****

中海油能源发展股份有限公司

信科公司网络安全运营场景人工智能应用建设技术支持服务

**采购技术要求书**

 编制：

 审核：

 批准：

# 项目概况及总体要求

本项目旨在为海油发展有限责任公司网络安全部门构建一套基于前沿大语言模型（LLM）技术的智能化网络安全应用体系。面对日益严峻复杂的网络安全态势，传统的安全运营模式在处理海量多源异构告警、深度理解攻击意图、快速响应零日威胁、高效利用安全知识以及辅助复杂决策等方面面临巨大挑战。本项目通过引入并深度定制化大语言模型技术，力求在关键安全场景实现质的突破，显著提升安全运营的智能化水平、研判精准度、响应速度和决策效能。

总体要求项目承建方必须深刻理解网络安全攻防对抗的本质，具备扎实的网络安全专业知识与实践经验，同时精通大语言模型技术的原理、应用、调优及安全风险管控。项目建设需紧密围绕“智能攻击研判”、“渗透测试智能应用”、“实时自然语言数据分析”、“智能网络安全知识问答”、“网络安全数据决策分析”以及“安全运营一体化管理平台”六大核心服务内容展开。具体要求如下：

### 深度融合网络安全业务逻辑

 所有基于大语言模型的应用开发（如告警聚合降噪、攻击链重构、风险量化、动态建模、问答引擎、报告生成等）必须严格遵循网络安全领域的专业规范和业务流程（如MITRE ATT&CK框架、杀伤链模型、渗透测试方法论、安全运营流程等）。模型的设计、训练和部署需内嵌领域知识，确保输出结果具备业务可解释性和实际指导价值，杜绝“黑箱”操作。

### 充分发挥LLM核心能力优势

 有效利用大语言模型在自然语言理解与生成（NLU/NLG）、复杂模式识别与推理、多源异构信息融合与摘要、上下文动态学习与适配等方面的强大能力。重点应用于：

**深度语义分析：** 解析安全日志、告警、报告、合规文本、渗透测试结果中的复杂语义，理解攻击者战术意图（TTPs）。

**智能聚合与关联：** 跨越不同来源和格式的数据（日志、流量、资产、漏洞、威胁情报），识别潜在关联，构建完整的攻击链条。

**动态建模与预测：**基于历史数据和实时输入，辅助构建零日攻击行为模型，预测潜在攻击路径和影响。

**人机协同与决策辅助：**提供清晰、可操作的研判建议、风险解释、处置步骤，充当安全分析师的“智能副驾驶”；通过自然语言交互界面（NLI）赋能管理者进行数据查询、态势理解和防御推演。

**自动化内容生成：**高效生成精准、合规、可读性强的渗透测试报告、风险报告、知识条目、差距分析报告等。

**知识库构建与问答：** 高效整合、理解、更新多源权威安全知识（漏洞库、威胁情报、合规标准、最佳实践），提供精准、溯源的智能问答支持。

### 确保数据治理与模型安全

构建强大的多源异构安全数据治理引擎是基础前提。必须确保输入模型的数据质量、一致性、及时性，并严格遵守数据安全和隐私保护要求。同时，模型本身必须具备鲁棒性，能够抵御针对性的对抗攻击（如Prompt注入、数据投毒），并建立严格的访问控制、审计跟踪和输出内容安全过滤机制，防止模型被恶意利用或产生有害输出。

### 实现闭环验证与持续进化

 所有智能化应用，特别是攻击研判、渗透测试辅助、决策分析等，必须建立自动化或半自动化的闭环验证机制（如利用沙箱环境、历史数据回测、专家评审反馈）。模型需具备持续学习和优化能力，能够根据验证结果、新的威胁情报和业务变化进行迭代更新，确保其有效性和时效性。知识库必须实现动态更新。

### 构建一体化智能基座

“安全运营一体化管理平台”作为核心承载平台，需提供信创化全栈安全基座，整合上述智能应用能力，实现多模态威胁智能分析（结合LLM与其他AI技术）、自动化响应处置与运营闭环，并确保平台的高性能、高可靠性和可扩展性。平台应提供统一的自然语言决策交互与可视化中枢，为不同层级用户提供便捷的智能服务入口。

### 强调落地性与可交付性

 最终交付的不仅是一系列模型和代码，更是能无缝融入现有安全运营体系、切实提升安全团队工作效率和防护能力的可运行、可度量、可维护的智能化应用系统与服务。需提供完善的文档、培训和技术支持，确保用户能有效使用和运维。

本项目要求承建方具备强大的技术整合能力、深厚的网安领域知识沉淀和成熟的LLM工程化落地经验，最终交付一套业界领先、切实赋能海油发展网络安全智能化升级的核心能力体系。

# 服务内容和范围

【本服务部分引用《数据治理数据分析服务》CGBZ213-2021中的4.服务要求-4.2.业务模型与数据标准建设、4.3主数据标准建设、4.4源头规范建设、4.5数据质量规范建设与工具完善、4.6数据保障管理体系、4.7数据清洗迁移】

**以下为引用标准中所列重要内容：**

**4.2 业务模型与数据标准建设**

4.2.1 对本服务范围内业务流程、业务单元、业务活动、数据集等进行梳理与完善，完善业务逻辑关系形成业务模型，同时保障模型提醒未来的可持续建设。

4.2.2 标准建设成果与国家及行业相关标准相匹配，并具备开发生产适用性、满足通用性原则。

4.2.3 组织各专业权威专家对相应的成果进行评审及确认，保障成果可靠、适用、统一。

**4.3 主数据标准建设**

4.3.1 梳理业务周期所涵盖的主数据，包括但不限于主数据的标准属性、主数据间的关联信息及与专业中主数据的映射关系，最终完善差异描述，补充主数据的现况分析。

4.3.2 确定主数据的描述规范、编码规范，并对现有规范进行完善，保证主数据的一致性应用。

4.3.3 建立主数据的质量控制、主数据规范及管理制度，确保主数据源头唯一、数据一致与完整，保证主数据质量。

**4.4 源头规范建设**

4.4.1 梳理现有采集规范和源头业务系统，建立源头数据规范，确保业务上数据的源头采集和数据的唯一性。

4.4.2 建立数据采集规范，为数据采集、管理、维护、上报等提供管理方式和配套规章制度。

**4.5 数据质量规范建设与工具完善**

4.5.1 要求对明确约束条件的全部业务数据制定质量检验规则，保障对数据检验的完整性与精确性。

4.5.2 通过工具完善实现数据的一致性、及时性、准确性的校验。

4.5.3 对特殊的采集需求，进行定制模板的建设与维护，配合进行采集入库的数据验证规则制定与完善。

**4.6 数据保障管理体系**

4.6.1 进行数据管理制度的设计工作，规范数据的采、存、管、用等工作，最终形成包括但不限于《数据标准》、《数据质量规则》、《数据采集规范》等文档。

4.6.2 围绕业务数据应用范畴建立数据安全管理策略与制度，通过数据分级、用户级别以及权限定义进行数据访问安全管理。

4.6.3 安全体系的建设要包括安全策略、安全组织、安全技术及安全建设与运行。

4.6.4 数据安全建设要求和同类系统安全等保级别约定条件。

**4.7 数据清洗迁移**

4.7.1 梳理主数据、参考数据和业务数据，按照标准规范和治理流程进行数据清洗和迁移，以保障数据的一致性，达到数据资产可视化和开发生产数据共享的目标。

4.7.2 通过一致性检查无效值和缺失值的处理对数据库中残缺数据、错误数据、重复数据进行清洗并统一迁移至标准库。

## **服务内容**

### 智能攻击研判应用开发服务

本项目要求供应商构建具备攻防对抗水准的智能攻击研判系统，该核心平台须融合前沿大语言模型（LLM）技术与网络安全攻防知识体系，实现对海油发展全域、全栈、全流量安全数据的智能化、自动化、高精度攻击识别与响应决策支持。具体服务范围要求如下，供应商须具备相应专业技术储备与大规模复杂系统实施能力：

