国泰君安证券股份有限公司

关于杭州安恒信息技术股份有限公司

2022年半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》、《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持续督导工作指引》等有关法律、法规的规定，国泰君安证券股份有限公司（以下简称“国泰君安”或“保荐机构”）作为杭州安恒信息技术股份有限公司（以下简称“安恒信息”、“上市公司”或“公司”）持续督导工作的保荐机构，负责安恒信息上市后的持续督导工作，并出具本持续督导跟踪报告。

一、持续督导工作情况

序号	工作内容	持续督导情况
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了持续督导制度，并制定了相应的工作计划
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	保荐机构已与公司签订《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，并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、现场检查等方式，了解公司业务情况，对公司开展了持续督导工作
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	2022年半年度公司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	2022 年半年度公司在持续督导期间未发生构成违法违规或违背承诺的事项
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务规则及其他	在持续督导期间，保荐机构督导公司及其董事、监事、高级管理人员

序号	工作内容	持续督导情况
	规范性文件，并切实履行其所做出的各项承诺	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	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	保荐机构已督促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	保荐机构对公司内控制度的设计、实施和有效性进行了核查，公司的内控制度符合相关法规要求并得到了有效执行
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	保荐机构对公司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	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	2022 年半年度，公司及其控股股东、实际控制人、董事、监事、高级管理人员未发生该等事项
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	2022年半年度，公司及其控股股东、实际控制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与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	2022 年半年度，经保荐机构核查，不存在应及时向上海证券交易所报告的情况
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	2022 年半年度，公司不存在前述情况

序号	工作内容	持续督导情况
	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	制定对上市公司的现场检查工作计划，明确现场检查工作要求，确保现场检查工作质量	保荐机构已制定了现场检查的相关工作计划，并明确了现场检查工作要求
16	上市公司出现下列情形之一的，保荐机构、保荐代表人应当自知道或者应当知道之日起15日内进行专项现场核查：（一）存在重大财务造假嫌疑；（二）控股股东、实际控制人、董事、监事或者高级管理人员涉嫌侵占上市公司利益；（三）可能存在重大违规担保；（四）资金往来或者现金流存在重大异常；（五）上海证券交易所或者保荐机构认为应当进行现场核查的其他事项。	2022 年半年度，公司不存在前述情形

二、保荐机构和保荐代表人发现的问题及整改情况

无。

三、重大风险事项

在本持续督导期间，公司目前面临的主要风险因素如下：

（一）业绩亏损且大幅下滑的风险

公司归属于母公司所有者的净利润、归属于母公司所有者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变动幅度较大，主要系：软件企业员工工资性支出等成本所占比重较高，本期公司员工人数大幅增加及员工平均薪酬增加，薪酬在年度内较为均匀的发生。且由于公司处于快速发展阶段，上述工资性支出等成本增长较快，导致季节性亏损加大；公司实施了2020年、2021年、2022年限制性股票激励计划，本期股份支付费用较上年有所增长；公司上年同期非经常性损益影响较大主要是由于上年同期非同一控制下企业合并原参股公司形成投资收益，而本期并未发生前述事项。

（二）核心竞争力风险

1、技术更新迭代风险

公司的核心技术主要应用于网络信息安全行业。随着新一代信息技术的高速发展，网络信息安全领域的技术也处于快速成长期，若公司不能准确及时地预测

和把握网络信息安全技术的发展趋势，持续保持技术领先优势，将可能面临被竞争对手赶超或者核心技术发展停滞甚至被替代的风险。

2、技术研发失败风险

网络信息安全行业是技术密集型行业，为保持市场领先优势，提升技术实力和核心竞争力，公司需要不断进行新技术创新、新产品研发，以应对终端客户日益增长的多样化需求。近年来公司一直保持较高的研发投入，发生的研发费用直接影响公司当年的净利润水平。由于对未来市场发展趋势的预测存在一定不确定性，公司可能面临新技术、新产品研发失败的风险，从而对公司经营业绩和持续经营带来不利的影响。

3、核心技术人员流失风险

随着行业竞争日趋激烈，企业对人才的竞争不断加剧。维持技术人员队伍的稳定，并不断吸引优秀技术人员加盟，关系到公司能否继续保持技术竞争优势和未来发展的潜力。如果公司核心技术人员大量流失，将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。

（三）经营风险

1、新市场开拓风险

目前公司客户群体主要集中在政府（含公安）、金融机构、教育机构、电信运营商等单位，公司也正在加大营销网络建设方面的投入，建立多级销售渠道，以不断拓展中小企业客户，同时服务现有客户软件升级和新增业务的需要。但若公司的新行业拓展策略、营销服务等不能很好的适应客户需求，公司将面临新市场开拓风险。

2、经营业绩季节性波动引起股价波动的风险

受政府部门和大型企事业的采购周期影响，该部分用户大多在上半年对全年的投资和采购进行规划，下半年再进行项目招标、项目验收和项目结算，导致公司近年来的营业收入呈现出上半年较低，而下半年较高的季节性特征。同时，由于公司员工工资性支出、固定资产摊销等成本所占比重较高，造成公司净利润的

