永信至诚（688244.SH）

2023 年 05 月 24 日

网络靶场龙头，“数字风洞”打开新空间

——公司首次覆盖报告

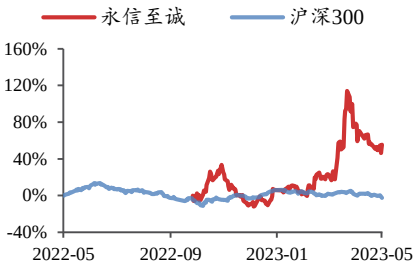
投资评级：买入（首次）

陈宝健（分析师）
chenbaojian@kysec.cn
证书编号：S0790520080001

刘逍遥（分析师）
liuxiaoyao@kysec.cn
证书编号：S0790520090001

日期	2023/5/24
当前股价(元)	93.55
一年最高最低(元)	133.12/51.20
总市值(亿元)	43.81
流通市值(亿元)	9.31
总股本(亿股)	0.47
流通股本(亿股)	0.10
近 3 个月换手率(%)	525.57

股价走势图



数据来源：聚源

● 网络靶场和人才建设领域领军企业，首次覆盖给予“买入”评级

公司经过多年的研发和实践，形成了网络空间平行仿真技术和网络空间攻防对抗技术两大类核心技术，并推出网络靶场系列产品、安全管控与蜜罐系列产品、安全工具类产品、安全防护系列服务、网络安全竞赛服务和其他服务，其他服务主要包括线上线下培训服务。我们预计公司 2023-2025 年归母净利润为 0.86、1.27、1.77 亿元，EPS 分别为 1.84、2.71、3.77 元/股，当前股价对应 PE 分别 51.0、34.5、24.8 倍。公司估值低于同行可比公司平均估值水平，考虑公司在网络靶场领域的领先地位，首次覆盖给予“买入”评级。

● 春秋云境网络靶场平台技术优势突出，市场份额业内领先

目前春秋云境网络靶场已覆盖教育、通信、交通、国防工业、能源等十余个行业，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，已支撑国家多个部委主办的数十场网络安全演练活动及多个行业的靶场建设工程，实现赛事演练、人才培养、智慧城市安全测试、案件线索追踪实战、业务模拟仿真、人工智能攻防、复杂业务安全推演及综合应用等“7+1”应用场景落地。据 IDC 报告显示，公司凭借春秋云境网络靶场产品以 20.4%的市场份额位居第一名。

● 发布“数字风洞”产品体系，开启安全测试评估专业赛道

公司依托于过去多年来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，发布了“数字风洞”产品体系，开启测试评估领域专业赛道。目前已经形成面向城市、行业和单位等不同用户群体的全场景、全要素、全生命周期的安全测试评估解决方案，全面助力网络安全合规保障、风险预控、标准践行和投入回报。未来“数字风洞”产品有望成为公司新增长点，同时也有望探索更加多样的商业模式。

● 风险提示：应收账款余额较高且回款慢；市场竞争加剧；客户需求不稳。

财务摘要和估值指标

指标	2021A	2022A	2023E	2024E	2025E
营业收入(百万元)	320	331	480	664	892
YOY(%)	9.8	3.3	45.3	38.2	34.3
归母净利润(百万元)	47	51	86	127	177
YOY(%)	11.3	7.9	69.2	47.8	39.0
毛利率(%)	56.8	59.6	60.6	62.6	62.3
净利率(%)	14.7	15.4	17.9	19.1	19.8
ROE(%)	9.4	5.0	7.5	10.1	12.3
EPS(摊薄/元)	1.01	1.08	1.84	2.71	3.77
P/E(倍)	93.1	86.2	51.0	34.5	24.8
P/B(倍)	8.9	4.2	3.9	3.5	3.0

数据来源：聚源、开源证券研究所

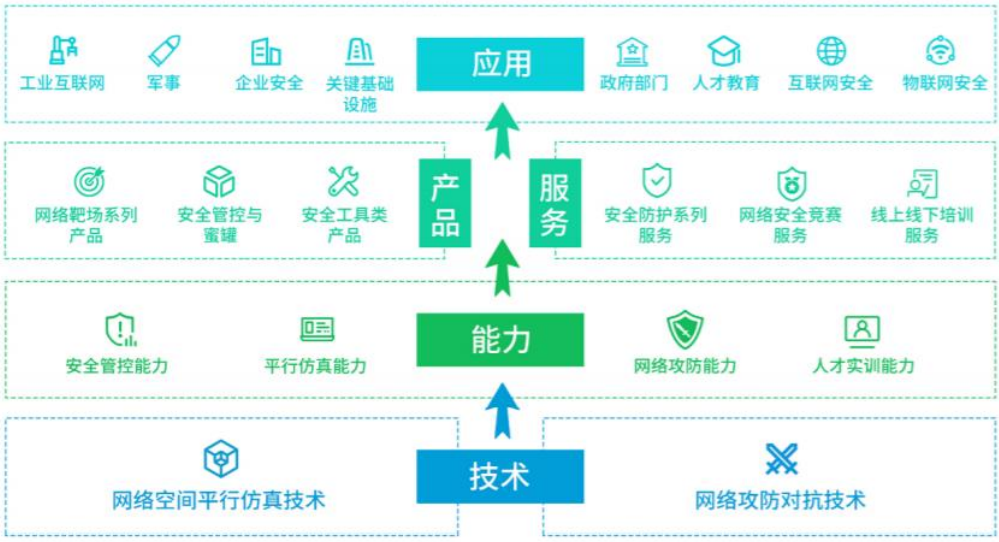
目　录

图表目录

1、 公司简介：网络靶场和人才建设领域领军企业

永信至诚是网络靶场和人才建设领域领军企业。公司经过多年的研发和实践，形成了网络空间平行仿真技术和网络空间攻防对抗技术两大类核心技术，并推出网络靶场系列产品、安全管控与蜜罐系列产品、安全工具类产品、安全防护系列服务、网络安全竞赛服务和其他服务，其他服务主要包括线上线下培训服务。

图1：公司是网络靶场和人才建设领域领军企业



资料来源：公司招股说明书

公司自 2010 年成立至今，发展历程可以为六个阶段：（1）公司成立至 2013 年，以团队“人”才为核心，奠定网络攻防能力；（2）2014 年至 2015 年，以“人”才培养为理念，推出实训、竞赛产品；（3）2015 年至 2017 年，以“人”才实战为指导，研发网络靶场；（4）2018 年，以“平行仿真、攻防技术”为基础，升级网络靶场、开发安全管控与蜜罐平台；（5）以“带给世界安全感”为愿景，构筑了三大品牌全场景产品及服务体系；（6）发布“数字风洞”产品体系，开启安全测试评估专业赛道。

表1：公司自 2010 年成立至今，发展历程可以为六个阶段

时间	经营成果
2010 至 2013 年	● 以团队“人”才为核心，重点聚焦和研究网络安全攻防技术，涉及操作系统安全、数据库安全、Web 安全等技术方向，形成了未知漏洞发现、攻防辅助工具集、安全渗透测试方法论等一系列技术积累，建成了一支具备多元化攻防能力的网络安全技术团队，奠定了公司在安全技术科技创新方面的关键基础。
2014 至 2015 年	● 2014 年至 2015 年，公司基于自主研发的春秋云平台，发布了 e 春秋网络安全实验室培训平台 V1.0、V2.0，平台提供网络安全实训功能。 ● 2015 年，网络空间安全成为国家一级学科，公司发布 i 春秋实训平台，提供网络安全在线培训服务。同年，公司发布了 e 春秋网络安全实验室竞赛平台 V1.0，创新研发了“攻防兼备”的 AWD 竞赛模式，开展了一系列的网络安全赛事运营服务，开始成为国内主要网络安全赛事的专业技术服务提供商。

