中国国际金融股份有限公司
关于亚信安全科技股份有限公司
2024 年半年度持续督导跟踪报告

中国国际金融股份有限公司（以下简称“中金公司”或“保荐机构”）作为亚信安全科技股份有限公司（以下简称“亚信安全”或“公司”）首次公开发行股票并在科创板上市的保荐机构，根据《证券发行上市保荐业务管理办法》《上海证券交易所科创板股票上市规则》《上海证券交易所上市公司自律监管指引第 11 号——持续督导》等法律、行政法规、部门规章及业务规则，负责亚信安全上市后的持续督导工作，并出具本持续督导半年度跟踪报告。

一、保荐机构持续督导工作情况

序号	项目	工作内容
1	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
2	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，明确双方在持续督导期间的权利义务，并报上海证券交易所备案	保荐机构已与上市公司签署了《保荐协议》，协议明确了双方在持续督导期间的权利和义务，并已报上海证券交易所备案
3	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	保荐机构通过日常沟通、定期或不定期回访、尽职调查等方式，对上市公司开展持续督导工作
4	持续督导期间，按照有关规定对上市公司违法违规事项公开发表声明的，应于披露前向上海证券交易所报告，并经上海证券交易所审核后在指定媒体上公告	2024年上半年，上市公司未出现按有关规定须保荐机构公开发表声明的违法违规情况
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，应自发现或应当发现之日起五个工作日内向上海证券交易所报告，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，保荐人采取的督导措施等	2024年上半年，上市公司及其相关当事人未出现违法违规或违背承诺等事项
6	督导上市公司及其董事、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	保荐机构督导上市公司及其董事、监事、高级管理人员遵守法律、法规、部门规章

	的业务规则及其他规范性文件，并切实履行其所做出的各项承诺	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	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、监事会议事规则以及董事、监事和高级管理人员的行为规范等	保荐机构督促上市公司依照相关规定健全完善公司治理制度，并严格执行公司治理制度
8	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	保荐机构对上市公司内控制度的设计、实施和有效性进行了核查，上市公司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	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上海证券交易所提交的文件不存在虚假记载、误导性陈述或重大遗漏	保荐机构督促上市公司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	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及时督促公司予以更正或补充，公司不予更正或补充的，应及时向上海证券交易所报告；对上市公司的信息披露文件未进行事前审阅的，应在上市公司履行信息披露义务后五个交易日内，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，应及时向上海证券交易所报告	保荐机构对上市公司的信息披露文件进行了审阅，不存在应向上海证券交易所报告的情况
11	关注上市公司或其控股股东、实际控制人、董事、监事、高级管理人员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，并督促其完善内部控制制度，采取措施予以纠正	2024年上半年，上市公司及其相关当事人未出现该等事项
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，及时向上海证券交易所报告	2024年上半年，上市公司及其相关当事人不存在未履行承诺的情况
13	关注公共传媒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披露未披露的重大事项或披露的信息与事实不符的，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	2024年上半年，上市公司未出现该等事项

	的，应及时向上海证券交易所报告	
14	发现以下情形之一的，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）涉嫌违反《上市规则》等相关业务规则；（二）证券服务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）公司出现《保荐办法》第七十一条、第七十二条规定的情形；（四）公司不配合持续督导工作；（五）上海证券交易所或保荐人认为需要报告的其他情形	2024年上半年，上市公司及相关主体未出现该等事项
15	上市公司出现以下情形之一的，保荐人应自知道或应当知道之日起十五日内或上海证券交易所要求的期限内，对上市公司进行专项现场检查：（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、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）上海证券交易所或者保荐人认为应当进行现场核查的其他事项	2024年上半年，上市公司未出现该等事项

二、保荐机构发现公司存在的问题及采取的措施

无。

三、重大风险事项

公司目前面临的风险因素主要如下：

（一）业绩下滑或亏损的风险

2024 年上半年，公司实现营业收入 6.61 亿元，较去年同期增加 17.31%，主要系公司运营商行业收入恢复稳定增长，同时聚焦高增长、高潜力、高价值的细分市场，做深、做强重点行业的策略取得了预期成果。2024 年上半年，公司整体毛利率略有下降，从去年同期的 55.81%降至 54.86%；销售费用较去年同期增加 7.72%，管理费用较去年同期下降 1.97%，研发费用较去年同期增加 6.54%。2024

年上半年，公司实现归属于母公司所有者的净利润-1.92 亿元，较去年同期亏损略有扩大；归属于母公司所有者的扣除非经常性损益后的净利润-1.97 亿元，较去年同期相比基本持平。公司所处的网络安全行业具备高销售及高研发投入的特征，且产品市场需求受宏观经济环境、网络安全事件、政策法规影响较大，若公司业务拓展及收入增长未达预期，销售及研发投入持续增加，公司可能面临业绩持续下滑甚至亏损的风险。

（二）核心竞争力风险

1、技术不能保持先进性的风险及相关技术迭代风险

伴随计算机、互联网和通信技术的高速发展，信息安全科技水平不断进步与创新。与此同时，各种威胁信息系统安全的手段也层出不穷，信息安全漏洞危害性越来越大，这对公司的技术水平和研发能力提出了较大的挑战。另一方面，尽管公司一直致力于科技创新，力争保持在网络安全领域的技术领先优势，但不排除国内外竞争对手或潜在竞争对手率先在相关领域取得重大突破，而推出更先进、更具竞争力的技术和产品，或出现其他替代产品和技术，从而使本公司的产品和技术失去领先优势。

2、新产品的研发风险

公司的主要收入来源于数字信任及身份安全产品、云网边安全产品、端点安全产品和网络安全服务。未来公司将在现有业务的基础上，积极布局其它网络安全领域，拓展公司的主营业务。公司所处的网络安全行业的技术发展日新月异，行业发展趋势存在不确定性，可能会导致公司在新技术的研发方向、重要产品的方案制定等方面不能及时做出准确决策。公司可能面临新产品研发失败或销售不及预期的风险，从而对公司业绩产生不利的影响。

（三）经营风险

1、客户集中的风险

报告期内，公司销售收入客户集中度较高。公司与主要客户建立了长期稳定的合作关系，且这些客户多为信誉度较高的优质客户，但公司若不能通过技术、产品创新等方式及时满足上述客户的业务需求，或上述客户因为市场低迷等原因

使其自身经营情况发生变化，导致其对公司产品的需求大幅下降，公司将面临一定的因客户集中度较高而导致的经营风险。

2、核心技术人员流失风险

经过多年积累和发展，公司形成了以核心技术人员为首的多个强有力的研发团队。为保障公司高级管理人员和核心技术人员稳定，公司制定了合理有效的股权激励机制，并同主要核心技术人员签署了保密协议和竞业禁止协议。虽然公司的核心技术并未严重依赖个别核心技术人员，但不排除掌握核心技术的部分人员不稳定，可能造成在研项目进度推迟、甚至终止，或者造成研发项目泄密或流失，给公司后续新产品的开发以及持续稳定增长带来不利影响。

