第三章　用 户 需 求 书

一、项目基本情况

1.项目名称：琼海市人民医院网络安全整改技术服务项目

2.项目编号：HNYZ-2023-013

3.预算金额（总资金）：2323900.00 元

4.服 务 期：自合同签订生效之日起 3 年。

5.服务地点：采购人指定地点

6.付款方式:合同签订生效之日起 7 个工作日内支付合同金额的 20%的预付款，货到调试完成后 7 个工作日内支付合同金额的 20%，三年服务期每服务满一年支付合同金额的 20%。(具体以双方签订的合同为准）。

二、采购需求清单

序号	安全服务名称	安全服务要求	数量	备注
1	边界实时防护服务	1、针对内网服务区、外联出口，借助于安全边界防护工具，利用用户策略、应用策略和行为策略等智能控制手段，提供 7*24 的内网安全边界防护服务，实现琼海市人民医院内网的安全控制、流量分类、攻击防护等，并定期提供琼海市人民医院内网边界安全访问控制报告。 2、服务应实现对威胁信息、接口流量、连接信息、应用流量、用户流量、网站类型流量、VPN 流量、在线用户等对象进行监控展示；需提供策略命中分析、策略冗余分析、策略冲突检查、策略包含分析的展示；整个服务过程自动化，无人工参与。 3、服务应提供丰富而直观的可视化信息，可以方便地查看策略实施效果、定位网络问题，能够指导网络管理员进行更合理的规划； 4、边界安全监测服务需具备边界安全策略检测的专业方法，提供第三方权威机构技术证明； 5、服务期内应提供业务网与互联网边界区至少 1 台（含 1 台）、业务服务区边界至少 1 台的边界安全防护工具（最大并发连接数≥300 万；每秒新建≥7 万/秒；整机吞吐量（1518 字节）≥6G），需具备计算机软件著作证书和销售许可证书，提供相关证明材料；同时需提供其特种库升级等服务； 6、▲服务工具需采用多核多线程 ASIC 并行操作系统，需具备高安全等级的 VSOS 安全操作系统和高性能应用层流量处理引擎，需提供证明材料。	1 项	

		7、支持基于 IPv6 的入侵防御、病毒防御、DDOS 防御、URL 过滤、WEB 防护、流量控制、连接限制（要求截图证明并加盖公章）； 8、支持源 NAT、目的 NAT、静态 NAT，支持一对一、一对多和多对多等形式的 NAT；支持 Sticky NAT 开关，使相同源 IP 的数据包经过地址转换后为其转换的源 IP 地址相同（要求截图证明并加盖公章）； 9、▲支持 DNS Doctoring 功能，能够将来自内部网络的域名解析请求定向到真实内网资源，提高访问效率，同时支持通过配置多条 DNS Doctoring，实现内网资源服务器的负载均衡（要求截图证明并加盖公章）； **服务频率：7X24 小时不间断服务。** **服务交付：按月输出以下交付成果：** **一、《综合风险分析报表》**		
2	上网行为管理服务	1、提供 7*24 上网行为管理服务，对内部主机访问互联网行为进行管理和控制，其中包括对网页访问过滤、网络应用控制、带宽流量管理、用户实名认证、收发信息审计、用户行为分析，实现对海市人民医院内网用户互联网访问行为的全面管控，并定期提供琼海市人民医院内网用户互联网访问行为报告。 ▲2、服务可针对系统运行过程中的应用统计，支持应用的热度图；可提供支持广告推送，支持 PC 端推送 4 个方位的广告，手机端支持推送全屏广告提供；提供服务能力相关证明。 3、提供 HTTPS 解密服务，支持页面及命令行配置解密策略，包括入接口、源地址对象、目的地址对象、https 对象、域名排除等。支持针对 HTTPS 网站、HTTPS 搜索记录、HTTPS 邮箱等内容进行审计；HTTPS 邮箱支持审计主题、内容、附件等；支持 HTTPS 域名库，预定义域名以及自定义域名。 ▲4、提供智能策略分析服务，支持策略命中分析、策略冗余分析、策略冲突检查，并可在 WEB 界面显示检测结果；支持实时和周期性对所有安全策略进行分析；提供服务能力相关证明。 5、提供不少于 2 台服务工具，要求接入带宽：≥500M；每秒新建连接：≥10 万；最大并发连接数：≥190 万，应用特征数支持 7200+，移动应该不少于 2000+，提供相应证明材料。 6、系统支持软件补丁升级，以及热补丁技术（要求截图证明并加盖公章）； ▲7、支持 IPS 功能，支持基于源、目的、规则集的入侵检测；支持针对 WEB 服务器防护，包括木马/后门、挖矿、病毒蠕虫、SQL 注入、木马外联、间谍软件、工控攻击等（要求截图证明并加盖公章）； **服务频率：7X24 小时不间断服务。** **服务交付：按月输出以下交付成果：** **一、《行为管理报表》**	1 项	
3	安全态势监测服务	1、针对琼海市人民医院内网，提供 7*24 的在线态势感知监测服务，包含资产分析与管理、安全事件管理、关联分析、标准脆弱性管理、风险评估、情报管理、响应管理、基础态势呈现（资产态势、脆弱性态势、攻击态势），以场景化为基础，以满足实战化为目的，以威胁为驱动手段，提供监测预警、态势评估、响应处置的安全服务，提供集成的威胁	1 项	