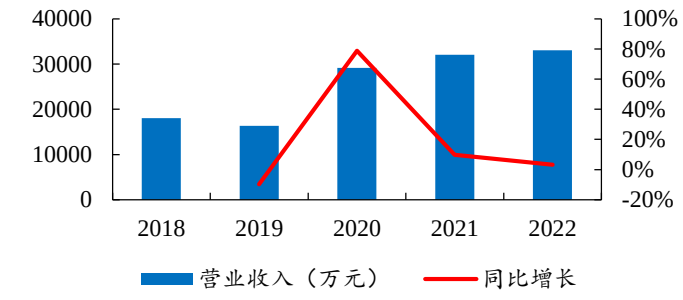
时间	经营成果
2015 至 2017 年	● 基于春秋云平台的底层技术，并综合公司已有技术积累，形成了网络平行仿真技术体系的核心竞争优势，并陆续发布了 e 春秋实验室级网络靶场、企业级网络靶场产品。
2018 年	● 随着公司网络靶场相关技术的不断成熟，公司网络靶场复杂度和规模能力已达到“城市级”。2018 年在成都举办的“巅峰极客”网络安全技能挑战赛中，公司推出了国内首个城市级网络靶场，确立了公司在网络靶场领域的行业领先地位，同时陆续推出了蜜罐及态势感知系统 V1.0、V2.0，监测、分析和展示网络攻击的宏观态势和微观行为，并可主动诱捕来自外部和内部的非法入侵。
2019 年至 2022 年 10 月	● 公司在核心资源上不断深耕、拓展，形成了目前独特的产品体系及品牌优势，即网络靶场系列产品、安全管控与蜜罐产品、安全工具类产品、安全防护系列服务、网络安全竞赛服务、其他服务等六大产品和服务，及结合聚焦攻防实战技术水平的“KRLab”、全国知名网络安全在线培训平台及学习社区“i 春秋”、网络安全赛事领军品牌“春秋 GAME”等三大品牌。
2022 年 10 月至今	● 公司依托于过去多年来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，发布了“数字风洞”产品体系，开启测试评估领域专业赛道。目前已经形成面向城市、行业和单位等不同用户群体的全场景、全要素、全生命周期的安全测试评估解决方案，全面助力网络安全合规保障、风险预控、标准践行和投入回报。

资料来源：公司招股说明书、公司官方微信公众号、开源证券研究所

1.1、 市场地位不断巩固，收入和利润规模波动上升

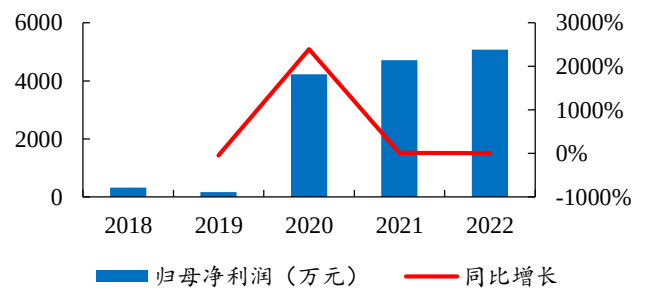
2018-2022 年，公司收入和归母净利润的复合增长率分别为 16.3%和 99.1%，公司规模总体上呈波动上升趋势。主要得益于随着公司对研发的不断投入，技术不断提高，公司地位不断巩固，获取订单能力增强。同时，国家政策支持网络靶场发展，用户使用网络靶场需求增加。

图2：2018-2022 年公司收入复合增长率为 16.3%



数据来源：Wind、开源证券研究所

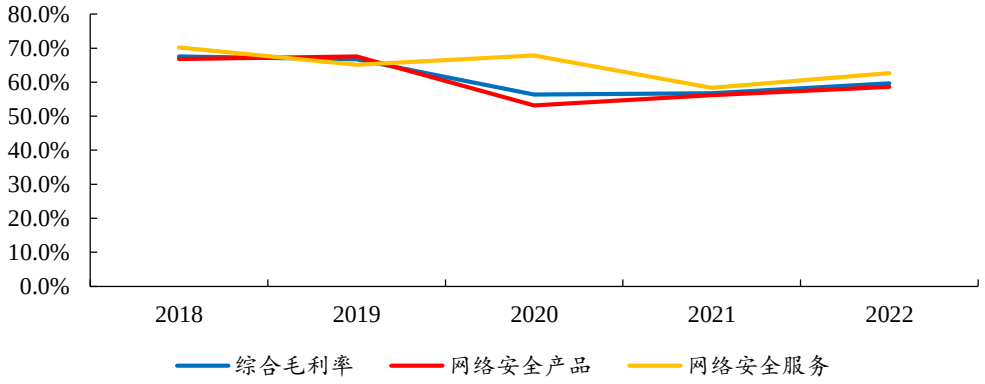
图3：2018-2022 年公司归母净利润复合增长率为 99.1%



数据来源：Wind、开源证券研究所

2018-2022 年公司综合毛利率波动下降。公司 2020 年的网络安全产品毛利率下滑明显，主要原因系公司 2020 年承接了网络安全科技馆项目，项目毛利率为 45%左右，从而拉低了公司 2020 年的网络安全产品毛利率。2021 年毛利率增幅较小的主要原因是公司出于战略发展的长远需要，扩大公司业绩规模，提高公司市场地位，为战略客户提供更有竞争力的价格，项目毛利率偏低。2022 年毛利率继续增长，实现两连升的主要原因是公司产品标准化程度不断提高叠加项目管理效率提升。

图4：2018-2022 年公司综合毛利率波动下降

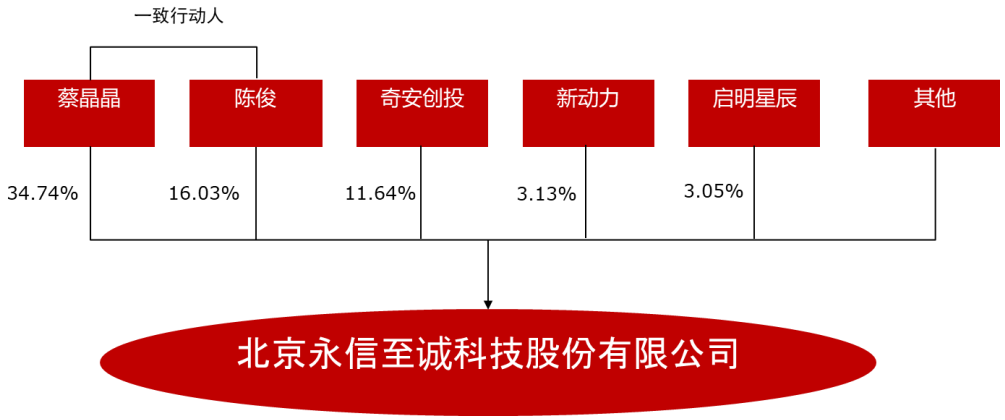


数据来源：Wind、开源证券研究所

1.2、 股权结构稳定，激励到位绑定核心骨干

公司的实际控制人为蔡晶晶和陈俊，截至 2022 年底，其直接持有公司 50.77%股份，通过员工持股平台及战略配售计划间接持有公司 1.67%股份，直接或间接持有公司 52.44%股份。

图5：公司的实际控制人为蔡晶晶和陈俊（截至 2022 年年报）



资料来源：Wind、开源证券研究所

上市前，公司成立了信安春秋、信安春秋壹号两个以公司董事、监事、高级管理人员、核心技术人员及员工为合伙人的合伙企业，目前两个员工持股平台合计持有公司 0.95%股权。上市后，公司发布限制性股票激励计划，拟授予激励对象的限制性股票数量为 56.2 万股，约占公司总股本的 1.20%。首次授予激励对象共计 118 人，授予价格为 35.44 元/股。激励计划有利于激发核心管理、技术和业务人才的积极性，提高经营效率，降低经营成本。

表2：激励计划有利于激发核心管理、技术和业务人才的积极性

归属期		业绩考核目标
首次授予的限制性股票及在公司 2023 年第三季度报告披	第一个归属期	2023 年营业收入不低于 4.80 亿元；
	第二个归属期	2024 年营业收入不低于 5.80 亿元；

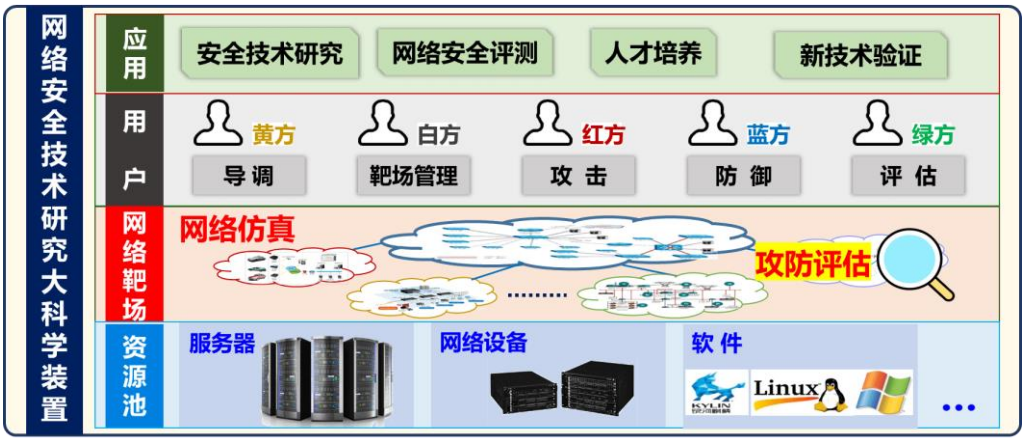
归属期		业绩考核目标
露前授予的预留限制性股票	第三个归属期	2024 年营业收入不低于 7.00 亿元；
在公司 2023 年第三季度报告披露后授予的预留限制性股票	第一个归属期	2024 年营业收入不低于 5.80 亿元；
	第二个归属期	2024 年营业收入不低于 7.00 亿元；

