

证券代码：688244

证券简称：永信至诚

永信至诚科技集团股份有限公司
投资者关系活动记录表

编号：2025-002

投资者关系 活动类别	☒ 特定对象调研 ☐ 分析师会议 ☐ 媒体采访 ☐ 业绩说明会 ☐ 新闻发布会 ☐ 路演活动 ☒ 现场参观 ☐ 其他
参与单位名 称及人员姓 名	累计接待 24 家机构，接待调研 29 人，详细信息请参阅文末附表
时间	2025 年 3 月 11 日-13 日
地点	北京“数字风洞”测评中心 公司会议室
上市公司接 待人员姓名	副总经理：付磊 董事会秘书：张恒 投资者关系总监：周华东
投资者关系 活动主要内 容介绍	1、请介绍一下公司接入 DeepSeek 大模型测评的具体情况？ 公司依托在网络靶场和数字安全测评领域的深厚技术积累与业务实践成果，构建春秋 AI 测评“数字风洞”平台，该平台以春秋 AI 大模型为核心，拥有基础数据集 100 余个，总测评用例超过 500 万条，模拟红队的 AI 越狱和变异性检测载荷 2 万余个，集成了超过 100W 余条安全检测数据和 2W 余种攻击载荷模板，可以依据公司独创的“数字风洞 ISAC24”测试标准，从智能度、安全度、匹配度、一致度对 DeepSeek 大模型以及其他国内外主流 AI 大模型进行量化和科学评估。 测评结果证明，DeepSeek-r1 大模型多个维度测评成绩领先，在性能层面也有领先优势。在当前市场环境下，DeepSeek 系列大模型为预算有限的中小企业用户提供了拥抱 AI 时代最具性价比

	的解决方案。 2、请问公司如何看待 DeepSeek 等大模型在私有化部署以及后续使用过程中的风险问题？有何好的解决方案？ 随着 DeepSeek 大模型的发布，私有化部署固然越来越简单便捷，但是在部署过程中与生俱来的安全缺陷有可能让使用者和二次开发人员暴露在巨大的网络和数据安全风险之中。国家网络安全通报中心此前通报，开源跨平台大模型工具 Ollama 默认配置存在未授权访问与模型窃取等安全隐患，鉴于目前 DeepSeek 等大模型的研究部署和应用非常广泛，多数用户使用 Ollama 私有化部署且未修改默认配置，存在数据泄露、算力盗取、服务中断等安全风险，极易引发网络和数据安全事件。 此外，大模型本地化部署的风险仅仅是其安全问题的冰山一角，许多安全隐患还隐藏在大模型应用、数据、网络、系统和供应链等多个层面。因此，构建 AI 大模型的原生安全能力，将安全融入模型的全生命周期，才是应对安全风险的关键所在。基于这一理念，永信至诚依托“数字风洞”产品体系，构建了针对 AI 大模型整个生命周期的风险管理机制，围绕 AI 大模型构建、部署到运营的各个阶段，开展多维风险测评与验证，为 AI 大模型铭刻安全基因，保障 AI 大模型的“数字健康”。 3、关于公司提出的大模型“原生安全”理念，能否详细介绍一下？ AI 的终极目标是实现通用人工智能（AGI），这意味着不能再以“修复机器”的方式来治理 AI 大模型产品安全，而是需要将 AI 大模型视为一个“有机体”，像保护生物体健康一样，关注其数字健康。“原生安全”，便是强调从 AI 大模型的内在架构、数据处理、算法训练、工作流量等方面进行安全管理，确保安全从模型的源头就被构建起来。 基于这一理念，公司依托“数字风洞”产品体系构建了针对 AI 大模型整个生命周期的风险管理机制。该机制以实现 AI 大模
--	--

