

题目编号：SH-24

AI Agent 驱动的动态攻防推演靶场平台 比赛方案

一、发榜单位

杭州安恒信息技术股份有限公司

二、题目名称

AI Agent 驱动的动态攻防推演靶场平台

三、题目介绍

为落实《网络安全法》和《国家网络安全战略》关于提升实战化攻防能力的要求，响应“十四五”规划中强化关键信息基础设施安全防护的部署，聚焦网络安全攻防演练与关键人才培养过程中的动态化、智能化需求，当前存在三大核心痛点亟待突破：

场景静态化与威胁动态化矛盾：传统靶场无法及时模拟最新业务场景和新型攻击手段，导致演练效果滞后于实际威胁；

攻击路径单一性与实战复杂性脱节：人工设计的攻击路径无法覆盖多样化的渗透手段，缺乏智能推演能力；

评估主观化与量化反馈缺失：演练效果依赖人工复盘，缺少对攻防态势和人员能力的自动化评估。

针对上述问题，以网络安全攻防动态推演为突破方向，依托生成式 AI、AI Agent、大数据分析等技术，设计具备动态演

化能力的靶场系统，实现以下四大核心功能：

1. 动态场景生成：自动生成与真实业务相关的多维攻防场景，并能实时调整环境参数；

2. 智能攻击模拟：通过攻击 AI Agent 模拟复杂的攻击链，如高级持续性威胁（APT）和社会工程攻击，支持攻击路径的自主决策；

3. 自适应防御决策：防御 AI Agent 动态优化安全策略，实现自动化的漏洞修复、威胁阻断和攻击溯源；

4. 演练评估自动化：构建量化模型，自动生成演练评估报告，并提供参与人员的技能画像和提升引导。

四、参赛对象

本题目只设学生赛道。

参赛对象为 2025 年 6 月 1 日以前正式注册的全日制非成人教育的各类高等院校在校专科生、本科生、硕士研究生、博士研究生（不含在职研究生），参赛人员年龄在 40 周岁以下，即 1985 年 6 月 1 日（含）以后出生。

同一作品不得同时参加第十九届“挑战杯”全国大学生课外学术科技作品竞赛（以下简称第十九届“挑战杯”竞赛）其他赛道的评比。

参赛对象可以团队或个人形式参赛，每个团队不超过 10 人，每件作品可由不超过 3 名指导教师进行指导。可以跨专业、跨学校、跨单位、跨地域组队，但同一团队所有成

员均应符合本赛道相关年龄、身份要求。每件作品只可由 1 所高等院校作为参赛主体提交申报。

五、答题要求

参赛者应完成“动态攻防推演靶场平台”研发，实现“动态场景生成”、“智能攻击模拟”、“自适应防御决策”、“演练评估自动化”等功能。作品形式应包括如下三部分内容：

1. 文档材料：包括但不限于方案设计文档、开发文档、测试文档、用户手册、方案介绍 PPT、阐述演示视频等。

2. 程序材料：包括但不限于程序源代码、安装程序等（建议提供一键部署方案或者完整部署手册）。

3. 声明函：参赛方案原创性及保密性声明。

其他参赛者认为对参赛作品有辅助作用的材料均可作为附件提交，附件的质量和丰富度也会作为打分的参考之一。

六、作品评选标准

本选题初审和终审决赛的作品评选标准如下：

1. 完成度（40%）：动态场景生成、攻击模拟、防御决策、演练评估核心功能的完整性与可用性。

2. 实用性（20%）：已生成靶场支持的业务场景覆盖面、与真实业务的贴合度。

3. 可靠性（20%）：系统在攻防推演中的稳定性、Agent 决策的有效性。

4. 用户体验（10%）：可视化攻防态势界面、功能项的可

理解性、操作交互流畅度。

5. 扩展性（10%）：支持第三方信息源的接入、自定义场景编辑、多 Agent 协作框架扩展情况。

需要注意的是，本选题终审决赛由两部分组成：第一部分采用靶场逐层渗透比赛，晋级终审决赛的团队须挑选 3 人参加；第二部分采用线下集中答辩形式，按照作品评选标准开展评审。两部分成绩加权相加后形成每个参赛队伍的最终总分。

七、作品提交时间

2025 年 5 月-8 月，各高校组织学生参赛，安排专业人员给予指导，为参赛团队提供支持保障。

2025 年 8 月 15 日前，各参赛团队通过大赛申报系统提交作品，具体要求详见作品提交方式。

2025 年 8 月底前，由大赛组委会会同发榜单位共同完成初审，确定入围终审擂台赛的晋级作品和团队。

2025 年 9 月，发榜单位安排专门团队提供帮助和指导，各晋级团队完善作品，冲刺攻关参加终审擂台赛，角逐“擂主”。

八、参赛报名及作品提交方式

（一）报名方式

（1）参赛选手登录“挑战杯”官网 2025.tiaozhanbei.net，在“揭榜挂帅”擂台赛报名入口注册账号，登录大赛申报系统在线填写报名信息。报名信息提交后，下载打印系统生成的报名表。

