

采购内容及项目要求

一、系统概况

山东大学网络安全智能化提升服务，包括 AI 安全风险降噪、AI 事件研判、安全智能体开发、AI 大模型安全服务算力等内容。

二、技术要求

序号	名称	技术规格指标	数量
1	AI 安全告警降噪服务	投标人需提供 AI 大模型安全服务工具，与山东大学现有安全态势感知平台（免费向中标人开放 API）对接，对平台收集的海量告警日志信息进行实时智能化分析，进行告警降噪。通过大模型微调形成告警降噪安全分析能力，综合分析研判告警行为是否恶意，告警结果是否成功，并可根据研判结果输出告警解读。	1
2	AI 事件研判服务	投标人需提供 AI 大模型安全服务工具，与山东大学现有安全态势感知平台（免费向中标人开放 API）对接，针对重大事件开展深入分析与研判，通过关联对应告警，同时自动收集并分析相关日志和网络流量数据，迅速识别异常活动模式，通过学习正常网络行为，有效检测出偏离常态的行为模式，减少误报和漏报概率。	1
3	AI 报告撰写服务	投标人需提供 AI 大模型安全服务工具，依托 AI 自然语言识别与理解技术，对山东大学现有态势感知系统等安全基础设施输出的各类安全报告进行风险信息、数据指标等核心内容的快速精准提取，根据运营人员自定义报告模板与输出格式，实现多源安全报告的自动化整合与分析，最终输出逻辑清晰、高质量的安全分析报告。	1
4	安全智能体开发服务	投标人需提供 AI 大模型安全服务工具，可根据山东大学特殊安全需求，开发零代码或低代码智能体。	1
5	AI 大模型安全服务工具算力要求	△投标人需提供 AI 大模型所需算力要求： CPU≥2 颗，（单颗 2.0GHz，12 核 24 线程），GPU 计算卡≥8 块（单卡 FP32 运算能力≥59TFLOPS，显存≥48G），内存≥32GB*4，硬盘≥8TB*4，网络接口≥2*万兆光（含 2 个多模光模块），≥4*千兆电口（投标人需在本地	1

		部署算力资源，同时提供承诺函并加盖投标人公章)。	
6	AI 大模型安全服务工具性能要求	服务工具具备推理能力：推理速度不低于 30 字符/s，支持打字机模式输出，在模拟真实场景的输入和输出情况下，同时处理的请求数不低于 20；安全垂域知识块综合准确率不低于 95%（知识块包含但不限于：安全通用知识、安全运营、工具操作指导、代码编写、安全法规、敏感词）；支持不少于 32K token 长度上下文。	1
7	AI 大模型服务工具统一展示能力	智能体交互中枢搭载多模态交互引擎，支持自然语言指令的智能解析与响应；安全智能体开发平台内置可视化编排引擎，通过零代码/低代码拖拽式界面支持用户快速构建、测试及部署智能体服务，并提供运营管理；提供≥100 个智能体包含：安全规划与设计、安全建设与实施、安全运行与维护、安全应急与防御等领域的专业级智能体应用，覆盖威胁检测、风险评估、合规审计等场景。	1
8	AI 大模型服务工具智能体扩展能力	△服务工具具备智能体扩展能力：在智能体与异构业务平台对接时，以 open API 接口的形式集成到异构业务系统中，如有双方数据定义存在不同时，支持修改智能体接口参数，调整智能体出参入参要求的方式，提升接口适配工作的开放性与兼容性。（提供证明材料）	
9	AI 大模型服务工具具备异构模型调度能力	△服务工具具备异构模型调度能力：具备对其他异构模型的兼容性，支持将本地通用大模型（如 DeepSeek）或业务大模型注册并进行调度使用。（提供服务工具真实功能截图，并加盖投标人公章）	
10	AI 大模型服务工具生态共享能力	#服务工具具备良好的生态共享能力：对外支持以扩展插件、API 接口等形式实现智能体的调用；对内支持以 API、MCP 等多种形式接入外部能力，如本地设备的数据接入与操作下发。	
11	AI 大模型服务工具开放 API 接口能力	△服务工具具备开放 API 接口能力：支持提供数据分类分级开放服务接口；支持智能体开放服务接口，提供智能体服务使用指南；支持知识检索与创作-开放服务接口。（提供服务工具真实功能截图，并加盖投标人公章）	

12	结构化条件约束能力	△服务工具具备结构化条件约束能力:当检测到结构化约束超出可承载范围时,将判断是否支持该输出,并向用户提供优化建议,以保障推理服务稳定、连续运行。当结构化约束复杂时,平台和接口返回错误提示信息,保证系统稳定。(提供服务工具真实功能截图,并加盖投标人公章)	
13	AI 大模型服务工具安全智能体	△服务工具具备智能体开发能力:至少支持以下两种方式的智能体组合创建,零代码与低代码方式。(提供服务工具真实功能截图,并加盖投标人公章)	1
14	服务工具代码执行插件能力	#服务工具具备代码执行插件能力:通过容器服务整合多项隔离技术与动态资源管理机制,适合高并发场景下的多租户隔离需求。	1
15	服务工具智能体管理能力	#服务工具具备智能体管理能力:支持公开发布智能体/组合筛选,支持按多个维度进行筛选;支持公开发布智能体/组合使用,要求提供提示词输入、切断会话、清空记录、收藏、复制等功能。	1
16	服务工具安全插件管理能力	△服务工具具备安全插件管理能力:支持代码执行器、文档解析器、图片处理工作集、知识检索工具集等种业务及安全插件能力调用,满足告警研判、应急处置等相关智能体的自主构建需求。(提供服务工具真实功能截图,并加盖投标人公章)	1

注: 1、本项目功能要求中的所有名词(除国家标准、行业标准已规定的之外),仅代表采购人对功能的需求,不代表该功能的名称被指定。

2、招标软件产品的各功能模块划分,仅代表系统架构和系统实现的一种合理组合,投标人可提供覆盖本项目技术需求的其他架构软件或模块组合后的产品进行报价,并逐条列明参数响应情况。

三、商务要求

山东大学采购商务条款响应一览表

项目序号	项目名称	采购人要求
1	成交价	人民币
2	交付期	合同签订在 1 个月内完成主体开发并部署。
3	付款方式	合同签订 1 个月内支付 100%的费用。
4	服务验收	A. 服务验收由专家组和中标人联合在山东大学进行, 验收条件按照合同规定执行, 验收合格后, 开具验收报告。 B. 中标人应提供各种文档资料和中文电子版说明书以及调试所需要的工具。
5	培训	中标人应对用户人员进行技术培训。使其能掌握有关系统的使用、维护和管理等工作要求。