国信证券股份有限公司
关于永信至诚科技集团股份有限公司
2025年年度持续督导跟踪报告

根据《证券发行上市保荐业务管理办法（2025年修正）》《上海证券交易所上市公司自律监管指引第11号——持续督导（2025年4月修订）》《上海证券交易所科创板股票上市规则（2026年4月修订）》等有关法律、法规的规定，国信证券股份有限公司（以下简称“国信证券”或“保荐机构”）作为永信至诚科技集团股份有限公司（以下简称“永信至诚”或“公司”）持续督导工作的保荐机构，负责永信至诚首次公开发行股票并在科创板上市后的持续督导工作，并出具本持续督导年度跟踪报告书。

一、持续督导工作情况

序号	工作内容	持续督导情况
1	保荐人或财务顾问应当建立健全并有效执行持续督导工作制度，并针对具体的持续督导工作制定相应的工作计划。	保荐机构已建立健全并有效执行了持续督导工作制度，并制定了相应的工作计划。
2	保荐人和财务顾问应当根据中国证监会相关规定，在持续督导工作开始前，与上市公司或相关当事人签署持续督导协议（以下简称协议），明确双方在持续督导期间的权利义务，并报本所备案。	保荐机构与永信至诚签订了《持续督导协议》，该协议明确了双方在持续督导期间的权利和义务。
3	保荐人或财务顾问应当通过日常沟通、定期回访、现场检查、尽职调查等方式开展持续督导工作。	2025年度，保荐机构通过日常沟通、定期或不定期回访、现场检查等方式，对永信至诚开展持续督导工作。其中，保荐机构于2025 年7 月8日对上市公司进行了2025 年上半年募集资金现场核查，于2025 年12月30日对上市公司进行了年度现场检查。
4	持续督导期间，保荐人或财务顾问按照有关规定对上市公司违法违规事项公开发表声明的，应当向本所报告并经本所审核后在指定媒体上公告。	2025年度，永信至诚在持续督导期间未发生按有关规定须保荐机构公开发表声明的违法违规情形。
5	持续督导期间，上市公司或相关当事人出现违法违规、违背承诺等事项的，保荐人或财务顾问应当自发现或应当发现之日起5个交易日内向本所	2025年度，永信至诚在持续督导期间未发生违法违规、违背承诺等事项。

	报告，报告内容包括上市公司或相关当事人出现违法违规、违背承诺等事项的具体情况，保荐人或财务顾问采取的督导措施等。	
6	保荐人应当督导上市公司及其董事、取消监事会前的监事、高级管理人员遵守法律、法规、部门规章和本所发布的业务规则及其他规范性文件，并切实履行其所作出的各项承诺。	在持续督导期间，保荐机构持续督导上市公司及其董事、取消监事会前的监事、高级管理人员遵守法律、法规、部门规章和上海证券交易所发布的业务规则及其他规范性文件，切实履行其所做出的各项承诺。
7	保荐人应当督导上市公司建立健全并有效执行公司治理制度，包括但不限于股东大会、董事会议事规则以及董事、取消监事会前的监事和高级管理人员的行为规范等。	保荐机构督促永信至诚依照相关规定健全和完善公司治理制度，并严格执行公司治理制度。
8	保荐人应当督导上市公司建立健全并有效执行内控制度，包括但不限于财务管理制度、会计核算制度和内部审计制度，以及募集资金使用、关联交易、对外担保、对外投资、衍生品交易、对子公司的控制等重大经营决策的程序与规则等。	保荐机构对永信至诚的内控制度的设计、实施和有效性进行了核查，永信至诚的内控制度符合相关法规要求并得到了有效执行，能够保证公司的规范运行。
9	保荐人应当督导上市公司建立健全并有效执行信息披露制度，审阅信息披露文件及其他相关文件，并有充分理由确信上市公司向本所提交的文件不存在虚假记载、误导性陈述或重大遗漏。	保荐机构督促永信至诚严格执行信息披露制度，审阅信息披露文件及其他相关文件。
10	保荐人可以对上市公司的信息披露文件及向中国证监会、上海证券交易所提交的其他文件进行事前审阅，对存在问题的信息披露文件应当及时督促上市公司予以更正或补充，上市公司不予更正或补充的，应当及时向本所报告；保荐人对上市公司的信息披露文件未进行事前审阅的，应当在上市公司履行信息披露义务后 5 个交易日内，完成对有关文件的审阅工作，对存在问题的信息披露文件应当及时督促上市公司更正或补充，上市公司不予更正或补充的，应当及时向本所报告。	保荐机构对永信至诚的信息披露文件进行了审阅，不存在应及时向上海证券交易所报告的情况。
11	保荐人应当关注上市公司或其控股股东、实际控制人、董事、取消监事会前的监事、高级管理人员受到中国证监会行政处罚、本所监管措施或者纪律处分的情况，并督促其完善内部控制制度，采取措施予以纠正。	2025年度，永信至诚及其控股股东、实际控制人、董事、取消监事会前的监事、高级管理人员未受到中国证监会行政处罚、上海证券交易所纪律处分或者被上海证券交易所出具监管关注函的情况。