#### 多源异构告警智能聚合与降噪

供应商需构建具备大规模实时处理能力的告警中枢，无缝对接并解析来自海油发展全网部署的超过15类异构安全设备与系统（涵盖但不限于：下一代防火墙（NGFW）、入侵检测/防御系统（IDS/IPS）、高级威胁检测（APT）沙箱、端点检测与响应（EDR/XDR）、云安全态势管理（CSPM）、工业控制系统（ICS）安全监测、Web应用防火墙（WAF）、数据泄露防护（DLP）、安全信息和事件管理（SIEM）、网络流量分析（NTA）、身份认证与访问管理（IAM）日志、漏洞扫描器、威胁情报平台等）产生的原始告警事件。利用大语言模型（LLM）的上下文理解、语义关联与模式识别能力，结合图神经网络（GNN）与无监督/半监督学习算法（如自编码器、隔离森林等），实现告警事件的跨设备、跨协议、跨时间窗口的智能上下文关联、因果链重构与根源分析，彻底滤除误报与低价值告警（要求降噪比不低于99.5%），精准提炼出表征真实、高优先级、潜在定向攻击的告警簇，形成攻击事件链（Incident Chain）雏形。系统需具备动态自适应学习能力，持续优化降噪模型以适应海油发展特有的网络环境与攻击模式演变，相关算法模型需提供严格的数学证明与可验证的鲁棒性测试报告。

#### 攻击意图推理与杀伤链重构

基于聚合后的高质量告警簇与原始数据（包括全量数据包捕获PCAP、进程树、注册表变更、内存镜像片段等取证数据），供应商须开发具备战略级威胁狩猎（Strategic Threat Hunting）能力的推理引擎。该引擎须内嵌基于大语言模型（LLM）构建的网络安全专家知识图谱（需整合MITRE ATT&CK框架全矩阵战术技术、洛克希德马丁杀伤链模型、钻石模型、自定义内部威胁模型及海量实战攻防经验），结合贝叶斯推理、因果推断模型与强化学习算法，实现对攻击者战术、技术与过程（TTPs）的毫秒级语义解析与意图推演。要求系统能自动识别攻击阶段（侦查、武器化、投送、利用、安装、命令控制、目标达成），精确重构完整的、动态演化的攻击杀伤链（Kill Chain），并精准推断攻击者的最终目标（如数据窃取、系统破坏、勒索加密、工控停摆等）和下一步潜在攻击动作。推理过程需具备完全可解释性（XAI），提供详尽的推理路径与置信度评估，误判率须严格控制在0.1%以下，并通过第三方红队模拟攻击进行有效性验证。

#### 零日攻击行为动态建模

为应对APT组织常用的零日（0-Day）漏洞利用与无文件攻击等高级威胁，供应商须开发基于大语言模型（LLM）与异常检测（Deep Anomaly Detection）的动态行为建模系统。该系统需利用LLM强大的少样本/零样本学习与生成能力，结合图表示学习（Graph Representation Learning）与时间序列预测模型（如Transformer-based, LSTM-NDT），在海油发展正常业务行为基线（需覆盖所有关键业务系统、工控环境、云环境、用户实体行为）的基础上，实时建模网络、主机、应用、用户等多维实体间的复杂交互关系与行为模式。要求系统能在缺乏已知签名或规则的情况下，通过检测微观行为序列的异常偏差（如特权命令的异常序列、进程间通信的隐蔽通道、网络流量的时空异动、内存访问模式的细微变化等），动态构建并更新零日攻击行为特征模型，实现对未知威胁的早期预警（Early Warning）与高置信度检测（检出率>98%，误报率<0.5%）。模型需具备在线增量学习能力，确保对新出现攻击手法的快速适应，并提供对抗样本鲁棒性测试证明。

#### 研判决策智能辅助系统

 基于前述模块的输出，供应商须构建一个面向海油发展网络安全分析专家的智能辅助决策中心（AI-Augmented SOC）。该系统核心是高度专业化、领域微调（Domain-Tuned）的大语言模型（LLM），该模型需内化海量网络安全知识库（包括但不限于CVE漏洞详情、补丁信息、攻击技术手册、应急响应预案、海油发展内部安全策略与合规要求）、历史处置案例库及实时威胁情报。要求系统能自动生成：

攻击事件综合分析报告： 包含攻击链全景图、攻击者画像、影响范围评估（精确到受影响资产、业务系统、数据类别）、关键证据链。

定制化响应策略建议： 提供可立即执行的、分步骤的、优先级排序的遏制、根除、恢复措施，如防火墙规则建议、隔离策略、补丁/加固指南、威胁狩猎（Threat Hunting）查询语句、取证收集指令等，并自动关联到海油发展现有安全编排自动化与响应工单中。

影响评估与风险量化： 利用LLM结合定量风险模型（如FAIR），自动计算攻击事件可能造成的财务、运营、声誉损失。

合规性影响说明： 自动关联攻击事件触发的国家等级保护、关基条例、行业法规（如能源行业特定要求）的合规义务与报告要求。

#### 自动化研判闭环验证机制

为确保研判结果的准确性与响应措施的有效性，供应商须设计并实现一个强化的自动化闭环验证体系。该体系需包含：

仿真验证沙箱： 基于研判结果与响应建议，自动在隔离的高保真网络靶场中部署攻击场景复现与响应措施模拟执行，利用LLM驱动的自动化攻击模拟引擎（模拟APT攻击者行为）与防御效果评估引擎，对研判结论和响应策略进行动态对抗性验证。

效果评估与反馈学习： 实时监控验证过程中的攻击阻断效果、系统恢复状态、潜在副作用（如业务中断），生成量化的验证报告（成功/失败指标、置信度提升/下降）。验证结果须实时反馈至前述的聚合降噪、意图推理、行为建模、决策辅助等模块，驱动LLM模型与关联算法的在线迭代优化与知识库更新（要求闭环反馈延迟低于5分钟）。

未知威胁发现增强： 在验证过程中主动尝试突破现有防御模型的“对抗样本”，探索潜在防御盲区，并将发现反馈至零日攻击行为建模模块，持续增强未知威胁检测能力。
该闭环机制是实现系统自我进化、持续提升防御智能水平的核心，供应商需提供详细的自动化验证覆盖率（要求>95%关键响应动作）与模型迭代效率（如每周模型性能提升指标）保障方案。所有模块需与海油发展现有安全技术栈实现双向API集成（提供不少于20个关键接口的详细设计），确保研判结果与响应指令的无缝流转与执行。供应商须承诺系统在验收时达到所有预设的技术指标（如告警降噪比、攻击链重构准确率、零日检出率、决策采纳率、闭环验证覆盖率等），并提供可量化的持续优化承诺。

