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
2023 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	2023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	2023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的业	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、部门规章和上

	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	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	2023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	2023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的，应及时向上海证券交易所报告	2023年上半年，上市公司未出现该等事项
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；	2023年上半年，上市公司及相关主体未出现该等事项

	（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	
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	2023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）业绩亏损的风险

2023 年上半年，公司实现营业收入 5.63 亿元，较去年同期降低 5.01%，主要系云网虚拟化基础软件业务收入下滑导致公司营收规模整体下降，公司其他业务条线收入均保持增长。2023 年上半年，公司整体毛利率有所上升，从去年同期的 49.25%升至 55.81%；销售费用较去年同期降低 0.80%，研发费用较去年同期增加 24.43%。2023 年上半年，公司实现归属于母公司所有者的净利润-1.71 亿元，较去年同期基本持平；归属于母公司所有者的扣除非经常性损益后的净利润-1.92 亿元，较去年同期相比亏损有所收窄。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、网络安全政

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，公司可能面临全年业绩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。

3、因最终客户发生数据泄密及其他网络安全事件时，公司承担罚款或被最终客户追责的风险

发行人作为网络产品、服务的提供者，在生产经营过程中应确保其提供的网络产品、服务符合相关标准并持续提供安全维护，在规定或者当事人约定的期限内，不得终止提供安全维护；在发现其网络产品、服务存在安全缺陷、漏洞等风险时应立即采取补救措施并履行相关告知和报告义务，涉及收集用户信息的应取得用户的同意并遵守个人信息保护的相关规定，如发行人无法履行该等义务，则有面临被有关主管部门责令改正、给予警告、没收违法所得或罚款等风险。

此外，当最终客户发生数据泄密及其他网络安全事件时，如主管部门认定公司在提供相应产品或服务时违反了国家与网络安全和信息安全相关的法律法规，公司可能承担相应的法律责任，并可能需根据销售合同的约定向客户承担相应的赔偿责任，从而给公司的经营带来一定风险。

（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。2023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1,276.66万元，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

网络安全行业过去一直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。但是网络安全行业本质上是一个伴生的行业，与IT的整体发展紧密相关，受IT投入的影响比较大。随着网络安全的渗透率日益提高，长期来讲，面临着行业增长动能减缓的情况。同时，受企业网络安全投入预算的影响，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。

（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

2023 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

2023 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	56,322.47	59,291.54	-5.01%
归属于上市公司股东的净利润	-17,135.39	-17,060.25	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	-19,208.46	-19,681.78	不适用
经营活动产生的现金流量净额	-39,642.24	-35,894.80	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	233,536.59	264,602.17	-11.74%
总资产	326,632.82	368,153.10	-11.28%

2023 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）	-0.4284	-0.4412	2.90%
稀释每股收益（元／股）	-	-	-
扣除非经常性损益后的基本每股收益	-0.4802	-0.5250	8.53%

（元 / 股）			
加权平均净资产收益率（%）	-6.64	-12.28	增加 6.54 个百分点
扣除非经常性损益后的加权平均净资产收益率（%）	-7.44	-14.62	增加 7.18 个百分点
研发投入占营业收入的比例（%）	37.15	28.36	增加 8.79 个百分点

1、2023 年上半年，公司营业收入下降 5.01%，主要系公司云网虚拟化基础软件业务收入下滑所致。公司云网虚拟化软件业务主要为响应客户项目中的需求而开展，上半年客户需求有所下滑，导致公司营业收入整体下滑。除云网虚拟化软件业务外，公司端点安全产品、数字信任与身份安全产品、云网边安全产品构成的安全产品体系同比增长 4.89%，安全服务业务同比增长 113.74%，网络安全产品与网络安全服务合计同比增长 8.20%。

2、2023 年上半年，公司销售费用较去年同期降低 0.80%，研发费用较去年同期增加 24.43%，管理费用较去年同期增加 7.69%，三项费用合计增加 4,512.24 万元。公司实现归属于母公司所有者的净利润-1.71 亿元，较去年同期基本持平；归属于母公司所有者的扣除非经常性损益后的净利润-1.92 亿元，较去年同期相比亏损有所收窄。