季节性波动比营业收入的季节性波动更为明显。因此，公司经营业绩存在季节性波动引起股价波动的风险。

3、因最终客户发生数据泄密及其他网络安全事件时，公司承担罚款或赔偿的风险

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、股权激励导致股份支付金额持续较大的风险。

公司计划通过股权激励吸引并留住核心人才，未来新增对员工的股权激励有可能导致股份支付金额较大，从而对当期及未来财务情况造成不利影响。

2、税收优惠风险

报告期内，公司享受高新技术企业所得税的税收优惠和研发费用加计扣除。如果中国有关税收优惠的法律、法规、政策等发生重大调整，或者由于公司未来不能持续取得中国高新技术企业资格或不满足研发费用加计扣除的条件等，将对公司的经营业绩造成一定影响。

（五）行业风险

随着网络信息安全行业的发展，不同细分领域的技术将会融合、协同，不同细分市场客户的需求将会交叉、重叠，不同细分行业的领先者将展开直接竞争，行业的发展对公司提供整体解决方案的能力将提出更高的要求，公司与行业内具有技术、品牌、人才和资金优势的厂商之间的竞争可能进一步加剧，行业整体竞争加剧可能影响行业总体毛利率，从而导致公司毛利率存在下降的风险。

（六）宏观环境风险

政府一直对高新技术企业进行鼓励和扶持，公司享受的税收优惠均与公司日常经营相关，具有一定的稳定性和持续性。如果公司未来不能持续保持较强

的盈利能力或者国家税收政策和相关扶持政策发生变化，则可能对公司发展产生一定的影响。另外，公司面向的企业级客户一般采取预算制，且部分行业客户的投资来自于财政拨款，宏观经济环境如出现不景气可能影响部分行业客户的IT投资预算，进而可能对公司的业务产生不利影响。

（七）新冠疫情风险

全球新冠疫情难以平息，防疫抗疫对经济发展产生直接的影响，公司将密切关注疫情变化，及时作出应对措施。如果疫情导致国内外经济或经营环境变差，将对公司业务产生不利影响。

除上述因素外，公司不存在其他重大风险事项。

四、重大违规事项

2022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

2022年上半年，公司主要财务数据如下所示：

单位：万元

主要会计数据	本报告期	上年同期	增减变动幅度
营业收入	53,462.45	46,175.66	15.78%
归属于上市公司股东的净利润	-37,153.76	-17,469.15	-112.68%
归属于上市公司股东的扣除非经常性损益的净利润	-38,428.44	-25,282.04	-52.00%
经营活动产生的现金流量净额	-51,540.74	-34,577.12	-49.06%
主要会计数据	**本报告期末**	**上年度末**	**增减变动幅度**
归属于上市公司股东的净资产	273,443.61	309,146.58	-11.55%
总资产	438,686.81	485,176.65	-9.58%

2022年上半年，公司主要财务指标如下所示：

主要财务指标	本报告期	上年同期	增减变动幅度
基本每股收益（元/股）	-4.73	-2.36	-100.42%
稀释每股收益（元/股）	-4.73	-2.34	-102.14%
扣除非经常性损益后的基本每股收益（元/股）	-4.90	-3.41	-43.70%

主要财务指标	本报告期	上年同期	增减变动幅度
加权平均净资产收益率	-12.78	-10.61	减少 2.17 个百分点
扣除非经常性损益后的加权平均净资产收益率	-13.22	-15.35	增加 2.13 个百分点
研发投入占营业收入的比例	57.49	47.12	增加 10.36 个百分点

上述主要财务数据及指标的变动原因如下：

1、公司归属于母公司所有者的净利润、归属于母公司所有者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变动幅度较大，主要系：（1）公司所处网络信息安全行业存在明显的季节性特征，下半年（特别是第四季度）营业收入较高，而作为软件企业员工工资性支出等成本所占比重较高，在年度内较为均匀的发生，且由于公司处于快速发展阶段，上述工资性支出等成本增长较快，导致季节性亏损加大；（2）公司实施了2020年、2021年、2022年限制性股票激励计划，本期确认股份支付费用为7,079.91万元，比上年同期增长60.50%；（3）公司上年同期非经常性损益影响较大主要是由于上年同期非同一控制下企业合并原参股公司形成投资收益7041.19万元，而本期并未发生前述事项。

2、经营活动产生的现金流量净额较上年同期变动幅度较大主要系本期支付职工薪酬增加所致。

六、核心竞争力的变化情况

凭借优秀的技术研发团队及强大的技术创新能力，公司在Web应用安全、数据库审计、态势感知、云安全及大数据安全等领域实现了多项技术突破。截至报告期末，公司共拥有48项核心技术，其中22项是公司基于云安全、大数据安全、物联网安全和智慧城市安全等新兴安全领域进行深入研发积累所得，该等核心技术确保了公司在多个相关细分市场处于行业领先位置。公司现有核心技术按照技术应用方向主要可以分为13项大类技术，该等核心技术先进性及产业应用情况具体如下：