### 渗透测试智能应用开发服务

供应商需构建具备APT组织对抗能力的下一代渗透测试智能平台，融合大语言模型（LLM）的认知推理能力、强化学习算法及安全知识体系，实现对海油发展全域混合环境（涵盖海上钻井平台边缘计算节点、工业控制系统（DCS/SCADA）、多云混合架构、供应链第三方接入点及深海勘探数据链）的自动化、持续性、对抗性安全验证。该平台需突破传统渗透测试工具的静态局限，具备战略级攻击面演化预测、战术链自主决策及动态防御博弈能力，具体服务内容要求如下，供应商须提供攻防实战项目案例及AI安全领域核心专利证明：

#### 智能渗透测试策略生成与优化

供应商须开发具备多目标博弈能力的策略引擎，基于实时接入的20+类异构数据源（包括全流量元数据、云安全配置快照、工控网络通信矩阵、源代码漏洞特征、暗网监控情报、资产指纹库、历史攻击链数据库及实时防御策略快照），利用图神经网络（GNN）构建万亿级节点的动态攻击面知识图谱。要求引擎内嵌经APT攻防数据微调的LLM决策核心，结合蒙特卡洛树搜索（MCTS）与强化学习（DRL），在毫秒级时间内生成千级并发的自适应渗透策略：需动态权衡攻击路径可行性（综合0day漏洞利用链成功率、权限提升路径隐蔽性）、资源消耗（计算成本、时间窗口）及规避检测概率（绕过WAF/EDR/NDR的数学模型验证），并实时优化策略以应对防御策略突变（如防火墙规则更新、蜜罐诱捕）。策略生成需覆盖从初始突破到横向移动、权限维持、目标达成的全生命周期，关键路径识别准确率≥99%，策略迭代响应延迟≤3秒，并通过实时对抗验证有效性。

#### AI驱动的漏洞分析与验证

供应商须构建具备漏洞认知革命能力的分析中枢，基于LLM的代码语义理解与跨模态关联能力（融合CVE描述、PoC代码、二进制特征、补丁差分、环境上下文），实现对高危漏洞的智能验证与武器化改造：

动态可利用性评估：通过LLM驱动的符号执行引擎，解析漏洞触发条件与现有防护措施（ASLR/DEP/WAF规则）的对抗关系，量化漏洞在特定环境中的可利用概率（要求计算误差率≤0.5%）；

智能载荷生成：利用LLM的对抗性代码生成能力，结合环境参数（操作系统版本、服务配置）动态构造绕过现有检测机制的漏洞利用链（包括无文件攻击内存注入载荷、工控协议畸形报文、云原生容器逃逸脚本），并自动验证载荷有效性（成功执行率≥98%）；

未知漏洞挖掘增强：基于图注意力网络（GAT）构建代码缺陷模式库，对海油发展自研工业控制软件及云原生应用进行跨版本差异分析，实现高危0day漏洞的主动狩猎。所有漏洞分析需输出武器化等级评分（Weaponization Score）及动态修复紧迫性指数，并通过隔离的工控沙箱环境进行爆炸半径验证。

#### 自动化渗透测试报告与修复指导

供应商须开发具备合规审计级精度的智能报告工厂，基于LLM的多维度信息融合与自然语言生成能力：

攻击链可解释性重建：自动关联漏洞利用证据、权限提升步骤、数据泄露路径及防御规避手法，生成符合MITRE ATT&CK战术矩阵的可视化攻击图谱（节点覆盖率100%）。

智能修复方案生成：利用LLM解析漏洞根因与业务影响，动态生成精准修复指令集（包括Ansible加固剧本、云安全策略JSON配置、工控防火墙规则片段、补丁热替换方案），并关联资产管理系统自动标记受影响设备。

风险量化决策支持：集成FAIR风险模型，计算单点漏洞的潜在业务损失（精确到停产分钟数、数据泄露赔偿金额）、修复成本ROI及合规违约代价，生成高管级风险决策树。报告生成延迟须≤5分钟，关键事实错误率≤0.01%，且修复方案需通过自动化验证沙箱进行有效性预检（验证覆盖率≥95%）。

#### 攻击面智能监控与主动防御推演

供应商须构建具备战场预判能力的动态监控体系，通过LLM驱动的时序预测模型（Transformer-XL）推演框架：

攻击面演化预测：实时分析开源情报（GitHub/Shodan）、暗网交易数据及漏洞披露趋势，预测未来72小时内海油发展特定资产可能遭遇的新型攻击手法及武器化漏洞，生成概率化攻击热力图。

主动防御推演：在数字孪生环境中模拟千级并发的APT攻击流，基于强化学习训练防御策略优化模型（DRL-Defense），动态生成防御策略调整建议（如防火墙规则优先级重构、蜜罐部署坐标优化、流量清洗阈值调整），并量化策略变更后的风险收敛曲线（要求攻击成功率降低≥80%）。

红蓝对抗知识闭环：自动抽取攻防对抗中的TTPs特征，反馈至策略生成引擎与漏洞分析中枢，实现系统自进化（要求每周战术库更新率≥15%）。推演系统需与现有SOC平台集成，实现防御策略的自动下发与效果追踪（延迟≤30秒）。

供应商须承诺平台与海油发展现有安全生态实现原子级API集成（提供≥25个双向接口），确保渗透结果实时驱动防御体系优化。验收标准包含技术指标（如漏洞验证准确率、攻击路径预测率、修复方案执行率），并需提供第三方机构出具的对抗测试报告。所有模块需满足等保2.0三级加密要求及深海作业环境抗干扰认证，数据血缘追溯粒度至毫秒级。

### 实时智能数据分析开发服务

供应商需构建具备安全运营中心（SOC）认知级能力的实时自然语言智能分析平台，融合大语言模型（LLM）的语义理解、多模态关联及动态推理能力，实现对海油发展全域安全运营数据的秒级智能决策支持。该平台需突破传统日志分析工具的静态局限，构建覆盖千亿级异构数据源的认知计算中枢，具体要求如下，供应商须具备关键信息基础设施防护经验及大规模语言模型工程化能力：

#### 多源异构安全数据治理引擎

供应商须开发实时数据融合引擎，要求纳管15类以上异构数据源（包括但不限于：全流量包捕获（PCAP）元数据、EDR/XDR终端进程树日志、云原生Kubernetes审计事件、工业控制系统（DCS/SCADA）操作指令集、防火墙策略变更记录、漏洞扫描原始报告、暗网威胁情报流、开源情报（OSINT）爬取数据、内部安全知识库文档、应急响应团队语音记录转写文本、第三方供应商评估PDF、工控协议二进制流、深海勘探卫星通信数据、海上作业平台传感器告警及内部IM通讯记录）。利用LLM驱动的跨模态语义对齐技术（需融合BERT-GPT跨架构模型），实现非结构化文本（如渗透测试笔记）、半结构化日志（如Syslog）及二进制流（如Modbus TCP）的智能实体抽取（准确率≥99.5%），构建万亿级节点的动态安全知识图谱。引擎需实现毫秒级数据血缘追溯（延迟≤3秒），支持对阿拉伯语、俄语等小语种威胁情报的实时翻译与语义消歧，数据治理完整率不低于99.9%。

#### 攻击链动态感知与推理引擎

供应商须构建具备APT狩猎能力的认知推理核心，基于LLM微调的战术决策模型（融合MITRE ATT&CK 150+战术技术、钻石模型及海油发展私有攻击模式库），结合时序因果推断（如TCDF算法）与概率图模型，实现：