（四）财务风险

1、收入季节性波动的风险

公司通常上半年营业收入较低，而下半年（特别是第四季度）营业收入较高，存在一定的季节性特征，主要原因在于公司目前的主要客户集中于运营商、金融、政府等行业和领域，这些客户往往实行集中采购制度和预算管理制度，其采购活动具有较强的季节性。许多客户在每一年的上半年对本年度的采购及投资活动进行预算立项、设备选型测试等，下半年进行招标、采购和项目建设、验收、结算，因此每年的第三、四季度往往出现收入增加的现象，导致公司的经营业绩呈现较明显的上下半年不均衡的分布特征。

2、政府补助变化产生的风险

政府对高新技术企业予以重点鼓励和扶持。2024年上半年，公司除增值税退税外政府补助形成的其他收益为1,574.61万元，金额较大。如果公司所处行业及高新技术企业的扶持政策发生变化，将对公司的发展产生一定的影响。

（五）行业风险

1、市场竞争加剧的风险

我国网络安全行业市场空间已颇具规模，多年来保持了快速增长态势，为公司提供了获取更大市场份额的机会。但随着用户对网络安全产品及服务的需求不

断增长，行业内原有竞争对手规模和竞争力的不断提高，加之新进入竞争者逐步增多，可能导致公司所处行业竞争加剧。如果公司在市场竞争中不能有效保持技术领先水平，不能充分利用现有的市场影响力，无法在当前市场高速发展的态势下迅速扩大自身规模并增强资金实力，公司将面临较大的市场竞争风险，有可能导致公司的市场地位出现下滑。

2、行业增长速度下降的风险

网络安全行业过去多年保持较高的增长速度，行业需求比较旺盛，行业内企业均取得了较好的发展。但是网络安全行业与IT的整体发展紧密相关，受IT投入的影响比较大。受企业网络安全投入预算的影响，行业增长与整体的经济环境、企业盈利状况密切相关，当整体经济状况下行时，面临预算收缩的压力，行业增长速度面临下降的风险。此外，随着网络安全的渗透率日益提高，网络安全行业面临着行业增长动能减缓的情况。

（六）宏观环境风险

1、产业政策变化产生的风险

国家重视信息技术及网络安全产业，并给予重点鼓励和扶植，网络安全产业政策陆续出台。在相当长的一段时期内，国家仍将会给予信息技术及网络安全产业政策支持。如果国家对信息技术及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。

（七）与趋势科技合作稳定性风险

根据亚信安全（香港）与趋势澳洲签署的《知识产权许可及合作协议》和其他相关协议，公司与趋势科技目前在中国大陆地区进行独家合作，合作内容包括趋势科技品牌产品独家分销合作、源代码合作、独家技术服务以及趋势科技品牌产品的OEM合作等。虽然公司自主研发能力较强，对趋势科技的依赖度有限，且公司与趋势科技已建立长期全面合作关系，但如果未来因经济形势、政治环境等原因影响，公司未能与趋势科技继续合作，仍然可能对公司短期的业务开展造成一定的影响。

四、重大违规事项

2024 年上半年，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

2024 年上半年，公司主要财务数据如下：

单位：万元

项目	本报告期	去年同期	变动幅度
营业收入	66,070.67	56,322.47	17.31%
归属于上市公司股东的净利润	-19,210.98	-17,135.39	不适用
归属于上市公司股东的扣除非经常性损益的净利润	-19,741.70	-19,208.46	不适用
经营活动产生的现金流量净额	-30,893.13	-39,642.24	不适用
项目	**本报告期末**	**上年度末**	**变动幅度**
归属于上市公司股东的净资产	194,562.81	211,793.85	-8.14%
总资产	385,205.42	340,097.75	13.26%

2024 年上半年，公司主要财务指标如下：

项目	本报告期	去年同期	变动幅度
基本每股收益（元／股）	-0.4803	-0.4284	不适用
稀释每股收益（元／股）	-	-	-
扣除非经常性损益后的基本每股收益（元／股）	-0.4935	-0.4802	不适用
加权平均净资产收益率（%）	-9.46	-12.28	增加 2.82 个百分点
扣除非经常性损益后的加权平均净资产收益率（%）	-9.72	-14.62	增加 4.90 个百分点
研发投入占营业收入的比例（%）	33.74	37.15	减少 3.41 个百分点

1、2024 年上半年，公司营业收入同比增长 17.31%，主要系公司运营商行业收入恢复稳定增长，同时聚焦高增长、高潜力、高价值的细分市场，做深、做强重点行业的策略取得了预期成果。

2、2024 年上半年，公司销售费用较去年同期增加 7.72%，研发费用较去年同期增加 6.54%，管理费用较去年同期下降 1.97%，三项费用合计增加 2,994.72

万元，同比增加 5.72%。公司实现归属于母公司所有者的净利润-1.92 亿元，较去年同期亏损略有扩大;归属于母公司所有者的扣除非经常性损益后的净利润-1.97 亿元，较去年同期相比基本持平。

六、核心竞争力的变化情况

（一）核心竞争力分析

1、领先的研发创新能力和产品地位

公司自成立以来一直高度重视研发创新，拥有美国软件工程学会颁发的 CMMI5 权威认证，在软件开发过程的改善能力、质量管理水平、软件开发的整体成熟度居于行业前列。公司经过多年的探索和积累，已掌握了云安全、终端安全、身份安全、安全管理、高级威胁治理、威胁情报等领域的重要核心技术，并形成了一系列具有自主知识产权的技术成果。

公司在北京、南京、成都设立了三大研发中心，公司与国家计算机病毒应急处理中心（CVERC）在天津共建病毒实验室，共同开展高级持续性威胁（APT）方面的研究，持续为 CVERC 通报病毒信息；公司建成了亚信网络安全产业技术研究院，拥有网络安全态势感知中心、高级威胁调查取证中心、网络安全攻防实验室，开展前瞻性基础研究和技术创新。亚信安全第一时间意识到 5G 对数字化未来世界的重要性，积极参与运营商 5G 试点项目，致力于 5G 安全共性关键技术以及成果转化，搭建创新平台，赋能行业发展。

公司具备支撑国家级项目建设的研发能力，可以满足大规模高稳定的复杂用户需求。公司为国务院办公厅电子政务办公室建设了国家政务服务平台统一身份认证系统，支撑全国一体化政务服务平台的统一身份互认，提供“威胁识别、精准监管、整体协同、预警响应”的一体化管理能力。

