北京天融信教育科技有限公司
参与北京网络职业学院人才培养年度报告

（2023）

企业名称：北京天融信教育科技有限公司

院校名称：北京网络职业学院

目录

一、企业概况

1. 天融信公司介绍

天融信科技集团，1995 年成立，是中国领先的网络安全、大数据与安全云服务提供商。从 1996 年率先推出填补国内空白的自主知识产权防火墙产品，到自主研发的可编程 ASIC 安全芯片，再到全球首发新一代可信并行计算安全平台；天融信公司坚持自主创新路线的同时完成了国内安全产品跟随、跟近甚至超越国际知名产品的过渡。2001 年天融信率先推出"TOPSEC"联动协议标准，2005 年提出"可信网络架构（TNA）"，2008 年构建"可信网络世界（TNW）"。

据权威机构统计，天融信品牌连续多年位居中国信息安全产品市场占有率领先地位。时至今日，公司已经发展成为中国知名的信息安全技术研究、产品开发和安全服务的高科技企业，正在努力向世界级信息安全企业的目标迈进。天融信 将"可信网络 安全世界"作为品牌理念，以"可信安全管理(TSM)"为架构核心， 携手客户和合作伙伴整合资源，共同创建一个可信的、自由

的、安全的网络世界。

天融信现有员工约 6000 名，其中研发技术人员超过 4000 名，并设有天融信阿尔法实验室、博士后科研工作站和安全技术基地。其中阿尔法实验室是国内一流的攻防技术研究实验室，多次被国家相关机构评为漏洞报送突出贡献单位。天融信向广大客户提供安全防护、安全检测、安全接入、数据安全、云安全、大数据、安全云服务、云计算和企业无线九大类产品及服务，满足客户的一站式安全需求。

公司现有资质包括:

网络安全应急服务支撑单位证书(国家级)

中国通信企业协会通信网络安全服务能力评定证书（风险评估二级）

中国通信企业协会通信网络安全服务能力评定证书（安全培训一级)

中国通信企业协会通信网络安全服务能力评定证书（应急响应服务一级)

高新技术企业证书

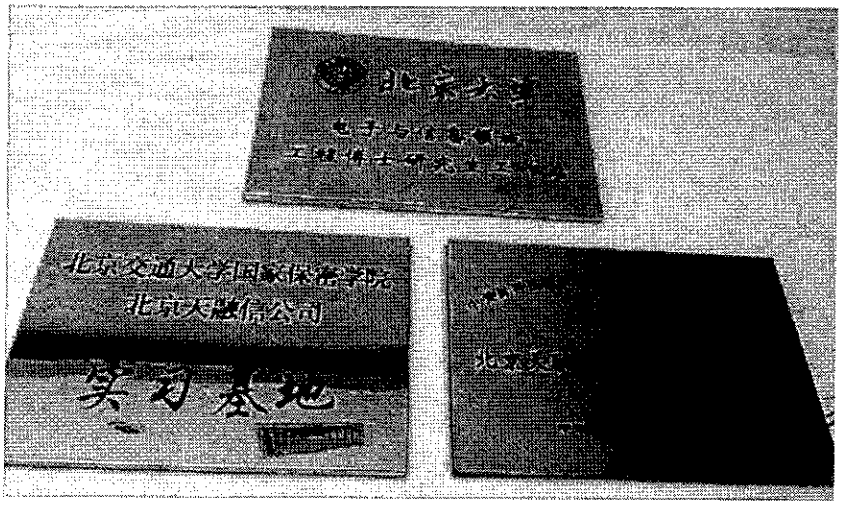
软件企业认定证书

中国保密协会会员单位证书

中国信息安全测评中心　CISP　首家授权单位

全国信息安全职业教育集团第一届理事会理事成员单位

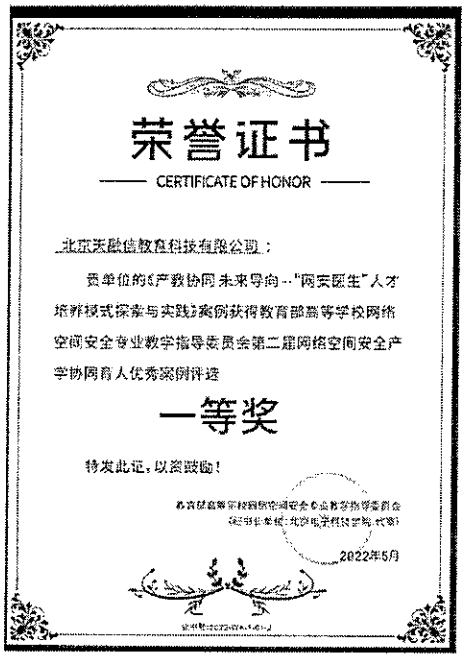
质量管理体系认证证书



二、企业参与办学总体情况

1.专业共建

专业共建截至 2022 年底，已经与 15 所高校签署合作，其中在第二届网络空间安全产学协同育人中四川大学作为优秀安全荣获一等奖，宁波大学科学技术学院作为优秀案例评选并且获二等奖。


荣誉证书

CERTIFICATE OF HONOR

北京天融信教育科技有限公司：

贵单位的《产教协同 未来导向--"网安医生"人才培养模式探索与实践》案例获得教育部高等学校网络空间安全专业教学指导委员会第二届网络空间安全产学协同育人优秀案例评选

一等奖

特发此证，以资鼓励！

教育部高等学校网络空间安全专业教学指导委员会

（秘书长单位：北京电子科技学院 代章）

2022年5月


荣誉证书

CERTIFICATE OF HONOR

北京天融信教育科技有限公司：

贵单位的《宁波大学科学技术学院信息安全专业产教融合校企共建项目》案例获得教育部高等学校网络空间安全专业教学指导委员会第二届网络空间安全产学协同育人优秀案例评选

二等奖

特发此证，以资鼓励！

教育部高等学校网络空间安全专业教学指导委员会

（秘书长单位：北京电子科技学院 代章）

2022年5月

2.攻防实验室建设

“天阶”网络安全攻防对抗平台是天融信打造的原创网络安全平台，已有（42）所高校投入并使用，平台持续更新目前已经到 v4.0 版本，例如宁波大学科学技术学院、金陵科技学院、湖北师范大学文理学院、辽宁理工职业大学、河南科技职业大学、商丘工学院、思源学院、内蒙古机电职业技术学院等等

3.师资培训

天融信教育通过线上或线下等多种形式已与 400 多所高校完成师资培训，以企业需求为导向，紧跟网络安全发展趋势，支持网络安全攻防课程群建设，使得培养方案更加契合网络安全行业的发展需要。

4.网络安全学院建设

宁波大学科学技术学院、金陵科技学院、湖北师范大学文理学院、太原理工大学、山西大学、北京网络职业学院等校企双方共建网络安全现代产业学院，挂牌天融信网络安全人才基地，共建网络安全产业学院，校企双方设立专业建设指导委员会，邀请校方专业老师参加网 络安全教材的研发，并在出版时署名学院及老师；在学院设立学科建 设中心，双方围绕学校的特色专业共同打造优质学科群。