12	持续关注上市公司及控股股东、实际控制人等履行承诺的情况，上市公司及控股股东、实际控制人等未履行承诺事项的，保荐人应及时向上海证券交易所报告。上市公司或其控股股东、实际控制人作出承诺的，保荐机构、保荐代表人应当督促其对承诺事项的具体内容、履约方式及时间、履约能力分析、履约风险及对策、不能履约时的救济措施等方面进行充分信息披露。保荐机构、保荐代表人应当针对前款规定的承诺披露事项，持续跟进相关主体履行承诺的进展情况，督促相关主体及时、充分履行承诺。上市公司或其控股股东、实际控制人披露、履行或者变更承诺事项，不符合法律法规、上市规则以及上海证券交易所其他规定的，保荐机构和保荐代表人应当及时提出督导意见，并督促相关主体进行补正。	2025年度，永信至诚及其控股股东、实际控制人等不存在未履行承诺的情况。上市公司或其控股股东、实际控制人已对承诺事项的具体内容、履约方式及时间、履约能力分析、履约风险及对策、不能履约时的救济措施等方面进行充分信息披露。
13	保荐人应当关注公共媒体关于上市公司的报道，及时针对市场传闻进行核查。经核查后发现上市公司存在应当披露未披露的重大事项或与披露的信息与事实不符的，保荐人应当及时督促上市公司如实披露或予以澄清；上市公司不予披露或澄清的，应及时向本所报告。	2025年度，经保荐机构核查，永信至诚未出现应披露未披露的重大事项或披露的信息与事实不符的情形。
14	在持续督导期间发现以下情形之一的，保荐人应督促上市公司做出说明并限期改正，同时向上海证券交易所报告：（一）上市公司涉嫌违反《股票上市规则》等上海证券交易所相关业务规则；（二）中介机构及其签名人员出具的专业意见可能存在虚假记载、误导性陈述或重大遗漏等违法违规情形或其他不当情形；（三）上市公司出现《保荐办法》第七十条规定的情形；（四）上市公司不配合保荐机构持续督导工作；（五）上海证券交易所或保荐人认为需要报告的其他情形。	2025年度，永信至诚及相关主体未出现需要做出说明、改正并向交易所报告的情形。
15	在持续督导期间出现以下情形的，保荐人及其保荐代表人应当督促上市公司核实并披露，同时应当自知道或者应当知道之日起 15 日内按规定进行专项现场核查：（一）存在重大财务造假嫌疑：（二）控股股东、实际控制人及其关联人涉嫌资金占用；（三）可能存在重大违规担保；（四）控股股东、实际控制人及其关联人、董事、取消监事会前的监事或者高级管理人员涉嫌侵占上市公司利益；（五）资金往来或者现金流存在重大异常；（六）上海证	2025年度，永信至诚不存在需要进行专项现场核查的情形。

	券交易所或保荐机构认为应当进行现场核查的其他事项。	

二、保荐机构和保荐代表人发现的问题及整改情况

在本持续督导期间，保荐机构和保荐代表人未发现公司存在重大问题。

三、重大风险事项

（一）业绩持续下滑的风险

2025年，公司实现营业收入27,634.02万元，同比下降22.45%；实现归属于上市公司股东的净利润-4,898.67万元，较上年同期下降677.52%。2025年，公司首次由盈转亏，公司业绩受宏观经济、产业政策、行业竞争态势等多重影响，同时，也取决于公司技术研发、产品市场推广及下游市场需求等因素。后续，若公司不能通过技术、产品创新等方式及时满足客户的业务需求，或不能持续的开发新项目，或客户因为市场低迷等原因使其自身经营情况发生变化，导致其对公司产品或服务的需求大幅下降，或者公司不能持续拓展新的客户和市场，公司存在业绩进一步下滑或亏损的风险。

（二）核心竞争力风险

1、技术迭代、新产品研发风险

当下，随着人工智能、量子计算等新技术的快速发展，网络安全行业正面临着前所未有的产业变革与技术革新。人工智能技术的快速发展使得网络攻击手段呈指数级迭代升级，传统安全防御机制已经很难抵御层出不穷的新型威胁，而量子计算的快速崛起更是对传统加密体系的颠覆。

同时，卫星互联网、具身智能、低空经济、智能驾驶等新兴产业的快速发展，也在不断带动网络安全技术的创新和安全边界的拓宽，这对网络安全公司产品能力、服务响应能力等提出了更高的要求。公司必须持续推进技术创新以及新产品开发，以适应不断发展的市场需求。尽管公司一直致力于科技创新，力争在网络安全细分领域保持领先优势，但不排除国内外竞争对手或潜在竞争对手率先取得重大突破，推出更先进、更具竞争力的技术和产品，从而使本公司的产品和技术失去领先优势。

2、核心技术人员流失风险

网络安全行业是人才密集型行业，核心技术人员是公司保持技术领先的基础。

本公司核心技术人员均已在公司工作多年，在长期合作中形成了较高的忠诚度和凝聚力，为公司持续创新能力和技术优势作出了较大贡献。但随着市场竞争日益严峻，不同公司对核心技术人才争夺日趋激烈，不排除公司核心技术人员流失，可能造成在研项目进度推迟、中断甚至终止，或者造成研发项目泄密或流失，给公司后续产品及技术的开发以及持续稳定增长带来不利影响。

（三）经营风险

1、产品销售季节性风险

公司部分客户为政府部门、国央企等预算制单位，该类客户一般在上半年预算、立项及供应商评定，在年中或下半年进行合同签订、实施及验收，导致公司呈现上半年收入较少、下半年尤其第四季度收入较大的季节性特征。

2、市场竞争风险

经过多年的发展，公司已在测试评估、网络靶场、人才建设等网络安全细分领域取得领先优势，成为国内数字安全测试评估赛道领跑者，网络靶场和人才建设领军者。但随着网络和数据安全行业由“形式合规”向“实质合规”加强的趋势得到进一步强化，相关细分行业规模的持续增长以及客户需求的增加，将会吸引更多竞争者进入相关细分领域，届时，公司将会面临市场竞争进一步加剧的风险。