资料来源：公司公告、开源证券研究所

2、 我国网络靶场市场快速发展，成长前景可期

网络靶场是一种基于平行仿真技术，对真实网络空间中的网络架构、系统设备、业务流程的运行状态和运行环境，以及此环境中的行为和数据交互进行模拟、复现的技术或产品，以更有效地实现与网络安全相关的学习、科研、检验、竞赛、演习、推演、决策等行为，从而提高人员及机构的网络安全整体防护水平。网络靶场是数字化建设过程中安全性测试的重要基础设施，是检验和评估安全防御体系有效性的重要技术系统，是国家对重大网络安全风险和趋势进行推演和论证研判的重要科学装置，是防范化解重大网络安全风险的重要手段，也是政企、院校、科研机构等单位网络安全人才培养的重要支撑平台。

图6：网络靶场是数字化建设过程中安全性测试的重要基础设施



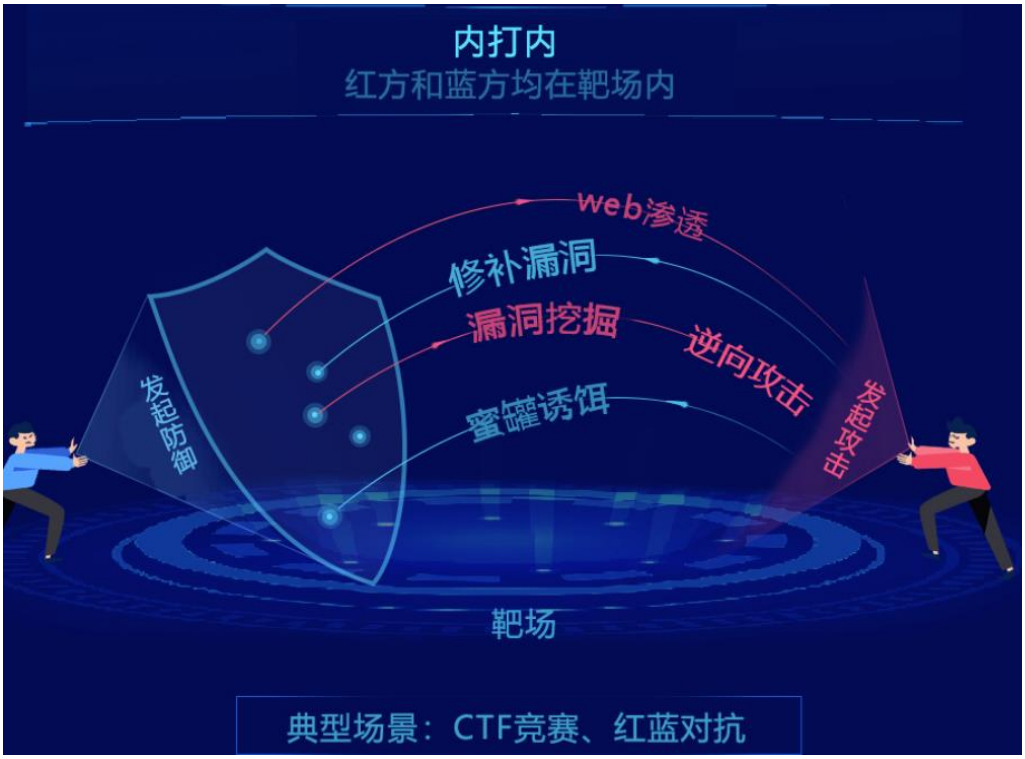
资料来源：鹏城网络靶场官网

网络靶场有三种类型的典型应用模式：内打内、内打外、外打内，也包括分布式靶场。

（1）内打内

红、蓝双方都在靶场内。典型应用场景为攻防对抗实训场景、安全方案或产品的内部测试测评等。

图7：网络靶场内打内是指红、蓝双方都在靶场内

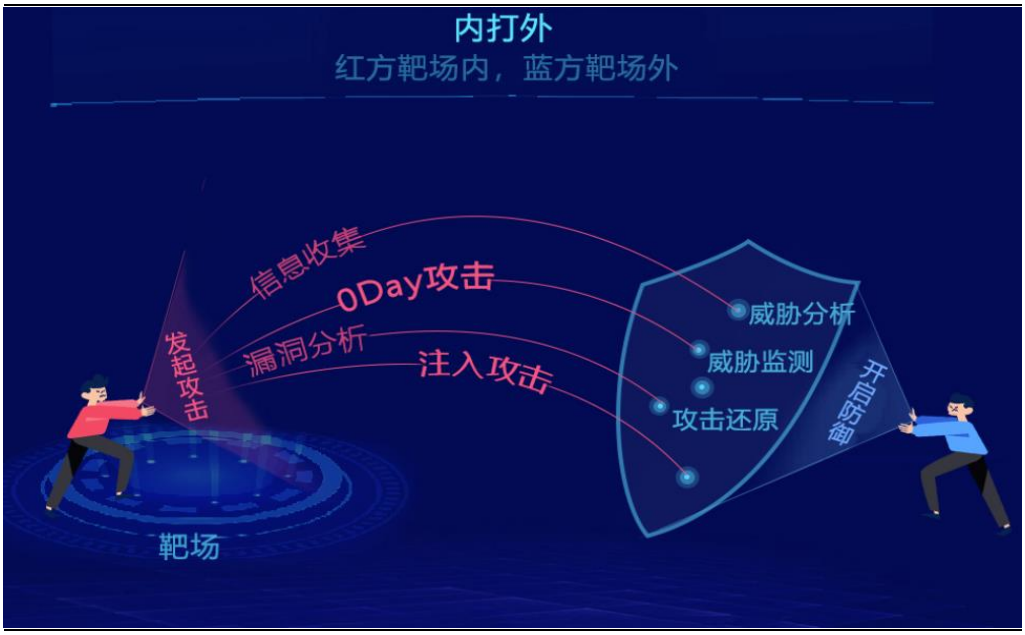


资料来源：新华三主动安全公众号

（2）内打外

内打外即红方在靶场内，蓝方在靶场外。测试人员基于靶场提供的统一环境来完成任务，重点是快速的为成规模的测试人员提供统一可靠并且条件完备的任务操作环境和链路等支持，并且实时的全面记录和管控测试行为并做审计，典型应用场景为科研或监管单位或部门对实网进行的各类安全测试和评估等。

图8：网络靶场内打外是指红方在靶场内，蓝方在靶场外

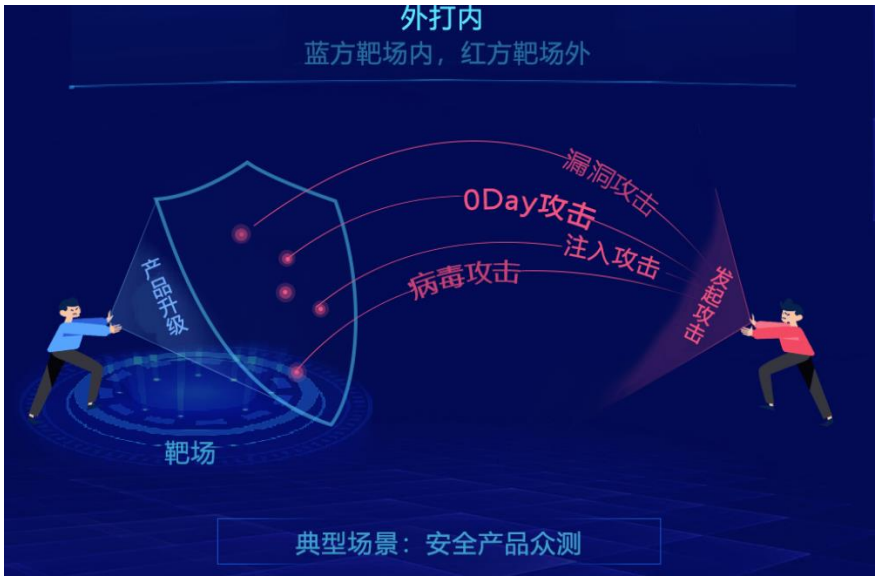


资料来源：新华三主动安全公众号

（3）外打内

外打内即红方在靶场外，蓝方在靶场内。利用靶场平台的快速场景构建能力和场景克隆复制能力，将被验证或测试的目标系统或目标网络生成于网络靶场内部，并根据相应的访问策略对互联网开放，所有具备授权的测试者均可以通过互联网对这个场景进行测试，而在测试过程中，靶场详实的记录测试者在靶场内的各种行为和对被测场景造成的影响，并进行各类评估和展示等，典型应用场景主要用于大规模产品测试、众测、多靶场场景间的联合测试、在线攻防竞赛、蜜罐蜜网防御等。