		可视、自动化相应处置能力。通过技术工具收集安全信息要素，基于面向总体安全态势的认知和监测进行智能分析，并且通过完整的预警通告及处置工作流程，并具备相应的应急处置预案，帮助运维人员实现安全运维处置的闭环；并且对接外部的开源及商业威胁情报信息，并且提供有效的威胁情报利用和分析手段。定期提供安全态势报告。 ▲2、服务需采用专业的业务安全分析的方法和专业的分析工具，提供服务能力证明材料。 3、服务提供综合展示界面，包括最近 30 分钟告警状态雷达图、最近 1 小时事件趋势图、最近 24 小时的 10 条告警列表，能够显示最新 5 分钟内的事件一览、包括各类型事件数量和等级，最近 24 小时资产告警排行 Top10 等以及事件量曲线； 4、服务提供提供网络拓扑、机架拓扑等功能，以及对网络设备、安全设备、主机服务器的可用性与性能监控功能。该模块包括内置的本地性能采集器，用于采集各类设备及系统的性能信息。 5、至少提供 1 套态势感知分析平台+态势感知探针。能够对各种不同厂商的安全设备、网络设备、主机的性能与可用性进行集中化实时监控； ▲6、态势感知分析平台须获得中国信息安全认证中心颁发的符合《安全管理平台产品安全技术要求》的信息安全认证证书，投标方提交的认证证书必须明确载明产品遵照《安全管理平台产品安全技术要求》。具有《IPv6 Ready Logo Phase-2》认证证书。服务工具支持编解码工具，至少包含 Unicode 编码、UFT-8 编码、URL 编码/解码、Hex 编码/解码、Bse64 编码/解码和时间戳转换等六种解码方式（要求截图证明并加盖公章）；内置 Cisco PIX 和交换机的事件编码知识库；Windows、Linux、Solaris、AIX 操作系统的事件 ID 知识库；Oracle、SQL Server、MySQL、Informix、DB2 数据库的事件编码知识库（要求截图证明并加盖公章）； ▲7、态势感知探针支持基于不完整会话流的单包攻击检测能力；支持自定义规则，可结合用户业务进行深度检测，自定义内容包括源 IP、源端口、目的 IP、目的端口、协议、事件威胁等级、主机状态、事件类型、攻击阶段、攻击结果、攻击手段；支持关联规则分析，进行双向检测规则编写，兼容业界主流 snort 规则（要求截图证明并加盖公章）；具备通过 web 页面导入 pcap 包离线回放检测能力，单个导入回放的数据包最大支持 1G，支持批量导入或选择文件夹导入，最多支持导入 100 个数据包，支持选择回放流量业务口（要求截图证明并加盖公章）；支持通过页面，对告警前后存储报文数量进行配置，最多支持存储和下载告警前 50 个和后 50 个数据包（要求截图证明并加盖公章）； **服务频率：7X24 小时不间断服务。** **服务交付：按月输出以下交付成果：** **一、《综合风险报告》** **《脆弱性感知报告》**		
4	远程安全访问服务	1、借助于国家商用密码算法专用设备，提供远程办公接入服务，建立基于国密算法的加密传输通道，实现琼海市人民医院远程办公接入的需求，实现安全网关和客户端之间数据传输的机密性及完整性保护。 2、服务可提供基于 PC、Android、IOS 等移动智能终端设备接入注册与审批，未经审批的终端禁止接入；支持用户与设备绑定关系，用户必须	1 项	