（四）财务风险

1、税收优惠风险

报告期内，公司享受高新技术企业所得税税收优惠和研发费用加计扣除。若国家未来相关税收政策或公司及子公司自身条件发生变化，导致无法享受上述税收优惠政策，将会对公司未来经营业绩带来不利影响。

2、应收账款风险

报告期内，公司不断加大对应收款项的催收和管理力度，并对客户信用进行有效管理，同时对应收账款计提了充足的坏账准备。若未来市场环境或者主要客户信用状况持续发生不利变化，可能使公司营运资金紧张，进而会对公司的生产经营造成不利影响。

（五）行业风险

报告期内，尽管公司客户结构得到进一步优化，但政府部门等单位收入仍是公司重要的收入来源。近年来，上述行业客户的网络安全产品及服务需求主要由

信息化投资加大、安全威胁加剧、网络安全监管趋严等因素驱动。未来，如因信息化投资增速、安全威胁程度、网络安全监管要求发生重大变化，可能导致该等行业客户的网络安全产品及服务需求发生波动，进而影响公司的经营业绩。

（六）宏观环境风险

“没有网络安全就没有国家安全”，党的十八大以来，党中央高度重视网络安全工作，多次对国家网络安全工作作出重要部署。随着《网络安全法》《数据安全法》《个人信息保护法》《关键信息基础设施安全保护条例》《信息安全技术 关键信息基础设施安全保护要求》《网络安全等级保护制度 2.0 标准》等一系列重大文件相继发布实施，进一步为网络安全产业健康发展提供了政策保障和法律依托，为网络安全技术创新、网络安全企业做大做强提供了宝贵机遇。如果国家对网络安全企业的扶持政策发生变化，将对公司的发展产生相应影响。

四、重大违规事项

报告期内，公司不存在重大违规事项。

五、主要财务指标的变动原因及合理性

报告期内，公司主要会计数据及指标如下所示：

（一）主要会计数据

单位：人民币万元

主要会计数据	2025年	2024年	本期比上年同期增减(%)	2023年
营业收入	27,634.02	35,632.63	-22.45	39,586.55
扣除与主营业务无关的业务收入和不具备商业实质的收入后的营业收入	27,634.02	35,632.63	-22.45	39,586.55
利润总额	-4,981.06	197.25	-2,625.23	3,210.74
归属于上市公司股东的净利润	-4,898.67	848.22	-677.52	3,110.54
归属于上市公司股东的扣除非经常性损益的净利润	-5,727.82	-205.77	不适用	1,103.04
经营活动产生的现金流量净额	-225.01	-4,630.06	不适用	-1,855.52
	2025年末	2024年末	本期末比上年同期末增减（%）	2023年末
归属于上市公司股东的净资产	97,192.69	102,652.06	-5.32	106,652.11
总资产	111,922.62	121,953.02	-8.22	124,786.84

注：数据若有尾数差，为四舍五入所致。

（二）主要财务指标

主要财务指标	2025年	2024年	本期比上年同期增减(%)	2023年

基本每股收益（元／股）	-0.32	0.05	-740.00	0.20
稀释每股收益（元／股）	-0.32	0.05	-740.00	0.20
扣除非经常性损益后的基本每股收益（元／股）	-0.38	-0.01	不适用	0.07
加权平均净资产收益率（%）	-4.90	0.82	减少 5.72 个百分点	2.94
扣除非经常性损益后的加权平均净资产收益率（%）	-5.73	-0.20	减少 5.53 个百分点	1.04
研发投入占营业收入的比例（%）	31.63	26.01	增加 5.62 个百分点	21.24

注：公司2025年实施了资本公积转增股本方案，以资本公积金向全体股东每10股转增4.8股，公司总股数发生变动。为保持基本每股收益可比性，公司根据《企业会计准则第34号——每股收益》第四章第十三条规定“发行在外普通股或潜在普通股的数量因派发股票股利、公积金转增资本、拆股而增加或因并股而减少，但不影响所有者权益金额的，应当按调整后的股数重新计算各列报期间的每股收益。上述变化发生于资产负债表日至财务报告批准报出日之间的，应当以调整后的股数重新计算各列报期间的每股收益”，对基本每股收益的上年同期数进行了调整。

2025年度，利润总额、归属于上市公司股东的净利润、归属于上市公司股东的扣除非经常性损益的净利润、基本每股收益和稀释每股收益较上年同期出现较大幅度变动，主要系公司营业收入减少、计提减值准备金额增加和投资收益下降所致，具体情况为：①市场因素：受市场环境变化等因素影响，公司部分客户预算投入减少，部分项目签订、交付、验收出现延期，导致公司整体营业收入同比下降；②应收账款减值准备：公司根据企业会计准则和公司应收账款管理制度，基于会计谨慎性原则，对可能发生信用损失的应收账款计提了充足的减值准备；③受理财收益率的影响，公司投资收益金额出现下降。综上因素导致公司业绩下降。

经营活动产生的现金流量净额增加，主要系收到其他与经营活动有关的现金增加和支付给职工以及为职工支付的现金减少所致。

六、核心竞争力分析

1、技术优势

（1）平行仿真技术

平行仿真是永信至诚全自主研发的技术体系，是数字化新一代关键技术的基座。通过平行仿真技术的应用，可以模拟与现实网络空间相对应的场景模型，构建高仿真业务环境，支撑各关键行业进行网络空间的测试、演练、实训、推演、研判、指挥、防御、实战等综合性安全业务开展。同时，仿真环境中所产生的结