多模态攻击链重构：通过关联语音记录（如“尝试使用永恒之蓝攻击”）、IM文本（如“已获取域管理员凭证”）及二进制日志（如LSASS内存dump特征），实时重构跨IT/OT环境的完整攻击杀伤链，要求误关联率≤0.1%。

意图推演：基于攻击者对话文本语义分析、战术动作上下文，推断攻击组织归属及战略目标，推演置信度≥98.5%。

实时威胁预警：利用LLM的少样本学习能力，从模糊告警（如“异常工控指令”）中提取潜在攻击特征，动态生成攻击模式假设并自动触发狩猎探针（Hunting Probe），预警准确率须≥95%。引擎输出需通过数字孪生环境进行对抗验证，并与现有网络安全平台实现指令级联动（响应延迟≤5秒）。

#### 风险驱动的智能问答核心系统

供应商须开发面向决策层的战略级认知辅助系统，基于千亿参数级领域微调LLM（需在能源行业攻防数据集上预训练），实现：

多跳推理问答：支持复杂自然语言查询（如“过去72小时办公网络遭受的所有与APT28相关的攻击步骤，按业务影响排序”），要求系统自动拆解问题语义、关联多源数据（如EDR告警）、生成证据链支撑的决策树（引用具体日志ID、攻击截图、资产拓扑），回答准确率≥99%。

动态风险量化：集成FAIR模型与业务影响矩阵（BIA），实时计算单次攻击的潜在损失（精确到原油停产吨数、SCADA系统重启时长、合规罚款金额），输出风险热力图及修复ROI分析。

合规智能映射：自动解析等保2.0三级、NIST CSF 1.1及ISO 27001条款，将攻击事件映射至具体合规项，生成差距分析报告。系统需通过对抗性测试（Adversarial QA），确保在故意误导性提问下错误率≤0.5%。

#### 动态风险报告生成

供应商须构建自动化报告工厂，要求：

多维度实时报告：利用LLM文本生成与摘要技术，每5分钟自动输出高管风险简报（含TOP5攻击链可视化图谱）、技术分析（含攻击载荷逆向代码片段）及合规证据包（自动关联GDPR/关基条例条款）。

智能修复链生成：基于漏洞上下文（如工控系统固件版本），动态生成包含Ansible加固剧本、云安全策略JSON配置、防火墙规则片段及人员培训提纲的修复方案，并预验证方案有效性（通过沙箱模拟执行验证率≥97%）。

攻击面态势投射：集成LSTM-Transformer时序模型，预测未来48小时攻击面演化趋势，生成防御资源调度建议。报告需支持中英双语自动转换，关键事实错误率≤0.01%。

供应商须承诺平台与海油发展现有20+系统（含IT/OT-SIEM、云安全网关、工控防火墙、漏洞管理平台、海事通信系统）实现原子级API集成（提供≥25个双向接口），支持每秒百万级事件实时处理。验收标准包括：攻击链重构准确率≥99%、多语种语义解析错误率≤0.3%、报告生成延迟≤3分钟。供应商需提供实验室出具的对抗测试报告。

### 网络安全智能运营一体化平台开发服务

### 1.智能网络安全知识通解助手开发服务

供应商需构建具备网络安全智库认知水平的智能问答系统，融合大语言模型（LLM）的语义理解、多跳推理及动态知识演化能力，实现对海油发展全域网络安全运营的毫秒级战略决策支持。该平台需突破传统知识库静态检索局限，构建覆盖万亿级专业实体、千类异构数据源的认知作战体系，具体要求如下，供应商须具备关键信息基础设施知识工程经验及大规模领域模型微调能力：

#### 多源权威知识库构建与动态更新

供应商须构建知识中枢，要求实时纳管并智能融合20+类权威数据源（包括但不限于：MITRE ATT&CK框架全矩阵技术细节、CVE/NVD漏洞库全量数据（含历史漏洞武器化记录）、国家漏洞库（CNNVD）工控专项条目、等保2.0/ISO 27001/NIST CSF法规原文及司法解释、海油发展内部安全策略文档（含深海作业特殊条款）、全球APT组织战术手册（含俄语/朝鲜语原始报告）、红队实战攻击链案例库（含截屏、视频记录及语音复盘）、工业控制系统（DCS/SCADA）协议安全白皮书、云原生安全配置基准（CIS Benchmark）、漏洞利用代码（PoC/Exp）仓库、威胁情报平台（TIP）IoC/IOA数据流、第三方审计报告（含PDF扫描件）、深海勘探设备通信安全规范及海上平台边缘计算安全指南）。利用LLM驱动的跨模态知识抽取技术（融合BERT-BiLSTM-CRF模型），实现非结构化文本（如渗透测试手绘草图OCR）、多语言文档（含阿拉伯语工控协议文档）及音视频资料（如应急响应会议录音）的智能实体-关系三元组抽取（准确率≥99.7%），构建动态演化的万亿节点安全知识图谱。要求系统实现知识自动化验证（通过隔离沙箱执行漏洞验证代码）与实时更新，知识完整度≥99.9%，支持基于区块链的版本溯源（追溯粒度至单个条款修订记录）。

#### 合规条款智能解构与差距诊断

供应商须开发具备解析能力的合规引擎，基于千亿参数领域微调LLM（需预训练于全球网络安全法规语料）：

多法规交叉映射：自动解构等保2.0三级、ISO 27001:2022、NERC CIP、IMO 2021海事网络安全规范等15+套合规框架，建立条款级语义关联网络（如“等保8.1.4条款”与“NIST PR.AC-7”的等效性证明），生成跨法规合规矩阵。

智能差距诊断：通过实时比对海油发展安全配置（防火墙策略表、云安全组规则、工控设备固件版本）与合规要求，利用LLM驱动的因果推理识别潜在违规点（如“南海钻井平台控制网络未满足IMO 2021第6.3条的双因子认证要求”），诊断覆盖率达100%。

动态影响推演：量化单点合规差距的连锁风险（如“未修复CVE-2023-1234将导致等保三级测评失败，触发500万元罚款及平台停产风险”），生成多层级修复优先级清单。要求诊断结果通过第三方律所验证，误差率≤0.01%。

#### 精准溯源式问答引擎

供应商须构建具备证据链溯源能力的问答核心，要求：

多跳推理决策树：支持复杂语义查询（如“展示近半年所有利用云容器漏洞攻击地质勘探数据库的攻击链，并关联APT组织及修复方案”），系统需自动拆解问题、关联知识图谱中分散实体（漏洞CVE-2023-5678 → 攻击组织Lazarus → 利用容器逃逸技术 → 影响SGY-2023号勘探船），生成带完整证据链的可验证回答（引用具体日志ID、漏洞验证视频、合规条款）。

对抗性问答鲁棒性：在攻击者故意注入误导信息（如“永恒之蓝漏洞仅影响Windows 7系统”）时，通过知识图谱交叉验证确保回答准确性（错误率≤0.3%）。

实时战术推演：针对新型攻击手法（如“利用ChatGPT生成的鱼叉邮件”），结合历史TTPs模式生成防御方案推演树（含检测规则YARA语法、邮件网关过滤策略）。问答响应延迟≤2秒，证据链完整率≥99.5%。