1、全网资产测绘技术

该技术旨在探测全球联网资产信息及脆弱性，提供安全感知、威胁预警以及

风险检测能力。该技术结合大数据处理算法能实现高并发、低时延、全网覆盖、快速迭代的网络信息数据收集，并发探测速度达到60万每秒，能够识别分析20万种设备及300多种协议，在2小时内可完成全网探测。相比传统网络扫描技术，公司全网资产测绘技术采用大数据群集架构、插件化开发方式，具备更好的兼容及探测性能。该技术迭代紧跟新协议的应用、新安全漏洞发现频率，与全网资产及前沿技术产品紧密相关，需要对全网资产通讯协议及设备指纹进行长期持续的分析和数据积累，以覆盖大量通讯协议及IP数据，技术门槛较高。目前国际范围内同类技术主要有Shodan和Zoomeye，公司该项技术在识别指纹量、并发的探测速度方面有较大优势，处于国际领先水平。

该技术是目前新兴的全球联网设备探测技术，未来主要向支持所有已知工控协议、物联网协议、网络通信协议的资产探测发展，并不断积累指数级别增长的全网实时数据，从而提升实时威胁预警、全网态势感知、精确脆弱性分布探测能力。

2、多协议解析与数据治理技术

目前业界传统的数据解析与治理手段，主要基于静态的协议解析规则进行匹配，难以从云环境获取流量进行解析，无法实现对数据解析精准度的动态优化调整，公司该技术实现了对协议解析内容的动态跟踪，进一步反馈闭环调整提升了数据解析准确率，适用于VMware、阿里云、华为云、天翼云等90%以上国内外主流云环境，在协议解析识别广度（物理环境与云环境）、协议识别深度（协议行为特征、传输内容特征等）、协议检测精准度（数据库操作行为、邮件病毒、邮件域名、邮件附件别名等）较传统技术而言具有较大的优势。当该技术应用于数据库行为审计和邮件行为审计时，能实现对数据库操作行为数据和邮件行为数据的全方位解析，公司基于该项技术的日志审计产品和数据库审计产品均排在国内行业前列。

3、运维访问控制审计技术

该技术可实现各种传统环境、专有云、公有云平台等各类资产的运维接入，一机多用降低了企业内控建设的成本。基于该技术的深度协议代理解析引擎能够兼容支持市场上3,200多种不同品牌及版本的资产设备，相比业内通用的协议有

损还原，该技术可100%还原协议细节特性及运维操作过程，保证了审计日志的权威性，是业内领先的运维审计控制技术，公司基于该项技术的运维审计产品目前市场占比居于国内领先地位。目前该技术已经趋于成熟，迭代周期为6-9个月，技术的核心难度在协议代理兼容性、业务模型、用户运维习惯、统一认证平台、资产管理平台集成等方面的实践积累，短期内很难实现与该技术相当的功能水平，替代难度较大。

4、Web应用透明代理与深度攻击检测防护技术

该技术主要应用于透明网络环境下的各种web攻击检测，在网络接入层面兼容性强，转发性能相比于传统内核态转发技术，具有快速转发、低时延等优势，最高单机可处理10Gbps的应用层转发任务。基于该技术的用户态协议代理引擎具备实时双向数据包检测的能力，能识别包括无特征的攻击行为及0day攻击行为等在内复杂攻击行为，提升Web攻击防护准确率。

该技术大幅提升了公司Web应用安全产品的业务兼容性及数据包代理转发的性能，降低了攻击检测的误报率和漏报率，有效弥补了传统特征引擎检测技术高误报、高漏报等缺点，帮助公司WAF产品获得领先的Web攻击检测能力，使得公司成为国内WAF产品领先者。目前该技术日趋成熟，技术架构迭代周期约为6个月，攻击行为检测迭代周期1-7天。该技术需要在网络数据包快速转发、业务兼容、攻击检测算法模型方面大量实践经验积累，很难在短期内有较大的技术突破，替代难度较高。

5、基于网络流量的未知威胁及APT攻击检测技术

基于对样本的动静态分析及基因图谱分析能力，该技术能有效发现0day样本及变种木马。在动态沙箱检测恶意文件领域，该技术通过对Windows文件过滤驱动实现文件重定向等功能，使沙箱具备防虚拟机检测、防调试器检测和防钩子检测等能力，共200种防逃逸机制、近似零时间消耗的快速还原检测环境的技术及单沙箱并发检测多个样本的能力，目前单沙箱一天可检测非PE文件达4,000个，根据不同文件类型，一套沙箱系统一天可检测文件12万以上，处于业界领先位置。

该技术涉及的Windows内核层隔离模块在所有内核驱动开发中属于难度层

级高、文档资料少的领域。因Windows系统的闭源特点，部分功能开发甚至需要逆向工程技术并配合复杂的调试过程，精通该类内核开发、调试并兼具逆向工程的高端开发人才稀缺，使得该技术具备较高的准入门槛；同时该技术包含的基因图谱分析需要通过对大量恶意样本进行深入分析和归纳，并通过软件块化、片段化、归一化及数据库存储和搜索技术来制定软件基因库，由于相关的二进制分析高度专业性以及收集大量恶意样本所需的渠道与时间成本，使得该技术准入门槛很高，可替代性较低。