2、以网络安全软件为主导，身份安全、终端安全、云安全国内领先

区别于传统的以硬件为主导的网络安全公司，公司的优势产品和解决方案主要集中在网络安全软件与服务领域。公司在中国网络安全软件市场处于领先地位，

2024 年 5 月在 IDC《2023 年下半年中国 IT 安全软件市场跟踪报告》，身份和数字信任产品市场份额连续 7 年位居第一；2024 年 5 月在 IDC《2023 年下半年中国 IT 安全软件市场跟踪报告》，终端安全产品市场份额连续多年位居第二；2024 年 5 月在《IDC 中国 WAAP 厂商技术能力评估 2024》中，亚信安全 WAPP 斩获中国 WAPP 市场技术代表厂商；2024 年 6 月在 IDC《中国私有云云工作负载安全市场份额，2023：CNAPP 助力企业实现全方位云原生安全防护》中,云主机安全产品市场份额位居第三；2024 年 6 月在《IDC MarketScape：中国扩展检测与响应（XDR）平台 2024》 中，XDR 凭借综合实力荣登“领导者”象限，在营收规模、战略能力上均位列前茅。

公司的泛身份安全类产品聚合了可信身份能力、可信认证能力、可信访问能力及合规审计能力，拥有业界先进的身份管理与认证、自适应智能身份认证、基于 SIM 卡的密码服务等多项核心技术，满足用户在传统 IT 架构、物联网、云计算、大数据环境下的泛在身份管理需求。

公司的终端安全产品依托下一代云客户端基础架构“智能防护网络”，使用户可以不受物理位置的限制实时获取云端威胁情报注入的智能防护能力；将恶意软件检测引擎、攻击行为检测引擎、 机器学习检测引擎和威胁情报数据湖的“三擎一湖”技术融入到防御组合中，从而有效防护已知和未知威胁；同时集成漏洞防护（VP）、终端安全检测与响应（EDR）、桌面管控、终端准入、数据备份等安全模块，与威胁情报共享协同，为客户提供完整的一体化终端安全防护方案。

云安全是公司重点布局的领域之一，领先实力获得广泛认可，连续两年入选 Gartner CWPP 应用示范厂商，在沙利文《2021 年中国云主机安全市场报告》中创新指数排名第一。2023 年 10 月公司完成对厦门服云信息科技有限公司（品牌名：安全狗）的收购，服云信息 2013 年成立于厦门，长期专注于云安全领域，是国内较早引入云工作负载安全（CWPP）概念，并成功构建相应产品线的专业云安全厂商，在云主机安全、公有云 SaaS 产品、私有云安全平台、容器安全、云原生安全、微隔离等方面，拥有业内领先的技术和产品，服务于国家部委、地方政府、央企、国企、世界 500 强、独角兽企业等在内的数千家政企客户，获得广泛认可。公司与服云信息将深度融合云安全的产品技术能力，形成云安全最强

实力组合，加速云原生安全创新发展，构筑完整的云安全体系，形成国内云安全赛道能力最完整的网络安全公司。

3、擅长提供综合性安全解决方案和卓越的服务能力

公司擅长为拥有大型网络和复杂 IT 架构的客户量身打造满足其特殊需求的综合性安全解决方案。公司经过多年的发展，逐步形成了涵盖泛身份安全、泛终端安全、云及边缘安全、大数据分析及安全管理、5G 云网边管理、高级威胁治理等多个领域的网络安全产品和解决方案体系，形成了较强的综合服务能力，可有效满足用户构建综合性安全防护体系的需求。

在网络架构、业务系统高度复杂、对系统稳定性、业务连续性要求极高的电信运营商和金融领域，基于对客户业务的深入理解和卓越的软件开发服务能力，公司的综合性安全解决方案得到了大量应用。公司解决方案应对大型复杂系统的安全防护能力和电信金融级别的高速响应能力经历了多年实践的检验，有效地保障了客户系统的安全性和业务连续性，得到了客户的广泛认可。

经过多年的发展，公司形成了覆盖广泛、立体响应、及时高效的客户服务体系，形成了涵盖安全规划、安全攻防、安全评估、安全培训、应急响应等多个方面的服务能力，能够为客户提供 7×24 小时现场和远程支援，有效响应客户的需求。公司曾多次受邀为国家重大活动提供安全保卫服务，多次因优秀的服务表现收到相关单位的感谢函。

4、与电信运营商多年合作积累的“懂网”能力与业务资源

作为电信运营商的长期合作伙伴，公司与运营商共同推进行业标准与业务规范的制定，在既有业务合作、新业务机会拓展和商业模式探索等方面建立了坚实基础与领先优势。公司的产品和系统附着在电信运营商的基础网络内，覆盖了核心网、接入网和支撑网，为电信运营商提供了支撑其业务开展和运营的系统能力和安全防护，构成了电信运营商的基础网络安全能力机制。经过多年的合作，公司积累了对运营商网络的深刻理解，与运营商各部门建立了深厚的合作关系及信任基础。

凭借与电信运营商的紧密业务合作关系，公司是最早进入 5G 安全领域的安全厂商之一，积极参与电信运营商 5G 试点项目；公司的统一身份认证与访问管理系统针对 5G 应用场景做了研发升级，目前已经在电信运营商 5G NFV 网络、5G SA 网络中试点接入网元设备；公司互联网接入认证系统在电信运营商 5G VPDN 安全认证系统中得到了应用，同时在 5G 物联网接入认证系统中得到了应用，为基于 5G 的物联网业务提供网络接入安全认证能力支撑；5G 全流量安全检测与响应平台是亚信安全重点打造的 5G 安全产品，依托公司在通信和安全领域深耕多年的独特优势，站在 5G 角度看安全并提出安全内生的概念，能够从 5G 信令、用户流量、虚拟化、容器、安全边界等多个层面提供全方位、立体式防护，作为一套统一的端到端的安全解决方案，能够对 5G 网络威胁进行全面可视、全局联动，具备网络安全防护、风险感知、事故预防和安全处置等核心能力，有效保护 5G 关键基础设施建设、5G 应用安全、防护勒索病毒等各类 APT 高级威胁，确保安全风险可控，避免极端事故的发生，为 5G、5G-A 行业应用蓬勃发展打造数字化安全底座。依托与电信运营商多年合作积累的“懂网”能力与业务资源优势，公司针对 5G 架构下的安全产品和解决方案将为 5G 安全提供重要支撑，随着 5G 在产业互联网应用的加速推广，公司也将在护航产业互联网的道路上迎来新一轮的发展机遇。

5、智能联动的平台级安全防护体系和突出的威胁情报能力

经过多年的研发攻关，公司不同安全防护能力的产品和解决方案实现智能联动，帮助客户构建全方位的平台级安全防护体系，公司已经初步形成了安全威胁治理运维（XDR）和安全中台两套平台级安全防护解决方案。