果，也会平行影响并提升真实业务系统的安全防御能力。公司“基于平行仿真的大规模网络靶场构建技术及应用”项目荣获北京市科学技术奖一等奖，参与申报的“超大规模多领域融合联邦靶场（鹏城网络靶场）关键技术及系统”项目，荣获国家科学技术进步奖二等奖。

（2）网络攻防技术

公司连续多年参加国家级网络安全实战攻防演习，连续三年荣获企业组第一名；公司拥有五大专注于网络安全前沿核心技术、实战技术、竞赛技术和靶场场景研究实验室，在操作系统安全技术、漏洞分析与挖掘技术、机器学习与自动化技术、Web安全与渗透测试等方向拥有深厚积累，长期跟踪国内外最新网络安全漏洞研究动向，在主流系统及其应用的安全缺陷研究领域具备丰富实践经验，曾多次为微软检测发现最高级别安全漏洞；连续多年为国家和各省市相关政府部门提供高能效网络犯罪情报采集和侦察服务。

（3）春秋云专有云

春秋云是永信至诚全自主研发的专用私有云，具备先进的资源管理、灵活调配和工程化运营服务能力，能够有效保证计算、网络、虚拟、存储等资源的高频调度和高效使用，可应对行业级、城市级等各种规模级别的多层级复杂场景仿真和构建。成功经历过2万人同时竞技的高并发洗礼，圆满支撑全球最大规模网络安全赛事演练“网鼎杯”现场2,000人同场演练。

（4）多循环数字风洞测试评估技术

多循环数字风洞测试评估技术是基于公司在网络靶场和人才建设领域深厚的技术与数据积累形成的，是公司“数字风洞”产品体系的核心技术支撑。通过该技术可以实现在风洞时光机的高仿真场景下，基于数字风洞平台统一的测评载荷、测评流程和测评结果管控，通过智能化的反复多次复测来帮助用户解决传统网络和数据安全风险控制中面临的供应链风险修复不及时、安全闭环测试时效性差、企业实质合规量化手段缺乏等难题，从而实现对数字化系统全生命周期的各个阶段进行反复高度自动化的系统性安全验证，度量安全建设成效，保障“数字健康”。

（5）基于对抗生成的多维大模型安全测试评估技术

基于对抗生成的多维大模型安全测试评估技术是基于公司在数字安全测试评估以及网络靶场领域深厚的技术积累与业务成果研发形成，是公司AI大模型安全测试评估“数字风洞”平台核心技术底座。在该技术的加持下，AI大模型安全测试评估“数字风洞”平台可验证AI大模型在智能度、安全度、匹配度和一致度的能力水平，以模测模，以模强模，对目标模型能力进行量化和科学地评估，多维度保障大模型基因健康、系统健康、数据健康和业务健康。以独立、科学的测评视角，为AI的研究者、开发者和采购者提供决策建议和优化解决方案。

2、团队优势

（1）核心团队长期深耕于网络和数据安全行业

公司董事长蔡晶晶是正高级工程师、国家“万人计划”科技创业领军人才、中央网信办国家网络安全优秀人才、科技部第三届“杰出工程师”、国家网络安全实验平台项目专家、公安部网络安全专家等；公司副董事长兼总经理陈俊是正高级工程师、2019年度北京市科学技术奖一等奖获奖者、2023年度国家科学技术进步奖二等奖获奖者，拥有二十年以上网络安全从业经历；董事兼副总经理张凯先后担任通信、电力、网络安全行业技术团队负责人，专注于网络安全技术产品化和工程化以及人工智能等前沿领域技术研发和产品落地，是春秋云平台的总架构师。

（2）技术团队拥有雄厚的研发实力

截至报告期末，公司拥有研发人员215人，占员工总人数比例达52.83%，支持了公司产品的研发、迭代和不断创新。公司致力于网络安全产品的研发，并形成具有自主知识产权的网络安全产品体系，截至报告期末，公司共获取66项发明专利；拥有计算机软件著作权320项和2项科学技术成果。公司参与起草或修订多项标准，牵头完成了国标《信息技术系统安全工程能力成熟度模型》标准的修订；深度参与起草的《网络靶场产品安全技术要求和测试评价方法》（CCRC-TR132-2023）标准已于2023年10月26日发布并实施；同时，公司还参与起草了信安标委国标《信息安全技术网络空间安全人员角色分类和能力要求》，以及《网络靶场基于技战术模型的安全测评方法》（T/CSAC 001—2023）《网

络靶场能力分级指南》（T/CSAC 002—2023）《网络靶场资源描述要求》（T/CSAC 003—2023）《网络靶场试验任务导调总体要求》（T/CSAC004—2023）4项网络靶场团体标准；春秋云境网络靶场荣获中国网络安全审查技术与认证中心颁发的首个网络靶场类IT产品信息安全认证证书，也是国内网络靶场产品第一个国家权威认证证书。

3、产品先发优势

公司自2015年开始推出网络靶场产品，并对产品持续进行更新迭代，截至目前公司网络靶场系列产品已覆盖政府部门、能源、电力、电信、金融等十余个关键行业高价值用户群体，积累了数百个行业级场景，近百个城市级仿真互联网场景，近千个网络安全CVE漏洞靶标，数千个安全实训靶标，百余个人工智能漏洞挖掘训练集等。通过公司组织和支撑的超过850场重点赛事演练和实网测试评估演练，网络靶场产品技术得以不断迭代升级并达到国内领先水平。网络安全场景是漏洞研究、漏洞利用、应急处置、靶场组件构建、蜜罐陷阱部署等的关键支撑资源。公司在网络安全场景的积累优势，确保了公司在网络安全研究、产品升级迭代中的竞争优势。同时，也为公司下一步产品研发提供了明确方向。