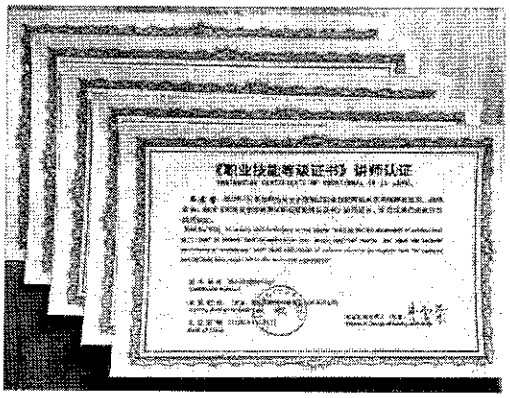
5.1+X 证书建设

5.1 师资培训：网络安全渗透测试 2022 年师资培训 2 次即 2022 年 1 月 5-8 日，2022 年 7 月 11 日--7 月 15 日共计 172 所院校高职院校 77 所，本科院校 83 所，行业客户 12 家两次培训共计培训课时 64 课时，培训 455 人次，签发证书 402 张；

5.2 考前培训：网络安全渗透测试 2022 年考前培训 2 次即 2022 年 11 月 15-16

日（初级）；2022 年 11 月 17-19 日（中级），共计培训 285 人次，10 所院校，预计 2022 年 12 月 27 日组织考试；

5.3 考点申报：2022 年在山西、内蒙古、山西、湖北、北京申报考核站点；



6.产教融合协同育人

在教育部指导下，开展产学合作协同育人项目，包含新工科建设、教学内容和课程体系改革、师资培训、实践条件和实践基地建设、四大类已立项 400 余个项目，270 与所院校。

（一）新工科建设项目

面向开设或拟开设“网络安全”、“数据安全”、“大数据”、“人工智能”等专业（或方向）的本科院校。高校在新工科建设与实践方面有明确的思路和具体规划

（二）教学内容和课程体系改革项目

1.示范课程建设项目。成果须包含课程内容和典型教学案例两部分，形成完整的项目建设内容。申报课程应以现有课程为基础，要求该课程至少已开设 2 年以上。不接受之前没有开课基础的课程申报；申报课程学时安排应不少于 32 学时，平均每年开课次数不少于一次。同等条件下，优先考虑受益面大的课程申报。

2.教改项目。之前在相应课程建设和教学方面已经积累 3 年或以上经验。请选择具体课程方向，专注于某门课程、课程群或者专业，形成有参考和实践价值的教学改革方案。请具体明确该教学方案将是可公开、可共享的。同样地，教改方案需要包含完整的开发资料，不仅限于发表教改论文。

（三）师资培训项目

将针对网络安全、数据安全、大数据、人工智能等主题与伙伴高校合作举办师资培训与课程建设研讨班，承办师资培训活动的高校须提供 100 平米以上的培训场地（符合标准机房建设要求，PC 机数量 30 台及以上）和必要的教学设备（如投影仪、教师机等）。

（四）实践条件与实践基地项目

将针对开设有网络安全、大数据、人工智能等专业（或方向）的高校共同建立联合实践基地，申报高校需要满足硬件及专业建设与教育教学的相关要求，其中

1. 基础设施

（1）实验室使用面积 100 平米以上，符合实验室机房建设标准要求；

（2）实验室 PC 机数量 30 台以上，满足 30 人以上授课使用；

（3）实验室须提供必要的教学设备（如投影仪、教师机等）；

（4）实验室具备 Internet 网络功能，带宽不低于 10M。

2. 专业建设及教育教学方面

院校要明确实践基地在院校未来专业建设及人才培养上的必要性，包括本专业未来的人才培养目标及人才培养规模；具备利用实践基地提升人才培养及专业建设的水平；明确实践基地未来的发展规划及阶梯化的建设远景。

此外请注意：每位老师请申报上述项目中的一项，我们不鼓励多项申报。对于之前 3 年内已经获得同类资助的老师，我们不再接受申报。但欢迎进行错开申报，即选择申报其它未获得过该类资助的项目类型。

三、企业资源投入

1. 有形资源

1.1 从 1996 年率先推出填补国内空白的自主知识产权防火墙产品，到自主研发的可编程 ASIC 安全芯片，到云时代超百 G 机架式"擎天"安全网关，天融信坚持自 主创新完成了国产防火墙跟随、跟近甚至超越国际知名产品的过渡。连续 10 年以上位居中国信息安全市场防火墙、安全网关、安全硬件第一，天融信始终引领和见证着中国信息安全产业发展的每一个里程碑。

1.2 早在 2004 年，天融信就成立了"天融信安全运维中心"，为企业用户提供安全运维外包服务，这是国内第一个商业化的安全运维服务组织。2007 年起，天融 信分别与电信、联通合作，成立了两家安全运维中心，充分利用双方的优势资源为广大企业客户提供安全运维服务。2012 年天融信互联网安全云服务中心成立， 可为全国范围内的企业用户提供 7*24 小时远程安全事件监控、分析、预警和响应服务，同时可提供本地化的现场运维服务，帮助用户快速、有效地解决安全问 题。经过八年多的探索与发展，天融信带领着 7000 余名的优秀员工累计为 5800 多家企业提供过远程安全

运维服务。

1.3 网络无界、安全无限，天融信正以全球视点，推动安全业务的稳步发展。天融信是 INTEL 全球信息安全合作伙伴，并在北京建有联合实验室，致力于 INTEL 架构平台在安全领域的开拓性研究。天融信还在美国硅谷建设了**中国第一个海外安全分析与监测实验室**，全面跟踪国际互联网安全态势。

2. 无形资源

2.1 公司自 2019 年发布云计算产品以来，产品与解决方案持续完善，行业客户实现快速覆盖。报告期内，公司持续加大分布式存储、服务器虚拟化、云容器、桌面虚拟化等核心技术研发，发布了多云融合的“天融信太行云”2.0、支持双栈融合的超融合 2.0、VDI+VOI+WDI 三引擎合一的桌面云 3.0 以及国产化桌面云产品，并与腾讯深度合作联合发布太行云一体机，为客户提供集 IaaS、PaaS 于一体的综合私有云解决方案，为客户业务安全上云、数字化转型、敏捷交付奠定基础，现已在政府、医疗、教育、企业、运营商等 10 余个行业形成规模化应用。同时，公司进一步将自身安全基因融入云计算产品体系，在云计算平台上新发布包括下一代防火墙、安全审计、漏洞扫描、基线管理、安全策略管理等 11 种安全网元，保障云上业务安全运行。报告期内，公司作为

核心成员单位参与《面向云计算的超融合系统技术要求》等4项云计算相关标准制定。截至报告期末，公司已拥有云计算专利34项，参与9项国家标准、行业标准、白皮书编制，牵头或参与多项国家项目攻关。在国产化生态建设方面，公司云计算产品全面支持国内外主流服务器、操作系统、数据库、中间件等，目前已取得兼容性认证60余项。