#### 自适应能力评估与实训推演

供应商须构建具备红蓝对抗强度的动态演训系统：

个性化能力画像：通过LLM分析用户历史问答记录、应急响应操作日志，构建多维能力模型（漏洞识别准确率、法规理解、攻击链重构速度），生成个性化薄弱点热力图。

自适应攻防推演：在数字孪生环境（镜像海上钻井平台网络+工控系统）中，利用强化学习驱动攻击代理（RL-Attacker）动态生成攻防场景（如“模拟台风期间通过卫星链路渗透SCADA系统”），根据用户处置动作实时调整攻击强度（难度动态浮动范围±90%）。

智能复盘引擎：自动生成带视频回放的战术复盘报告（含攻击路径动态图谱、决策失误时间戳、合规条款违反点），并推送定制化学习材料（如工控协议安全手册精选章节）。要求系统支持千人并发推演，场景生成延迟≤3秒，推演结果通过第三方红队认证。

供应商须承诺系统与海油发展20+作战平台（含SOC知识库、网络安全平台剧本库、漏洞管理系统、工单系统、海事通信平台）实现指令级集成（提供≥30个双向API），支持毫秒级知识注入。验收标准包括：知识库动态更新延迟≤1分钟、合规诊断准确率≥99.99%、问答溯源完整率≥99.5%、推演场景真实性评级≥4.8/5.0。

### 2.网络安全数据决策应用开发服务

供应商需构建具备网络空间作战指挥级别的智能决策平台，融合大语言模型（LLM）的战略推演能力、多模态认知计算及动态博弈算法，实现对海油发展全域网络安全态势的秒级风险量化、毫秒级防御决策及闭环作战演进。该平台需突破传统安全分析工具的认知局限，构建覆盖千亿级实时数据流、万亿级战术知识节点的决策中枢，具体服务内容要求如下，供应商须具备关键信息基础设施防御指挥系统建设资质及大规模对抗性AI研发经验：

#### 攻击链智能研判与风险量化引擎开发

供应商须开发攻击链认知引擎，要求纳管25+类异构实时数据源。利用LLM驱动的跨模态关联技术（融合Transformer-XL与图卷积网络），实现非结构化语音指令（如平台紧急广播）、二进制工控协议、多语言威胁报告（含俄语/波斯语）的毫秒级语义融合（延迟≤3秒），构建动态攻击链知识图谱（节点规模≥10万亿）。引擎需内嵌经红蓝对抗数据微调的LLM推理核心，结合贝叶斯攻击树（BAT）与强化学习算法，实现：

攻击链概率化推演：实时计算百万级潜在攻击路径（从卫星链路渗透到钻机控制系统停摆），精确量化路径可行性（综合0day漏洞利用链成功率、防御规避数学模型、环境干扰因子），输出攻击成功概率置信区间（误差率≤0.3%）。

战场级风险量化：集成FAIR模型与海油专属业务影响矩阵，动态生成风险热力图（需区分勒索软件/数据窃取/工控破坏的损失曲线）。

战术级威胁狩猎：通过LLM解析模糊告警（如“异常扭矩传感器读数”），自动生成攻击假设并触发深海作业网络取证探针（证据链完整率≥99.9%）。研判结果需通过数字孪生环境进行爆炸半径验证（覆盖率100%）。

#### 自然语言决策交互与可视化中枢

供应商须构建面向指挥层的认知作战系统，基于千亿参数领域LLM：

战略级语义决策：支持自然语言复杂指令（如“模拟台风期间南海X平台遭受国家背景APT攻击时，优先保障钻井控制系统或地质数据库的防御资源分配方案”），要求系统自动解构指令语义、关联实时作战图谱（资产拓扑/防御资源/漏洞状态）、生成多方案决策树（含各方案业务中断时长预测、合规违约代价、防御资源消耗模型）。

多模态态势呈现：利用LLM驱动可视化引擎，动态生成三维作战沙盘（融合工控网络拓扑、攻击流实时轨迹），支持语音交互式钻取分析。

对抗性决策强化：当接收到虚假情报（如“漏洞扫描显示无风险”）时，通过知识图谱反向验证（关联漏洞库/威胁情报流）自动修正决策（误判率≤0.1%）。系统响应延迟须≤2秒，决策方案需通过蒙特卡洛万次模拟验证稳定性。

#### 主动防御推演与闭环管理机制

供应商须开发具备预判能力的动态防御体系：

防御博弈推演：在镜像生产环境的超仿真数字孪生体（涵盖IT/OT/云/边缘计算节点）中，部署基于强化学习（DRL）的攻防代理集群，模拟APT组织的自适应攻击策略（TTPs动态进化速度≥每小时15%）。防御引擎需利用LLM生成的战术决策树，实时推演防御策略变更（如防火墙规则优先级重构、流量清洗阈值调整、蜜罐坐标优化）对攻击成功率的影响（要求推演准确率≥99%）。

闭环作战演进：建立毫秒级反馈学习机制——将推演结果（攻击阻断率、误杀业务代价、资源消耗比）实时反哺至攻击链研判引擎与决策中枢，驱动LLM模型在线进化（模型迭代延迟≤5分钟）。要求每周提升防御策略效率≥10%（以攻击路径阻断率为核心指标）。

自愈式知识更新：自动抽取推演中新发现的TTPs特征（如“利用声呐数据干扰信号渗透”），生成防御规则（YARA语法/Snort规则/工控防火墙配置）并注入生产环境（自动化实施率≥95%）。推演系统需支持千级并发场景，时延≤30秒。

供应商须承诺平台与海油发展现有系统实现原子级指令集成，确保决策指令秒级下达至边缘设备。验收标准包括：攻击链推演误差≤0.5%、风险量化模型偏差≤0.2%、防御策略推演准确率≥98.5%、决策闭环延迟≤45秒。

### 3.安全运营一体化管理平台建设服务

供应商需构建具备关键信息基础设施防护等级的自主可控安全运营中枢平台，深度融合大语言模型（LLM）的认知决策能力、多模态威胁解构技术及军工级高可靠架构，实现对海油发展全域网络安全防御体系的原子级管控、智能作战推演及毫秒级自愈闭环。该平台须基于全栈信创化技术生态构建，突破传统SOC工具链的碎片化局限，达成万亿级实时数据流的战场级指挥效能，具体服务内容要求如下：

#### 信创化全栈安全基座需实现硬件至应用层国产化适配

供应商须构建从芯片层到应用层的全自主安全基座，要求：

硬件级可信：基于申威SW64或飞腾FT-2000+/64处理器架构构建分布式集群，搭载符合GM/T 0028《密码模块安全技术要求》的国密硬件加密卡（支持SM2/SM3/SM4/SM9算法），实现数据存储与传输的量子抗性加密（密钥强度≥3072位）。

深度适配国产OS：在麒麟Kylin V10或统信UOS操作系统内核层部署安全强化模块（实现SecComp-BPF策略编译、SELinux策略自动生成），要求全栈兼容性认证覆盖中创中间件、达梦数据库、瀚高数据库等15类以上核心组件。

LLM信创化部署：采用完全自主训练的千亿参数领域大模型（需提供训练数据主权证明），在申威芯片集群上实现稀疏化推理加速（时延≤50ms/query），模型权重加密存储符合GB/T 39786-2021等保2.0四级要求。基座需通过信创适配认证，单集群支持EB级数据湖存储，故障切换时间≤0.3秒。

