

题目编号：XH-202614

AI+安全大模型平台的智能体研究 比赛方案

一、发榜单位

深信服科技股份有限公司、张家口默然教育科技有限公司

二、题目名称

AI+安全大模型平台的智能体研究

三、题目介绍

当前人工智能已成为引领新一轮科技革命与产业变革的战略性技术，其安全、可靠、健康发展受到国家高度重视。2025年9月，《人工智能安全治理框架》2.0版正式发布，明确提出要构建涵盖技术防护、价值对齐、协同治理的可信AI准则，并特别强调应对AI应用衍生出的社会与环境等次生风险确保AI始终处于人类控制之下。技术层面，以大模型为代表的AI技术正深刻重塑网络安全的攻防格局。一方面，GPT-4、DeepSeek等基础模型的突破性进展，展现了强大的代码理解、语义分析和复杂任务推理能力，为构建能够理解安全业务、自动化执行复杂分析任务的“安全智能体”奠定了技术基础。另一方面，安全领域面临的挑战日益严峻：攻击方可能利用大模型生成更具迷惑性的钓鱼邮件、自动化挖掘漏洞，甚至生成难以检测的

恶意代码，使得传统依赖规则和单一小模型的检测手段难以应对。为了解决这些 AI+网络安全中的业界难题，因此特挂榜此赛题。

本赛题依托深信服 AI 安全平台，以“智能融合、化繁为简、实战有效”为核心理念。参赛团队需利用平台提供的安全大模型底座（集成 DeepSeek、Qwen 及深信服自研安全 GPT 等）、AI 共创引擎及安全数据底座，结合当前主流的大模型、智能体开源技术框架，探索大模型在网络安全领域的深度应用。竞赛采用“分层递进”的任务模式，旨在考察参赛团队从基础的智能体编排到复杂的自主决策系统的全栈能力。

主要任务包括：

1.基础任务：场景化安全智能体构建

基于深信服 AI 安全平台内置的垂域大模型（运营 GPT、检测 GPT 等）和低代码编排引擎，开发解决单一特定安全痛点的智能体（Agent）。如“安全报告自动生成”“告警误报剔除”“漏洞排查与闭环”等高频安全运营场景。

2.进阶任务：领域知识增强与工具扩展

利用高级技术增强模型的专业深度，或通过代码开发扩展智能体的行动能力。如构建高质量的安全垂直领域知识库（如行业监管政策、最新的 0day 漏洞原理、ATT&CK 技战术图谱），或利用 RAG（检索增强生成）技术，解决大模型在特定领域的“幻觉”问题，提升回答的准确性与合规性。

3.挑战任务：构建“超级智能体”与自主闭环

（1）目标：打造具备复杂逻辑推理能力和跨域协同能力的“超级智能体”（**SuperAgent**）。

（2）任务要求：

其一，思维链（**CoT**）应用：要求智能体在处理复杂攻击事件时，能展示完整的“思维链”推理过程（例如：从流量异常→关联终端进程→定位身份账号→判定内鬼行为）。

其二跨域协同与闭环：智能体需能充分理解用户指令，根据多源安全数据（流量、端点、日志），并能自主规划任务，决策并调用各类安全工具（如防火墙封禁、**EDR** 隔离），并有观测、反馈、重新规划的 **ReAct** 能力，实现从发现威胁到处置闭环的全自动化，挑战“零人工干预”的安全运营极限。

四、参赛对象

学生赛道：2026 年 6 月 1 日以前正式注册的国内全日制非成人教育的普通高等学校在校专科生、本科生、硕士和博士研究生（不含在职研究生），以及全日制职业教育本科、高职高专在校学生，可通过学生赛道申报作品参赛。

高校青年教师在指导学生参赛的同时不得以参赛人员身份参加同一选题比赛。发榜单位及同发榜单位有相关隶属关系单位的青年不得参加本单位选题比赛。

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、科研院所等作为参赛主体提交申报。

五、答题要求

参赛者应完成“基于 AI+安全大模型平台的智能体”研发，作品形式应包括如下内容：

1. 文档材料：内容包括但不限于程序源代码、设计文档、开发文档、测试文档和总结报告等。
2. 宣讲 ppt 和演示视频（3 分钟以内）
3. 系统部署：完成智能体研发，确保可正常运行。