		使用通过审批且绑定的设备方可通过认证接入;注册审批功能可通过配置开启或关闭；支持用户最大可关联绑定设备数量配置。 3、服务需对访问行为持续、动态的检测，一旦发现不符合访问控制策略的行为变化，可动态回收访问授权、阻断访问等，提供服务能力证明材料。 4、需提供支持针对不同 B/S 应用开启屏幕水印服务，支持隐式水印和显示水印两种技术，支持点阵式水印，水印内容包括：用户名+当前日期，有效预防数据泄露； ▲5、服务工具支持 SDWAN overlay 组网 支持邮件零配置开局部署，分支节点无需单独配置策略，通过点击邮件链接自动下拉策略，自动完成组网，提供功能截图证明； ▲6、服务工具明文整机吞吐≥5G，国密加密吞吐量≥400M；单台设备建议最大并发用户≥2000 个；提供≥50 个并发用户授权；支持双系统引导，可在管理员界面直接配置启动顺序，管理员可自由选择当前启动系统，每个系统拥有独立的配置文件，且分别支持加密导入导出。 ▲7、SDP 控制器支持本地创建账户体系或与第三方认证系统联动实现用户接入设备信任基线的安全认证，确保接入主体身份可信（要求截图证明并加盖公章）；支持自建 CA，支持用户使用国际/国密算法 USBKey 认证接入（要求截图证明并加盖公章）；支持与第三方 CA 联动实现在线申请证书功能。支持导入 8 套以上的第三方 CA 证书链，支持基于 CRL、增量 CRL、OCSP 及 SCEP 协议在线获取数字证书（要求截图证明并加盖公章）； **服务频率：7X24 小时不间断服务。** **服务交付：按季度输出以下交付成果：** **《用户流量统计报表》**		
5	运维实时审计服务	1、针对琼海市人民医院信息运维人员日常运维，提供 7*24 运维审计服务，对运维人员维护过程进行全面跟踪、控制、记录、回放；并细粒度分配运维人员的访问权限，实时阻断违规、越权的访问行为，同时提供维护人员操作的全过程的记录与报告;消除传统行为审计系统中的审计盲点，加强琼海市人民医院信息系统的内控、内审机制。 2、通过服务可限定配置中可指定用户通过指定的应用发布服务器对资源进行访问；同时可实现资源自动发现和添加，便于快速添加资源。 ▲3、服务工具支持内置 USB-KEY 认证、动态口令认证、国密动态口令认证、手机令牌认证，可集成其它外部认证协议： Windows AD、RADIUS、LDAP、短信、北京 CA、吉大正元等第三方认证，提供证明材料。 4、服务工具支持 Oracle、Postgresql、Sybase、MySQL、SQL server 数据库下行返回行数记录；支持在 Oracle 数据库运维，运维人员对变量进行绑定，执行 SQL 后，堡垒机系统可审计对应 SQL 中唯一标识符的具体值，协助审计员分析安全事件，提供证明材料。 ▲5、服务工具支持≥600 路字符会话或 200 路图形会话并发，提供≥100 个资源授权，需支持 IPv6，提供 IPv6 Ready Logo 测试认证证书。 ▲6、服务工具支持 C/S 客户端模式：提供 C/S 客户端功能，用于运维人员和管理员通过 C/S 客户端登录进行运维操作和管理操作，整个运维过程不依赖任何 Active 或 Java 控件（要求截图证明并加盖公章）；支	1 项	