安全威胁治理运维（XDR）解决方案以威胁感知运维中心作为集中管控平台，叠加搭载公司的泛终端安全类产品、高级威胁治理类产品、云及边缘安全类产品等系列产品，结合云端威胁情报，通过预先精密编排的各种威胁响应预案，实现检测、分析、响应到阻断的自动化处置，从而有效地帮助用户更早地发现威胁、处置威胁、修复系统，提升系统防护能力。

安全中台是 5G 云网时代安全业务、安全能力、安全数据的汇聚协同中心，是“云化、联动、主动化、智能化、服务化”的新一代安全架构。安全中台打破

原有安全系统“烟囱式”架构，融聚安全共性能力上台，通过数据共享、系统融合、能力汇聚、业务滋养、融云赋能五个方面逐步构建“云化编排、智能决策、自动处置、场景业务”能力，实现便捷、高效、随选的安全能力供给与服务。

公司通过对海量多源异构数据进行收集，利用大数据和人工智能技术，进行分析和关联，为安全产品和解决方案赋能。突出的威胁情报能力大大提高了公司产品和解决方案应对复杂攻击威胁的检测和响应能力，是公司多层注智、打造数据驱动智能安全平台的重要基础和优势。

6、广受认可的品牌形象和高素质的人才队伍

经过多年发展，“亚信安全”已成为中国网络安全领域的领导品牌之一。公司凭借自身的产品、技术和综合服务能力优势，获得了国内外市场研究机构、政府主管部门和行业内专家和客户的认可。

公司核心产品与技术以及公司市场影响力获得了国内外市场研究机构的广泛认可，在身份和数字信任软件市场、终端安全软件市场、网络安全检测与响应（NDR）、云安全市场等领域均位于市场领先地位，奠定了在中国网络安全软件市场的领先地位。

公司客户广泛分布于电信运营商、金融、政府部委、能源等行业领域，公司的重要客户包括三大电信运营商、中国人民银行总行、五大国有银行、大型股份制银行、国家部委等重点中央部门以及国家电网、南方电网、中石化等重点企业。

公司拥有一支高素质的人才队伍。公司把人才培养和组织能力建设作为一项战略投资，通过一系列有效的聘用、培养和激励机制保障团队稳定。公司对人员培养持续投入，保证源源不断的人才供给和内部人员的能力提升。公司落实优秀校招人才战略，确保形成自己的人才供应链，保障优秀校招生在中长期成为公司人才梯队的中坚力量，培养生力军。公司注重管理干部的规划和建设，建立干部资源池，通过选拔、任用、培养、评估的干部管理流程，不断优化各层干部群体的知识结构和综合管理能力。

（二）核心竞争力变化情况

2024 年上半年，公司的核心竞争力未发生重大变化。

七、研发支出变化及研发进展

（一）研发支出及变化情况

2024 年上半年，公司研发费用为 2.23 亿元，研发投入占营业收入的比例为 33.74%，与去年同期研发费用率 37.15%相比，下降 3.41 个百分点。公司的研发投入的情况如下表所示：

单位：万元

项目	本报告期	去年同期	变动幅度
费用化研发投入	22,291.53	20,924.10	6.54%
资本化研发投入	-	-	-
研发投入合计	22,291.53	20,924.10	6.54%
研发投入总额占营业收入比例（%）	33.74	37.15	下降 3.41 个百分点
研发投入资本化的比重（%）	-	-	-

（二）研发进展

2024 年上半年，公司主要在研项目具体如下：

单位：万元

序号	项目名称	预计总投资规模	本期投入金额	累计投入金额	进展或阶段性成果	拟达到目标	技术水平	具体应用前景
1	海鸥威胁行为检测引擎（AttackIO）	1,000.00	347.84	833.81	相关产品已进入市场，稳定开发优化阶段。	基于 ATT&CK 模型和 AI 算法，构建高精度的行为检测引擎。引擎依托 agent 端收集、研判、聚合受保护主机日志，产生战术点告警事件；依托云端聚类、降噪、关联产生杀伤链告警。使用户摆脱告警风暴，并了解攻击路径和应对方法。云端引擎具备学习能力，以应对不断变化和增长的网络攻击方法。	1、具备未知威胁检测能力；2、检测规则覆盖 14 个战术点，超过 400 个黑客攻击技术点，达到行业先进水平；3、检测规则数量超过 2000 条，为覆盖 ATT&CK 更多战技术点，还在持续增加中；4、与 AttackIO 云端分析引擎互动，进一步提高检测能力。	可应用于网络安全行业，对安全有较高要求的企事业单位，与传统安全引擎形成纵深防御体系，解决系统中存在的安全问题。
2	梦蝶文件防病毒引擎（MalDetect）	3,000.00	347.84	2,564.61	相关产品已投入市场，目前已获得客户认可。	新一代的轻量级文件防病毒引擎，增强对新型威胁的检测能力，如国产化平台的病毒，WebShell、无文件攻击等热门威胁的检测。	基于特征码的传统病毒检测技术对于未知威胁的检测效果一般，新一代的文件防病毒引擎融合特征码、云查杀、启发式、机器学习及一些新型的检测技术，以海量样本威胁数据作为支撑，并构建起小时级的威胁发现，反馈和全网免疫闭环通道，具备	可广泛用于对安全有较高要求的关键基础设施行业，为自研安全产品提供基于静态文件病毒的检测与阻断。

序号	项目名称	预计总投资规模	本期投入金额	累计投入金额	进展或阶段性成果	拟达到目标	技术水平	具体应用前景
							强大的对未知威胁的检测能力。	
3	怒狮网络防病毒引擎（NetStack）	3,000.00	364.64	2,561.45	相关产品已进入市场，稳定开发优化阶段。	新一代高性能的网络威胁检测引擎，适配主流平台及国产化系统，满足产品的定制化需求，持续增强网络威胁的检测能力，加强新型漏洞的查杀能力。	1、已知威胁覆盖全面，覆盖超过 10000 个国内外重要漏洞，超过 70 种黑客工具，超过 100 个网络攻击技术点；2、有效发现真实攻击，内置 10+机器学习模块，80+深度研判模块，对于多种攻击技术点深度研判；3、具备 0Day 漏洞的检测能力和新兴攻击技术的检测能力。	可广泛用于对安全有较高要求的关键基础设施行业，为自研安全产品提供基于网络流量的检测与阻断。
4	魔龙盾威胁指标评估引擎（Maldium）	2,000.00	207.30	1,680.85	相关产品已进入市场，稳定开发优化阶段。	基于数据湖海量威胁情报数据以及亚信安全的“智能防护网络”云端研判服务，构建高性能威胁指标评估引擎提供 Web 信誉、失陷指标检测、勒索风险预警能力，增强网关、APT 及终端类产品威胁检测能力，形成了情报运营闭环。	1、亚信安全基于底层数据湖威胁情报，依托蜜罐云、沙箱云、网络测绘技术手段，通过深度学习、数据挖掘、专家规则等近百种情报生产模型和算法用于情报生产、研判。利用反馈机制辅助修正保证情报强时效、高精准与低误报；2、引擎端内置多种缓存机制，本地缓存机制与云端联动机制，在产品的威胁检测能力极大提升的同	魔龙盾威胁指标评估引擎，可以为云安全、身份安全、终端安全、安全管理、数据安全、高级威胁治理等各类安全产品提供高质量的情报评估服务。适用于运营商、金融等多种行业和场景。