依托过去在网络靶场领域的深厚技术积累及上千家政企用户网络安全建设的丰富实战经验，2022年11月19日，公司发布了“数字风洞”产品体系，开启并领跑数字安全测试评估专业赛道，产品先发优势明显。数字风洞是为数字化建设提供安全测试评估的基础设施，基于永信至诚独创的风险趋于“证无”理念，以“3×3×3×（产品×服务）”安全感公式为方法论构建而成，全面助力政企用户网络和数据安全工作实现合规的保障、风险的预控、标准的践行和投入的回报，保障“数字健康”。

在生成式AI技术迅猛发展的背景下，构建私有化AI能力已成为政企用户数智化转型的关键所在。2025年上半年，公司依托“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，以原生安全为核心，率先打造“元方”系列产品及方案，并发布基础版、专业版和大师版“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，以差异化的应用场景适配能力满足关键行业用户的多元化需求，助力企业数智化转型。

4、协同优势

（1）生态协同

目前公司已与国内多所大学、高等职业教育院校在网络安全教学与实践方面建立合作，连续多年成为教育部批准的产学合作协同育人项目支持单位。此外，公司还与国内知名大学和专业机构在网络安全领域建立了产学研基地，其中包括：中国科学技术大学、中国人民大学、哈尔滨工业大学、东南大学、中国人民公安大学、北京航空航天大学、广东省信息安全检测中心等。公司与高等院校的合作形成双赢局面，不仅有利于高等院校教学体系的完善，而且也是公司网络安全人才生态的重要基础，有利于巩固公司在网络安全人才流量入口优势。公司分别与知名互联网企业建立众测平台，充分利用众测方式帮助互联网企业进行产品的漏洞发现，不仅有利于i春秋人才生态的完善，而且提高了公司与知名互联网企业之间的合作粘性，提高公司行业影响力。

（2）业务协同

公司i春秋是网络安全专业学习社区，2015年6月上线以来，累计注册网安实战学习者超过80万人。此外，公司还是国内知名的网络安全赛事运营者。二者协同，形成了从实训培养到比赛提高的网络安全人才选拔途径，使公司在网络安全人才方面占据了流量入口，并建成了网络安全人才生态。通过人才生态运营促进了公司技术迭代，推动了网络空间平行仿真技术发展，奠定了“数字风洞”产品体系和网络靶场系列产品的技术基础，“数字风洞”产品体系和网络靶场系列产品不仅提供了网络安全赛事运营的技术基础，也使公司拥有了风险测试验证能力。

5、中立的生态优势

公司于2022年11月19日战略发布“数字风洞”产品体系，以第三方中立的生态位置开启并领跑数字安全测试评估专业赛道。作为沪深两市唯一一家以测试评估、网络靶场、人才建设为主营业务的网络和数据安全上市公司，依托在网络靶场、测试评估领域的深厚技术积累与服务经验，公司以独立的第三方安全视角，为客户提供独立、专业、客观的测试评估产品和服务，帮助用户持续关注数字健康状况，提升安全免疫效能，量化验证安全投入有效性，更有助于获得客户的信

任与认可；同时，基于上千家政企用户网络和数据安全建设的丰富实战经验，公司还可以为客户提供与风险载荷配套的热修复方案，帮助客户快速完成风险控制与修复处置，推动风险趋于“证无”，保障“数字健康”。

七、核心技术及研发进展

（一）核心技术及其先进性以及报告期内的变化情况

公司产品的底层技术为网络空间平行仿真技术、网络攻防对抗技术、多循环数字风洞测试评估技术和基于对抗生成的多维大模型安全测试评估技术，公司自建研发体系持续进行产品底层技术的研发，形成了标准化的产品体系和功能模块，并取得了相关的发明专利、软件著作权等自主知识产权。

（1）网络空间平行仿真技术

①基于混合虚拟化的属性平行仿真技术

提出平行仿真环境中关键要素属性平行仿真方法，按照目标场景的架构特点和靶标属性，利用自动化方式对各级网络中的资产进行信息采集，结合人工分析形成标准化描述报告和场景模板的蓝图。

②基于靶标分层同步的行为平行仿真技术

在数据和业务仿真方面，采用分层数据流采集的模式，提升仿真效果；在行为模拟方面，利用自动化脚本的方式提升仿真效果并内置丰富的攻击模拟智能化程序，从而提升了整个攻防行为的逼真性。

③面向平行仿真的高性能靶场平台搭建与服务技术

利用虚拟资源动态资源感知均衡调度技术，将云中心的资源调度过程分为三个阶段：资源初始分配、资源动态调度以及资源动态整合，实现对靶场云计算环境中的虚拟资源进行高效的分配与管理，解决了在模拟仿真过程中云资源有效利用的问题。

④基于可扩展元场景的复杂业务模拟技术

针对大规模网络靶场业务复杂、节点众多、拓扑多样等特点，提出基于可扩展元场景的复杂业务模拟技术，提出基于最小元场景的多分区管理、多场景要素整合的复杂场景模型描述方法，解决了精准、高效描述复杂场景模型的难题。

⑤基于镜像差分压缩和分级存储的节点快速重构技术

针对大规模网络靶场存储性能差、节点实例化难度大、节点存储拥塞等特点，提出基于镜像差分压缩和分级存储的节点快速重构技术，实现靶机虚拟机文件无存储压力复制，并保证存储网络具有足够的带宽和充足的性能。

⑥基于多重隔离的高并发异步靶场构建技术

针对场景实例化难以保持稳定、高速，步骤繁琐以及时间消耗突出的问题，提出基于多重隔离的高并发异步靶场构建技术，将繁琐任务进行拆分并分散到不同的计算节点服务器上并发执行，提高了创建效率，缩短了场景构建时间。