		持通过应用发布开启运维屏幕水印，运维本地无法篡改水印内容，震慑不规范的运维行为，提升运维过程数据安全性； **服务频率：7X24 小时不间断服务。** **服务交付：按月输出以下交付成果：** **一、《运维管理巡检报告》**		
6	日志实时审计服务	1、通过主被动结合的手段和工具，提供内网 7*24 的日志审计服务，对内网中的安全设备、网络设备、主机、操作系统、以及各种应用系统产生的海量日志信息进行实时采集，并进行集中化存储、备份、查询、审计、告警、响应，获悉琼海市人民医院内网的整体安全运行态势，实现全生命周期的日志管理，并定期提供琼海市人民医院内网日志审计报表、报告。 2、服务工具需支持 SNMP Trap、Syslog、ODBC\JDBC、文件\文件夹、WMI、FTP、SFTP、NetBIOS、OPSEC 等多种方式完成日志收集功能； ▲3、提供日志范式化服务，范式化字段至少应包括事件接收时间、事件产生时间、事件持续时间、用户名称、源地址、源 MAC 地址、源端口、操作、目的地址、目的 MAC 地址、目的端口、事件名称、事件摘要、等级、原始等级、原始类型、网络协议、网络应用协议、设备地址、设备名称、设备类型等；针对不支持的事件类型做范式化不需改动编码，通过修改配置文件即可完成，提供服务能力证明材料； 4、服务需包含不同分析场景，包括各种实时分析场景、历史统计场景、实时统计等，并支持支持自定义场景； ▲5、要求服务工具日志处理性能（平均）≥4000EPS，支持≥130 个审计对象授权，内置 Cisco PIX 和交换机的事件编码知识库；内置 Windows、Linux、Solaris、AIX 操作系统的事件 ID 知识库；内置 Oracle、SQL Server、MySQL、Informix、DB2 数据库的事件编码知识库；能够查看系统内置的事件库中事件类型名称及其描述信息，提供截图证明。 ▲6、支持对国内主流国产化数据库进行日志数据采集，包括武汉达梦、人大金仓、南大通用、神州通用等；支持动态表名模式进行数据库采集，能按照时间或者数字的规则动态每天递增采集日志表（要求截图证明并加盖公章）；支持多种告警方式和告警动作，包括弹出提示框、播放警示音、发送邮件、发送 SNMP Trap、发送短信、执行命令脚本、设备联动、发送飞鸽传书、发送 Syslog 等（要求截图证明并加盖公章）； **服务频率：7X24 小时不间断服务。** **服务交付：按月输出以下交付成果：** **一、《资产日志综合报表》**	1 项	
7	终端安全监测服务	1、为琼海市人民医院内网终端、服务器，提供 7*24 终端安全监测服务，包含准入控制、基线管理、终端加固、终端防病毒、非法外联、主机防火墙、软件/补丁分发、外设及移动存储管理、数据防泄露、文档加密、终端审计等多方面，实现“不可信终端进不来”、“入网终端管得住”、“敏感数据出不去”的效果，并定期提供琼海市人民医院内网终端安全管理报告。 2、服务包含：桌面管理、安全基线、资产管理、部门策略检查、终端审计、消息分发、补丁分发、软件分发、应用商店、设备管理、移动存储管理、主机防火墙、准入控制、数据防泄漏、文档加密、文档安全外	1 项	