2.2 自主创新是天融信的基因，开放融合是天融信的理念。作为最早布 局信创产业的网络安全企业之一，天融信从自主ASIC芯片研究到国产CPU芯片应用研究、从推出国内首款自主知识产权的ASIC架构防火墙到发布基于国产软硬件的天融信昆仑系列网络安全产品体系，始终走在网络安全自主创新的前沿。

2.3 国内首屈一指的漏洞挖掘、攻防分析、软件代码分析、安全研究、安全服务人员负责跟踪和分析互联网的安全威胁形势，为所有天融信公司产品提供安全技术、内容 及支持，实时保证了安全产品的有效性。自动化的互联网应用与内容分析平台及持续人员投入保障天融信各类产品拥有领先的应用识别与内容分析能力。可编程 ASIC安全芯片及高性能加密芯片的研制开发为相关安全硬件产品提供了强大的动力，实现了安全产品的高性能。云计算、工业系统、物联网、IPV6、WLAN等新兴产业或业态的安全研究也取得众多阶段性成果或者局部应用。

2.4 虚拟化及安全技术的创新性研究将极大地提升终端安全及云端安全的防护水平。国内可靠性最高、性能最强、网络适应性最

好的网关专用安全操作系统保证了天融信 防火墙在银行、证券、电力等关键行业的大规模应用与高占有率。高度集成的一体化智能过滤引擎技术能够在一次数据拆包过程中，对数据进行并行深度检测，保证 了协议深度识别的高效性。基于更大规模、更多种类的数据采集、存储、处理、关联分析的安全管理平台将真正成为客户安全运维与管理神经中枢。

2.5 伴随客户业务、安全需求以及数据安全技术的发展，数据安全建设已逐步进入体系化、工程化阶段。基于“自上而下、分域管控、持续运营”的整体数据安全防护理念，报告期内公司推出涵盖数据安全治理评估、数据安全组织结构建设、数据安全管理制度建设、数据安全技术保护体系建设、数据安全运营管控建设及数据安全监管建设的“六步走”数据安全治理体系，在政府、运营商、能源、金融、教育等 10 余个行业大型客户中规模化实践落地，同时，项目覆盖范围已延展到工业互联网、车联网等领域。在数据安全标准建设方面，公司累计主导或参编数据安全相关国家/行业标准 35 项，申请专利 50 余项，报告期内重点参与运营商及互联网行业，以及车联网、工业互联网领域相关标准编撰，在重点领域持续深耕。

2.6 公司提出“基于 IPDRR 的工业互联网安全解决方案"，从识别、防护、检测、响应与恢复方面落实安全能力的全面覆盖，并以此为基础向工业互联网数据安全、工业互联网应用安全持续拓展与实践。结合工业领域数字化发展与整体安全需求，公司率

先提出将功能安全与信息安全充分融合的"双安融合"理念。面向工业互联网全业务流程，公司围绕设备、控制、网络、标识、平台、数据安全防护需求进一步提升了工业互联网场景化安全防护能力。在标准建设方面，报告期内，公司重点参与 10 余项工业互联网领域标准制定，涉及工业企业安全数据分类分级、工业防火墙、工业网络安全隔离与交换系统等方向。

3. 人才资源

3.1 天融信早在 2000 年就已经开展网络安全培训，2017 年正式成立天融信教育公司开展职业教育方面的探索，截至目前已与全国 **80** 余所知名高校建立校企合作机制，每年向国家输送大量网络安全专业人才，完成 **200+**产学合作协同育人项目。

3.2 天融信是注册数据安全治理专业人员认证（CISP-DSG）、数据安全官（CISP-DPO）的独家运营机构，也是 CISSP、CISP、CISP-PTE、CCSK、CCSRP 等网络安全人才认证证书的授权培训机构。截至目前，天融信已拥有九大培训资质，累计为国家培养了**上万名专业持证人员。**

3.3 天融信一直关注基础学科研究，大力支持从安全理论到安全实践的多项赛事，已连续六届联合主办全国高校密码教学挑战赛、连

续三届独家支撑世界智能网联驾驶挑战赛、连续三届支撑大学生信息安全竞赛创新实践能力赛等专业赛事，不断探索和拓宽网络安全人才挖掘和培养模式。

3.4 天融信作为“网络安全万人培训资助计划”培训机构，2021 年首批签约入驻国家网络安全人才与创新基地，并携手网络安全人才培养与创新基地、武汉大学和华中科技大学等成立校企联合培养中心，为校企合作育人提供重要平台。截至目前，已累计开展网络安全培训 20 期，共计 6 万余学时课时，**累计培养专业人员 2000 余人。**

3.5 2022 年，在中央网信办指导下，网络安全学院学生创新资助计划正式启动。天融信作为资助方之一，与其他网信企业、中国互联网发展基金会网络安全专项基金共计出资 7800 万元，连续五年资助 1200 名学生开展创新研究，并对资助学生择优奖励。**截至目前，天融信已完成上海交大、中科大、武汉大学、北京邮电大学等十所一流网络安全学院示范高校资助计划的宣讲工作。**

四、企业参与教育教学改革

1. 专业共建

1.1 金陵科技学院

金陵科技学院网络安全学院与天融信教育合作信息安全（嵌入式）专业，校

企互为补充，优势明显：一方面高校可通过专业重组、方向组建，推动了高校特色专业的发展；另一方面通过与天融信教育合作，利用企业资源完善实践教学环节，充分了解网络信息安全企业对人才的需求，获得了企业一线实践技能。双方多年校企合作的实践，从人才培养到师资培训，再从课程建设到实验实训基地建设，双方在多领域的深度合作。

1.1.1 专业特色

（1）实战型的课程驱动就业，全面还原职场真实体验，所有知识体系与技能体系，全部由项目反推还原，使学生在切身体验中领悟职场技巧；

（2）去掉讲师岗位由项目经理角色替代，使之快速掌握安全项目的基本技能，达到真正能满足企业用人需求，填补国内安全项目大量用人荒的局面；

（3）师资力量的保障。项目经理全部为 10 年以上授课经验+安全项目经验；

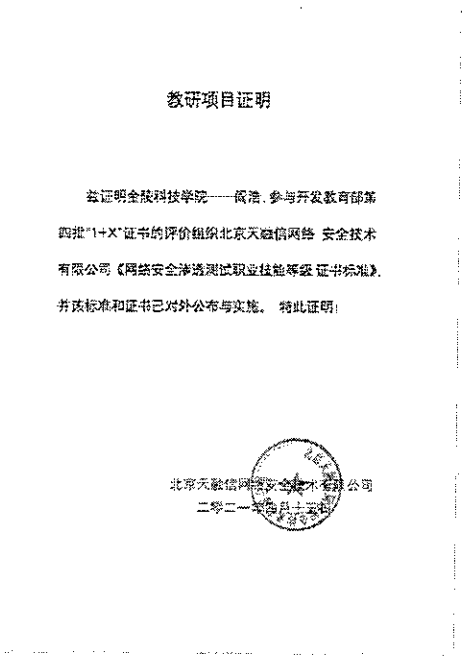
（4）齐全的资源保障。为所有学说提供高质量的培训课件、教材及考试学习手册、复习资料,全面融合人才培养方案；