6、分布式漏洞发现与验证技术

相较业内同类技术，该技术具备漏洞发现率高、误报率低、对目标系统运行影响低等特点，凭借公司积累的40,000量级漏洞库实现业内领先的漏洞覆盖率。该技术通过分布式扫描方式加快了漏洞扫描速度与稳定性，扫描速度较传统技术提升30%，同时利用动态流量控制方式减少了扫描对目标系统的影响。公司安全研究院借助该项技术多次在全球首先发现包括JAVA框架Struts2的S-045、S-046等在内的重大漏洞，基于该项技术的漏洞扫描系列产品目前市场占比排名前三。

该技术的迭代频率一般与漏洞挖掘的频率和网络公开漏洞的频率保持一致，通过实时爬取网络漏洞的方式，进行每日自动更新。由于该类技术的漏洞发现率和误报率性能改良需要掌握大量渗透测试技术、网络爬虫技术、流量控制技术以及代码语言特性的分析技术，壁垒较高，可替代性低。

7、基于云架构的安全扫描与监测技术

业界的安全检测技术主要通过硬件盒子方式实现，检测能力受硬件性能限制，存在慢报及误报等问题。公司基于云架构的安全扫描与监测技术是国内首批运用SaaS模式进行安全检测的技术。该技术基于网站安全领域的安全事件监测技术，通过运用机器学习技术对全国670万ICP网站首页抽检样本进行分析、训练，能够实现文本语义准确分析识别，并结合公司威胁情报能力有效解决了孤链监测问题，丰富和扩展了黑名单库，大幅降低监测误报率并提升检测范围，能实现大容量、高并发、高准确率、高检出率的网站实时监测。该技术能做到检测数据完全自动标签化，自动化数据校验率达到90%以上，同时支持对关键漏洞和事件自动截图取证。当前监测网站数量峰值达到1,096,725个（次）/天，平均监测值约为476,880

个（次）/天。

相比较传统安全事件监测技术，公司的监测技术依托云端大数据能力处理分析海量安全事件样本，监测发现率不低于95%。目前国内掌握同类技术的企业主要有知道创宇、奇安信等，公司监测技术在发现率和准确率上有较大优势，处于领先水平。

自研的基于IOC的漏洞VPT技术，能够在海量的风险下，以资产为核心为维护提供合理的风险管理方式，解决用户遇到的风险多、杂、修复难等问题。

8、SaaS化云安全防护技术

业界的安全防护产品主要通过硬件方式，部署运维困难，防御能力受设备性能限制，检测误报率高且较难发现复杂的黑客攻击，难以对超大流量DDoS新型攻击进行防范。公司基于SaaS化云架构的安全防护技术在用户端无需部署任何软硬件，通过网络接入系统后，即可为用户提供远程实时安全防护，网络层最大清洗能力达到2.5T/sDDoS。该技术区别于传统规则检测，通过自然语言处理和人工智能深度学习算法对云端每日22.8亿次访问数据进行采样分析，支持语义语法的识别，能够大幅提高召回率，降低误报率，2021年度识别扫描IP69.4万个，每天拦截扫描攻击近1.3亿次，误报率仅为1‰，实现对入侵、篡改、数据窃取、CC、bots等多种攻击的防护，支持蜜罐技术捕获攻击流量,技术领先性受到学术认可，曾被《信息安全研究》期刊收录，是国内首批运用云端威胁情报能力进行防范的技术。

该技术利用云端每日十亿级的访问数据采样分析过程进行模型训练，可以周为单位快速迭代优化自身安全检测算法，而传统安全防护技术并不具备该等庞大的云端数据基础支持。随着时间推进，公司该项技术将进一步拉开与业界主流的传统防护技术的性能差距。

9、云平台融合对接和统一编排管理技术

目前业界云平台的API开放性、标准性较低，导致众多云安全解决方案和云安全产品难以交付、使用复杂、防护效果较差。公司是国内首批开展和云平台对接融合的安全厂商，已与华为云、浪潮云、OpenStack等3家国内主流云服务商完

成对接融合，并在此基础上研发提炼了一套云平台融合对接和统一编排管理技术。该技术可实现云管理平台、云安全管理平台、云安全产品三者的统一认证、授权、监测及管理，能够将安全产品与云平台的对接时间控制在10天左右，而行业平均对接时间在30天以上，单个安全模块的交付时间从数十分钟缩短到60秒以内。