#### 多模态威胁智能分析功能需具备工业级对抗能力

供应商必须开发具备认知级威胁解构能力的作战引擎：

跨模态语义融合：利用LLM驱动的多模态Transformer架构（融合ViT/CLIP/Wav2Vec模型），实现二进制协议流、传感器振动波形、多语种文本的联合特征提取（如从钻机异常振动频谱中识别针对SCADA系统的物理层攻击），关联准确率≥99.99%。

动态威胁狩猎：基于信创图数据库（如TuGraph）构建十万亿级节点战术知识图谱，通过强化学习驱动的攻击路径推演（RL-Pathfinder），实时计算千级并发攻击链的爆炸半径。

零日威胁预言：利用LLM的少样本生成能力，主动构建未公开漏洞（0day）的行为特征模型，要求每周产出≥5个可验证高危威胁特征（检出率98%，误报率≤0.1%）。分析引擎处理延迟须≤100毫秒，并通过数字孪生环境进行战场级验证。

#### 自动化响应处置与运营闭环需构建AI Agent决策框架

供应商必须开发具备认知级威胁解构能力的作战引擎：

跨模态语义融合：利用LLM驱动的多模态Transformer架构（融合ViT/CLIP/Wav2Vec模型），实现二进制协议流、传感器振动波形、多语种文本的联合特征提取（如从钻机异常振动频谱中识别针对SCADA系统的物理层攻击），关联准确率≥99.99%。

动态威胁狩猎：基于信创图数据库（如TuGraph）构建十万亿级节点战术知识图谱，通过强化学习驱动的攻击路径推演（RL-Pathfinder），实时计算千级并发攻击链的爆炸半径。

零日威胁预言：利用LLM的少样本生成能力，结合全球漏洞披露趋势与工控设备固件差分分析，主动构建未公开漏洞（0day）的行为特征模型，要求每周产出≥5个可验证高危威胁特征（检出率98%，误报率≤0.1%）。分析引擎处理延迟须≤100毫秒，并通过数字孪生环境进行战场级验证。

#### 性能优化与高可靠保障需满足生产环境指标

供应商须实现较高的系统可靠性：

EB级实时计算：基于自主可控的分布式流式计算框架（如开源欧拉操作系统优化版Flink），实现日均50PB数据的亚秒级处理（P99延迟≤800毫秒），资源调度算法需通过形式化验证（提供TLA+证明）。

战时级韧性：在遭受APT组织高强度攻击（如TB级DDoS）时，通过LLM驱动的动态资源调度（如自动隔离受损云容器并启动边缘计算备份节点），保障控制功能的持续运行（RTO≤1秒，RPO=0）。系统需通过第三方模拟战时压力测试（持续720小时APT攻击下服务降级率≤0.001%）。

验收标准包括：信创全栈兼容性100%、威胁分析误报率≤0.01%、处置闭环延迟≤300毫秒、系统可用性99.999%。

## **2、工作量清单**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 服务项 | 数量 | 单位 | 评估工作量（人天） |
| 1 | 智能攻击研判应用开发服务 | 1 | 项 | 约140人天 |
| 2 | 渗透测试智能应用开发服务 | 1 | 项 | 约120人天 |
| 3 | 实时智能数据分析开发服务 | 1 | 项 | 约110人天 |
| 4 | 网络安全智能运营一体化平台开发服务（含：（1）智能网络安全知识通解助手开发服务（2）网络安全数据决策应用开发服务（3）安全运营一体化管理平台建设服务等三项服务）  | 3 | 项 | 约230人天 |
|  |  | 总计 |  | 约600人天 |

## **3、服务地点**

北京

## **4、服务期限**

自合同签署后6个月

# 执行标准/规范

**下列标准规范对于本文件的应用是必不可少的，本次采购主要引用的采购标准如下，当标准规范与技术文件相冲突时，应按照文件优先级执行：在寻源和合同的执行过程中，如果技术文件和各类标准等文件之间出现矛盾，卖方应在交货之前向买方提出澄清申请。文件的优先执行顺序由高到低为：**

**●中华人民共和国强制执行的国家法律、法规和标准**

**●中国海油集团公司强制执行的行业标准**

**●项目所在地强制执行标准**

**●本技术文件所附文件**

**●非强制执行的行业标准**

**●非强制执行的国家标准**

**●通用的国际标准**

本项目执行标准/规范详见技术要求各设备引用标准，其中企业制定的标准详见附件：

|  |
| --- |
| CGBZ213-2022 数据治理数据分析服务 |

# 服务要求

## **服务具体要求：**

## **业务调研与分析**

1. 通过对建设目标的详细分析并逐步细化确定调研范围、内容、具体要求，保证不遗漏且分析到位。
2. 对业务域、业务对象、业务活动进行全面梳理分析，从实际业务应用出发对成果资料进行标准化处理。
3. 收集服务相关资料包括但不限于系统资料、数据编码、数据库设计资料、数据规范的国标、行标等。保障业务系统、业务数据的梳理与分析的全面性。

## **业务模型与数据标准建设**

1）对本服务范围内业务流程、业务单元、业务活动、数据集等进行梳理与完善，完善业务逻辑关系形成业务模型，同时保障模型提醒未来的可持续建设。

2）标准建设成果与国家及行业相关标准相匹配，并具备开发生产适用性、满足通用性原则。

3）组织各专业权威专家对相应的成果进行评审及确认，保障成果可靠、适用、统一。

## **(3) 源头规范建设**

1）梳理现有采集规范和源头业务系统，建立源头数据规范，确保业务上数据的源头采集和数据的唯一性。

2）建立数据采集规范，为数据采集、管理、维护、上报等提供管理方式和配套规章制度。

## **(4) 数据质量规范建设与工具完善**

1）要求对明确约束条件的全部业务数据制定质量检验规则，保障对数据检验的完整性与精确性。

2）通过工具完善实现数据的一致性、及时性、准确性的校验。

3）对特殊的采集需求，进行定制模板的建设与维护，配合进行采集入库的数据验证规则制定与完善。

## **(5) 数据保障管理体系及安全要求**

1. 数据保障管理体系

进行数据管理制度的设计工作，规范数据的采、存、管、用等工作，最终形成包括但不限于《数据标准》、《数据质量规则》、《数据采集规范》等文档。

1. 围绕业务数据应用范畴建立数据安全管理策略与制度，通过数据分级、用户级别以及权限定义进行数据访问安全管理。
2. 安全体系的建设要包括安全策略、安全组织、安全技术及安全建设与运行。
3. 数据安全建设要求和同类系统安全等保级别约定条件。
4. 服务人员的约束和保密要求，包括保护客户信息、保密技术资料等

服务方需与甲方签署保密协议，须对技术文件以及由甲方提供的所有资料、技术文档和信息等予以保密，未经甲方书面同意，服务方不得以任何形式将招标人保密信息披露向第三方（包括与合同无关的投标人员工和政府部门等），亦不得将该等信息用于与本合同无关的用途。 保密信息包括但不限于：本合同内容：甲方提供的与本合同有关的任何技术信息、图纸、样本、资料等：甲方提供的或服务方获得的与项目或甲方有关的任何技术和商务信息。

1. 服务人员的知识产权要求

服务方在项目工作中产生的所有软件开发成果物及成果物所属的发明、设计、构思、资料、技术、技术文档等（以下简称为相关发明），以及开发成果物与相关发明的知识产权（包括软件著作权、发明专利、实用新型专利和外观设计专利、论文发表等权利）及申请权，均归甲方所有。乙方不得就本项目实施相关工作所涉及的技术、理论撰写并发表论文。