（5）就业保障，天融信具备完善的学生就业服务体系，从：就业前——就业中——就业后，多个维度帮助辅导学生进行择业就业，为学员提供管家式就业服务。

1.1.2 教育部 1+X 证书《网络安全渗透测试职业技能等级证书》标准起草和证书论证

1+X 证书体系建设，是党中央、国务院出台"职教改革 20 条"方案后，教

育部在职业教育领域的一次系统性改革。1+X 证书体系建设是明确写入《国家职业教育改革实施方案》和《教育部办公厅等三部门关于推进 1+X 证书制度试点工作的指导意见》等政策文件中的，也是各级教育行政主管部门着力推动的一项重点工作。教育部负责政策统筹，职业教育中心研究所负责专业指导，国家开放大学负责综合平台建设，各省级教育行政主管部门负责统筹本省试点工作。天融信联合金陵科技学院在内的 14 家高校、协会和龙头企业共同成功申报了《网络安全渗透测试职业技能等级证书》



教研项目证明

兹证明金陵科技学院——倪浩，参与开发教育部第四批"1+X"证书的评价组织北京天融信网络 安全技术有限公司《网络安全渗透测试职业技能等级 证书标准》，并该标准和证书已对外公布与实施。 特此证明！

北京天融信网络安全技术有限公司

二零二一年[illegible]

1.1.3 教育部产教融合协同人项目合作

产教融合项目是高等学校教育教学改革有利于发挥学校和企业的各自优势，共同培养社会与市场需要的人才，是特色办学的显著特征之一，有助于加强学校与企业的合作、教学与生产的结合。校企双方互相支持、互相渗透、双向介入、优势互补、资源互用、利益共享，是实现职业教育现代化，促进生产力发展，使教育与生产可持续发展的重要途径。

2021 年（未立项），通过教育部共有 6 个项目在新工科建设项目合作。

项目批次	项目类型	项目名称	项目负责人
2021 年 5 月	新工科建设项目	新工科背景下《信息安全管理与法律规范》课程教学内容的建设和改革	邱硕
2021 年 5 月	新工科建设项目	新工科背景下《计算机网络与安全》课程建设和改革	柳亚男
2021 年 5 月	新工科建设项目	《信息隐藏技术》线上线下混合教学模式改革与实践	吴秋玲
2021 年 5 月	新工科建设项目	新工科背景下密码学教学模式探索与实践	黄丹丹
2021 年 5 月	新工科建设项目	面向新工科的应用型本科院校信创 人才培养生态系统的研究和实践	肖芳雄
2021 年 5 月	新工科建设项目	新工科背景下的 Web 应用系统安全性设计	朱咸军

1.2 宁波大学

宁波大学科学技术学院与天融信教育合作计算机科学与技术专业（信息安全实验班），校企互为补充，优势明显：一方面高校可通过专业重组、方向组建，推动了高校特色专业的发展，增加了学校品牌专业；另一方面通过与天融信教育合作，利用企业资源完善实践教学环节，充分了解网络信息安全企业对人才的需求，获得了企业一线实践技能。双方多年校企合作的实践，从人才培养到师资培训，再从课程建设到实验实训基地建设，双方在多领域的深度合作。

1.2.1 2018 级顶岗实习情况

按照人才培养方案要求，2018 级本学期开展顶岗实习，共计 35 人，其中天融信集团实习 17 人，其他企业 18 人，参与企业顶岗实习安服岗位 17 人，渗透测试岗位 10 人，其他相关安全运维和安全测试岗位 8 人。顶岗实习工资 5000 元以上 3 人，4000-5000 元 10 人，3000-4000 元 21 人，不足 3000 元 1 人。整体顶岗实习平均薪资符合市场规律，（高于同类计算机科学与技术、软件工程等专业顶岗实习工资。

1.2.2 教育部 1+X 证书《网络安全渗透测试职业技能等级证书》标准起草和证书论证

1+X 证书体系建设，是党中央、国务院出台"职教改革 20 条"方案后，教育部在职业教育领域的一次系统性改革。1+X 证书体系建设是明确写入《国家职业教育改革实施方案》和《教育部办公厅等三部门关于推进 1+X 证书制度试点工作的指导意见》等政策文件中的，也是各级教育行政主管部门着力推动的一项重点工作。教育部负责政策统筹，职业教育中心研究所负责专业指导，国家开放大学负责综合平台建设，各省级教育行政主管部门负责统筹本省试点工作。天融信联合宁波大学科技技术学院在内的 14 家高校、协会和龙头企业共同成功申报了《网络安全渗透测试职业技能等级证书》，其中钟才明教授作为特聘论证专家，符强和张君华老师参与证书的标准起草工作。

教研项目证明

兹证明宁波大学科学技术学院—张君华，参与开发教育部第四批"1+X"证书的评价组织北京天融信网络安全技术有限公司《网络安全渗透测试职业技能等级证书标准》，并该标准和证书已对外公布与实施。

特此证明！

北京天融信网络安全技术有限公司

二零二一年[illegible]

教研项目证明

兹证明宁波大学科学技术学院—符强，参与开发教育部第四批"1+X"证书的评价组织北京天融信网络安全技术有限公司《网络安全渗透测试职业技能等级证书标准》，并该标准和证书已对外公布与实施。

特此证明！

北京天融信网络安全技术有限公司

二零二一年[illegible]

前　言

本标准按照GB/T 1.1-2020《标准化工作导则 第1部分：标准化文件的结构和起草规则》的规定起草。

本标准起草单位：北京天融信网络安全技术有限公司、北京天融信教育科技有限公司、北京天融信科技有限公司、[illegible]通信建设有限公司、[illegible]、华中科技大学、西安邮电大学、[illegible]科技学院、[illegible]师范学院、宁波大学科学技术学院、湖北民族大学、[illegible]职业技术学院、[illegible]职业学院、[illegible]职业技术学院、西藏职业技术学院。

本标准主要起草人：[illegible]、张君华、符强、[illegible]。

声明：本标准的知识产权归属于北京天融信网络安全技术有限公司，未经北京天融信网络安全技术有限公司同意，不得印刷、销售。

1.2.3 教育部产教融合协同人项目合作

产教融合项目是高等学校教育教学改革有利于发挥学校和企业的各自优势，共同培养社会与市场需要的人才，是特色办学的显著特征之一，有助于加强学校

与企业的合作、教学与生产的结合。校企双方互相支持、互相渗透、双向介入、优势互补、资源互用、利益共享，是实现职业教育现代化，促进生产力发展，使教育与生产可持续发展的重要途径。 自 2018 年到 2020 年（2021 未公示立项），通过教育部共有 4 个项目分别在师资培训、新工科建设实践条件和实践基地建设的项目合作。通过师资培训提升专业教师实践授课能力，学院教师先后参加了 2018 年哈尔滨渗透测试技术专项师资培训班，2020 年武汉黄鹤杯网络安全技术论坛，2021 年贵阳 CISP 认证培训班等