序号	项目名称	预计总投资规模	本期投入金额	累计投入金额	进展或阶段性成果	拟达到目标	技术水平	具体应用前景
							时,也保证了高检测性能。3、在 Web 信誉、失陷指标检测、勒索风险预警能力在业界处于一流水平。	
5	亚信安全威胁数据湖（AIS-TIDL）	3,000.00	207.30	2,737.18	项目正处于相关模型与关键技术的稳定开发阶段	广泛收集内外部威胁数据，包括开源情报，付费情报，反馈情报与合作情报，利用大数据技术妥善保存和管理威胁情报，沉淀亚信安全在威胁情报领域的数据资产。针对多源异构情报进行数据标准化，形成情报元数据库，面向各类应用场景构建数据资产目录，使得数据成为公司显性核心资产。	1、已集成上百家以上情报源，包括战术级情报源与战略级情报源；2、已积累有效威胁数据，互联网类超过 100 亿，文件类超过 10 亿；3、已集成自动化分析流程超过 20 个，文件类情报更新频率小于 4 小时，互联网类情报更新频率小于 1 小时；4、数据资产目录达 100 个。	赋能 XDR 平台，提升威胁治理能力，最终达到全网免疫能力。
6	一体化终端安全平台研发	7,000.00	1,224.86	7,047.22	相关产品已投入市场，稳定开发优化阶段。	1、终端安全防护平台组件管理框架能力持续提升，增强产品平台管理能力；2、优化高级威胁终端检测与响应系统资产管理功能，完	基于下一代终端防病毒技术，利用机器学习，行为监控，云查杀和传统特征库结合的方式，有效防范恶意威胁软件，勒索病毒，挖矿软件等已知和未知威胁，同时	广泛用于对安全有较高要求的金融、高端制造和关键基础设施等行业，为用户提供终端安全防护

序号	项目名称	预计总投资规模	本期投入金额	累计投入金额	进展或阶段性成果	拟达到目标	技术水平	具体应用前景
						善 EPP+EDR+资产管理方案；3、更新核心引擎，增强防病毒能力；4、提升无文件攻击检测能力；5、增强机器学习的本地模式，强化用户在无法连接到互联网时也可以得到机器学习的保护能力。	插件化的方式构建终端安全一体化平台，全面覆盖威胁防御和终端安全管理，支持大规模分级部署，并可与第三方管理平台集成实现统一管理和态势感知。	平台化和整体性解决方案。
7	高级威胁发现与分析平台研发	6,000.00	899.36	6,070.73	相关产品已投入市场，稳定开发优化阶段。	1、增强网络内容检测引擎能力，提升网络流量解析及网络流量威胁检测性能；2、增强网络文件内容恶意行为分析引擎能力，提升网络文件内容深度扫描和检测性能；3、提升沙盒检测能力，提升对 APT 攻击的动态分析检测能力；4.增强以失陷资产为核心的威胁关联分析和威胁溯源能力。	能侦测所有端口及 100 多种通讯协议的应用，用规则引擎、威胁情报、机器学习、沙箱动态模拟分析等技术，能快速发掘并分析恶意文档，恶意软件、恶意网页，违规外联、勒索软件以及传统防护无法侦测到的内网攻击以及定向 APT 攻击活动。	可广泛用于对安全有较高要求的金融、高端制造业等客户，为客户提供业界领先的 APT 检测和分析能力，帮助客户应对日益变化的攻击场景，提供持续的防护。满足基于等保合规和客户实际需要的网络边界防病毒需求，聚焦的行业包括政府、小金融、制造业。

序号	项目名称	预计总投资规模	本期投入金额	累计投入金额	进展或阶段性成果	拟达到目标	技术水平	具体应用前景
8	DNS 域名解析产品研发	5,000.00	547.98	3,057.82	相关产品已进入市场，稳定开发优化阶段。	1、提高产品高并发处理能力，降低缓存响应时延，保持 DNS 产品市场领先性；2、持续增加产品的国产化适配能力，增强市场竞争力。	1、域名解析产品可支持缓存超过 4000 万条域名记录，在高并发处理场景下，DNS 缓存应答处理时延低至 1ms 内；2、对主流国产芯片的兼容，产品同时进行了 X86 和 ARM 架构的兼容适配，保证了高性能解析技术在不同硬件架构下都能达到较高的性能水平；3、对主流国产操作系统的兼容，产品进行了国产操作系统龙蜥、欧拉、CTyunOS 的兼容适配，提升了国产化适配能力；4、基于全新设计的框架，引入新的策略处理机制、策略匹配算法，减少内存资源占用，提升冷加载速率。	DNS 全业务域名解析系统已经部署全国 20 多个省级运营商，为数亿手机和家宽用户提供安全、快速、稳定、智能的域名解析服务，支撑互联网业务发展。
9	安全运营及态势感知平台	8,000.00	377.23	7,964.20	相关产品已投入市场，稳定开发优化阶段。	升级现有产品的架构，提高系统的可扩展性和性能，增强生态兼容能力，满足集群化部署和节点可扩展。系统处理性能和第三方设备	1、具备亿级以上数据量秒级统计、查询、展示能力，支持大数据+分布式架构，硬件化部署，支持横向扩展；2、单服务器处理能力达到 2 万 EPS，3 节点集群处理能	提供安全顶层聚合能力，以 AI 和大数据分析为支撑，以主动防御为核心，建立安全数据汇聚、检测预警、分析研判、协