⑦基于脆弱点感知的高甜度蜜罐构建技术

针对传统的静态靶标系统伪装程度不高的现状，提出了脆弱点感知的靶机动态伪装技术，从靶标漏洞特征方面，靶标系统预置大量被攻击场景以及漏洞特征，同时具备了漏洞场景靶机实时的切换能力，满足攻击者不同意图、不同手段的“需要”。

⑧内核级攻击行为全景捕获与复现技术

针对现实网络中被攻击的行为不能全量捕获，导致分析不够全面并且需要人工分析的问题，提出基于平行被攻击行为捕获和分析技术，对攻击者的攻击手段、攻击样本、攻击路径进行捕获，并从中分析出攻击者的攻击意图。

⑨面向应激反制的交互式对抗环境生成技术

该技术是在威胁激励下通过感知和归因分析做出有目的的反制响应，实现在对抗环境内对攻击者的行为的捕获、追踪、溯源和反击，从而提高了攻击诱捕、数据分析、反制的对抗环境模拟能力。

⑩渐进式安全威胁激励生成技术

该技术基于威胁工具、威胁流量、自动化威胁利用脚本等实现自动化、可重放、可衡量的威胁激励，以可控、可叠加、可动态调整的方式实现对被试体进行体系化和快速的高逼真威胁测试评估。

⑪多循环激励响应控制技术

该技术可生成数据驱动的、机器可读的统一描述方式，将安全评估的环境、测评方案和量化要求、测评威胁载荷等进行统一封装和重放，基于风险载荷以稳定的测试强度和测评流程进行高度自动化的多循环测评，以量化结果推进系统迭代。

⑫综合风险评估测评技术

该技术按应用场景对典型威胁进行分级、分类、分阶段建设指标体系，实现对人员、系统进行定性与定量相结合的效果评估，给出更加科学准确的评估结果。

⑬面向防御演练的高性能靶场资源调度技术

采用动态资源感知与智能负载均衡技术，将防御靶场的资源调度分为三个阶段：防御资源预分配、实时动态调整和资源弹性回收，确保在防御演练过程中计算、存储和网络资源的高效利用，支持大规模防御场景的稳定运行。

⑭物理场景云联化智能融合仿真靶场技术

采用工控实验箱物理设备与虚拟仿真环境相结合的架构，通过工业总线网关、数据转发代理等组件实现两者的实时数据交互与状态同步，满足不同层级工控安全实验与演练需求。

（2）网络空间攻防对抗技术

①恶意代码检测分析技术

该技术通过总结各种恶意代码对被感染系统的控制过程和留存方式，抓住恶意代码的核心行为特征，综合利用静态特征匹配与动态沙箱行为匹配相结合的方式，实现对恶意代码的发现和定位。

②漏洞挖掘及利用验证技术

该技术利用靶场环境的多样性和资源快速调度的优势，结合智能 FUZZ 平台，可以大幅提升漏洞挖掘的速度和质量，同时验证环境还能为漏洞利用代码的快速验证和留存积累提供良好的协作支持。

③基于单流特征与关联特征相融合的流量检测技术

该模型由单流内部流量特征的贝叶斯网络识别算法与多流之间行为特征的支持向量机识别算法组成，通过此关联模型，将确保准确性和效率，可大规模应用在实际环境中。

④智能身份元数据萃取识别技术

该技术采用基于协议结构和身份元数据进行特征萃取的方式，实现从数据中全面准确的提取身份元数据的目标。

⑤智能算法混淆加密视频处理技术

该技术基于不可逆加密算法，采用多项行业先进技术对视频文件进行周密的动态保护、内置了自主研发的防注入、防调试及自变异特性等加密引擎和超高清数字解码引擎。

⑥分布式存储及深度分析技术

该技术基于大数据组建形成分布式基础数据存储分析架构，利用合理架构分布式数据仓库、海量数据收集、数据总线、计算框架、搜索引擎、交互式分析等组件实现对安全信息数据的接入与处理分析。

⑦基于对抗的非接触高精度溯源反制框架技术

该技术可梳理出针对不同攻击手段的溯源反制流程，实现对指纹 ID 的分析与追踪、对攻击 IP 的分析与反渗透、钓鱼邮件的分析与反制、恶意程序的逆向分析与反连域名的追踪、对情报线索的深度利用，实现智能化的溯源反制框架。

⑧基于环境特征感知的动态验证技术

该技术基于多维度动态因子融合的智能验证体系。采用应用指纹、时间因子和动态特征码等三种因子进行计算，并通过不可逆加密算法进行动态保护，生成具有时空唯一性的动态标识。

⑨基于动态多重隔离的渗透场景应用技术

该技术采用元场景动态编排引擎，实现虚拟机的智能组合与拓扑变异，通过动态编排引擎解析攻防对抗意图，实现网络架构的智能重构，开发自适应变异控制算法，结合遗传算法，强化学习模型。

⑩智能攻防机器人技术

该技术采用动态对抗样本生成器，结合图神经网络的动态攻击路径规划；通过蒙特卡洛树搜索与多智能体强化学习构建战术动作的策略，并利用生成对抗网络实现攻防场景的动态变异。依托分布式协同架构、轻量化通信协议及网络靶场仿真技术，支持高并发博弈与拓扑实时重构。

（3）多循环数字风洞测试评估技术

①沉浸式安全测评环境构造技术

该技术从属性仿真和行为仿真两个方面全面模拟接近实战的信息系统攻防对抗环境构建技术，建立资产与攻击行为相关的安全属性体系模型，建立标准的数字化沉浸式安全测评环境描述方法和技术。