该技术采用软件定义网络和容器化技术，相对同行业安全公司的手动编排和引流技术，实现了资产安全防护和安全流量路径的自动化编排，使得云上安全使用更加灵活简易。目前该技术能够兼容国内主流云平台，支持不同云平台的统一用户和管理，在对接效率、编排能力方面国内领先，云平台的对接成功数量，落地的实际案例也处于领先地位。公司与华为云、浪潮云融合对接的云安全解决方案，通过获得了CSA云安全联盟和公安部第三研究所的测评认证，获得了颁发的云计算产品信息安全认证证书和CSACSTR增强级证书和云计算产品信息安全认证证书（增强级），是业界首例安全厂商和云平台厂商融合对接云安全解决方案家的联合认证。

目前该技术和华为云、浪潮云版本基本保持同步更新迭代，平均迭代周期为一个季度。由于目前国内云平台标准化、开放性较低，要建立一套能够适配多云的对接方案，并提炼出标准API具有较高的技术难度。同时，云平台的融合具有较强的兼容依赖性，云平台厂商迁移成本高，因此该技术不可替代性较高，先发优势明显。未来该技术将向自动化、数据融合、接口标准化发展。同时，平台内云安全组件向轻量化发展，公司后续将探索云安全组件的全容器化，提升资源利用率和跨云平台的支持，以满足未来公有云和混合云的云安全防护需求。

目前公司已完成了云原生架构升级改造，相对同行业安全公司的NFV云安全解决方案，云安全管理平台可扩展性、可适配性、可迭代性和可维护性得到提升；18种云安全产品均由单租户应用升级改造到SaaS集群多租户应用，极大降低产品的资源成本和运维成本，安恒云系列产品在市场上的竞争力显著增强。

10、大数据深度安全检测与分析技术

传统安全检测多采用规则的方式，存在数据量小、检测手段单一、时效性差、分析结果准确度低、风险事件定位难等问题。公司在国内率先提出安全分析模型自适应理念，并在产品中实现功能化。相比业界通用的安全检测分析技术，该技

术在国内率先实现周期性异常事件检测，解决了多源异构数据的快速复杂关联分析与检索问题，并利用基于机器学习的扫描IP分类、策略自学习和优化、DGA域名快速判别等200多个安全场景识别方法，能够实现多维度、细粒度的安全事件分析与跟踪，大幅提升风险定位的准确度，同时利用自研大的数据建模框架，实现多个安全分析模型的关联和嵌套分析，可提高数值类安全告警准确度80%以上，公司基于此项技术产品已发布多个迭代版本，技术处于国内领先水平。

11、态势感知分析与挖掘技术

业内大多态势感知技术或产品仅停留在基于日志搜集统计可视化或网站漏洞扫描统计可视化阶段，以少量维度的数据采集手段，加上简单的统计排序分析手段，配以可视化页面，实现初步的态势感知功能。公司大数据态势感知分析与挖掘技术真正围绕网络安全态势感知的三要素:态势获取、态势理解和态势预测，以发掘深度威胁和隐患为目标，对能够引发网络安全态势发生变化的要素进行全面、快速、准确地捕获和基础分析。相比业内同类技术，该技术具备实时在线还原恶意样本和域名能力，通过使用内置威胁情报匹配辅助验证功能，使流量的有效识别率提升至99%以上，告警准确率达到90%以上。并为恶意样本提供沉浸式的运行环境和无感调试，大幅降低恶意样本的反调试成功率，从恶意特征匹配转变为基于样本异常行为检测技术，该技术处于国内领先水平。基于该技术的态势感知平台产品在实战中多次输出具有重要价值的网络战情报，尤其是在重大活动网络安全保障期间多次输出黑客攻击的预警和攻击的发现。威胁线索分析和网络攻击追溯能力处于领先水平，对同源黑客的追踪和匹配上准确率达到95%。

12、物联网可信互联与智能防护技术

该技术具备较强的跨平台能力和较好的可移植性，能够实现端到端的安全加密，密钥分发能力高达20000次/S，单次加密延时低于1.66ms，对终端数据传输效率几乎无影响。相比于传统网络层安全防护技术，该技术可以深入物联网终端内部进行安全防护，通过驱动级安全防护结合云端智能分析的防护能力构建完整的物联网安全防护体系，技术具有独创性。

13、面向工业控制系统安全的定量评估和全生命周期防护技术

该技术是公司围绕国内火电、核电、冶金、石化的工业安全现状，在现有安全防护技术的基础上，提出的一种被动防御与主动防御相结合的安全防护技术。针对工控系统攻击机理和系统架构与业务特征，实现了覆盖工控系统各层级、全业务流程的异常检测，以及对工控系统未知威胁的主动发现，解决了跨越信息物理空间未知威胁的检测难题。该技术在线实时测评技术框架，综合考虑了各种度量因子，突破了工控安全难以度量、评估的技术瓶颈，在安全防护体系和主动防御理念方面均具有先进性，能够深度解析超过30种私有工控协议，共提取1000种以上关键的工业控制系统网络协议功能码，相关技术正在申请国家专利，已达到国内领先水平。

综上所述，2022年上半年公司核心竞争力未发生不利变化。

七、研发支出变化及研发进展

（一）研发支出及变化情况

2022年上半年，公司研发费用为3.07亿元， 公司研发投入占营业收入的比例为57.49%，与2021年度同期研发费用率47.12%相比，增加10.37%。公司的研发投入的情况如下表所示：