(2) 申报人在报名表对应位置加盖所在学校公章。

(3) 将盖章版报名表扫描件上传至报名系统，等待系统审核。请参赛选手注意查看审核状态，如审核不通过，需重新提交。

(4) 系统开放报名时间为 2025 年 5 月 30 日—6 月 30 日，逾期后系统将自动关闭报名功能。

(二) 作品提交方式

请各参赛团队将参赛作品统一打包压缩提交至大赛申报系统，压缩包命名方式为：申报人所在单位-申报人姓名-作品名称-联系电话（例如：XX 大学-张 XX-XX 方案-手机号）。

九、赛事保障

根据实际需求为参赛学生团队配备专门指导人员，介绍技术细节要求、定期解答疑问。

赛事办公室设在安恒信息数字人才创研院，参赛过程中，参赛团队如需本单位提供与项目相关的其他必须帮助，请提前与赛事办公室联系，我们将在许可范围内给予参赛团队帮助。

十、设奖情况及奖励措施

1. 设奖情况

根据评分规则，综合评定参赛队伍成绩。设擂主 1 个(在特等奖中产生)，特等奖 5 个，一等奖 6 个，二等奖 8 个，三等奖 10 个。奖项不重复，奖金按队伍所获最高奖项授予。

2. 奖励措施

(1) “擂主”：奖金 10 万元，并向团队全体成员优先提供实习实践、就业岗位、人才引进等机会；

(2) 特等奖：奖金 2 万元，并向团队主要负责人（1 名）优先提供实习实践机会、就业岗位机会；

(3) 一等奖：奖金 1 万元，并向团队主要负责人（1 名）优先提供实习实践机会、就业岗位机会；

(4) 二等奖：奖金 0.5 万元，并向团队主要负责人（1 名）优先提供实习实践机会、就业岗位机会；

(5) 三等奖：奖金 0.2 万元，并向团队主要负责人（1 名）优先提供实习实践机会、就业岗位机会。

3. 奖金发放方式

以上奖金以汇款方式兑现，获奖者需提供接收奖金的银行卡信息，奖金在赛事结束并经公司审批后 3 个月内发放。全部获奖团队中应届毕业生参与杭州安恒信息技术股份有限公司招聘时，符合应聘条件者，直接进入面试环节，同等条件下可优先录用。

十一、比赛专班联系方式

1. 专家指导团队

顾问专家：丁老师，联系电话：17557280625

负责比赛期间技术指导保障。

2. 赛事服务团队

联络专员：叶老师，联系电话：15958032775

联络专员：王老师，联系电话：15068862417

负责比赛期间组织服务及后期相关赛务协调联络。

3. 联系时间

比赛期间工作日（9:00-17:00）

附：发榜单位简介

杭州安恒信息技术股份有限公司（简称“安恒信息”）成立于 2007 年，于 2019 年在科创板上市（股票代码：688023），注册资本 10249.8747 万元。公司现有员工 3000 余人，在全国设有 2 大总部，6 大产业基地，30 多个分公司及办事处，拥有数百位全国一线的核心安全专家以及具有创新力和自主知识产权的网络安全产品线，2024 年公司营收 20.4 亿元。

作为行业领导者之一，安恒信息依托恒脑·安全垂域大模型，形成以 DAS（D 即 Data-数据、A 即 AI-人工智能、S 即 Services-服务）为企业核心战略支撑，以网络安全、数据安全、云安全、信创安全、密码安全、安全服务等为主的数字安全能力，为逾 10 万家政企单位提供数字安全产品及服务。

公司研发创新实力强大，技术人员占比约为 65%，截至 2024 年 12 月，共申请专利 2956 项，参与制订信息安全类国家标准 50 项。先后成为“大数据网络安全态势感知及智能防控技术国家地方联合工程研究中心”，国家级重保核心单位，国家级博士后科研工作站，并承担“国家发改委信息安全专项”、“工信部创新发展工程项目”国家级、省市级科技计划项目 50 余项。公司先后获评全球网络安全创新 500 强、中国品牌 500 强、2023 年度卓越上市公司、2024 全国数字贸易企业百强、领军型浙江数商等荣誉，荣登“2024 民营企业发明专利 500 家”榜单等，入选浙江省产教融合试点企业、浙江省职业技能等级认定试点企业。