②渐进式安全威胁激励生成技术

该技术通过研究建立网络攻击原子行为谱系，构建风险载荷知识图谱并研究统一的语义规则实现对原子威胁行为和由满足攻击逻辑的多个系列威胁行为及配套环境上下文共同形成针对特定漏洞的风险测试载荷。

③被试体全维响应采集技术

该技术通过内核级攻击行为全景捕获与复现技术、基于应激反制的交互式对抗环境生成技术、基于 LibVMI 的带外采集技术和特征流量采集技术等技术，全面获取被试体在受到风险载荷攻击后的状态及反馈信息，为进行量化评估和优化建议提供详尽数据支撑。

④多循环激励响应控制技术

该技术通过融合虚拟化技术、云管理技术、大数据技术等研究整合测试任务、环境、载荷、结果形成测试验证场景快照及重放引擎控制技术，实现多循环渐进式安全威胁激励体制为核心的武器装备安全测试验证方法。

⑤应急快速热修复技术

该技术通过构建资产地图及风险传播模型，根据风险载荷详细拆解被试体经测试评估发现的风险性质及被利用方法，为被试体提供对应的在内外部网络边界和终端主机等位置的热修复方案帮助被试体快速修复，完成迭代优化。

⑥三维全息可视化引擎构建技术

该技术通过动态拓扑重构技术实现网络架构的立体化呈现与多维度透视。支持用户通过视角旋转、拓扑缩放及节点穿透式探查完成网络流量路径的实时追踪和设备关联关系的智能解析，实现网络空间拓扑的透明化解析。集成攻击行为模拟引擎，支持在弹性扩展的异构网络拓扑中实施红蓝对抗推演。结合防御态势感知矩阵，形成覆盖“攻击注入-防御响应-策略优化”的全周期闭环验证体系，显著提升网络防护体系的主动防御能力和协同处置效率。

⑦基于 WASM 虚拟机的跨平台安全沙箱主机探针技术

该技术基于 WebAssembly 字节码与虚拟机技术，构建了一套任务行为运行于安全沙箱的跨平台主机探针技术，探针行为空间与宿主机环境隔离，对核心业务应用零扰动，实现极高的应用稳定性及可靠性，在确保业务应用具备高可用性要求的场景下，提供可靠技术保障。

⑧基于主被动综合探测分析的僵尸隐形资产发现技术

该技术基于资产存活主动探测、被动流量采集分析与日志解析，结合多源异构化数据的归一化转换与处理技术，对多个来源、多种形式的不同类型数据进行综合关联分析，实时检测网络环境中存在的僵尸隐形资产，实现全面的资产管理与测绘，消除资产管理死角。

⑨自动化载荷生成与验证优化技术

该技术根据已探测的漏洞特征信息、业务场景交互信息及安全漏洞利用技术知识，基于大语言模型的推理与思考能力，融入循环式智能体任务执行架构，不断生成自适应利用载荷与执行测试，根据执行反馈验证载荷适用性并持续优化可利用性。

⑩多源异构漏洞情报采集与整合技术

该技术通过研究多个不同来源、不同类型的情报数据字段，识别情报间共性数据并设计统一的情报语义，将多来源、多类型的异构情报数据映射至统一情报结构体，保证在长周期、不间断、高频率情报收集与整合任务的稳定性与扩展性。

⑪基于工作树的多轮次任务沙箱隔离管理

该技术通过沙箱化技术，针对长周期多轮次的复杂任务执行提供隔离环境管理能力，并结合工作树机制针对不同任务间执行数据与结果数据提供独立存储与共享能力，保障复杂场景长周期下自动化任务执行的稳定性。

⑫基于环境建模的业务安全威胁检测技术

该技术通过融合多种资产探测技术手段，对主机、端口、服务、接口、参数等不同层级的资产信息进行采集与整合，结合大模型推理与分析能力进行业务场景建模，将原本各自独立的零散数据融合为具备特定业务含义的场景建模，并在此基础上完成攻击路径收缩，大幅度提升安全测试准确性与效率。

⑬基于逐级索引的知识渐次披露技术

该技术通过建立多层级索引式的知识结构，将网络安全、软件研发、运维保障等多种领域的知识进行统一管理，并设计知识与记忆的缓存加载机制，提供知识层面的逐级索引、按需加载的渐次加载技术，大幅度提升知识加载的准确性，降低非必要知识对上下文的污染。

⑭基于多源数据的资产拓扑绘制技术

该技术通过集成如主机端探针、OpenAPI 接口、syslog 日志、文件内容、网页特征等多种数据源采集与对接机制，实现对多源数据的整合能力，并结合大模型推理与分析能力，识别其中的通信、引用、声明特征，从多角度综合推理并绘制资产拓扑。

⑮基于多智能体集群的自动化渗透任务编排与优化技术

该技术基于多智能体集群架构，按照规划、探测、评估、分析设计不同的子智能体，并建立模型任务循环机制，融入反馈优化能力，让任务在循环执行过程中可自我迭代与提升，最终在每个子智能体内与集群层面间均具备智能化编排与反思提升能力。

（4）基于对抗生成的多维大模型安全测试评估技术

①基于对抗生成、强化学习方法等多维度方法的大模型安全性测评技术

该技术按照目标模型的功能特性和潜在风险，利用先进的强化学习（RL）和引导式对抗生成（GCG）等技术，自动化生成多类型的对抗样本，结合人工智能伦理准则，形成标准化的安全性评估报告和风险等级模板。