序号	项目名称	预计总投资规模	本期投入金额	累计投入金额	进展或阶段性成果	拟达到目标	技术水平	具体应用前景
						的对接能力达到业内前列。发布支持国产化操作系统的产品。	力达到 4 万 EPS；3、已完成 150 余款第三方安全设备与十余款自有安全产品的联动处置响应对接；4、具备基于 BI 能力的工作台和报告生成；5、支持麒麟、统信、欧拉等操作系统。	同防御、安全可视于一体的安全运营和态势感知中心。产品应用于政府、金融、运营商、公安、企业等行业单位。
10	零信任产品研发	4,000.00	328.34	3,242.10	相关产品已进入市场，稳定开发优化阶段。	以 SDP 为关键组件，统一身份，以 AI 智能可信分析决策引擎为大脑，融合终端安全，形成亚信安全的零信任安全架构体系，同时联动态势感知、威胁引擎，基于零信任身份，贯穿“云、网、端”全域全流程安全业务访问，实现持续信任评估，安全动态的访问控制，全面保护业务安全。	通过隐身网关、WEB 网关、隧道网关、控制中心、持续信任评估引擎、访问控制引擎等核心组件，融合终端安全能力，实现身份可信识别能力、持续信任评估能力、网络访问控制能力、应用访问控制能力和全面安全防护及可视化能力。	满足企业远程安全办公、多云多数据中心安全访问、终端安全一体化等场景需求。
11	运维安全管理与审计系统	3,000.00	441.36	2,861.66	相关产品已进入市场，稳定开发优化阶段。	迭代升级技术架构，增强安全能力，支持联动登录能力，扩充管理端	通过运维协议代理网关，应用发布网关来提供运维用户全生命周期管理，运维访问控制细粒度授权与命令控	辅助企业完成等级保护等法令法规对企业运维的合规要求，并提供验证，授

序号	项目名称	预计总投资规模	本期投入金额	累计投入金额	进展或阶段性成果	拟达到目标	技术水平	具体应用前景
						国产化整体兼容性，提升产品整体交互体验。	制、对运维资产和应用工具集中管理、单点登录、操作日志录像关联审计；提供运维文件传输病毒防护能力。	权等账号资源管理功能的统一安全运维管理方案，满足本地运维管理、混合云安全管理、密评检测场景需求。
12	网络威胁入侵防护系统	4,000.00	718.88	3,180.45	相关产品已进入市场，稳定开发优化阶段。	在确保高吞吐、低时延的条件下，对网关侧流量进行实时检测和分析，能够根据需要对威胁流量进行阻断和通知终端客户，而且相关技术能够不断迭代和更新，能够对新型的威胁攻击如勒索等事件进行防护。此外，系统需要具备很高的稳定性，提供各种方式便于管理和运维，具备较高的开放性，能够和其他威胁检测和防御产品协同作战，为客户提供威胁立体防御能力。	1、基于高级威胁扫描引擎以及文件高速还原技术，支持HTTP、FTP、SMTP、POP3、SMB(v3)等超过 100 种协议的识别、分析和扫描，具备业界领先的虚拟补丁技术，能够对网络入侵威胁事件进行实时、有效的拦截；2、高并发、高性能网络流量处理技术，综合威胁检测和防御吞吐能力达到了 20G 以上。	广泛用于对安全有较高要求的金融、高端制造、政府等关键基础设施等行业，为用户提供网关侧病毒防护以及漏洞利用等入侵威胁防护整体性解决方案。

序号	项目名称	预计总投资规模	本期投入金额	累计投入金额	进展或阶段性成果	拟达到目标	技术水平	具体应用前景
13	信舱共享免疫 SaaS 系统	4,000.00	707.20	2,576.07	相关产品已投入市场，目前已获得客户认可。	通过 EDR/XDR 检测手段结合威胁情报、云沙箱和威胁图，能够有效检测传统防病毒无法检测到的真实威胁；为客户提供 7*24 的托管运营服务，对真实威胁实现“早发现”、“早诊断”和“早处置”，领先攻击者一步抵御高级威胁。	1、目前已覆盖超过 360 个 ATT&CK 技术点，结合威胁情报、云沙箱和云端威胁狩猎，以异常行为检测来帮助用户发现传统防病毒检测不到的真实威胁；2、通过失陷 IOC 特征库（超过 200 万条）检测用户环境中的 C&C 连接，以数据驱动 AI 原生的方式提升 7*24SOC 服务的效率，达成一地检测、全网免疫的防护效果。	广泛应用于制造、金融、能源和运营商等行业客户，通过 7*24 的托管运营服务让客户以更好的性价比来享受安全专家服务，以 EDR 为核心构建 XDR SaaS 平台，通过云端威胁狩猎检测到专业黑客团伙的入侵攻击，通过 AI 达成降噪和提纯的效果，提供更加精准的真实威胁检测和响应服务。
14	云原生安全(容器安全)	6,000.00	2,402.60	5,049.74	相关产品已投入市场，目前已获得客户认可。	在云原生场景下，通过一个“N 合 1”安全基座，以工作负载为中心构建覆盖宿主机安全、容器安全、网络微隔离和云原生态势感知全栈安全需求的一站式平台，可以支撑满足具有“高度监管、技术安	1、创新实现镜像分层扫描能力，达到镜像间的相同层不重复扫、支持按照镜像画像标签作优先级排序，提升镜像扫描效率 5 倍以上；2、支持常见的国产信创操作系统镜像(Neokylin、OpenEuler、Anolis、UOS、BC-Linux、alibaba cloud Linux)、信舱中	可广泛应用于公有云、私有云和混合云场景，在守护央企、运营商、金融和大型企业的业务环境安全中发挥着较大作用，主要目标客户群体为金融、运营商、云计算服务商、5G

序号	项目名称	预计总投资规模	本期投入金额	累计投入金额	进展或阶段性成果	拟达到目标	技术水平	具体应用前景
						全性和稳定性要求严苛”的关键信息基础设施高级云原生安全场景需求。	间件镜像的扫描检测和运行时容器安全防护；3、容器模式部署支持非特权，不再挂载主机敏感目录。	MEC 边缘云、政府、医疗、教育、中大型企业等行业客户群体。
15	大模型安全与管控	6,000.00	2,010.60	2,433.78	通过概念验证，目前处于开发阶段。	针对大模型的安全风险，提供端到端的安全防护策略，从数据清理、模型训练、微调、推理到大模型部署，线上运营监控等所有环节进行安全评估和实时监控。	提供大模型幻觉检测、训练数据投毒、提示词注入攻击、模型对抗攻击、越狱攻击、模型萃取攻击、法律法规风险等主要安全风险监测和防护能力。	应用于大模型私有化部署场景，例如金融、运营商等行业。
16	外部攻击面管理平台	6,000.00	1,197.69	1,197.69	相关产品已投入市场，目前处于测试优化阶段	打造一款基于攻击视角下的自动攻击弱点发现及轻量化渗透的平台。同时在易用性上实现一键任务下发、报告导出即交付，快速帮助防守方理解并及时收敛攻击风险，提升防御能力。	1、具备本地化部署、SaaS 两种服务方式；2、互联网资产检测覆盖 8 种线索，10000+产品指纹，具有影子资产、暴露面检测能力；3、商业泄密检测覆盖 40+网盘、文库、代码托管数据源，累计 3000+数据清洗规则，检测准确率行业内 TOP3。	广泛应用于实网攻防演练前的暴露资产摸排；多分支集团企业的日常常态化运营；监管单位对于区域/行业的内各重点企业的监督管理几个场景
17	数据安全与治理平台	5,000.00	2,293.75	2,293.75	相关产品已投入市场，	以数据安全大数据分析为支撑，以数据安全全生命周期管控为核	1、数据资产梳理支持扫描传统关系型数据库/表/数据资产，至少支持	广泛应用于运营商、金融、能源和医疗等行业客户，除单机部