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，已掌握了终端安全、身份安全、云安全、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，拉通全国 32 个地方和 46 个部委的用户互认体系，提供稳定的安全能力支撑。公司同时承建了国家电子政务外网安全监测平台，承担中央级政务外网数据总线的角色，对接全国 31 个省级外网平台，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，身份安全与终端安全国内领先

区别于传统的以硬件为主导的网络安全公司，公司优势产品和解决方案主要集中在网络安全软件领域。公司在中国网络安全软件市场处于领先地位，根据 2023 年 4 月、7 月 IDC 发布的研究报告，2022 年公司在身份和数字信任软件市场排名第一，在终端安全市场排名第二，在私有云云工作负载安全市场排名第三。

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。

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。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

2023 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

2023 年上半年，公司研发费用为 2.09 亿元，研发投入占营业收入的比例为 37.15%，与去年同期研发费用率 28.36%相比，增加 8.79 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	20,924.10	16,816.22	24.43%
资本化研发投入	-	-	-
研发投入合计	20,924.10	16,816.22	24.43%
研发投入总额占营业收入比例（%）	37.15	28.36	增加 8.79 个百分点
研发投入资本化的比重（%）	-	-	-

（二）研发进展

2023 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	84.20	401.77	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、目前已具备检测未知威胁的能力。2、目前检测规则已覆盖12个战术点，180种黑客攻击技术点。3、检测规则数量180+还有待增加，需覆盖ATT&CK更多战技术点。4、需要与AttackIO 云端分析引擎互动，提高检测率。	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	252.60	1,964.17	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，具备强大的对未知威胁的检测能力。	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静态文件病毒的检测与阻断。

3	怒狮网络防病毒引擎（NetStack）	3,000.00	252.60	1,944.21	相关产品已进入市场，稳定开发优化阶段。	基于已有的高性能的恶意流量检测引擎，适配主流平台及国产化系统，满足产品的定制化需求，持续增强最新漏洞的检测能力，加强新型漏洞的查杀能力。	1、已知威胁覆盖全面，覆盖 5300+国内外重要漏洞，70+黑客工具，100+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，40+深度研判模块，对于多种攻击技术点深度研判。3、拥有专家队伍持续支持最新的漏洞，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	168.40	1,141.76	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”在线研判服务，构建高性能威胁指标评估引擎提供 Web 信誉、文件信誉评估能力，增强网关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通过深度学习、数据挖掘、专家规则等近百种情报研判模型为用户提供实时场景化威胁情报评估服务，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情报评估有机融合在产品的威胁检测能力极大提升的同时,也保证了高检测性能，适用于运营商、金融等多种行业和场景。	云端具备海量的威胁情报（文件、网址、IP）数据，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核心安全数据服务能力，从而使各个接入云端的产品具备业界一流的安全检测能力。

5	亚信安全威胁数据湖（AIS-TIDL）	3,000.00	715.71	1,270.41	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	漏洞防护技术优化项目	2,000.00	168.40	1,885.89	相关产品已投入市场，目前处于测试优化阶段。	1、优化深度包检测技术，实现基于主机的过滤器来检测和清理网络流量，在不中断应用程序和业务运营的情况下，更高效地修正或阻止有可能会攻击漏洞的应用程序网络流量。3、优化嵌套层过滤技术，通过相关接口建立嵌套层，对所有虚机流量进行过滤，从而实现漏洞防护的作用。4、优化网络报文过滤技术，实现针对非法流量报文的阻断或丢弃。	1、具备根据漏洞被利用的方式建立的漏洞特征识别规则（虚拟补丁）的能力。2、防护规则支持 ATT&CK 网络攻击技战术框架模型。3、漏洞特征识别规则库涵盖 100 多种应用程序，规则库数量超过 2 万条以上规则。4、支持预先漏洞扫描；5、支持对操作系统、应用程序、文件系统等的预先漏洞扫描。6、支持回退机制。7、防堵已知漏洞及零日攻击。8、支持在十	可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，为用户提供老旧操作系统的虚拟补丁防护方案。

							分钟内将防御策略部署至上千个的虚拟化服务器。	
7	一体化终端安全平台研发	4,000.00	1,605.77	4,030.72	相关产品已投入市场，目前处于测试优化阶段。	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。	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。	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平台化和整体性解决方案。
8	高级威胁发现与分析平台研发	6,000.00	994.46	4,293.30	相关产品已投入市场，目前处于测试优化阶段	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。	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。