②基于 LLM 驱动的自适应多维网络安全智能渗透测试框架（ATLAS-PT）

该技术集成了先进的大语言模型（LLM）技术，结合动态知识图谱（DKG）和强化学习（RL），实现了全方位的智能化网络安全渗透测试，不仅执行传统的 DAST 和 SAST，还融合了 IAST 和 RASP 技术，提供全生命周期的应用程序安全保障。通过量子启发算法（QIA）优化搜索策略，ATLAS-PT 能够更高效地探索复杂的攻击面。最终，该框架利用可解释 AI（XAI）技术，生成详细的测试报告和可视化威胁图谱，为组织提供全局、更多维度的安全洞察。

③基于开源基座模型的血缘相似度评测技术

该技术按照目标模型的关键属性，利用自动化方式对各个模型进行特征提取，记录每个模型的词表、模型架构、模型权重、安全特征字符串行为等相关信息。结合专家分析，形成标准化的模型特征描述报告和相似度评估模板。

④面向智能体复现的实验环境动态配套技术

该技术采用课程视频与专属实验环境模块结合的架构，通过课程关联组件与智能体环境快速配置接口实现视频学习与实验实操联动，两者配合解决智能体开发中环境配置复杂、工具链适配繁琐的问题，满足学员随看随练、高效复现智能体构建全流程的需求。

（二）报告期内获得的研发成果

报告期内，公司致力于网络安全产品的研发，并形成具有自主知识产权的网络安全产品体系，公司获得的知识产权情况如下：

项目	本年新增		累计数量	
	申请数（个）	获得数（个）	申请数（个）	获得数（个）
发明专利	12	4	162	66

实用新型专利	0	0	0	0
外观设计专利	0	0	7	2
软件著作权	23	23	323	320
其他	33	21	295	135
合计	**68**	**48**	**787**	**523**

截至报告期末，公司已累计获得发明专利66项，获得软件著作权320项；报告期内，公司获得发明专利4项，获得软件著作权23项。

（三）报告期内研发支出变化

报告期内，公司研发投入情况如下：

单位：万元

项目	2025 年度	2024 年度	变化幅度（%）
费用化研发投入	8,741.26	9,266.42	-5.67
资本化研发投入			
研发投入合计	8,741.26	9,266.42	-5.67
研发投入总额占营业收入比例（%）	31.63	26.01	增加 5.62 个百分点
研发投入资本化的比重（%）			

2025年度，公司持续进行研发投入达8,741.26万元，占营业收入比例31.63%，较2024年度增加5.62个百分点。

八、新增业务进展是否与前期信息披露一致

不适用。

九、募集资金的使用情况及是否合规

（一）募集资金专户存储情况

截至 2025 年 12 月 31 日，公司有 6 个募集资金专户，募集资金存放情况如下：

金额单位：人民币元

账户名称	开户银行	银行账号	期末余额	账户状态
永信至诚	北京银行股份有限公司中关村分行	20000029964300007620335	0.00	待注销
永信至诚	北京银行股份有限公司中关村分行	20000029964300006835924	0.00	待注销
永信至诚	北京银行股份有限公司中关村分行	20000029964300174024250	0.00	待注销
五一嘉峪	北京银行股份有限公司中关村分行	20000043262200174025030	0.00	待注销
五一嘉峪	北京银行股份有限公司中关村分行	20000043262200174025646	0.00	待注销
五一嘉峪	北京银行股份有限公司中关村分行	20000043262200174026122	0.00	待注销

（二）募集资金投资项目的变更情况

截至报告期末，公司未发生变更募集资金投资项目的情况。

十、控股股东、实际控制人、董事、监事、高级管理人员和核心技术人员的持股、质押、冻结及减持情况

截至本报告期末，公司控股股东、实际控制人、现任及报告期内离任董事、高级管理人员和核心技术人员持股变动情况如下：

单位：股

姓名	在公司担任的职务	直接持有公司股份情况		年度内股份增减变动量	增减变动原因
蔡晶晶	董事长、核心技术人员	35,631,237	52,734,231	17,102,994	资本公积金转增
陈俊	副董事长、总经理、核心技术人员	16,447,713	24,342,615	7,894,902	资本公积金转增
张凯	董事、副总经理、核心技术人员	0	0	0	不适用
张雪峰	董事、副总经理、核心技术人员	0	0	0	不适用
杨超	董事（离任）	0	0	0	不适用
姜登峰	独立董事	0	0	0	不适用
吕文栋	独立董事	0	0	0	不适用
姜朋	独立董事	0	0	0	不适用
刘明霞	财务负责人	0	0	0	不适用
张恒	董事会秘书	0	0	0	不适用
张丽	副总经理	0	0	0	不适用
付磊	副总经理	0	0	0	不适用
郑皓	核心技术人员	0	0	0	不适用
孙义	核心技术人员	0	0	0	不适用
黄平	核心技术人员	0	0	0	不适用

截至本报告期末，蔡晶晶、陈俊、张凯、张雪峰、刘明霞、张恒、付磊、孙义、郑皓、黄平通过北京信安春秋科技合伙企业（有限合伙）间接持有公司股份；陈俊通过北京信安春秋壹号科技合伙企业（有限合伙）间接持有公司股份。截至本报告期末，上述人员持有的公司股份不存在质押或冻结的情况。

十一、保荐机构认为应当发表意见的其他事项

截至本持续督导跟踪报告出具之日，不存在保荐机构认为应当发表意见的其他事项。

（以下无正文）

（本页无正文，为《国信证券股份有限公司关于永信至诚科技集团股份有限公司2025年年度持续督导跟踪报告》之签章页）

保荐代表人：

侯英刚　　李　艳

国信证券股份有限公司

2026年5月11日