单位：万元

项目	本期数	上期数	变化幅度
费用化研发投入	30,734.70	21,760.03	41.24%
资本化研发投入	-	-	不适用
研发投入合计	30,734.70	21,760.03	41.24%
研发投入总额占营业收入比例	57.49%	47.12%	增加 10.37 个百分点
研发投入资本化的比重	-	-	不适用

（二）研发进展

2022年上半年，公司主要在研项目如下：

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
1	工业互联网数据保护与信息安全关键技术研究及应用	9,000.00	5,963.53	16,031.74	项目正处于后期验收阶段	1.对工业互联网平台、工业企业进行安全漏洞威胁主动巡检以及工业互联网骨干节点的流量监测，实现工业互联网安全态势感知与数据保护； 2.为工业互联网及工业企业提供内部安全态势感知与预警服务，为政府提供重点区域、关键行业、特定企业的在线工业互联网网络威胁感知与应急服务等，实现对大规模工业互联网攻击、病毒、木马等安全事件的态势分析、综合研判、决策指挥和过程跟踪等功能，为主管部门开展风险上报、预警发布、事件响应、情况汇报等工作提供技术支撑。
2	天池云安全管理平台中台和分布式流量检测与编排系统建设	2,800.00	566.27	3,069.36	相关产品已投入市场，处于稳定开发迭代阶段。	构建一个统一管理、弹性扩容、按需分配、安全能力完善的“多云、多芯”的安全资源池，为用户提供一站式云安全综合解决方案，助力用户安全上云。
3	云安全 SaaS 管理平台项目	9,500.00	3,207.64	14,178.83	相关产品已投入市场，处于稳定开发优化阶段	1、构建行业领先的安全 SaaS 服务平台，集成实现云安全监测、防护及情报高防 DDOS。2、构建行业领先的托管式安全运营平台，集成安全设备托管、安全服务管理、安全运营管理能力，支撑互联网暴露面检测、资产发现与漏洞管理、威胁检测与响应、资讯及威胁情报等服务，帮助客户做好安全运营，让用户聚焦自身业务，把专业的安全服务工作交给安恒。
4	网关基础安全产品云化升级改造适配建设	9,500.00	59.87	8,676.70	相关产品已投入市场，处于稳定开发优化阶段	1.完成网关基础安全产品的云化环境部署和新商业模式的探索；2.完成基础产品标准南北向 API 的开放，便于与各种云平台的集成；3.满足网关基础产品的统一集中管理、负载均衡及租户隔离等云化场景的新需求。

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
5	AiLPHA 智能安全运营平台	4,200.00	1,565.47	6,306.22	相关产品已投入市场，处于稳定开发优化阶段	1.具备完整的安全事件运营支撑能力，包括基于攻击链的事件还原、基于上下文的事件溯源以及事件工单等功能；2.具备可编排的安全运营和安全管理能力，可自动化分析研判、处置联动、通报预警，大幅降低安全事件的处置时间，增强运营效率；3.具备海量安全告警存储能力以及基于 Investigation 的威胁情报、攻击趋势、攻击流向的取证能力。
6	物联网安全测试设备科研项目	7,000.00	2,498.72	10,863.29	相关工具已完成开发工作，目前已投入内部使用。在参与的 3 次物联网测试和 2 次车联网测试中均有成果产出。	研究便携式物联网安全测试设备，基于 Linux 系统的 USB 设备，并制作给种类型接口兼容不同类型的设备。此外 Linux 系统的 USB 设备具备无线网卡和存储空间，启动会自动加载串口驱动、usb 驱动和网卡驱动模拟成网关设备，能自动连接网络，并提供有线网络连接和无线网络连接。测试面包括伪装成网关拦截分析重放数据包、关键字检索、升级固件包自动拦截获取、IP 及 URL 自动扫描、移动应用程序自动扫描、固件自动扫描、端口 Fuzz 扫描、常用协议扫描等。
7	AiLand 数据安全岛平台信创改造及功能升级项目	6,124.35	2,042.86	2,858.06	相关产品已投入市场，处于稳定开发优化阶段	1.实现平台及相关产品在国产化软硬件环境中运行，并实现国产数据库及软件系统改造；2.具备基于信创环境软硬件的可信执行环境（TEE），保障多方数据交换计算的过程中，保护隐私；3.具备多方业务数据共享交换应用，支持数据权限分离管控、授权审核等，让参与各方都可以安全、便捷、灵活的进行数据共享和交换，保证数据安全和保护隐私；4.支撑国产加密算法，具备独立统一的信创环境下的密钥管理系统，并支持数据全链路加密；5.具备信创环境的区块链审计技术，实现任何操作行为上链，对其行为进行智能分析，及时发现异常现象，防止不合规的操作发生。
8	AiGuard 数据安全一体化平台（信创）项目	3,295.86	658.31	1,070.04	相关产品已投入市场，处于稳定开发优化阶段	1.实现平台及相关产品在国产化软硬件环境中运行，并实现国产数据库及软件系统改造；2.建立针对信创数据库、信创业务系统和网络环境的综合型数据安全解决方案；保障数据安全收集、安全使用、安全传输、安全存储、安全共享、安全交换，防止数据泄漏；3.建立符合政企信创环境下的数据安全能力建设体

