天融信自动化渗透测试系统

www.topsec.com.cn

产品概述

天融信自动化渗透测试系统（TopPTM）是一款深度融合大模型技术与多智能体协同架构的新一代自动化渗透测试平台，系统以“AI算力”为核心驱动力，深度模拟红队专家的对抗性思维与攻击链逻辑，提供“AI全自动渗透”与“Web漏挖掘”两大核心场景，将传统高度依赖人工经验的渗透测试，全面升级为自主化、智能化、可量化的智能安全评估体系。



设备示意图

产品特点

AI赋能，全面升级

产品以大模型为能力底座，采用RHP技术架构，重构了基于多智能体协作的自动化渗透测试体系，用智能引擎不断提升智能体的能力水平，用控制引擎管控智能体行为，全面提升产品的漏洞挖掘能力。

全面覆盖，精准定位

产品依托AI驱动的漏洞挖掘能力，可显著提高对逻辑、长链、复合等类型漏洞的发现能力，支持基于智能体的自动化漏洞验证和利用，可大幅降低漏洞挖掘的误报率。在国内外知名靶场的实测渗透成功率超过80%，在真实业务场景下测试效果显著。

一键执行，效率跃升

产品支持一句话任务描述与一键式任务下发，由智能体自动完成信息收集、攻击面分析、漏洞验证、漏洞利用、后渗透取证、报告生成等渗透测试全过程，大幅降低渗透测试的人力成本投入与时间周期。

专业服务，安全可控

产品配备自研的工具库、知识图谱和RAG语料库，可为用户提供专业的安全服务；支持实战经验自动本地沉淀，让智能体越用越智能；引入授权约定、人机回环等机制，确保智能体行为的安全可控。

典型应用

等保/合规驱动下的自动渗透测试

满足等保2.0和公安部176号文等行业合规对实战化渗透测试的刚性要求，从根源上避免因测试盲区导致的合规不通过风险。

攻防演练与红蓝对抗支撑

作为红队“AI攻击手”，抢占得分先机；同时可帮助蓝队提前发现防御盲区与响应短板，在正式演练前完成体系加固。

常态化安全治理与风险发现

实现7×24小时持续性自动化巡检，动态探测全量在线资产，适配动态变化的资产环境，将一次性检测升级为常态化安全治理。

软件应用上线前准入测试

帮助企业在上线前对软件应用进行全面安全“体检”，前置规避安全风险隐患，杜绝软件应用“带病”上线运行。