项目编号	项目类型	项目名称	项目负责人
202002057023	师资培训	产学合作信息安全方向师资培训	张君华
201902049002	新工科建设	产教融合背景下智能产业应用型人才培养模式研究	符强
201901048003	新工科建设	新工科模式下的信息安全专业建设与实践	符强
201802081005	实践条件和实践基地建设	面向信息安全的实践基地建设	陈勇旗

1.2.4 师资队伍建设

定制化师资培训

信息安全培训领域所积累的丰富经验，并结合天融信自身的强大科研及技术实例，

专门设计制定了专业化的教师培训课程体系；

职业资格认证

为高校教师提供一体化行业认证培训服务，参训教师可通过培训参加 TCSI、CISP 等相关行业认证考试，5 名获得 CISP 证书和天融信师资认证；

顶岗实践

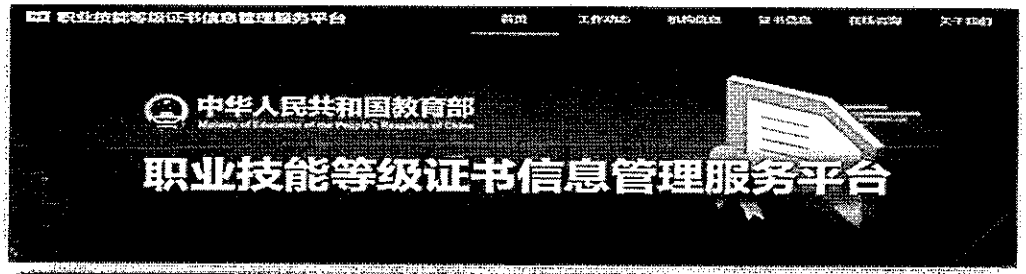
通过“带着教改任务下现场顶岗培训”和“师带徒一对一指导实践”的方式，显著提高教师的专业实践技能和职业教学能力；

主题技能师资培训

基于教育部“协同育人项目”根据各院校人才培养的需求结合网络安全发展态势的师资培训，旨在提升高校教师实训教学技巧与能力参与 4 次师资培训，累计培训 10 名教师；

1.2.5 教研成果输出

天融信联合宁波大学科技技术学院在内的 14 家高校、协会和龙头企业共同成功申报了教育部 1+X 证书《网络安全渗透测试职业技能等级证书》，其中钟才明教授作为特聘论证专家，符强和张君华老师参与证书的标准起草工作



职业技能等级证书

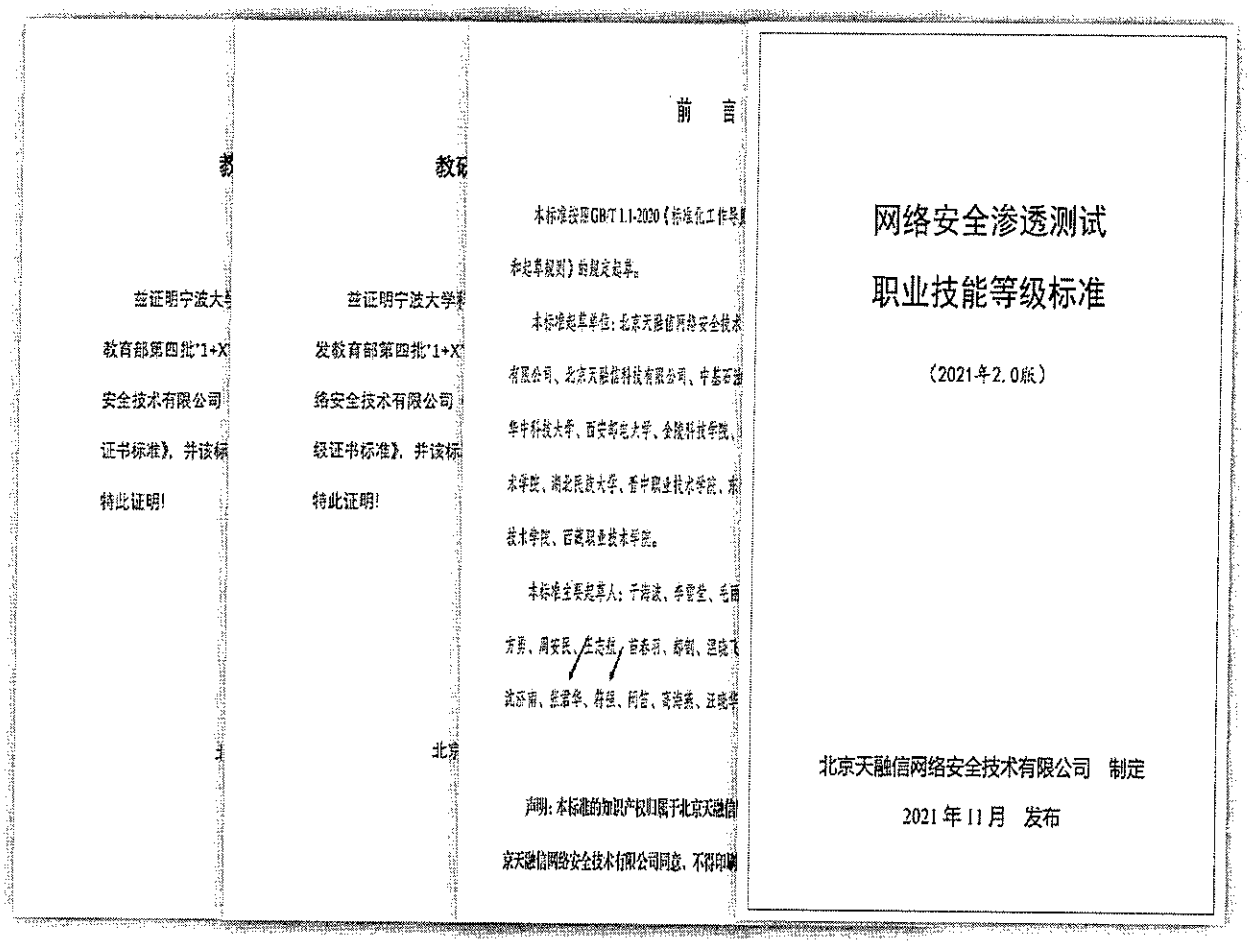
Certificate of Vocational Skill Level

xx 年 xx 月参加网络安全[illegible]职业技能等级水平考核，成绩合格，核发网络安全[illegible]职业技能等级证书（初级），学习成果已获职业教育国家学分银行认定。

This is to certify that [illegible] has passed the assessment in XX XX and is awarded the Primary Level of [illegible] The learning outcomes are recognized by the National Credit Bank for Vocational Education.

xxx
xxx xxx xxx

身份证号：
ID Number
证书编号：[illegible]
Certificate Number
发证机构：（盖章）
Issuing Authority (Seal)
发证日期：xx 年 xx 月 xx 日
Date of Issue
查询网址：http://www.ncb.edu.cn
Website of Verification
发证机构负责人（签章）：
Person in Charge of Issuing Authority
考核站点负责人（签章）：
Person in Charge of Assessment Site



教

兹证明宁波大学

教育部第四批"1+X"