图9：网络靶场外打内是指红方在靶场外，蓝方在靶场内

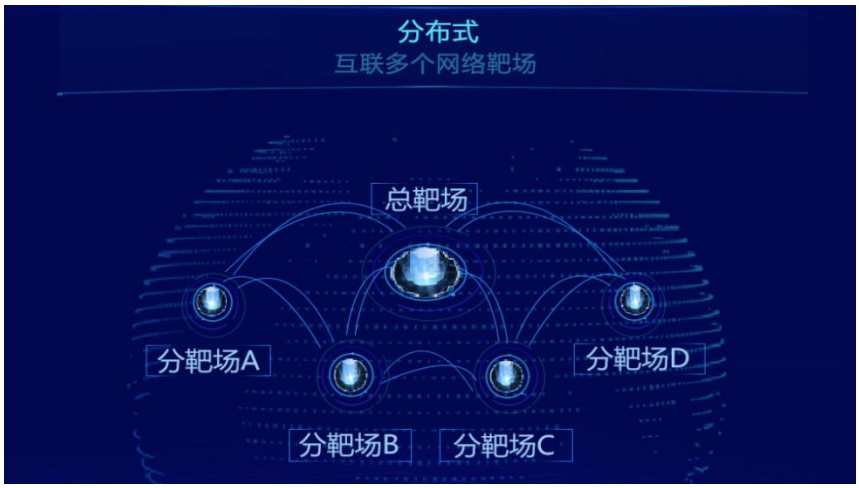


资料来源：新华三主动安全公众号

（4）分布式靶场

分布式靶场即通过互联多个网络靶场，实现网络靶场间的功能复用、资源共享。由于单个网络靶场的处理能力和资源都是有限的，分布式靶场可以将多个网络靶场的资源综合利用起来，并且这种利用对于使用人员是透明的。

图10：分布式靶场是指通过互联多个网络靶场，实现网络靶场间的功能复用、资源共享



资料来源：新华三主动安全公众号

按照靶场建设的用途，可以将网络靶场分为科研测试型靶场、教学培训型靶场、取证靶场、演练型靶场。

科研型靶场主要针对网络安全研究人员提供测试验证环境，支持在靶场上开展网络安全研究、技术开发、网络武器研究、效能测试、系统脆弱性检验等一系列研究工作，推动创新技术快速转化应用到生产领域，起到技术“中试基地”作用。因科研型网络靶场建设周期长、资金投入高，故科研靶场多为国家和各级政府主导建设并推广应用。

教学靶场内置了大量的课件、题库、实验环境以及相关评测辅助等功能，通常集成了普通网络拓扑场景以及能源、钢铁、有色、化工、装备制造等关系国计民生的典型行业的应用场景，提供了集成基础教学演练、综合能力实训、技能评估和后台资源统一管理分配等功能的实训平台，可支撑从教学、实践、使用、监控、评估等维度开展培训工作。目前，教学靶场应用最广泛、使用需求最大。

取证靶场主要模拟真实业务系统，部署在企业互联网出入口，当识别出攻击行为后将攻击者转到取证靶场，进行分析研判与取证。一般在旁路部署大量完全逼真的设备作为“影子系统”来吸引攻击者。

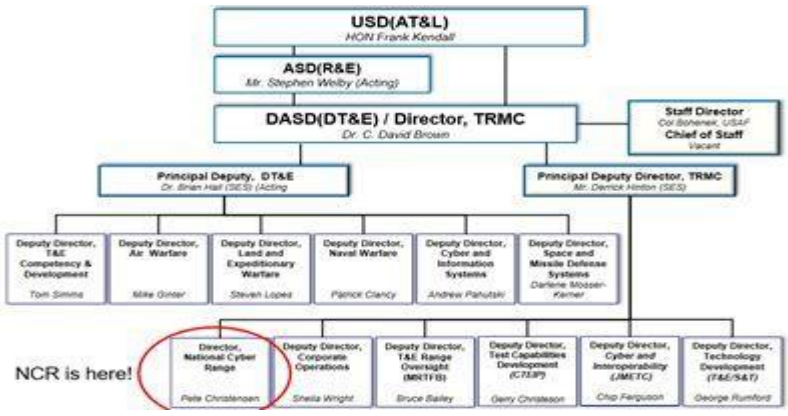
演练型靶场可提供全流程演练环境，在虚拟环境中对真实的攻击、事件进行模拟。演练型靶场主要分为攻防演练型靶场与应急演练型靶场。

2.1、 美国是网络靶场的先驱，市场应用已经进入成熟阶段

网络靶场最初起源于美国国防部高级研究计划局。2008 年 1 月 8 日，美国时任总统布什签署“国家网络安全综合计划”，“国家网络靶场（NationalCyber Range，NCR）”是该项目的重要组成部分。NCR 作为网络攻击与防御的有效性评估、网络武器有效性评估、网络战士训练、网络演习任务开展、网络战术/技术/过程（TTP）的开发等提供靶场化解决方案的基础设施，计划用 6~7 年时间，分为初步概念设计、交付靶场原型、交付基础设施、运行四个阶段进行实施。2012 年 10 月起，美国国防部（DOD）实验资源管理中心（TRMC）正式从 DARPA 接管 NCR，标志着 NCR 从实验室演示阶段正式进入部署应用阶段。

TRMC 负责将美国国防部测试、培训和试验的使用能力“操作化”，NCR 目前由洛克希德马丁公司管理，负责为试验鉴定部门（DoT&E）提供网络试验鉴定基础设施，目标是为美国国防部、陆海空三军和其他政府机构服务，提供虚拟环境来模拟真实的网络攻防作战，针对敌对电子攻击和网络攻击等电子作战的手段进行试验，以实现网络空间作战能力的重大变革，打赢未来网络空间战争。

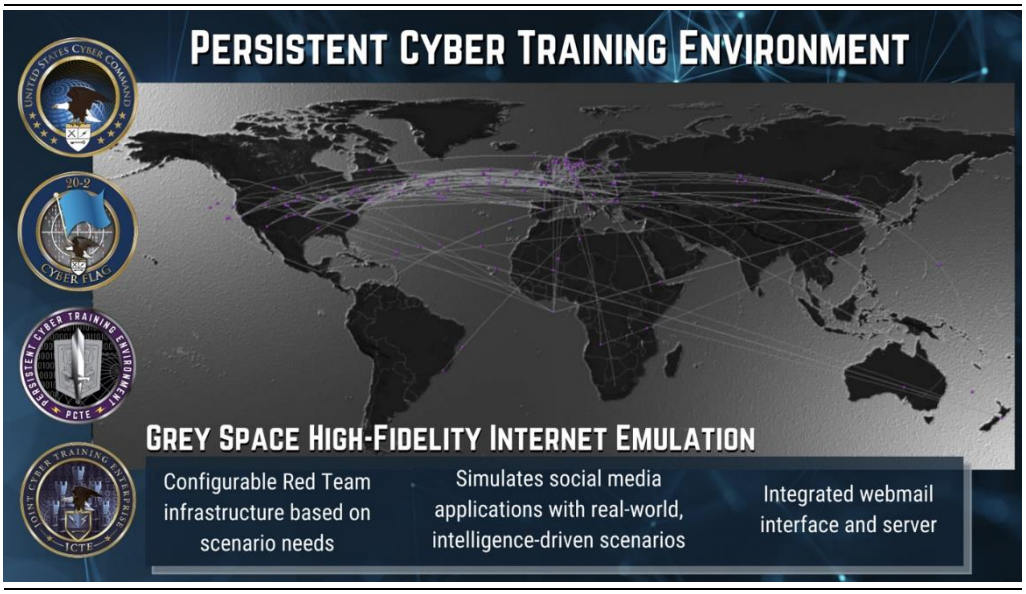
图11：NCR 在美国国防部试验资源管理中心处于重要地位



资料来源：中国保密协会科学技术分会公众号

2017 年美国又启动了持续网络训练环境（PCTE）建设，利用云端化平台方式满足分散各地、各军种网络作战部队的统一网络训练环境。PCTE 是美国陆军模拟、训练和仪器项目执行办公室 (PEO STRI) 开发和部署的系统，是美国继 NCR 之后又一重量级网络靶场建设项目。PCTE 是基于混合式云端服务训练平台，旨在通过高度接近真实的虚拟环境，为美军网络任务部队提供针对个人、团队、部队军种级别的标准化网络训练场景服务，实现点对点规划、准备、执行和评估网络作战演练，全方位增强美国网络任务部队的全频谱训练水平与战备状态。2019 年 11 月 25 日美国发布 PCTE 项目 CYBER TRIDENT（网络培训、就绪、集成、交付和企业技术）合同，项目合同金额近 9.570 亿美元。