序号	项目名称	预计总投资规模	本期投入金额	累计投入金额	进展或阶段性成果	拟达到目标	技术水平	具体应用前景
					目前处于测试优化阶段	心，以数据安全策略统一管控为抓手，构建集资产梳理、数据接入、分析研判、响应处置、安全可视于一体的数据安全运营平台，实现全域风险感知、自适应安全闭环。	mysql,oracle,greenplum,达梦(dm)16 种类型；2、数据资产梳理支持扫描大数据存储组件存储的数据资产，至少支持 hdfs,hive 等 6 种类型；3、数据分类分级支持基于 Aho-Corasick 自动机实现的多模式字典匹配算法，实现高效的字典匹配识别能力；4、数据安全告警支持从文件、账号、API 等 10+个视角展示、查询多种筛选条件的组合，如时间、告警状态等 100+种告警项。	署，DSOP 还支持集群化部署，横向提供产品采集、分析等能力，满足大规模分析的场景。
18	身份安全管理与认证系统	6,000.00	2,979.77	2,979.77	相关产品已投入市场，目前处于测试优化阶段	基于大模型、云化、插件化技术的用户身份管理系统拟实现以下目标：基于先进 AI 大模型技术，实现身份行为智能分析和全方位审计，显著提升安全性，同时减少人工介入工作量达 30%以上。打造全面云原生的身份	基于最新的大模型技术，融合先进的机器学习和深度学习算法，构建精准的用户行为模型和多维用户画像。通过自然语言处理和理解能力，实现智能化的攻击检测（支持 Shell、Python、SQL 脚本等 6 大类型脚本检测，支持 11 类 70 多种场景的攻击风险发现）、操作风险（支	在运营商、政府和头部企业等行业落地以下场景：智能身份管理：灵活配置多因素认证策略，提升安全性。零代码开发降低成本，优化用户体验。AI 驱动的风险检测和安全审计：利用大模型实现智能检

序号	项目名称	预计总投资规模	本期投入金额	累计投入金额	进展或阶段性成果	拟达到目标	技术水平	具体应用前景
						服务平台，实现跨云环境的无缝适配，支持一键式自动化部署和智能动态伸缩，大幅提升系统弹性和可靠性。采用创新的插件化架构，实现认证能力、金库管理、运维网关、应用网关等核心功能的即插即用，极大提升系统灵活性和可扩展性。	持业务应用类 7 种场景和运维类 17 种协议、3 种工具发布形态下的各类场景的操作风险）预警和业务审计，将安全防护提升到前所未有的高度；采用前沿的微服务架构和云原生技术，实现全容器化部署。通过智能调度和资源优化算法，确保系统能够根据业务负载实时自动扩缩容，保障服务质量的同时最大化资源利用效率。支持国产操作系统和数据库、国产浏览器种类超过 30 种；创新性地采用插件化设计理念，实现多样化认证方式（包括但不限于密码、生物识别、硬件令牌等 14 种认证方式）、金库模块、各类网关（协议堡垒、图形堡垒、H5、透明、Web 应用等 12 类业务模块）的灵活组合和无缝适配。这种高度模块化的架构	测、行为分析和自动化审计，提高效率和安全管控。全场景自动化服务：提供可自由组合的服务模块，增强业务适应能力，降低研发和实施成本。全面适配：兼容国产化环境和主流云平台，支持多样化 IT 基础设施，助力企业数字化转型。

序号	项目名称	预计总投资规模	本期投入金额	累计投入金额	进展或阶段性成果	拟达到目标	技术水平	具体应用前景
							确保系统能够快速响应不同业务系统的独特需求。	
19	终端安全立体化防护平台	3,000.00	1,224.86	1,224.86	相关产品已投入市场，目前处于测试优化阶段	1、基于终端安全，融合身份安全，业务安全，数据安全，构建立体化防御体系；2、基于身份的安全管理体系，构建基于身份的从终端、访问控制、数据安全的安全策略管理中心；3、平台化管理，基于平台，统一管理防病毒、EDR、运维管控、零信任、准入、DLP、数据沙箱等不同组件；4、统一客户端，融合各个功能模块、形成简单易用的融合终端。	融合 CTEM 技术、零信任技术、数据沙箱技术，通过精密编排各个功能组件，层层收敛，有效降低威胁可以入侵的暴露面。未知资产探测可识别 28 种设备类型，同时能够识别计算机名称、操作系统、供应商信息。Windows 办公场景下 100%探测精准度，能够准确探测出 windows 设备的计算机名、操作系统、设备类型。在威胁防御方面，通过防病毒和 EDR 结合，基于行文分析引擎、机器学习引擎、Att&CK 检测技术、关联分析算法，可以精准发现已知和未知威胁，帮助企业有效抵御勒索攻击和银狐木马攻击。病毒防护特征库已累积 10 亿量级，PE 类检测率达 98.6%。攻击行为检测规则数量	广泛用于对安全有较高要求的金融、高端制造和关键基础设施等行业，为用户提供终端安全勒索防护深度治理整体性解决方案。

序号	项目名称	预计总投资规模	本期投入金额	累计投入金额	进展或阶段性成果	拟达到目标	技术水平	具体应用前景
							1000 条以上，技术点覆盖度达 70%。精准检测银狐木马，防病毒检测率达 94.9%，行为规则 100%覆盖银狐攻击常用攻击手法。通过终端各类风险感知技术和零信任动态评估技术结合，进一步帮助企业提升威胁防御的效果。在数据安全方面，Tr 通过 DLP 技术、数据沙箱技术，叠加零信任技术，建立安全业务空间，有效避免数据泄露。	
合计		**85,000**	**18,829.40**	**61,557.74**	-	-	-	-