安全技术有限公司

证书标准》，并该标

特此证明！

教

兹证明宁波大学

发教育部第四批"1+X"

络安全技术有限公司

级证书标准》，并该标

特此证明！

北京

前　言

本标准按照GB/T 1.1-2020《标准化工作导

和起草规则》的规定起草。

本标准起草单位：北京天融信网络安全技术

有限公司、北京天融信科技有限公司、中基石油

华中科技大学、西安邮电大学、金陵科技学院、

术学院、湖北民族大学、晋中职业技术学院、

技术学院、四川职业技术学院。

本标准主要起草人：于海波、李雪生、毛

方勇、周安民、[illegible]、[illegible]、[illegible]、[illegible]、

[illegible]、[illegible]、[illegible]、[illegible]、[illegible]、[illegible]、[illegible]

声明：本标准的知识产权归属于北京天融信

京天融信网络安全技术有限公司同意，不得印

网络安全渗透测试

职业技能等级标准

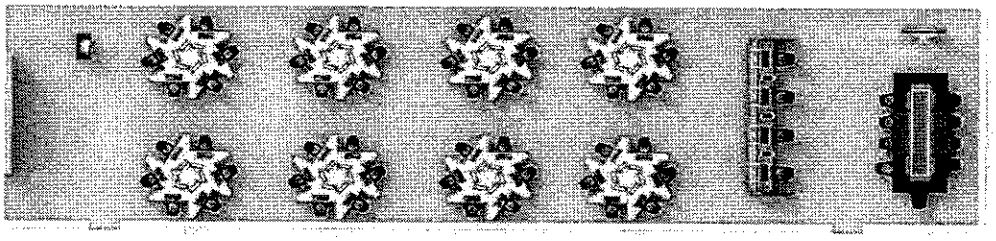
（2021年2.0版）

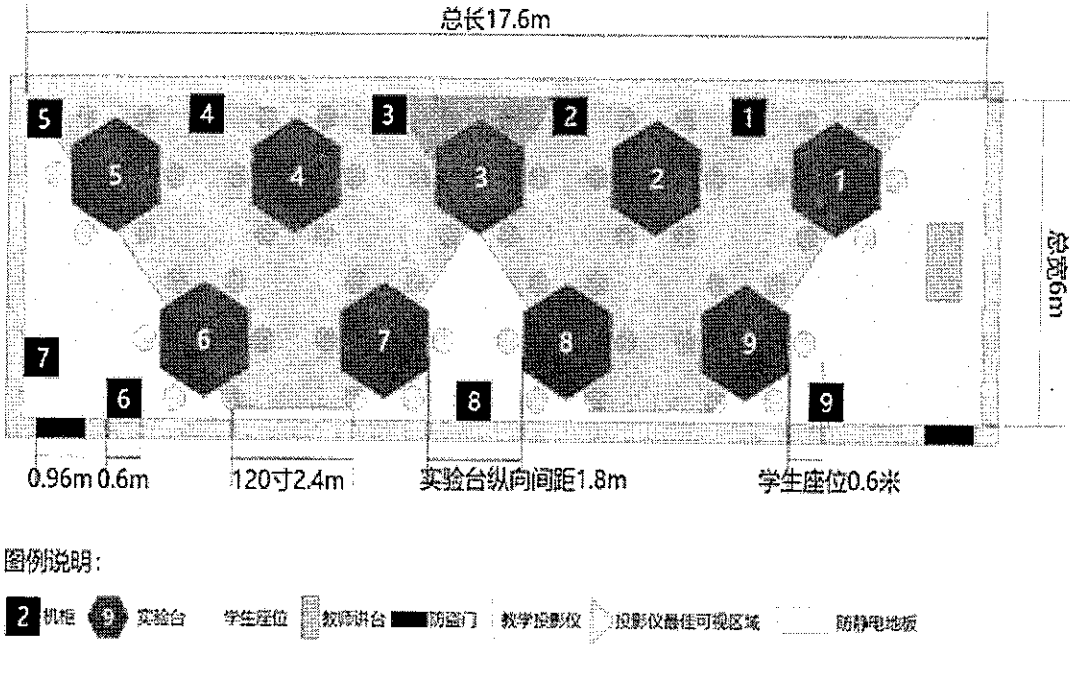
北京天融信网络安全技术有限公司　制定

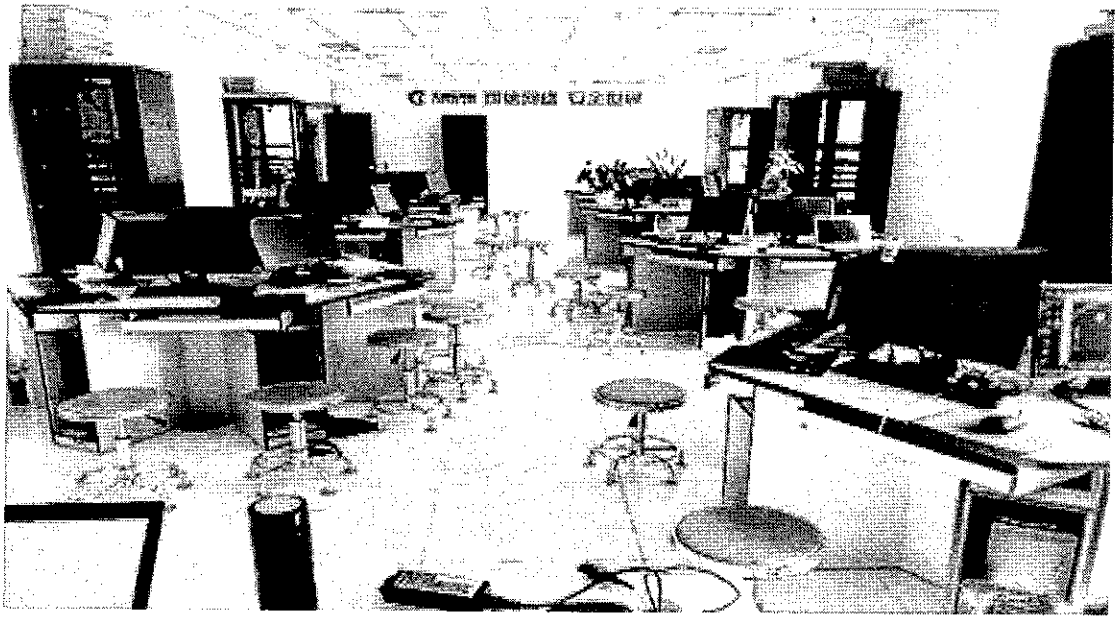
2021年11月　发布