		发、终端防病毒等功能模块统一运维管理、策略管控、报表查询等，提供服务能力证明材料。 ▲3、服务应采用终端身份溯源的专业技术方法，提供服务能力证明材料。 4、服务需实现对终端接入的移动存储设备提供认证、授权和审计，确保终端使用认证通过的移动储存设备，对数据进行授权共享，彻底杜绝通过移动存储设备的数据非法外泄，提供服务能力证明材料。 ▲5、服务提供≥1000 个 Windows 版本授权许可，提供≥100 个 Linux 版本授权许可，能够对已知、未知病毒、木马、恶意程序等进行检测、清除。能够对各种加壳的病毒文件进行病毒查杀，支持的加壳种类不少于 100 种，提供服务能力证明材料。 ▲6、为增加安全能力时效性，特征库需支持每一项独立升级，至少包含：系统版本、客户端病毒库、情报库、补丁库、弱密码库、webshell 规则库、web 应有组件规则库（要求截图证明并加盖公章）；支持详细记录终端指令信息，包括：IP、命令类型、次数、具体参数内容（要求截图证明并加盖公章） **服务频率：7X24 小时不间断服务。** **服务交付：按月输出以下交付成果：** **一、《终端风险报表》**		
8	安全运营服务	服务内容：安全运营服务以保障网络安全“持续有效”为目标，围绕资产、漏洞、威胁、事件四个要素，通过云端安全运营中心和安全专家团队有效协同的“人机共智”模式 7*24H 持续性开展网络安全保障工作，与用户一同构建持续（7*24 小时）、主动、闭环的安全运营体系。 **服务频率：7X24 小时不间断服务。** **服务交付：** **一、《安全服务运营报告》（按月输出）** **二、《安全运营报告》（按季度输出）** **三、《安全通告》** **四、《综合分析报告》** **五、《季度汇报 PPT》** **《年度汇报 PPT》**	1 项	
9	现场网络安全巡检	服务内容：针对院方等保备案系统进行全面巡检确保业务不间断的情况下对客户内外网系统进行检测，通过采用漏洞扫描、端口扫描等工具辅助巡检工作，找到资产中存在的脆弱点、漏洞等信息，并提供信息系统安全巡检汇报，使客户相关人员能够实时掌控信息系统的安全状况，及时发现网络故障和安全隐患，协助、指导院方对发现的安全隐患、风险进行处置，保障客户网络和系统处于健康、安全的状态，确保相关业务持续运行。 安全巡检的对象包括：应用系统、操作系统、服务器、数据库及其他设备，如路由器、交换机、防火墙等的运行状况、资源利用情况、网络连接情况等进行检查，检查系统健康状态。 **服务频率：每季度开展一次，一年四次，服务三年，总共 12 次。** **服务交付：** **一、《季度设备巡检报告》**	1 项	

10	网络安全渗透测试	服务内容：针对院方的等级保护备案信息系统提供的渗透测试工作，精通渗透测试技术的资深安全专家，在客户授权范围内，参考 PTES(渗透测试执行标准)对客户信息系统进行模拟黑客攻击的商业化测试服务，用于帮助客户评估信息系统当前的安全性。提供包括外网渗透测试、内网渗透测试、黑盒测试、灰盒测试等多种测试方法，覆盖信息系统中包含的网站、APP、服务器、数据库、中间件、网络设备、终端等相关软硬件资产。 **服务频率：一年一次，服务三年，总共三次。** **服务交付：** **一、《渗透性测试报告》** **二、《渗透性测试复测报告》**	1 项	
11	网络安全配置加固	服务内容：根据渗透测试中发现的问题开展安全加固服务，提供主机层面策略加固和网络安全层面配置加固，针对主机和网络安全设备配置中存在问题，进行相关配置层面的优化，确保满足等级保护的安全基线，加固范围为网络环境中的所有网络设备，安全设备，服务器，包括交换机、路由器、防火墙、主机等。 **服务频期：一年一次，服务三年，总共三次。** **服务交付：** **一、《系统加固指导书》** **二、《系统加固报告》**	1 项	
12	网络安全攻防演练	服务内容：根据国家法律法规要求，针对院方开展一次攻防应急演练，应急演练以演示或者模拟的环境的形式，以网络攻防进行编制再结合用户场景定制，应急演练结束后出具总结报告。 **服务频期：一年一次，服务三年，总共三次。** **服务交付：** **一、《应急演练方案》** **二、《应急演练总结报告》**	1	
13	网络安全培训服务	服务内容：根据最新的国家法律法规要求和政策要求，对院方开展网络安全培训，培训的内容包含等级保护、网络安全意识、网络攻防等培训以提高所有参训人员的信息安全意识和能力。 **服务频期：一年一次，服务三年，总共三次。** **服务交付：** **一、安全培训 PPT** **二、培训相关材料**	1	
14	网络安全应急响应服务	服务内容：针对院方可能发生或已发生的信息安全突发事件提供应急响应服务，包括但不限于：数据取证，攻击朔源，定位攻击路线；现场分析，协助恢复；协助报送主管单位等。 **服务频率：服务期内根据院方需求提供应急响应服务。** **服务交付：** **一、《应急处置报告》**	1	