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）实际募集资金金额、资金到位时间

根据中国证券监督管理委员会于 2022 年 1 月 5 日出具的《关于同意亚信安全科技股份有限公司首次公开发行股票注册的批复》（证监许可[2022]7 号），公司启动发行工作，向社会首次公开发行人民币普通股（A 股）股票 4,001 万股，每股发行价格为人民币 30.51 元，募集资金总额为人民币 1,220,705,100.00 元，扣除发行费用人民币 98,199,233.77 元（不含增值税金额）后，实际募集资金净额为人民币 1,122,505,866.23 元,上述募集资金已经全部到位。致同会计师事务所（特殊普通合伙）对本次公开发行新股的募集资金到位情况进行了审验，并于 2022 年 1 月 28 日出具了《验资报告》（致同验字（2022）第 110C000069 号）。

（二）2024年半年度募集资金使用及结余情况

募集资金到位后至 2024 年 6 月 30 日，公司募集资金使用情况为：以募集资金支付其他发行费用（不含税金额，不包括承销保荐费）2,495.69 万元、以募集资金直接投入募集资金投资项目（以下简称“募投项目”）104,663.96 万元，收到专户理财收益 3,059.06 万元，收到专户利息收入 793.35 万元，扣除专户手续费 1.59 万元。公司募集资金的具体使用情况如下：

项目	金额（万元）
募集资金总额	**122,070.51**
减：已累计投入募集资金总额	**114,483.88**
其中：以前年度投入募集资金用于支付承销费、保荐费（不含税金额）	7,324.23
以前年度投入募集资金用于支付其他发行费用（不含税金额）	2,495.69
本期投入募集资金用于支付其他发行费用（不含税金额）	-
募投项目支出	**104,663.96**
其中：以前年度募投项目支出	89,559.25

本期募投项目支出	15,104.70
加：利息收入	**793.35**
其中：以前年度利息收入	785.98
本期利息收入	7.37
加：理财收益	**3,059.06**
其中：以前年度理财收益	2,893.51
本期理财收益	165.55
减：手续费支出	**1.59**
其中：以前年度手续费支出	1.48
本期手续费支出	0.11
减：募集资金结项永久补充流动资金	**-**
募集资金余额	**11,437.45**
其中：募集资金账户余额	**3,602.23**
暂时闲置资金进行现金管理投资余额	**7,835.23**
其中：结构性存款	7,800.00
协定存款	35.23

截至 2024 年 6 月 30 日，公司尚未使用的募集资金余额为 11,437.45 万元（包括累计收到的银行存款利息、理财收益扣除银行手续费），其中用于现金管理 7,835.23 万元，募集资金账户余额为 3,602.23 万元。

（三）募集资金的管理情况

公司2024年上半年募集资金的存放与使用符合《证券发行上市保荐业务管理办法》《上海证券交易所科创板股票上市规则》《上市公司监管指引第2号——上市公司募集资金管理和使用的监管要求》《上海证券交易所科创板上市公司自律监管指引第1号——规范运作》等有关规定及公司募集资金管理制度，对募集资金进行了专户存放和使用，并及时履行了相关信息披露义务，募集资金具体使用情况与公司已披露情况一致，截至2024年6月30日，公司不存在变相改变募集资金用途和损害股东利益的情形，不存在违规使用募集资金的情形。

（四）募集资金专户存储情况

公司对募集资金采取专户储存制度，并与保荐机构、存放募集资金的开户银行签订了募集资金监管协议。截至2024年6月30日，募集资金具体存放情况如下：

单位：万元

公司名称	开户银行	银行账号	余额
亚信安全科技股份有限公司	招商银行股份有限公司南京鼓楼支行	125905906410555	0.00
亚信安全科技股份有限公司	中国工商银行股份有限公司北京长安支行	0200048519200863155	0.00
亚信安全科技股份有限公司	平安银行股份有限公司南京分行	15202201070177	0.24
亚信安全科技股份有限公司	南京银行股份有限公司南京分行	142290000002318	0.08
亚信科技（成都）有限公司	招商银行股份有限公司南京鼓楼支行	010900157010111	129.18
亚信科技（成都）有限公司	中国工商银行股份有限公司北京长安支行	0200048519200864181	28.59
亚信科技（成都）有限公司	南京银行股份有限公司南京分行	0187250000001743	3,443.53
南京亚信信息安全技术有限公司	南京银行股份有限公司南京分行	0187270000001742	0.60
募集资金账户余额			**3,602.23**
亚信安全科技股份有限公司	民生银行股份有限公司北京分行	633902478	-
亚信科技（成都）有限公司	民生银行股份有限公司北京分行	635590959	35.23
协定存款			**35.23**
合计			**3,637.45**

十、控股股东、实际控制人、董事、监事和高级管理人员的持股、质押、冻结及减持情况

（一）直接持股情况

报告期内，公司控股股东、实际控制人、董事、监事和高级管理人员直接持有公司股份情况如下表所示：

姓名/名称	类型	直接持股数量（万股）
田溯宁	实际控制人	58.65
亚信信远（南京）企业管理有限公司	控股股东	8,094.85
南京亚信融信企业管理中心（有限合伙）	控股股东一致行动人	6,201.36

天津亚信信合经济信息咨询有限公司	控股股东一致行动人	3,065.66
北京亚信融创咨询中心（有限合伙）	控股股东一致行动人	1,107.31
天津亚信恒信咨询服务合伙企业（有限合伙）	控股股东一致行动人	621.04

截至2024年6月30日，公司董事、监事和高级管理人员均未直接持有公司股票。

（二）间接持股情况

公司实际控制人、董事、监事、高级管理人员通过员工持股平台的间接持股情况如下：

姓名	与公司关系	报告期末持股数量（万股）
田溯宁	实际控制人	20,525.57
何政	董事长	1,164.37
陆光明	副董事长	220.39
马红军	董事、总经理	225.58
刘东红	董事、副总经理	299.51
胡婷	监事	20.65
吴湘宁	副总经理	129.36
张安清	副总经理	34.99
郭昊昊	副总经理	25.96
汤虚谷	财务总监	50.74

注 1：实际控制人田溯宁先生通过控股股东亚信信远及其一致行动人亚信融信、亚信信合、亚信融创、亚信恒信，以及亚信信安、亚信融安、亚信安宸、亚信铭安、亚信安宇、亚信信智、亚信乐信、亚信信宁、亚信信宇间接持有公司股权；2、公司实际控制人、董事、监事、高级管理人员任职为 2024 年 6 月末任职情况。

2024 年上半年，公司实际控制人田溯宁通过受让离职员工持有的员工持股平台份额的方式对公司股份进行了间接增持。除上述情况外，公司控股股东、董事、监事和高级管理人员持股情况未发生变动。

十一、上海证券交易所或保荐机构认为应当发表意见的其他事项

无。

（以下无正文）

（本页无正文，为《中国国际金融股份有限公司关于亚信安全科技股份有限公司2024年半年度持续督导跟踪报告》之签章页）

保荐代表人：

江涛　　徐石晏

中国国际金融股份有限公司

2024年9月6日