图12：美国的网络靶场发展主脉络主要分为两条线：军事靶场发展与军民融合靶场发展



资料来源：U.S. Department of Defense

2021 年 7 月，据美国国防部网站消息，美国已授权价值 24.10 亿美元的网络靶场相关合同。在未来的 10 年中，获得订单的公司将为军方网络任务部队提供事件规划和执行、场地安全、信息技术管理以及靶场现代化和作战支持，同时通过测试、规划和系列活动来支持国家网络靶场综合设施的运行。总体上，该合同的主要目标是为其国家网络靶场综合设施提供 IT 服务。

2.2、 我国网络靶场尚处于快速发展过程中，市场规模有望高速增长

我国网络靶场建设目前处于起步阶段。在国家网络靶场建设方面，无论从靶场基础理论研究、关键技术和产品研发，还是网络空间安全风险评估研究，与欧美国家相比，我国都还存在着一定差距。

国家政策鼓励网络靶场的建设。工信部在《网络安全产业高质量发展三年行动计划（2021-2023 年）（征求意见稿）》中指出，积极推进网络靶场技术研究，建设结合虚拟环境和真实设备的安全孪生试验床，提升网络安全技术产品测试验证能力。国家能源局在《关于印发 2021 年电力安全监管重点任务的通知》中要求，推进电力行业网络安全仿真验证环境（靶场）建设，组织开展电力行业网络安全攻防实战演练。

表3：国家政策鼓励网络靶场的建设

时间	部门	文件	内容
2021 年 1 月	国家能源局	《关于印发 2021 年电力安全监管重点任务的通知》	● 推进电力行业网络安全仿真验证环境（靶场）建设，组织开展电力行业网络安全攻防实战演练。
2021 年 7 月	工信部	《网络安全产业高质量发展三年行动计划（2021-2023 年）（征求意见稿）》	● 积极推进网络靶场技术研究，建设结合虚拟环境和真实设备的安全孪生试验床，提升网络安全技术产品测试验证能力。 ● 要研究人工智能系统可解释性、隐私性等安全要素，突破人工智能模型攻击与防御关键技术，设计实现人工智能系统自动攻防平台，构建人工智能安全靶场。
2022 年 10 月	国家标准化管理委员会	《信息安全技术 关键信息基础设施安全保护要求》(GB/T 39204-2022)	● 网络安全检测评估作为关键信息基础设施安全保护工作的六个主要内容及活动之一，成为落实保护关键信息基础设施安全的重要要求。同时，在安全防护内容中，针对安全建设管理，明确提出“应在关键信息基础设施建设、改造、升级等环节，实现网络安全技术措施与关键信息基础设施主体工程同步规划、同步建设、同步使用，并采取测试、评审、攻防演练等多种形式验证。必要时，可建设关键业务的仿真验证环境予以验证。”

资料来源：工信部、国家能源局等、开源证券研究所

各地政府积极支持建设攻防实验室，搭建网络安全攻防靶场。广东、浙江、广西、贵州等各地政府支持建设攻防实验室，搭建网络安全攻防靶场、模拟仿真环境，推进网络攻防演练工程；军队部门、国务院国资委对国有企业、国家能源局等部门亦发文推进网络安全仿真靶场建设，开展行业网络安全攻防实战演练。

表4：各地政府积极支持建设攻防实验室，搭建网络安全攻防靶场

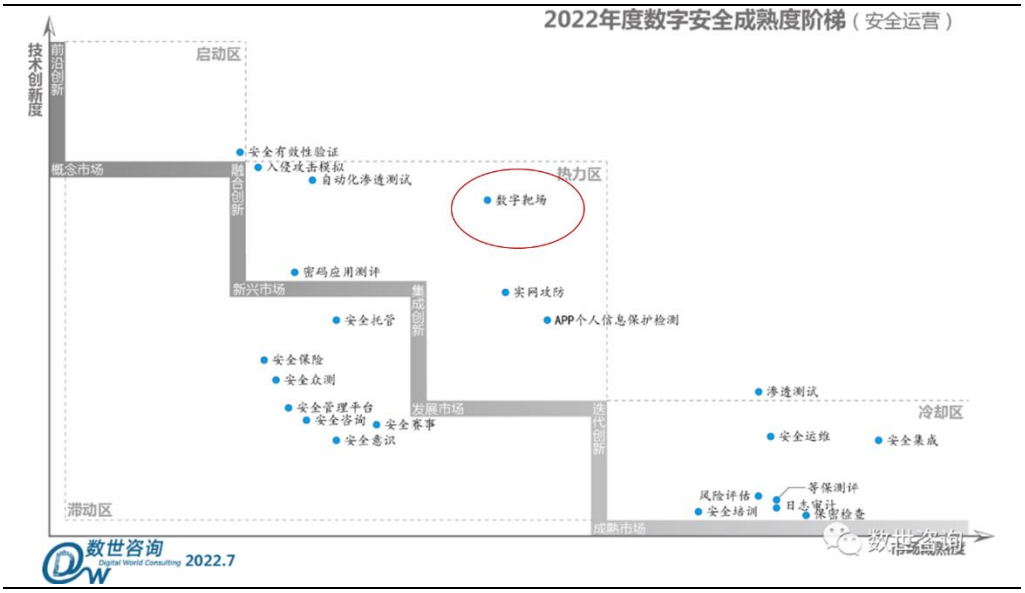
时间	文件	内容
2018 年 9 月	《浙江省数字经济五年倍增计划》	● 推进网络攻防演练工程。定期举办网络安全攻防演练大赛和网络安全比赛，加强技术交流。建设攻防实验室，搭建网络安全攻防靶场、模拟仿真环境，开展教学、实训、渗透攻击测试、研究以及专业培训。
2021 年 6 月	《广东省数字政府改革建设“十四五”规划》	● 将结合安全大数据和安全应用，打造安全攻防实验室，构建网络安全仿真 靶场与实训环境，持续开展“粤盾”攻防演练，提升数字政府整体安全实战能力。
2021 年 12 月	《贵州省“十四五”数字经济发展规划的通知》	● 加快贵阳经开区大数据安全产业园建设，提升建设国家大数据安全靶场，持续承接好国家大数据及网络安全对抗演练。
2022 年 1 月	《广西数字经济发展规划（2018—2025 年）（2021 年修订版）》	● 建设大数据安全靶场，开展大数据与网络攻防演练。推动合同、发票、证据、档案、凭证等电子化转变，加快构建安全可信的数字商务运行环境。

资料来源：各地方政府网站、开源证券研究所

自 2016 年以来，成都、天津、浙江、江苏、贵阳和广东等省份均建立了智慧城市网络靶场。以鹏城靶场为例，鹏城靶场是我国网络靶场理念、技术和实践的领导者之一。鹏城靶场属于鹏城国家实验室，历经十年研究发展，已步入第四代——联邦靶场的发展建设模式。2020 年，第三代系统成功实现国内首个单体超百万节点的大规模网络靶场，全面覆盖网络安全科研、安全性评测、攻防对抗训练、新技术验证等网络安全保障需求；2022 年，第四代系统实现国内首个联邦靶场，集成一批关键信息技术基础设施分靶场，为各地智慧城市建设保驾护航。

数字靶场在数世咨询数字安全能力图谱 2022 中位于安全运营下的安全演练分类中；在数世咨询的 2022 年度数字安全成熟度阶梯（安全运营）中位于热力区，市场成熟度属于发展市场，技术维度属于融合创新阶段。

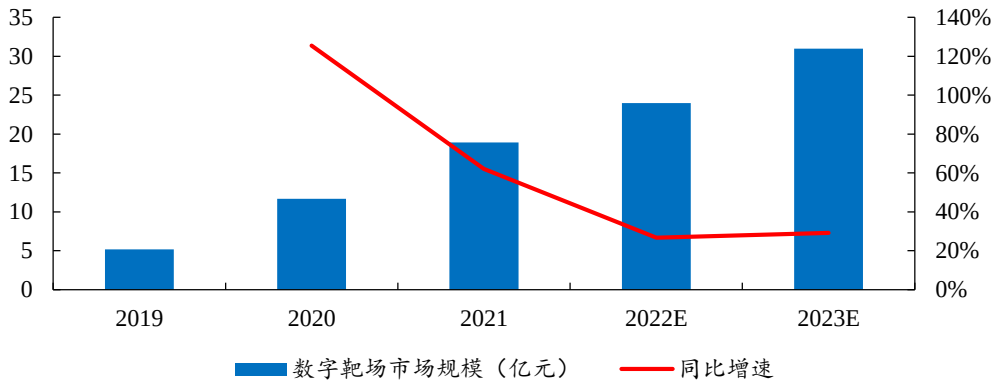
图13：数字靶场在数世咨询的 2022 年度数字安全成熟度阶梯（安全运营）中位于热力区，市场成熟度属于发展市场