	型的原生安全为目的，围绕 AI 大模型构建、部署到运营的各个阶段，针对不同阶段的防护目标与风险特点，提出“数字风洞”健康管理方案，通过建立 AI 大模型资产台账、开展全生命周期测试评估、风洞时光机全生命周期管理、威胁情报监控与“家庭医生”服务、实时防护的 AI 智能体内容合规和数据隐私的“安全围栏”等多种手段，让安全工作融入到 AI 大模型及其构建的数字智能体整个生命周期，释放智能时代数字生产力的价值。 4、请介绍一下公司近期发布的“元方”系列产品及方案和定位？ 依托“数字风洞”测试评估能力、十数年安全攻防经验以及在 AI 大模型研究方面的沉淀，公司以原生安全为核心，正式发布“元方”原生安全大模型一体机和原生安全行业大模型（量身定制）产品及方案，为企业提供从私有化部署到垂直场景应用的 AI 智能体建设方案。 其中，“元方”原生安全大模型一体机面向轻量化 AI 需求企业，集成大模型及智能办公套件，通过软硬件预调优实现“插电即用”，满足通用场景需求；原生安全行业大模型（量身定制）产品及方案针对金融、制造等垂直领域，通过持续预训练与微调技术打造行业专属大模型（量身定制）产品及方案，以满足行业用户在特定场景的深化应用。 “元方”系列产品及方案，凝聚了公司在大模型持续预训练、模型微调和数字安全测试评估等方面的实践积累，以“高性价比、高可控性、高安全性、可靠好用”的 AI 私有化解决方案，助力企业开启智能化跃迁之旅。 5、请介绍一下贵司“元方”原生安全大模型一体机的优势？ 针对企业在应用部署大模型过程中面临的安全、技术、应用、成本等难题，公司“元方”系列产品及方案优势如下： （1）原生安全，基因铭刻 基于“数字风洞”产品体系，“元方”已完成从硬件到系统
--	---

	再到应用的全维安全测试，涵盖代码安全、主机安全基线、基础设备安全和数据安全等多个维度，为企业私有化 AI 系统铭刻安全基因；内置兼顾性能和安全的 DeepSeek 及其它知识模型；并在 AI 大模型的持续运营中，“元方”安全管家系统将实时监控系统的“数字健康”状态，并联动“数字风洞”实现威胁情报同步防御，保障 AI 系统的稳定与安全。 （2）零帧起手，开箱即用 预装 DeepSeek R1 以及其他知识模型，通过深度调优的软硬件一体化方案，提高算力利用率，提升模型推理速度，并帮助用户将 AI 大模型部署从数周、数天缩短至“分钟级”。 （3）简单便捷，系统管理 操作界面简洁直观，管理功能均可在 3 次点击内完成，真正实现“零基础”无障碍使用。用户可在 5 秒内创建专属知识库，结合身份认证形成管理、审计、使用三权分立，并实现权限隔离、数据隔离，支持对话集的单独留存与删除，避免数据泄露。 （4）私有知识，快速构建 支持企业构建与更新私有知识库，并基于 DeepSeek 构建了 RAG 系统，检索企业专属知识库，并支持基于数据权限和安全策略对数据进行强管控的分级处置，并支持对特定数据进行脱敏处理，实现知识沉淀与安全调用的双重保障。 （5）精选应用，智能办公 内置了多个实用的智能应用，如招聘助手、营销分析、文案大师等。快速处理日常任务，解放人力、提高效率、挖掘价值。所有智能应用均经过“数字风洞”代码安全、组件安全、数据安全测试及权限管控机制加固，确保应用运行全程可管可控。		
附件清单(如有)	序号	机构名称	调研者姓名
	1	国金证券股份有限公司	李忠宇
	2	上海睿郡资产管理有限公司	陆士杰
	3	深圳固禾私募证券投资基金管理有限公司	纪双陆

	4	鹏扬基金管理有限公司	赵世宏
	5	众安在线财产保险股份有限公司	徐赛
	6	广东正圆私募基金管理有限公司	吴皓月
	7	深圳市康曼德资本管理有限公司	李俊松
	8	北京志开投资管理有限公司	周彬
	9	北京鸿道投资管理有限责任公司	符朝阳、韩啸锋
	10	上海煜德投资管理中心(有限合伙)	李曲波
	11	上海彤源投资发展有限公司	薛凌云
	12	深圳市恒健远志投资合伙企业(有限合伙)	周笑川
	13	渤海人寿保险股份有限公司	万冬
	14	东兴证券股份有限公司	王健辉
	15	广东瑞天私募基金管理有限公司	郝胜涛、林仲晞
	16	北京中承东方资产管理有限公司	魏志鹏
	17	北京盛华鼎鑫投资有限公司	郭钊
	18	北京神农投资管理有限公司	孙一鸣
	19	华夏基金管理有限公司	罗绍武、柯若凡、 王曼、高爽
	20	墨威（上海）投资管理有限公司	李长鸿
	21	卓尔奇投资	陈笛
	22	华创证券有限责任公司	胡昕安
	23	鹏华基金管理有限公司	杨凡
	24	河北源达信息技术股份有限公司	赵毅轩
关于本次活动是否涉及应当披露重大信息的说明	不涉及。		
日期	2025 年 3 月 13 日		