1. 服务人员的安全要求，需要遵守相关安全制度和规定，确保服务过程安全可靠。
2. 密码安全：服务人员应使用符合甲方网信安全管理规定要求的强密码，并且定期更新。
3. 防范网络钓鱼：服务人员应警惕来自不明来源的邮件，附件和链接，并避免点击可疑链接。
4. 安全浏览：服务人员应在访问网站时使用 HTTPS，确保数据传输加密。
5. 遵守公司政策：服务人员应遵循甲方网络安全政策，如禁止在工作场所使用私人设备，及定期进行安全培训。
6. 安全意识培训：服务人员应定期接受甲方网络安全培训，提高对网络威胁的认识。

## **(6) 数据清洗迁移**

1）梳理主数据、参考数据和业务数据，按照标准规范和治理流程进行数据清洗和迁移，以保障数据的一致性，达到数据资产可视化和开发生产数据共享的目标。

2）通过一致性检查无效值和缺失值的处理对数据库中残缺数据、错误数据、重复数据进行清洗并统一迁移至标准库。

## **(7) 培训要求**

1. 培训内容
2. 服务方需要为甲方定制培训方案（包括：培训教材、培训对象、目标、方式、计划、反馈等）来满足甲方的需要，培训工作由服务方承担,确保甲方有效的掌握系统的技术、业务、开发与维护等知识。
3. 服务方将为甲方提供开发、使用及维护等方面的培训，内容包括但不限于系统总体设计、系统业务流程、模型开发、训练、部署、系统运维等，培训时间不少于10天。培训中需要结合项目代码，并进行必要的操作。
4. 培训效果

根据甲方实际需求开展相关培训。通过培训，可达到以下效果：

1. 甲方用户可操作和使用系统；
2. 甲方用户可独立部署和运维系统，系统出现问题后，招标人能诊断并处理故障；
3. 甲方用户了解系统框架、关键开发技术、开发流程等；
4. 甲方用户可参与到系统搭建工作中。

# 配备资源要求

乙方应根据项目建设内容配备适当的项目实施团队资源，并提供符合要求的人员，给出具体角色和职责，团队构成建议，要求包括但不限于以下人员资质要求清单中人员岗位。

核心人员要求驻指定现场进行办公。保证项目团队稳定性，在项目实施过程中，不得随意更换关键成员。

## **人员要求**

1. 本合同履行过程中，乙方应建立并维系合法、适当的劳动关系。
2. 乙方自行承担提供服务人员的医疗、保险、劳保、福利、工资、奖金、管理费等所有福利待遇和其他一切费用。
3. 乙方应采取措施确保其工作人员在执行工作过程中严格遵守本合同和法律法规的规定。甲方有权要求乙方更换其工作人员，乙方应严格执行甲方的要求。
4. 具体人员资质要求如下:

|  |  |
| --- | --- |
| **岗位类型** | **能力要求** |
| 项目经理 | 1. 软件、信息化、计算机等相关专业本科以上学历；
2. 具备5年以上软件开发与实施项目工作经验；
3. 具备在有效期内的PMP认证证书；
 |
| 高级AI算法架构师 | 1. 至少5年从事相关工作背景，有学习应用模型、算法和训练/部署/优化从业经验；
2. 能熟练地使用AI领域科技语言和技术进行交流；
3. 能够独立完成设计和实现复杂的算法系统，确保其高效、可靠和安全。
4. 熟练掌握目标检测 / 图像分类/ GAN / RNN / Transformer / GPT / Bert / Auto Encoder 等经典模型的部分或全部；
5. 熟练使用诸如TensorFlow, PyTorch,Paddle等学习框架；
6. 具有人工智能应用领域的实际行业知识和经验；
7. 具有在GPU / TPU / CPU上加速AI训练或推断计算性能的经验；
 |
| 高级数据架构师 | 1. 通常要求具有5-10年的相关工作经验，特别是在大数据或数据库领域有深厚的经验积累‌ 。
2. 精通数据仓库建模理论、模型设计、ETL设计思路，熟悉数据仓库数据分层架构，精通维度模型设计。
3. 具备大型数据仓库架构设计、模型设计和处理性能调优等相关经验‌。
4. 熟练掌握关系型数据库、NoSQL数据库、数据湖等技术，并能评估不同技术的优缺点，为企业选择最优方案‌。
 |
| 后端开发工程师 | 1. 精通java语言，熟悉X86 、ARM开发平台；
2. 至少熟悉掌握2种数据库（一种结构化数据库、一种非结构化数据库）；
3. 熟悉mysql数据库事务和查询性能调优；
4. 熟悉java的web开发；
5. 熟悉主流的后端技术栈java开发，包括redis,nginx,主流mq；
 |
| 数据业务顾问 | 1. 收集各方需求，进行业务分析，协助评估需求的合理性；
2. 作为高级业务顾问，向产品经理提出业务产品需求、数据需求；
3. 从业务视角，评估能源产业链政策模拟和策略发展框架中数据产品功能的可用性、业务流程的合理性；
4. 本科及以上学历，5年以上相关框架体系建设工作经验，数学、统计、计算机相关专业背景者优先；
5. 具有数据分析挖掘、数据可视化、数据产品研发的实际开发实施经验；
6. 具有能源产业链相关工作经验；
7. 具备较强的沟通协调能力；
 |
| 测试工程师 | 1. 精通精通测试流程和测试用例设计方法,能主动进行问题查找和钻研；
2. 具备工业自动控制测试经验；
3. 有性能、安全、白盒测试等专业测试领域经验；
4. 熟悉一种编程语言者、具备一定的嵌入式开发经验；
5. 具备良好的沟通能力，高效的执行力，工作责任心强。
 |
| 前端开发工程师 | 1. 熟悉html5， CSS，VUE， Bootstrap， Javascript等技术；
2. 熟悉HTML/CSS等网页制作技术，熟悉页面架构和布局，了解各种主流浏览器之间CSS的兼容问题。
 |
| 数据标注工程师 | 1. 了解数据标注交付标准；
2. 熟悉labelImg，labelme等开源标注工具的使用；
3. 能写python脚本，对标注结果和样本进行处理；
4. 熟悉训练样本的采集；
5. 熟悉构建测试用例。
 |
| 高级数据工程师 | 1. 熟练掌握Python、Java、Scala语言；
2. 精通SQL，能高效开发、查询和优化基于Hive、Spark框架的数据开发任务；
3. 熟练使用PowerDesigner、PDManer、DataWorks、CDH等工具或平台；
4. 熟悉Hadoop、Spark等大数据处理框架；
5. 具备强大的分析、解决问题的能力和团队协作能力。
 |
| 中级数据工程师 | 1、至少2-4年数据相关工作经验，具备数据采集、清洗、转换、存储及分析全流程实践经验；2、熟练掌握SQL语言，能高效编写复杂查询语句，实现数据提取、处理和分析；3、能够独立设计和构建数据仓库或数据湖架构，确保数据存储的高效性与可靠性；4、精通至少一种数据处理工具或框架，如Hadoop、Spark、Flink等，可进行大规模数据处理与计算；5、熟悉Python或R等编程语言，能编写脚本实现数据自动化处理、数据可视化及简单的算法模型搭建；6、具备数据治理意识，能够制定数据质量标准，保障数据的准确性、完整性和安全性； |
| 运维工程师 | 1. 熟悉linux、windows、麒麟操作系统，熟练的shell脚本能力，能独立安装部署各类系统软件；
2. 熟悉mysql、oracle、人大金仓等数据库基础命令和运维；
3. 熟悉k8s、docker使用和安装部署；
4. 基础网络知识、熟悉基础网络问题的排查和处理；
5. 熟悉weblogic、tomcat等应用中间件运维和管理。
 |
| 大模型开发应用工程师 | 1、2-3年以上AI/机器学习相关开发经验，至少1年大模型相关经验2、熟练使用Python，熟悉PyTorch/TensorFlow/JAX等学习框架，熟悉CUDA/并行计算，能优化训练/推理性能，了解分布式训练（如FSDP、DeepSpeed、Megatron-LM等）3、熟悉Transformer架构，理解自注意力机制、位置编码、FFN等核心模块，掌握大模型预训练、SFT（监督微调）、RLHF（强化学习对齐）流程4、能设计高质量Prompt，优化Few-shot/Zero-shot学习效果，熟悉Embedding优化（如BGE、OpenAI Embedding），能结合检索系统（如ElasticSearch）提升生成质量5、能基于大模型构建Agent，熟悉ReAct、Tool Use、Planning等Agent框架，能结合外部API（如搜索引擎、数据库）增强Agent能力 |
| 技术架构师 | 1. 掌握分层架构、微服务、事件驱动等主流架构模式，能够设计高并发、高可用的分布式系统。
2. 精通至少1-2种编程语言（如Java/Python/Go），熟悉设计模式并能编写高质量、可维护的代码。
3. 熟悉分布式计算框架（如Spark）、消息队列（Kafka/RabbitMQ）、缓存（Redis）和数据库优化策略（SQL/NoSQL）。
4. 熟悉安全机制（OAuth2.0/JWT）、数据加密（TLS/AES）和合规要求（GDPR/CCPA）
5. 具备云原生技术栈能力（Docker/K8s），掌握CI/CD工具（Jenkins/GitLab CI）和基础设施即代码（Terraform）。
 |