资料来源：数世咨询、开源证券研究所

根据数世咨询调研，2020 年数字靶场市场收入已经达到 11.68 亿元（合同额），2021 年收入达到 18.94 亿元。预计 2022 年可达 24 亿元，2023 年收入有望超过 31 亿元。

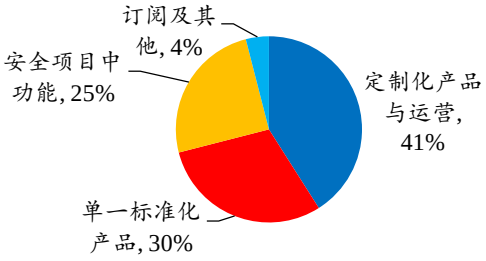
图14：我国数字靶场市场收入预计 2022 年可达 24 亿元，2023 年收入有望超过 31 亿元



数据来源：数世咨询、开源证券研究所

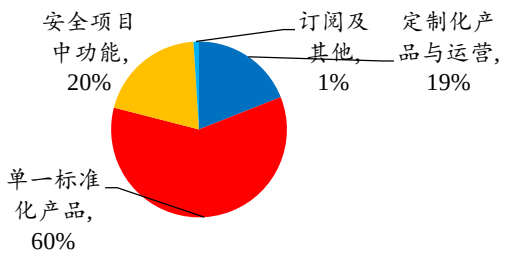
和 2019 年相比，数字靶场交付模式最大的变化在于从单一标准化产品转向了定制化产品与运营。单一标准化产品的占比从 60%下降了一半到 30%，而定制化产品与运营的方式则从 19%跃升至 41%。这一转变的一大原因在于数字靶场应用场景的变化。对于教学/实训、竞赛类的应用场景，往往单一标准化的数字靶场产品就已经足够了；但是对于演练、研究的落地场景，尤其是需要长期使用的数字靶场，则需要定制化或者长期运营服务的方式进行。

图15：2022 年数字靶场交付模式以定制化产品与运营为主



数据来源：数世咨询、开源证券研究所

图16：2019 年数字靶场交付模式以单一标准化产品为主

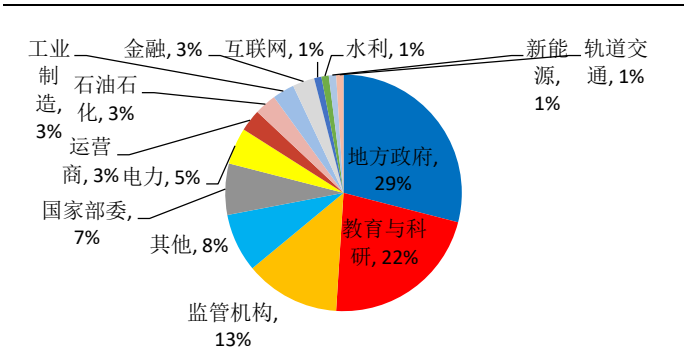


数据来源：数世咨询、开源证券研究所

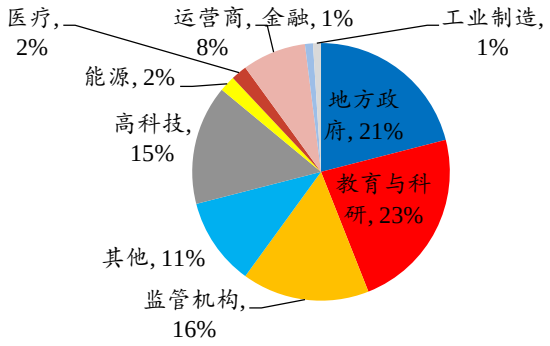
数字靶场当前最大使用行业为地方政府，占比 29%，相较于 2019 年占比增长了 8%，其原因是过去两年里，有大量的城市基地项目开始建立，其中包括了大量的靶场相关产品。教育与科研和监管机构占比变化不大，依然为第二和第三位置。

图17：2022 年数字靶场最大使用行业为地方政府

图18：2019 年数字靶场最大使用行业为教育及科研院所



数据来源：数世咨询、开源证券研究所



数据来源：数世咨询、开源证券研究所

3、 网络靶场市场优势突出，“数字风洞”产品开启安全测试评估专业赛道

3.1、 春秋云境网络靶场平台技术优势突出，市场份额业内领先

春秋云境网络靶场平台基于公司多年研发实践的平行仿真技术体系构建而成。该平台融合了主机虚拟化、网络虚拟化、软件定义网络、多维数据采集、3D 展示引擎和高可用云端架构等多种前沿技术，支持多种角色以不同权限和资源访问能力在同一靶场场景中进行联合交互和测试。实验和测试过程安全可控，数据采集准确详实，效能展示科学直观。

表5：春秋云境网络靶场平台基于公司多年研发实践的平行仿真技术体系构建而成

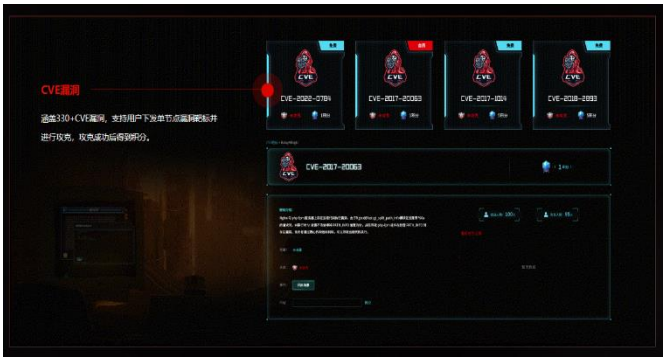
靶场能力	具体情况
支持的靶场类型	赛事演练靶场； 人才培养靶场； 智慧城市安全测试靶场； 案件线索追踪实战靶场； 业务模拟靶场； 人工智能攻防靶场； 复杂业务安全推演靶场； 综合场景应用靶场（涵盖科技馆、人才基地等）。
仿真及虚拟化能力	全自主研发的春秋云靶场专用管理平台； 支持 KVM、docker、VMware、Xen、QEMU 等多种类型的虚拟机导入，兼容 OpenStack 等云平台接口； 支持全虚拟机、容器虚拟化、数字仿真、模拟仿真、协议仿真、流量仿真六维融合仿真技术； 支持与终端设备、路由交换设备、网络设备等多种类型的实体设备结合构建隔离的软件定义隔离网络，并支持自动化部署脚本进行快速状态恢复； 支持基于流量、自动化脚本等进行业务或特定的行为仿真。
已公开验证过的最大节点部署规模	2020 年“网鼎杯”半决赛现场，单一场景 8000+全虚拟机节点
可支持的最大节点部署规模	百万级节点多集群联动
千级别节点实例化时间	分钟级

靶场能力	具体情况
单虚拟机节点实例化时间	秒级
并发及接入能力	支持多种类型的靶场任务并发下发，所有任务数据及虚拟化场景严格隔离； 支持单任务或多任务统一动态导调，支持动态数据采集及实时效能评估； 每个任务均支持攻击测试、防御、监管、厂商、供应链、普通应用者等多种角色按不同权限接入场景实时互动； 支持个人终端、VPN 远程、靶场操作虚拟机等各类接入模式
成功支持基于网络靶场的省部级以上竞赛及演习案例	网鼎杯、强网杯、护网杯、全国信息安全竞赛、巅峰极客网络安全大赛、粤盾演习、DefCon 中国赛、黄鹤杯 RHG 人工智能安全大赛等
靶标资源	百万级中低交互节点集群靶标； 操作系统虚拟机靶标 1500+； 高交互靶标 5000+； CVE 漏洞验证靶标 1000+； 漏洞知识库 20 万+； 各类漏洞环境 10000+； 高交互仿真场景 800+； 行业及城市级仿真场景 100+。
多级靶场级联或与其他平台兼容性	支持春秋云境靶场多级级联； 标准数据接口支持与其他网络靶场或管理系统进行兼容。

资料来源：公司招股说明书、开源证券研究所

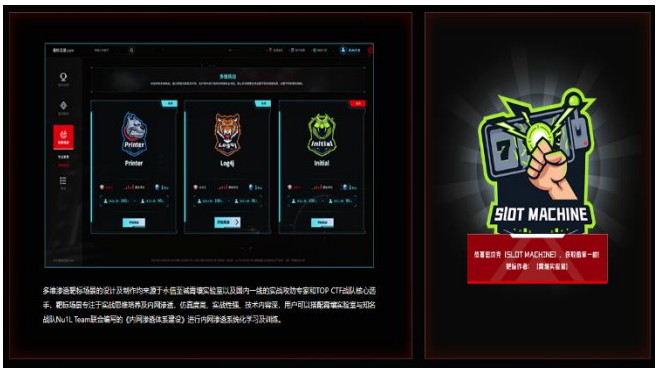
春秋云境网络靶场平台设计了漏洞靶标和仿真场景两大体系，为用户提供实战化、体系化的渗透测试体验。其中，漏洞靶标多为历史 CVE 漏洞以及国内热点漏洞，涵盖浏览器、数据库、网络设备、Web 等方向，用户可以根据自身培训、验证等需求，实时复现漏洞场景；仿真场景均源于真实网络安全案件、大型攻防演练等实战场景，具备独特剧情及技术点，仿真度高、实战性强、技术内容深，饕餮技术盛宴系统化淬炼网络安全实战思维。