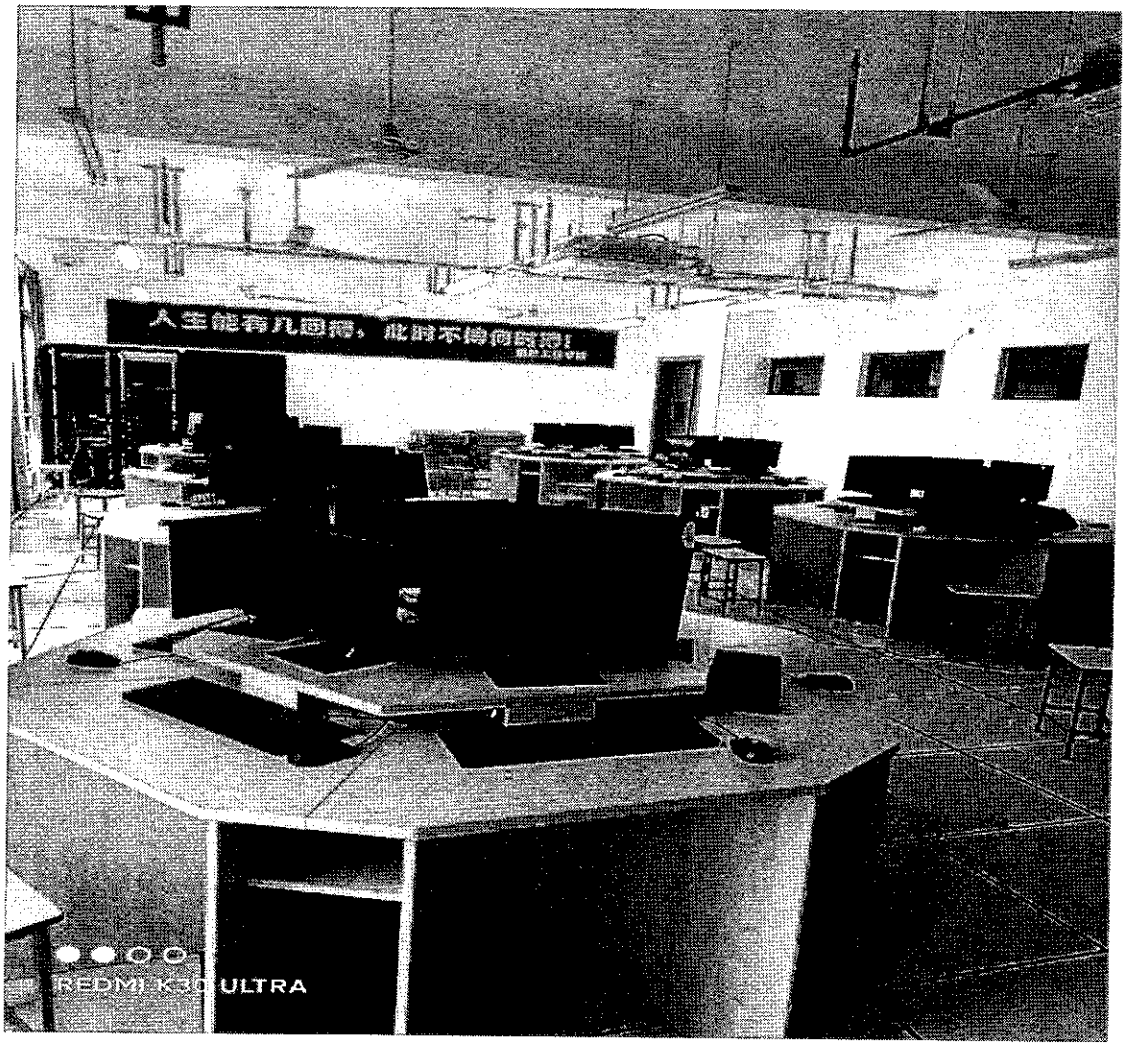
1.2.6 实验室建设

建立实验教学和实验室信息平台，实现网上辅助教学和网络化、智能化管理。建立以学生为中心的管理机制和有利于提高学生能力的多元考评机制，创造学生自主实验、个性化学习的实验环境。建立实验教学的科学评价机制，引导教师积极改革创新。建立实验教学开放运行保障机制，完善实验教学质量保证体系。







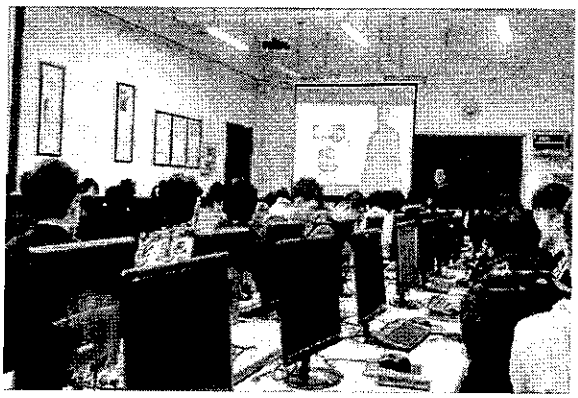

人生能有几回搏，此时不搏何时搏！
REDMI K30 ULTRA

1.3 西安交通大学城市学院

西安交通大学城市学院计算机学院与天融信教育达成合作，对网络工程专业开展产教融合校企合作，双方合作优势：一方面推动计算机学院特色专业的发展，增加学院品牌专业；另一方面利用天融信教育资源完善实践教学环节，使学院领导了解网络安全企业对于人才的需求，以及企业一线实践技能。双方从专业人才培养到核心课程建设，再到专业课程实践条件建设，促进双方在多领域的深度合作。

1.3.1 网络安全宣讲

借助总部“天融信‘活力智行’网络安全校园行”活动，目前已对 17 级至



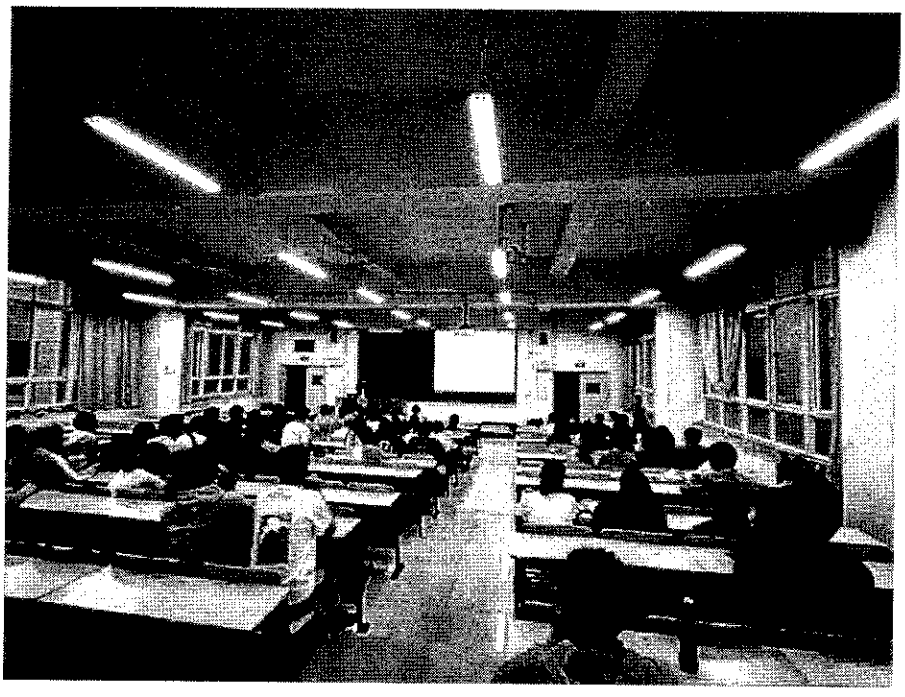
20 级网络工程、计算机应用等专业学生共同开展主题讲座，涵盖网络安全行业分享、技术演示和就业指导，将网络安全脱敏后的实际案例带给学生，并通过讲座拉近与学生的距离，加强天融信在学校的影响。