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
						系，覆盖数据安全风险核查、数据梳理、数据保护和监控预警共 4 大类数十项安全能力；4.具备从数据使用、存储、传输、共享、交换、流转的全流动视角，实时展现当前敏感数据流转的态势和数据安全风险，第一时间掌控数据安全态势，快速决策，有效指导运维团队定位和解决数据风险。
9	AiLPHA 大数据态势感知平台信创改造及功能升级项目	14,135.00	8,358.27	11,003.81	相关产品已投入市场，处于稳定开发优化阶段	1.实现平台及相关产品在国产化软硬件环境中运行，并实现国产数据库及软件系统改造；2.具备整合各类基础安全能力，对海量安全告警进行智能分析和研判，自动化处置安全事件，形成安全闭环；3.具备安全数据中台，实现对各类信创环境下的网络安全数据处理；4.具备基于 ATT&CK 的终端威胁建模能力，具备基于知识图谱的网络攻击推理技术。
10	物联网安全操作系统	8,786.75	780.25	1,387.93	初步形成车联网端点数据安全检测引擎能力。	该引擎可以应用于车联网端点资产与相关物联网资产中，可以为车联网相关资产端点提供入侵检测防护与数据安全检测保障。在车联网特殊的设备和场景约束下，帮助用户在满足信息安全防护能力的同时也能具备相应的数据安全应用能力，使其满足防护与法规需求。
11	网络安全实战演训云靶场	5,521.34	318.51	421.79	1.完成网络安全实战演训靶场业务平面和数据平面功能开发；2.完成节点大规模快速部署的技术实现和实战测试；3.完成安全能力评估建模；4.完成多网接入，异构接入的技术验证；5.完成全流量全数据采集技术实现	1. AI 扮演的参演角色及互动；2.基于参演人员行为和全量背景数据的人员能力评估能力；3.大规模异构网络融通及可视化编排 4.黑白流量编排、叠加与重放 5.异构计算资源和网络融合。
合计	/	**79,863.30**	**26,019.70**	**75,867.77**	/	/

报告期内，公司新申请专利119项，获得批准专利143项（均为发明专利），新增已登记的软件著作权13项。

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）募集资金使用及结余情况

1、公司首次公开发行股票募集资金

截至2022年6月30日，公司首发募集资金专户余额为人民币27,643.82万元（含募集资金利息收入扣减手续费净额），具体情况如下：

单位：万元

项目	金额
首次募集资金净额	**95,157.20**
减：募投项目支出	**69,281.72**
其中：2019 年募投项目支出	-
2020 年募投项目支出	25,500.82
2021 年募投项目支出	31,985.94
2022 年 1-6 月募投项目支出	11,794.96
加：利息收入扣除手续费	**4,768.34**
其中：2019 年利息收入扣除手续费	261.34
2020 年利息收入扣除手续费	2,425.55
2021 年利息收入扣除手续费	1,631.10
2022 年 1-6 月利息收入扣除手续费	450.35
2022 年 6 月 30 日募集资金余额	**30,643.82**
其中：2022 年 6 月 30 日现金管理余额	3,000.00
2022 年 6 月 30 日募集资金专户余额	27,643.82

2、2020年度向特定对象发行A股股票募集资金

截至2022年6月30日，公司再融资募集资金专户余额为人民币52,749.40万元（含募集资金利息收入扣减手续费净额）。具体情况如下：

单位：万元

项目	金额
2020 年度向特定对象发行股票募集资金净额	**131,101.57**
减：募投项目支出	**26,724.99**
其中：2021 年募投项目支出	11,987.31
2022 年 1-6 月募投项目支出	14,737.68
加：利息收入扣除手续费	**1,372.82**
其中：2021 年利息收入扣除手续费	354.17
2022 年 1-6 月利息收入扣除手续费	1,018.66
2022 年 6 月 30 日募集资金余额	**105,749.40**
其中：2022 年 6 月 30 日现金管理余额	53,000.00
2022 年 6 月 30 日募集资金专户余额	52,749.40

（二）募集资金专户存储情况

1、公司首次公开发行股票募集资金

截至2022年6月30日，公司募集资金专项账户的存储情况如下：

单位：万元

开户公司	开户银行	银行账户	存储方式	金额
安恒信息	杭州银行科技支行	3301040160014510609	活期存款	2,633.96
安恒信息	中国银行杭州江汉科技支行	375376639046	活期存款	1,583.09
安恒信息	工商银行杭州钱江支行	1202021429900545649	活期存款	5,912.95
安恒信息	建设银行杭州滨江支行	33050161812700002089	活期存款	1,580.65
安恒信息	宁波银行杭州分行	71110122000041547	活期存款	0.10
安恒信息	杭州银行科技支行	3301040160013544641	活期存款	15,933.07
合计				**27,643.82**