图19：漏洞靶标多为历史 CVE 漏洞以及国内热点漏洞



资料来源：春秋云镜官网

图20：仿真场景均源于真实网络安全案件、大型攻防演练等实战场景



资料来源：春秋云镜官网

春秋云境网络靶场已覆盖教育、通信、交通、国防工业、能源、金融、政法、电子政务、科技、互联网等十余个行业，积累了数百个行业级场景，近百个城市级

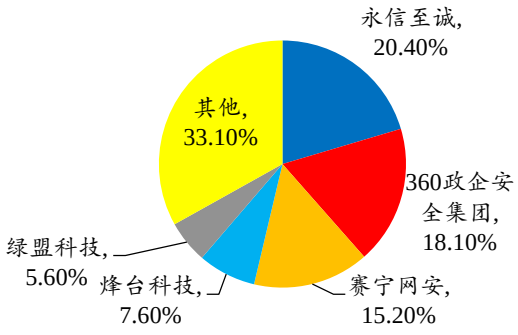
仿真互联网场景，近千个网络安全 CVE 漏洞靶标，数千个安全实训靶标，百余个人工智能漏洞挖掘训练集等，已支撑国家多个部委主办的数十场网络安全演练活动及多个行业的靶场建设工程，实现赛事演练、人才培养、智慧城市安全测试、案件线索追踪实战、业务模拟仿真、人工智能攻防、复杂业务安全推演及综合应用等“7+1”应用场景落地。

图21：春秋云境网络靶场已实现赛事演练、人才培养、智慧城市安全测试等各类应用场景落地

资料来源：公司官网

春秋云境网络靶场产品在国内网络靶场市场排名第一。据 IDC 研究报告显示，公司凭借春秋云境网络靶场产品以 20.4%的市场份额位居第一名。数世咨询发布《数字靶场能力点阵图，2022》显示，春秋云境网络靶场在应用创新力和市场执行力维度均位列行业第一。

图22：IDC 报告显示，春秋云境网络靶场产品以 20.4%的市场份额位居国内网络靶场市场第一名



数据来源：IDC、开源证券研究所

图23：数世咨询报告显示，春秋云境网络靶场在应用创新力和市场执行力维度均位列行业第一

资料来源：数世咨询

3.2、 发布“数字风洞”产品体系，开启安全测试评估专业赛道

公司依托于过去多年来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，发布了“数字风洞”产品体系，开启安全测试评估领域专业赛道。目前，已经形成面向城市、行业和单位等不同用户群体的全场景、全要素、全生命周期的安全测试评估解决方案，全面助力网络安全合规保障、风险预控、标准践行和投入回报。

面向城市级场景，公司配合数字城市规划单位，打造面向开发人员的深度检验测试平台、面向安全部门年度演练组织的攻防演练靶场平台和面向安全服务人员的风险评估平台，助力城市数字化建设。

面向行业级场景，公司助力用户在业务系统上线初期甚至在规划阶段就将风险反复验证，并在运营、处置等周期中基于高仿真环境测试验证风险。

面向单位级场景，公司助力重点单位进行网络安全任务测试评估。

此外，公司“数字风洞”产品在军工、公安、金融、电信、电力、医疗、交通等各关键行业及工业互联网安全、数据安全、人工智能、信创、车联网安全等新兴领域均实现了场景落地，全面支撑数字化领域中，人、系统、数据等核心要素的安全测试与评估，贯穿规划、运营和处置整个生命周期的风险防范与化解。

图24：公司连续三年支撑广东省“粤盾”数字政府攻防演练

资料来源：公司官方微信公众号

图25：公司助力能源行业网络安全测试评估

资料来源：公司官方微信公众号

3.3、 AIGC 浪潮已至，网络靶场和数字风洞产品护航 AI 安全

4 月 11 日，国家互联网信息办公室发布关于《生成式人工智能服务管理办法（征求意见稿）》公开征求意见的通知，其中第六条提到“利用生成式人工智能产品向公众提供服务前，应当按照《具有舆论属性或社会动员能力的互联网信息服务安全评估规定》向国家网信部门申报安全评估，并按照《互联网信息服务算法推荐管理规定》履行算法备案和变更、注销备案手续”。

公司在投资者互动平台表示，公司网络靶场和数字风洞产品均是人工智能（AI）安全测试评估的基础设施平台。人工智能在不同行业、不同领域的应用有不同形态，例如 ChatGPT 类的人工智能平台，一般会出现接口类、越权类等网络安全风险，还可能存在隐私泄露、数据泄露等数据安全风险，公司的网络靶场和数字风洞产品具备对该类产品和风险进行安全测试评估的能力。

4、 盈利预测与投资建议

4.1、 核心假设

（1）收入端：一方面，国内数字靶场尚处于快速发展期，公司作为国内网络靶场的龙头，收入有望高速增长；另一方面，公司发布了“数字风洞”产品体系，开启安全测试评估专业赛道，有望带来新增长点。因此，我们预计 2023-2025 年收入增速分别为 45.3%、38.2%、34.3%；

（2）毛利率：未来几年公司毛利率有望保持较高水平，我们预计公司 2023-2025 年销售毛利率 60.6%、62.6%、62.3%。

（3）期间费用率：我们预计公司 2023-2025 年销售费用率为 18.0%、16.5%、16.0%；管理费用率为 9.5%、8.5%、8.5%；研发费用率为 19.0%、18.0%、18.0%。

4.2、 盈利预测与投资建议

我们预计公司 2023-2025 年归母净利润为 0.86、1.27、1.77 亿元，EPS 分别为 1.84、2.71、3.77 元/股，当前股价对应 PE 分别 51.0、34.5、24.8 倍。公司估值低于同行可比公司平均估值水平，考虑公司在网络靶场领域的领先地位，首次覆盖给予“买入”评级。

表6：公司 PE 低于行业可比公司平均水平（截止 2023.5.24 收盘）

证券代码	公司简称	当前市值（亿元）	归母净利润（亿元）			PE		
			2023E	2024E	2025E	2023E	2024E	2025E
002439.SZ	启明星辰	289.00	8.83	11.52	14.90	32.7	25.1	19.4
688489.SH	三未信安	82.00	1.59	2.23	2.97	51.6	36.8	27.6
300454.SZ	深信服	498.00	5.17	7.40	10.58	96.3	67.3	47.1
002212.SZ	天融信	118.00	4.93	6.40	8.14	23.9	18.4	14.5
	行业平均					**51.1**	**36.9**	**27.1**
688244.SH	**永信至诚**	**44.00**	**0.86**	**1.27**	**1.77**	**51.0**	**34.5**	**24.8**

数据来源：Wind、开源证券研究所 （启明星辰、三未信安、深信服、天融信盈利预测来自开源证券研究所）

5、 风险提示

（1） 应收账款余额较高且回款慢；

（2） 市场竞争加剧风险；

（3） 下游客户需求不稳定风险。

附：财务预测摘要

资产负债表(百万元)	2021A	2022A	2023E	2024E	2025E
流动资产	514	1058	1184	1547	2049
现金	362	669	972	1344	1805
应收票据及应收账款	116	210	0	0	0
其他应收款	5	4	9	9	15
预付账款	0	1	1	1	1
存货	17	9	28	20	45
其他流动资产	13	166	174	174	183
非流动资产	98	122	166	214	262
长期投资	3	2	2	1	1
固定资产	75	68	112	162	212
无形资产	6	33	33	32	31
其他非流动资产	14	19	20	19	19
资产总计	612	1180	1350	1761	2311
流动负债	101	116	196	477	849
短期借款	5	8	150	426	789
应付票据及应付账款	43	67	0	0	0
其他流动负债	53	41	46	51	60
非流动负债	18	12	16	18	18
长期借款	0	0	4	6	7
其他非流动负债	18	12	12	12	12
负债合计	118	128	211	495	867
少数股东权益	-1	2	1	2	4
股本	35	47	47	47	47
资本公积	365	859	859	859	859
留存收益	94	145	231	358	537
归属母公司股东权益	494	1051	1137	1264	1441
负债和股东权益	612	1180	1350	1761	2311

