4 重大敏感时期保障

为芜湖市妇幼保健院提供重大敏感事件安全保障，保障内容应包括：安全评估、事前备份、事前保障等。

### 1.1.5资产梳理服务

用户数据中心是由多种软硬件设备组成，包括接入链路、网络设备、主机设备、安全设备、存储设备、虚拟化平台、应用软件、域名/IP以及UPS、精密空调等各种物理环境设备，这些软硬件设备是组成其信息系统的重要资产。在日常的运维管理过程中需要用到相关资产的各种属性信息，包括品牌、型号、版本、配置、维保情况、国产化情况、物理位置、管理信息、连接信息、依赖关系、文档情况、供应商信息、厂商信息、服务方信息、重要性等各个方面，这些软硬件资产的相关详尽信息是运维管理工作的基础支撑数据。

对用户数据中心所有软硬件资产详尽信息的标准化梳理，并在此基础上实现资产信息的动态维护和随时随地的检索查询，是全面运维的基础。

资产梳理服务之后，最终向用户交付的文档主要如下：

《XX用户信息资产统计表》

《XX用户信息系统网络拓扑图》

《XX用户信息系统设备信息统计表》

《XX用户信息系统设备登录方式及帐号统计表》（如果有，单独保密交付）

## 1.2 服务要求

### 1.2.1 管理要求

通过专业的安全服务管理，为信息系统的安全与稳定运行提供有力的保障，及时有效解决信息系统在日常工作中出现的各类硬件系统、网络及其他相关方面出现的故障，有力保障系统的正常运作。通过对信息系统的安全风险评估及安全加固服务，为网络、软硬件系统的安全运行提供有力的安全保障，建立以人员、流程、产品、服务商（4Ps)为一体的数据中心运维管理体系。

（1）人员

人员是运维管理的基础，也是运维管理的核心。所需要管理的对象，包括基础设施、IT设备、系统与数据、管理工具和人员等。

（2）流程

流程是运维管理质量的保证。作为IT服务的物理载体，存在的目的就是保证服务可以按质、按量地提供。需要把现在的管理工作抽象成不同的管理流程，并把流程之间的关系、流程的角色、流程的触发点、流程的输入与输出等进行详细定义。通过这些服务工作的流程化使得整个服务提供过程可被监控、管理。

（3）产品

产品是运维管理的加速器。运维管理涉及的对象庞杂且重复性工作较多。若完全依靠人工去完成这些工作，一方面对人员的技能与数量有较高的要求，另一方面在工作质量的保证方面也存在风险。为此，越来越多的数据中心在开展运维管理工作时使用大量工具，目的是通过这些工具的部署取代一些监控、操作、配置文件、工作流管理等大量重复性工作，最终实现提升运维水平、降低运维风险、减少运维成本的目的。

（4）服务商

服务商是运维管理的支持者。作为专业化的运维管理，有效地整合管理对象，并最终为用户提供专业化的服务才是服务提供者的核心价值所在。

### 1.2.2 服务范围

芜湖市妇幼保健院信息系统。

实施地点：芜湖市妇幼保健院指定的服务地点。

### 1.2.3 服务的模式和要求

1)供应商应针对服务项目内容制定具体运维服务计划和日常实施方案；

2)供应商应设立服务台，开通服务电话和技术支持电话；

3)供应商应按照用户要求成立服务项目组，项目小组不少于5人，提供服务的工程师不少于1名，具备多年安全服务项目经验或多年集成项目实施经验，项目小组成员至少包含一名信息系统集成及服务管理人员（具有项目经理认证证书），至少包含两名保障人员（具有CISAW认证证书），一名注册信息安全专业人员（具有CISP认证证书）。以上人员需提供证书证明。

4)本次运维服务过程所涉及的工具类硬件设备，由中标方免费提供并保障设备在运维服务期内的正常使用，应由正规生产厂商生产，无知识产权纠纷等问题，业主方不承担因此产生的所有费用，并且如因下列设备的使用对服务对象产生影响，所产生的损失由中标方承担。