9	XDR 威胁感知运维中心	3,000.00	710.33	2,301.33	开发阶段	1、以身份、零信任为脉络，云、网、端、边、邮为触点，平台为基座，构建一个全栈联动的检测响应平台，应对现代网络威胁日益严峻零日漏洞利用、社会工程欺骗、供应链攻击。2、加强产品组件化、能力原子化，彻底解决多产品的配置管理、安全运营、安全可视问题，持续推进“一体化”安全解决方案，更好应对现代网络威胁挑战和企业的数字化转型。	构建了新型 XDR 勒索防护体系，基于全栈产品线的检测能力及底层数据，结合强大的本地威胁情报能力，提供全新的勒索感知、认知、治愈场景，有效保障企业安全，铸牢防护边界，开启了“平台+产品+服务”，勒索全面治理的新纪元。2、打通安全运营服务通道，实现一键开启远程安全运营服务，解决客户缺乏安全运营专家、内部失陷无法提前发现、可疑威胁难以厘定等安全运营难题。	XDR 威胁感知运维中心可对亚信安全产品的数据进行多维度分析，统一运维平台适用于多种安全运维管理场景，帮助企业打造全网安全感知、洞见、可控。用户可以通过平台一键接入安全服务专家，实现平台内所有产品远程托管运营，数据不上云的同时又可享受 7*24 无忧托管，通过提供优质产品与服务不断创造新价值。
10	服务器深度安全防护系统	5,000.00	1,244.15	4,624.75	相关产品已进入市场，稳定开发优化阶段。	新增信创防病毒支持、容器安全和自定义客户端资源使用率，并着重优化了策略集合和安装的易用性。	提供混合云、私有云、公有云及物理服务器、虚拟化服务、容器等工作负载的安全防护，一方面可通过虚拟化底层的安全接口，无须在虚拟机上部署客户端；另一方面可通过在物理服务器操作系统中安装轻量级客户端的方式，保护服务器的安全。	支持混合云场景，可为使用行业云、私有云、容器等解决方案的金融、能源、政府等行业，提供专业的轻量级的云主机安全防护能力。

11	统一帐号认证授权平台	5,000.00	315.15	3,814.86	相关产品已投入市场，目前处于测试优化阶段	推动统一帐号认证授权平台的持续演进，满足用户业务集中化模式的安全管理能力演进，支持省公司和集团公司之间的两级安全联动，并能访问集团集中化资源池的资源和全网一级应用。	1、采用先进的微服务架构，适应各类云环境的部署实施，实现服务节点自动伸缩，以及中台的集群、双中心、容灾能力，有效保障业务的健壮性；通过可视化的界面管理，实现个性化需求无代码的快速编排，快速响应客户需求，无需停止服务。2、支持灰度发布等业界先进技术。支持国产化硬件与操作系统、中间件、数据库、终端、浏览器。在用户操作过程中进行实时动态信任评估，实现从人到端点到网关、到应用到设备的零信任安全管控。处于业界先进水平，IDC 市场占有率持续排名第一。	面向广泛资源接入，将新增的主机、数据库、智慧中台组件等新型资源纳入 4A 平台；基于 4A 中的帐号、授权信息与零信任网络访问控制网关 SDP 结合，初步实现基于零信任的基础网络控制能力。
12	DNS 域名解析产品研发	5,000.00	94.87	1,539.77	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 3000 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	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。

							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、对国产操作系统龙蜥、欧拉、CTyunOS 的兼容，持续提升国产化适配能力。	
13	安全运营及态势感知平台	8,000.00	1,103.24	5,764.57	相关产品已投入市场，目前处于测试优化阶段	1、新增和优化功能，提升系统易用性，安全性、健壮性和可维护性；2、新增报表，简化用户配置；优化资产管理，提升易用性及资产类型涵盖面，同时接入资产数据；3、新增消息中心，即时向用户提供安全信息，提醒用户处理安全问题；优化数据分析能力，提升数据分析准确性及性能；4、优化日志接入，提高数据处理能力。	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、支持超过 43 类 370 多种各类智能关联分析规则与场景；3、已完成 120 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、初步具备画布编排展示能力，支持自定义大屏展示；5、持续提升系统易用性，安全性、健壮性和可维护性。	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。
14	零信任产品研发	4,000.00	348.79	2,249.24	相关产品已进入市场，稳定开发优化阶段。	以 SDP 为关键组件，以 AI 智能可信身份分析引擎为大脑，形成亚信安全的零信任架构体系，拉通态势、端点产品、威胁	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功能模块，实	满足企业远程接入，内外网准入，与终端结合部署零信任安全解决方案等应用场景

