

项目榜单

榜单名称	面向多源异构安全运营场景的大模型研究及应用		
行业领域	人工智能	专业方向	智慧安全运营
(计划)启动时间	2024年11月1日	计划完成时间	2026年12月31日
榜单提出目的	<p>2022年底 ChatGPT 横空出世，人们比较一致的看法是，它将引爆新一轮人工智能革命，加速智能化时代的来临，引发社会结构剧变，改变未来的产业生态以及我们的生产和生活方式。因此，大模型或许能够作为技术突破点，给安全运营带来了新的希望。2023 年来，国际领先安全厂商和国内的头部安全厂商都在研究大模型在安全场景的应用，并取得了一定的成果。但经过详细调研，现有安全大模型皆不能满足效果。</p> <p>针对信息安全领域网络结构多维、安全事件多源、场景任务多样等问题，一体化安全运营已被证明是网络安全防护最有效手段之一，但存在两大核心问题：安全碎片化、人力成本高。一方面，多源异构安全设备融合需要消耗大量人力成本，且技术难度较高，当前市面上并无将所有类型安全数据融合应用的平台类产品；另一方面，当前安全效果依赖于安全专家，然而安全类人才缺口较大，人力成本高昂。</p>		
榜单任务内容	<p>本项目拟研究大模型在多源异构安全运营场景中的应用与推广。大模型将基于智能认知与决策推理、模型攻防对抗、自适应学习等人工智能技术，重点面向工业、政务等现实应用场景，实现复杂安全系统的智能管控调度，提升安全防护精准化、敏捷化和智能化能力，革新安全运营技术，打造持久安全运营体系。</p> <p>本项目主要技术指标如下：</p> <p>1.大模型实现对平台所有开放接口按需调用，准确率达95%以上。</p> <p>2.通过大模型实现多源异构数据融合，至少支持9大类安全任务，30种以上安全任务。</p> <p>3.完成大模型训练和配套调度控制中枢系统研发，技术成熟度水平达8级。</p> <p>本项目主要产业化指标如下：</p> <p>1.大模型实现兼容5类以上安全系统和第三方总计9类安全系统的数据及API，构造纵深防御体系，解决安全碎片化问题，提升安全运营效率。</p> <p>2.大模型预计实现广东联通全省soc中心日常安全运营效率提升20%以上，安全运营成本降低80%以上。</p> <p>3.基于大模型，至少打造2个标杆案例，项目期间内拉动新增收入1.8亿。</p>		

<p>榜单效益目标</p>	<p>社会效益方面：</p> <p>1. 保障战略安全：大模型将围绕安全态势感知、网络智能攻防、数据泄露防护、工业安全等方面，强化风险防范与化解，推动国家网络安全治理体系和治理能力现代化。</p> <p>2. 优化产业生态：大模型与安全产业深度融合，推动软硬件技术攻关和协同创新，优化产业链供应链布局。同时大模型将在一定程度弥补各领域安全人才、安全管理等要素资源短缺，进一步优化安全产业生态。</p> <p>3. 护航产业转型升级：大模型将在安全防护能力和安全运营效率方面发挥优势，为企业数字化、网络化、智能化转型提供安全保障，确保产业转型升级行稳致远。</p> <p>经济效益方面：</p> <p>1. 降本增效：大模型将在工业、政务等领域提供全天候防护、监测、响应等服务，有效降低安全运营门槛，着力为企业安全运营降本增效。预计日常运营效率提升超20%，安全运营成本降低80%以上。如将 AI 安全大模型应用到安全运营平台体系，通过自动化和智能化技术手段，可提高网络安全防护的效率和准确性，同时减少人工干预的需求，能够完成 85%安全运营基础工作。</p> <p>2. 商业收入：根据最新的市场研究报告，预计2024年安全大模型及相关产品服务的市场规模将达到 5.85 亿元人民币。随着技术的不断发展和市场的进一步接受，安全大模型的应用范围和影响力预计将继续扩大。</p> <p>3.客户价值：项目成果将关注各领域安全测试和风险模拟，为用户提供安全研判和建议，极大降低网络攻击造成的经济损失。</p>
---------------	---