5）中标方须与采购人签订运维工程师保密协议，并提供运维资质证明，合同期内在未得到采购人允许前不得变更人员，否则采购人有权终止合同，投标方承担全部损失。

## 1.3 服务工具

在服务过程中提供如下服务工具供用户使用。

### 1.3.1 网络分析工具要求

功能需求：1）界面要求：支持全中文的分析界面和资料文档，支持中英文双语协议解码功能（提供功能截图）。2）故障分析功能：支持故障诊断视图功能，能够智能诊断网络中常见的故障，并提供故障参考原因和解决方法，同时可以对数据包进行深层解码，针对各种网络或应用的疑难杂症，实现数据包封装级别的故障分析和定位。（提供功能截图）。

### 1.3.2 威胁分析工具

功能需求：1）基于双向流量的报警成功失败判断：能够基于双向流量，判断报警成功失败；并且对成功后的危害等级准确识别判定（需提供截图证明）。2）甄别攻击者的目的、诉求和所用资源：通过流量分析，能够判断攻击者是否为针对性攻击；能够获取攻击者的地理位置，IP等信息，并给出在威胁情报中对应的情报信息（需提供截图证明）。3）自动识别和梳理开放后台：利用被动监听技术对企业对外开放后台，和管理页面，进行实时监控；及时发现后台对外情况，能够帮助企业尽快了解风险，并作出对应的响应措施（需提供截图证明）。4）提供终端代理工具进行终端行为分析：可提供终端上的轻量级代理，用于采集终端数据，如进程、文件、注册表等行为，自动联动本地检测中心进行终端恶意行为检测能力；对网络上的告警，可结合告警机器的代理工具采集的日志信息和文件检测信息，定位告警的源头到进程粒度（需提供截图证明）。

### 1.3.3 网站立体监控系统

功能需求：1）检测引擎：支持域名或IP地址形式的Web应用系统安全扫描；支持预登录或指定Cookie、指定Header，对于某些需要特定权限才能访问的网页，可以登录检测；支持自定义网站检测的入口地址。（需提供截图证明）。2）可用性检测：支持检测网站首页响应速度，判断网站是否掉线，支持DNS、Ping、HTTP请求等多种方式探测网站连通速度；支持检测域名劫持。（需提供截图证明）。3）挂马检测：支持云端挂马源址库，采用云端动态行为检测技术与静态特征匹配技术相结合；支持检查该页面所有的文件资源，包括脚本、框架、CSS；（需提供截图证明）。4）暗链检测：支持云端暗链源址库，利用静态分析技术对网页源代码进行分析，查找不可见的外链接，并对这些链接进行云特征匹配；对检测出各类暗链链接，提取相应的链接及关键词扩展"云特征库"；具备数据提取方法、装置及系统功能并提供证明文件；（需提供截图证明）。5）脆弱性检测：SQL注入检测功能，检测网站是否存在SQL注入漏洞。包括对：Get参数的注入检测、Post参数的注入检测、Cookie中变量的注入检测提供SQL注入后续验证功能，如数据库版本识别，数据库名称、用户名等信息的抓取等；支持XSS跨站脚本（CrossSiteScripting）检测，采用动态网页解析技术，准确分析网页脚本；支持网站管理后台弱密码检测；支持网站管理后台地址检测。（需提供截图证明）。

### 1.3.4 集中管理系统

功能需求：1）要求提供集中管理控制类软件，包含资产信息管理、性能监控告警、安全事件分析告警、流程工单管理、日志审计等功能，该平台能够符合等保2.0安全管理中心所有要求项，能够辅助符合安全管理体系要求项，提供制度和流程摸板。（需提供截图证明）；2）提供安全态势、漏洞管理、极限核查、弱口令检查、巡检管理等功能，满足持续安全运维的要求；3）提供CMDB功能，基于面向对象的思路，实现资产建模，建模内容包括属性建模，与关系约束建模；4）提供资产全生命周期管理功能，详细记录资产上线到报废过程中所有的管理、变更、配置等信息；5）提供在线运维操作入口，所有的操作必须通过在线操作入口进行，从而对操作资产的行为进行管控与审计。由在线操作入口对所有的操作进行授权，只有获得授权，才能执行操作。（需提供截图证明）

### 1.3.5 集中管理系统

功能需求：1）产品漏洞库涵盖目前的安全漏洞和攻击特征，支持56000种以上漏洞；2）支持扫描主流操作系统、web服务器、网络主机、应用及软件的安全漏洞。（需提供截图证明）