现金流量表(百万元)	2021A	2022A	2023E	2024E	2025E
经营活动现金流	10	-18	214	171	180
净利润	46	53	86	128	178
折旧摊销	13	14	14	19	23
财务费用	-1	-2	4	16	17
投资损失	-7	-6	-4	-5	-5
营运资金变动	-46	-92	124	27	-12
其他经营现金流	5	15	-9	-15	-20
投资活动现金流	0	-185	-53	-62	-67
资本支出	7	31	59	67	73
长期投资	0	0	1	1	1
其他投资现金流	7	-154	4	5	5
筹资活动现金流	-51	510	-0	-13	-15
短期借款	-31	2	142	276	363
长期借款	-9	0	4	2	1
普通股增加	0	12	0	0	0
资本公积增加	-0	494	0	0	0
其他筹资现金流	-11	1	-147	-291	-379
现金净增加额	-41	307	161	96	98

利润表(百万元)	2021A	2022A	2023E	2024E	2025E
营业收入	320	331	480	664	892
营业成本	138	134	189	248	336
营业税金及附加	2	2	3	4	6
营业费用	61	56	86	110	143
管理费用	31	29	46	56	76
研发费用	50	63	91	120	161
财务费用	-1	-2	4	16	17
资产减值损失	3	-1	-1	1	-1
其他收益	12	16	11	13	13
公允价值变动收益	0	0	0	0	0
投资净收益	7	6	4	5	5
资产处置收益	0	0	0	0	0
营业利润	55	57	85	140	193
营业外收入	0	0	0	0	0
营业外支出	0	0	0	0	0
利润总额	55	57	85	140	193
所得税	9	4	-0	12	15
净利润	46	53	86	128	178
少数股东损益	-1	2	-0	1	1
归属母公司净利润	47	51	86	127	177
EBITDA	57	52	80	142	206
EPS(元)	1.01	1.08	1.84	2.71	3.77

主要财务比率	2021A	2022A	2023E	2024E	2025E
成长能力					
营业收入(%)	9.8	3.3	45.3	38.2	34.3
营业利润(%)	13.2	3.7	49.2	64.3	37.7
归属于母公司净利润(%)	11.3	7.9	69.2	47.8	39.0
获利能力					
毛利率(%)	56.8	59.6	60.6	62.6	62.3
净利率(%)	14.7	15.4	17.9	19.1	19.8
ROE(%)	9.4	5.0	7.5	10.1	12.3
ROIC(%)	7.3	3.3	5.1	6.6	7.5
偿债能力					
资产负债率(%)	19.4	10.8	15.7	28.1	37.5
净负债比率(%)	-68.8	-61.8	-70.9	-71.1	-69.1
流动比率	5.1	9.1	6.1	3.2	2.4
速动比率	4.9	7.8	5.1	2.9	2.2
营运能力					
总资产周转率	0.5	0.4	0.4	0.4	0.4
应收账款周转率	3.2	2.0	0.0	0.0	0.0
应付账款周转率	3.6	2.4	5.7	0.0	0.0
每股指标（元）					
每股收益(最新摊薄)	1.01	1.08	1.84	2.71	3.77
每股经营现金流(最新摊薄)	0.22	-0.37	4.58	3.65	3.85
每股净资产(最新摊薄)	10.55	22.44	24.28	26.99	30.76
估值比率					
P/E	93.1	86.2	51.0	34.5	24.8
P/B	8.9	4.2	3.9	3.5	3.0
EV/EBITDA	70.6	71.6	44.8	24.5	16.4

数据来源：聚源、开源证券研究所

特别声明

《证券期货投资者适当性管理办法》、《证券经营机构投资者适当性管理实施指引（试行）》已于2017年7月1日起正式实施。根据上述规定，开源证券评定此研报的风险等级为R4（中高风险），因此通过公共平台推送的研报其适用的投资者类别仅限定为专业投资者及风险承受能力为C4、C5的普通投资者。若您并非专业投资者及风险承受能力为C4、C5的普通投资者，请取消阅读，请勿收藏、接收或使用本研报中的任何信息。
因此受限于访问权限的设置，若给您造成不便，烦请见谅！感谢您给予的理解与配合。

分析师承诺

负责准备本报告以及撰写本报告的所有研究分析师或工作人员在此保证，本研究报告中关于任何发行商或证券所发表的观点均如实反映分析人员的个人观点。负责准备本报告的分析师获取报酬的评判因素包括研究的质量和准确性、客户的反馈、竞争性因素以及开源证券股份有限公司的整体收益。所有研究分析师或工作人员保证他们报酬的任何一部分不曾与，不与，也将不会与本报告中具体的推荐意见或观点有直接或间接的联系。

股票投资评级说明

	评级	说明
证券评级	买入（Buy）	预计相对强于市场表现 20%以上；
	增持（outperform）	预计相对强于市场表现 5%～20%；
	中性（Neutral）	预计相对市场表现在－5%～＋5%之间波动；
	减持（underperform）	预计相对弱于市场表现 5%以下。
行业评级	看好（overweight）	预计行业超越整体市场表现；
	中性（Neutral）	预计行业与整体市场表现基本持平；
	看淡（underperform）	预计行业弱于整体市场表现。
备注：评级标准为以报告日后的 6~12 个月内，证券相对于市场基准指数的涨跌幅表现，其中 A 股基准指数为沪深 300 指数、港股基准指数为恒生指数、新三板基准指数为三板成指（针对协议转让标的）或三板做市指数（针对做市转让标的）、美股基准指数为标普 500 或纳斯达克综合指数。我们在此提醒您，不同证券研究机构采用不同的评级术语及评级标准。我们采用的是相对评级体系，表示投资的相对比重建议；投资者买入或者卖出证券的决定取决于个人的实际情况，比如当前的持仓结构以及其他需要考虑的因素。投资者应阅读整篇报告，以获取比较完整的观点与信息，不应仅仅依靠投资评级来推断结论。		

分析、估值方法的局限性说明

本报告所包含的分析基于各种假设，不同假设可能导致分析结果出现重大不同。本报告采用的各种估值方法及模型均有其局限性，估值结果不保证所涉及证券能够在该价格交易。

法律声明

开源证券股份有限公司是经中国证监会批准设立的证券经营机构，已具备证券投资咨询业务资格。

本报告仅供开源证券股份有限公司（以下简称“本公司”）的机构或个人客户（以下简称“客户”）使用。本公司不会因接收人收到本报告而视其为客户。本报告是发送给开源证券客户的，属于商业秘密材料，只有开源证券客户才能参考或使用，如接收人并非开源证券客户，请及时退回并删除。

本报告是基于本公司认为可靠的已公开信息，但本公司不保证该等信息的准确性或完整性。本报告所载的资料、工具、意见及推测只提供给客户作参考之用，并非作为或被视为出售或购买证券或其他金融工具的邀请或向人做出邀请。本报告所载的资料、意见及推测仅反映本公司于发布本报告当日的判断，本报告所指的证券或投资标的的价格、价值及投资收入可能会波动。在不同时期，本公司可发出与本报告所载资料、意见及推测不一致的报告。客户应当考虑到本公司可能存在可能影响本报告客观性的利益冲突，不应视本报告为做出投资决策的唯一因素。本报告中所指的投资及服务可能不适合个别客户，不构成客户私人咨询建议。本公司未确保本报告充分考虑到个别客户特殊的投资目标、财务状况或需要。本公司建议客户应考虑本报告的任何意见或建议是否符合其特定状况，以及（若有必要）咨询独立投资顾问。在任何情况下，本报告中的信息或所表述的意见并不构成对任何人的投资建议。在任何情况下，本公司不对任何人因使用本报告中的任何内容所引致的任何损失负任何责任。若本报告的接收人非本公司的客户，应在基于本报告做出任何投资决定或就本报告要求任何解释前咨询独立投资顾问。

本报告可能附带其它网站的地址或超级链接，对于可能涉及的开源证券网站以外的地址或超级链接，开源证券不对其内容负责。本报告提供这些地址或超级链接的目的纯粹是为了客户使用方便，链接网站的内容不构成本报告的任何部分，客户需自行承担浏览这些网站的费用或风险。

开源证券在法律允许的情况下可参与、投资或持有本报告涉及的证券或进行证券交易，或向本报告涉及的公司提供或争取提供包括投资银行业务在内的服务或业务支持。开源证券可能与本报告涉及的公司之间存在业务关系，并无需事先或在获得业务关系后通知客户。

开源证券研究所

上海
地址：上海市浦东新区世纪大道1788号陆家嘴金控广场1号楼10层
邮编：200120
邮箱：research@kysec.cn

深圳
地址：深圳市福田区金田路2030号卓越世纪中心1号楼45层
邮编：518000
邮箱：research@kysec.cn

北京
地址：北京市西城区西直门外大街18号金贸大厦C2座9层
邮编：100044
邮箱：research@kysec.cn

西安
地址：西安市高新区锦业路1号都市之门B座5层
邮编：710065
邮箱：research@kysec.cn