天融信AI智能体安全评估服务

www.topsec.com.cn

服务概述

天融信 AI 智能体安全评估服务，依托九维度标准化评估框架，覆盖 39 项通用标准化检查项，同时配套 OpenClaw、Hermes Agent、WorkBuddy 三款主流智能体专项检测清单，完整覆盖智能体底层硬件、系统环境、应用本体、渠道集成、插件 MCP、知识库、数据流转、网络传输、运营审计全生命周期安全检测。

九大评估维度



服务优势

检测覆盖AI智能体全生命周期风险

九大评估维度，完整覆盖AI Agent从部署到运营的全链路风险域，专门针对智能体可执行、可操作系统的高权限特性设计。39项通用标准化检查项，评估过程可复测、可量化，便于客户内部审计、问题闭环跟踪。

主流智能体专项检测能力

配套三款主流智能体专项检测清单。覆盖底层硬件、系统环境、应用本体、渠道集成、插件MCP、知识库等完整链路，解决智能体使用过程中带来的安全风险。

重点识别智能体高危风险

针对AI智能体高权限执行的核心风险，重点识别权限滥用、恶意篡改、漏洞利用、MCP插件风险等，区别于普通大模型内容安全检测。既测“模型输出内容安全”，更测“智能体执行动作带来的系统、业务风险”。