六、作品评选标准

初审总分 100 分，综合评定以下三方面情况，计算比赛结果。

1. 基础任务：场景化安全智能体构建；自主研发完成基于深信服 AI 安全平台的智能体并有一定的创新性，为 70 分。如未完成，按照完成度给予评定，最多不超过 40 分。

2. 进阶任务：领域知识增强与工具扩展；占比 20 分。

根据所开发的垂域大模型的准确性、完整性，以及本身符合商用标准的程度，综合评定 0—20 分。

3. “构建超级智能体”；占比 10 分。

根据开发的准确性、完整性，以及本身符合商用标准，综

合评定 0-10 分。

终审决赛和“擂台赛”阶段将结合网络安全对抗的形式进行。
(现场评委打分占比 60%，对抗赛占比 40%)

七、作品提交时间

2026 年 5 月—9 月，各参赛团队选择榜单中的题目开展研发攻关，9 月 15 日前向发榜单位提交作品；9 月 30 日前由发榜单位组织初审；11 月底前举行终审决赛（现场擂台赛）。

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 www.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或所在单位公章。

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 2026 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

请已在官网报名成功的团队，于 9 月 5 日前将盖章的参赛申报表 pdf、作品所有相关材料发送至发榜单位邮箱 daitingting@sangfor.com.cn，并抄送到 47215869@qq.com。参赛

团队作品文档材料、源代码、可执行程序、ppt 和演示视频打包，文件名统一为：“挑战杯-深信服-题目名称-参赛者（参赛团队名）”。提交具体作品时，务必一并提交 1 份报名系统中审核通过的参赛报名表（所有信息与系统中填报信息保持严格一致）。以上材料无需在“挑战杯”官网提交。

九、赛事保障

赛事办公室设在深信服教育事业部，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

（一）设奖情况

根据评分规则，综合评定参赛队伍。特等奖（5 名，含擂主 1 名）、一等奖（5 名）、二等奖（10 名）、三等奖（20 名）；奖项不重复，奖金按队伍所获最高奖项授予。

（二）奖励措施

1. 擂主：奖金税后 30 万元/个，团队全体成员将获得深信服科技面试权利，通过选拔后可以直接带薪实习；

2. 特等奖：奖金税后 3 万元/个，团队主要负责人（3 名）获得深信服科技面试权利，通过选拔后可以直接带薪实习；

3. 一等奖：奖金税后 1 万元/个，团队主要负责人（2 名）获得深信服科技面试权利，通过选拔后可以直接带薪实习；

4. 二等奖：奖金税后 0.5 万元/个，团队主要负责人（1 名）获得深信服科技面试权利，通过选拔后可以直接带薪实习；

5. 三等奖：奖金税后 0.2 万元/个，团队主要负责人（1 名）获得深信服科技面试权利，通过选拔后可以直接带薪实习。

（三）奖金发放方式

以上奖金以汇款方式兑现，赛后 50 个工作日内兑现，实习岗位现场签约。全部获奖团队中应届毕业生参与深信服科技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：彭老师，联系电话：13970977157

顾问专家：樊老师，联系电话：18911589114

负责比赛期间技术指导保障。

2. 赛事服务团队

联络专员：代老师，联系电话：13269852560

联络专员：潘老师，联系电话：18611409869

联络专员：刘老师，联系电话：13031018866

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

深信服科技股份有限公司（股票代码 300454）成立于 2000 年，总部位于深圳，全球共设有 50 余个直属分支机构，员工规模超过 7000 名，市值超过 600 亿，公司专注于企业级安全与云计算领域，致力于让用户的 IT 更简单，更安全，更有价值。在网络安全和云计算领域，深信服是中国最顶尖的领导厂商，长期服务中国共产党成立 100 周年庆祝活动、新中国成立 70 周年庆祝活动、全国两会、进博会、G20 峰会等国家级重大活动，全球有近 100,000 家用户正在使用深信服的产品。其中包含 90% 的政府部委单位，80% 的全球 500 强中资企业、95% 的 985、211 高校、排名前 20 名的银行单位。

第一批被认定为“国家高新技术企业”；连续被评为“国家规划布局内重点软件企业”（自 2010 年开始）；连续 8 届入围“亚太地区德勤高科技高成长 500 强”；连续 2 届获得《财富》杂志评选的“中国卓越雇主奖”；入围首届深圳品牌百强企业和深圳纳税百强企业；累计申请专利总数近 1500 件；“下一代互联网信息安全技术国家地方联合工程实验室”（国家发改委）；“国家级网络安全应急服务支撑单位”。