2、2020年度向特定对象发行A股股票募集资金

截至2022年6月30日，公司再融资募集资金存放专项账户的余额如下：

单位：万元

开户公司	开户银行	银行账户	存储方式	金额
安恒信息	杭州银行科技支行	3301040160018504517	活期存款	14,736.39

开户公司	开户银行	银行账户	存储方式	金额
安恒信息	浙商银行朝晖支行	3310011710120100026569	活期存款	12,610.25
安恒信息	浙商银行朝晖支行	3310011710120100026600	活期存款	6,201.71
上海安恒互联安全科技有限公司	工行钱江支行	1202021429900590394	活期存款	4,163.24
上海安恒智慧城市安全技术有限公司	宁波银行玉泉支行	71090122000202794	活期存款	10,258.14
成都安恒信息技术有限公司	宁波银行玉泉支行	71090122000202850	活期存款	4,779.66
合计				**52,749.40**

2022年上半年，公司严格按照《公司法》、《证券法》、《上海证券交易所科创板股票上市规则》以及中国证券监督管理委员会相关法律法规的规定和要求使用募集资金，并及时、真实、准确、完整履行相关信息披露工作，不存在违规使用募集资金的情形。

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

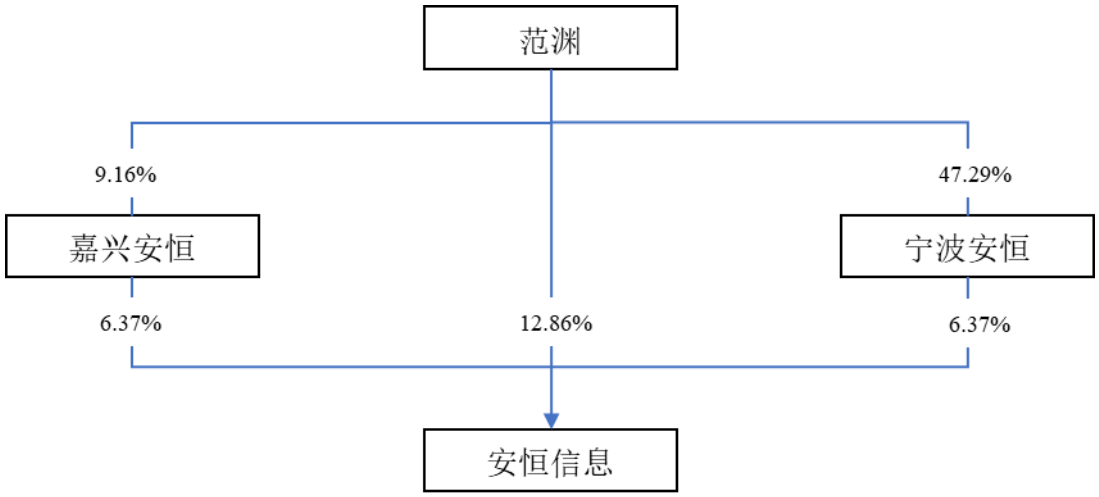
（一）报告期内公司董事、监事和高级管理人员变动情况

公司2022年第一次职工代表大会选举张越芳女士担任公司第二届监事会职工代表监事，原职工监事郑赳离任；2021年年度股东大会选举俞林玲女士为公司第二届监事会非职工代表监事，原监事王欣离任；前述监事任期与公司第二届监事会一致。

（二）截至期末，公司董事、监事和高级管理人员持股情况

公司控股股东、实际控制人为范渊，其任公司董事长，其直接持有公司股票10,096,705股，直接持股比例为12.86%，其通过嘉兴市安恒投资管理合伙企业（有限合伙）（以下简称“嘉兴安恒”）间接持有457,999股，对应间接持股比例为0.58%，其通过宁波安恒投资合伙企业（有限合伙）（以下简称“宁波安恒”）间接持有2,364,500股，对应间接持股比例为3.01%，故范渊直接和间接合计持股比例为16.46%。

范渊与宁波安恒、嘉兴安恒签署了《一致行动协议》，故范渊共控制公司25.60%的表决权。本半年度间接持股情况未发生变动。持股结构具体情况如下：



截至报告期末，除范渊外，公司其他董事、监事和高级管理人员均未直接持有公司股票。公司董事、监事和高级管理人员通过员工持股平台（嘉兴安恒及宁波安恒）间接持有公司股票。

公司控股股东、实际控制人和董事、监事和高级管理人员持有的股份均不存在质押、冻结的情形，报告期内嘉兴安恒、宁波安恒未发生减持。

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。

（本页无正文，为《国泰君安证券股份有限公司关于杭州安恒信息技术股份有限公司2022年半年度持续督导跟踪报告》之签章页）

保荐代表人：杨佳佳　　李宁

杨佳佳　　李　宁

国泰君安证券股份有限公司

2022年8月19日