## **场地要求**

根据甲方要求提供驻场服务。

# 服务进度跟踪

## 1、服务进度

包括项目计划、进度管理、进展报告、技术质量管理等方面的内容。

1. 在项目开展过程中，根据需要，甲乙双方需保持良好沟通，服务方每双周五中午前报送本双周周报，直至项目验收；
2. 合同签订一周内，服务方需提交项目进度计划、人员安排计划等；

## 2、监造

包括现场监造、质量监造等方面的内容，旨在确保服务的实现符合规定的技术标准，并保证服务过程中的质量和安全性。

1. 服务方应对本实施项目总体协调，承担项目实施过程中的项目管理责任，包括：针对项目方案设计、项目进度、实施风险、资源投入以及最终交付品的总体管理。
2. 服务方应在事前提出明确的项目质量管理标准和流程，提供确保其内部质量程序遵循项目管理的方法概要，提供甲方所要求的确保质量的活动。在项目启动后，该概要由双方人员共同商议，并由甲方人员最终认可。
3. 服务方应采用科学、高效、可行的项目管理方法来进行项目管理，须针对本项目成立专门的项目组，该项目组能够依据项目管理体系制定并严格执行项目实施过程中的需求方案、进度计划和其他管理方案，保证按计划在合同费用内、保质保量完成甲方委托的项目工作。

## 3、服务项目考核要求

1. 乙方应提供高效、及时的服务，确保按照项目计划按时完成各个阶段的任务；确保关键里程碑的完成时符合预定的时间节点。
2. 乙方应定期向甲方提交工作进度报告，包括但不限于周报、月报等形式，详细说明工作进展情况、存在的问题及解决方案等。
3. 乙方应确保项目执行过程中，与甲方沟通时，使用规定的沟通方式（如邮件、即时通讯软件）时能够及时响应。紧急问题需在 1 小时内响应，重要问题在 4 小时内响应，一般问题在 24 小时内响应。
4. 乙方须保证对甲方所提出的问题予以及时且有效的解决，确保问题解决情况达到甲方所要求的问题解决率标准。

## 4、服务人员的态度和素质要求

包括服务态度、沟通能力、职业道德等；

1. 管理人员逻辑分析能力强，善于沟通，有良好的沟通能力和团队合作能力，具有带领后端团队开发的能力。业务开发人员具备高效的执行力，工作责任心强抗压能力强，有敏锐的观察力，高品质的审美能力，善于沟通和坚守原则并富有创新精神。
2. 服务人员的数量和分工要求，需要根据服务需求确定所需服务人员数量和分工；

# 服务及验收标准

## 1、验收形式

双方应依据合同约定，由甲方按照里程碑节点对乙方的阶段工作情况执行分阶段验收。

## 2、验收标准

1. 乙方应根据经过甲方确认的业务需求完成蓝图设计方案，设计结果应形成统一完整的蓝图设计报告，并经甲方审核通过；
2. 乙方应按照合同约定完成项目全部功能需求的开发测试工作并完成上线审查，最终验收应形成双方签字版的完工验收报告，提交的验收文件包括但不限于以下内容：
3. 蓝图设计报告：
4. 完工验收报告；
5. 乙方应完成对甲方的用户培训、提供必要的用户手册等指导性资料。

# 质量保证

## 质保期时间要求

12个月

## 2、质保期内甲乙方各自具体责任

甲乙双方需要根据具体的服务合同定义确认双方的职责

1. 甲方责任：在质保期内，甲方有权按照合同约定和验收标准对乙方提供的服务和工作成果进行质量监督检查，及时向乙方反馈发现的问题，并为乙方开展质保工作提供必要的协助和支持，如提供系统运行环境信息、用户操作记录等。
2. 乙方责任：乙方应建立专门的质保团队和服务热线，在质保期内对系统进行定期巡检和性能监测，及时处理甲方反馈的问题。

## 3、故障处理保障

确保在服务发生故障时，会及时处理，并及时提供解决方案，确保不会影响服务质量。

1. 质保期内技术联络与响应：服务方在接到招标方通知24小时内给予答复，48小时内达到现场开始解决问题。
2. 质保期内，针对日常及重大活动期间出现故障的时候，须能够及时提供应急措施，以确保整个业务系统的不中断。用户界面程序异常停止后，不应影响服务器端系统和其它用户界面的正常运行。

## 4、违约责任要求

1. 甲乙双方需要根据具体的服务合同定义来确认违约责任要求，如乙方承诺，其任何工作和交付的工作成果符合本合同、法律法规、行业规范、标准和良好的行业惯例的要求，不存在任何缺陷。

## 5、风险管理保障

确保服务提供的安全性，例如法律风险、安全保密要求、知识产权等的保障。

服务方在项目工作中产生的所有软件开发成果物及成果物所属的发明、设计、构思、资料、情报、技术、技术文档等（以下简称为相关发明），以及开发成果物与相关发明的知识产权（包括软件著作权、发明专利、实用新型专利和外观设计专利、论文发表等权利）及申请权，均归甲方所有。服务方不得就本项目实施相关工作所涉及的技术、理论撰写并发表论文。

**5、相关证书、资质保证：**

证明服务提供商的合法、合规的证书和资质。