						引擎，形成基于身份安全为基础设施，对“云、网、端”全域全流程的安全的业务访问，动态的访问控制，持续的信任度量的零信任身份安全。	现无边界网络访问控制能力、无边界应用访问控制能力、身份可信识别能力、持续信任评估能力和安全能力可视化。	
15	运维安全管理与审计系统	3,000.00	30.62	1,445.93	相关产品已进入市场，稳定开发优化阶段。	升级现有产品的 UI 和交互、技术架构和安全能力，增加联动登录能力，扩充平台客户端兼容性。	提供运维用户全生命周期管理，自定义多因素认证方式，访问控制细粒度授权与命令控制、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，内置系统自身安全防护能力，集成文件防病毒引擎，提供防病毒安全网盘，业界独有的主机防绕行能力，解决主机绕行登录问题。	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、混合云安全管理等应用场景
16	网络威胁入侵防护系统	1,000.00	740.46	1,842.37	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	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 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。	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。

						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。		
17	信舱共享免疫 Saas 系统	4,000	563.96	1,192.20	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。	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；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，结合 7*24 SOC 服务帮助用户检测到高级威胁的入侵。	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。
合计		**62,000.00**	**9,393.71**	**41,707.25**	-	-	-	-

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）2023年半年度募集资金使用及结余情况

募集资金到位后至 2023 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）2,290.69 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”）70,883.47 万元，收到专户理财收益 2,207.26 万元，收到专户利息收入 753.81 万元，扣除专户手续费 1.12 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	**80,498.40**
上期投入募集资金用于支付承销费、保荐费（不含税金额）	7,324.23
上期投入募集资金用于支付其他发行费用（不含税金额）	2,290.69
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	**70,883.47**
其中：上期募投项目支出	33,098.22
本期募投项目支出	37,785.25

加：利息收入	**753.81**
其中：以前年度利息收入	563.64
本年度利息收入	190.17
加：理财收益	**2,207.26**
其中：以前年度理财收益	1,697.79
本年度理财收益	509.48
减：手续费支出	**1.12**
其中：以前年度手续费支出	0.94
本年度手续费支出	0.18
减：募集资金结项永久补充流动资金	**-**
募集资金余额	**44,532.07**
其中：募集资金账户余额	670.42
暂时闲置资金进行现金管理投资余额	43,861.65
其中：结构性存款	37,600.00
协定存款	6,261.65

截至 2023 年 6 月 30 日，公司尚未使用的募集资金余额为 44,532.07 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 43,861.65 万元，募集资金账户余额为 670.42 万元。

（三）募集资金的管理情况

公司2023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2023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2023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	121.16
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	6.13
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	16.02
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	63.48
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	129.00
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	67.58
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	266.44
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
合计			**670.42**

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（股）
田溯宁	实际控制人	586,492
亚信信远（南京）企业管理有限公司	控股股东	80,948,488
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	62,013,649
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	30,656,621
北京亚信融创咨询中心（有限合伙）	控股股东一致行动人	11,073,117
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	6,210,362

截至2023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	20,418.94
何政	董事长	1,164.37
陆光明	董事、总经理	220.39
蒋健	董事	839.72
童宁	董事	81.18
刘东红	董事	299.51
吴小霞	监事	3.38
马红军	副总经理	225.58
刘政平	副总经理	64.58
吴湘宁	副总经理	129.36
邹明达	副总经理	99.17
李伦文	副总经理	102.60
庄学阳	副总经理	70.34
张安清	副总经理	32.72
汤虚谷	财务总监	50.74
郑京	董事会秘书	101.48

注 1：实际控制人田溯宁先生通过亚信信远、亚信融信、亚信信合、亚信融创、亚信恒信、亚信信安、亚信融安、亚信安宸、亚信铭安、亚信安宇间接持有公司股权。

2023 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；公司新任副总经理张安清通过间接取得员工持股平台份额的方式进行了间接增持。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2023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

2023 年 8 月 30 日