1.3.2 实习实训

为加大校企合作业务，按照高校课程设计培养方案要求，发挥企业的优势，从 2020 年开始，天融信教育分别承担了 16 级至 19 级网络工程专业学生的生产实习。

1.3.3 课程服务

以校企长期合作为目标，天融信教育承接网络工程专业《网络安全技术与应用》课程教学工作，教学安排为理论 32 课时，实践 16 课时，共计 48 课时。为达到校企双方指定的教学效果，天融信教育为此提供“天阶”信息安全攻防对抗平台，提升实践教学环境。在工程师的言传身教下，学生对理论知识掌握扎实，通过实践环节加强对网络安全技术的理解和应用，在学院对课程的考评中，天融信教育对网络安全的专业性给予赞赏，也为后期与学院开展实验室建设奠定基础。



1.4 太原理工大学

1.4.1 太原理工大学校企合作“3+1”人才培养模式

学校和企业共同完成人才培养，四年制本科学生在校完前三年的学习任务， 最后一年到企业完成实践学习任务。 校企合作共同培养针对企业需要的人才是当今高校教育改革的新课题。

太原理工大学软件学院和北京天融信教育科技有限公司共同开展的网络安全渗透测试方向实习实训把我校学生的教育与企业所需人才的实际需求相结合，根据学分安排和实践操作要求，在大四学年到北京天融信教育科技有限公司的实训基地进行实习实训，由企业的讲师进行授课，使学生们能学到最前沿、最实用的技术，通过理论和实践相结合的方式促进学生实践能力、创新能力和综合素质的培养，实现学校、企业和学生三赢的人才培养模式。

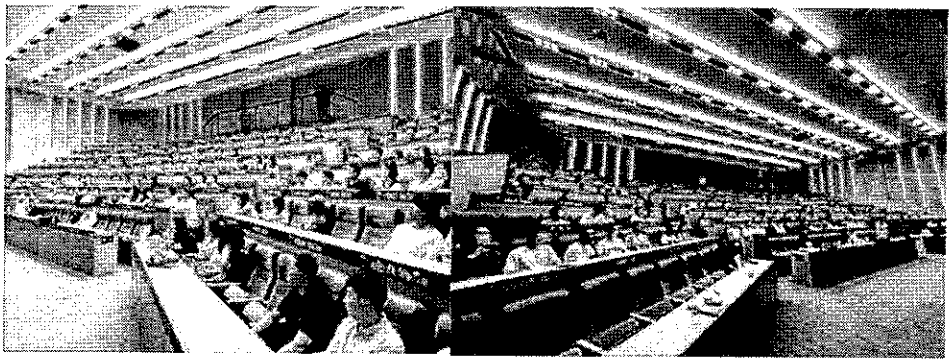
1.4.2 校企合作“3+1”人才培养模式的主要特征

（一）教师和学生的双重角色

在校企合作"3+1"人才培养模式中，教师不仅承担理论教学，而且指导学生的专业技能实践。教师不但要深入企业学习新的专业技能，而且要承担校外学生的实践指导和日常管理任务。学生进驻企业实习，必须以准员工的身份，参与企业所安排的各项工作，服从企业的管理，遵守企业的各项规章制度。不仅要按照学校的计划完成实习任务，而且要履行企业员工的岗位职责，在实践中培养职业技能和综合素质。

（二）高校和企业的协同育人

在校企合作"3+1"人才培养模式中，高校与企业签订合作协议后，人才培养由原先的高校独立培养模式转变为校企合作协同育人模式，教学内容要求理论与实践并重，学生需要通过企业的实战演练来完成实践课程的学习任务。在实践过程中，企业兼职指导教师和学校指导教师必须协同指导学生实践，指导教师和学生是师徒关系。学生在企业必须以准员工的身份参与工作，通过实践掌握工作的基本技能和基本规范，积累相关工作经验，为将来走向社会就业做好铺垫。



1.5 陕西邮电职业技术学院信息工程学院

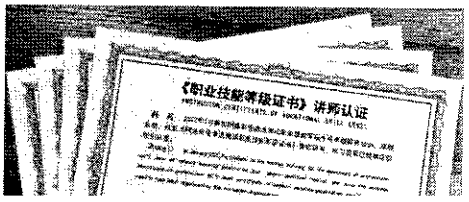
从2019年起，天融信教育与学院开展校企合作，鉴证了学院从计算机系发展成为信息工程学院的全过程，随着校企合作的深度发展，校企双方共同探索出新的合作模式。从2019年竞赛辅导开始，次年开展网络安全宣讲和专业课程实训，在2021年，校企合作达到新高度，共同开展天融信订单班合作，联合培养学生，提高学生就业质量。

1.5.1 网络安全宣讲与课程服务

从2019年至今，每年都会不定期为学院学生开展网络安全宣讲，主要从网络安全行业和网络安全技术开展对网络安全的认知，特别是在每年国家网络安全宣传周期间开展教育宣讲活动。在课程服务方面，通过校企合作加强专业共建，针对计算机网络技术和移动互联应用技术专业核心专业课《计算机网络》《Linux网络管理》《网络安全》开展实训教学，将企业需要的技术能力传授给学生，提高学生对理论知识的掌握。

1.5.2 师资培训

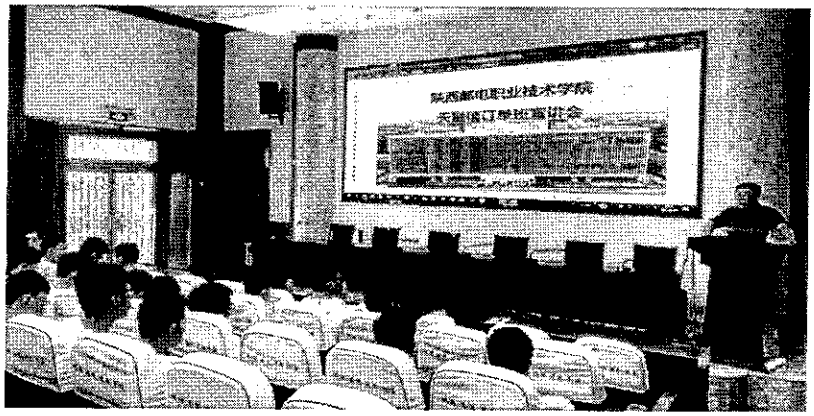
近几年学院热门专业报考学生增多，师资力量扩大，教学能力需要提升，在此背



景下学院组织四位老师，参加天融信教育举办的“天融信 1+X 网络安全渗透测试职业技能等级证书试点院校师资培训”，通过 3 天的线上学习和考试，最终四位老师均获得《网络安全渗透测试职业技能等级证》讲师认证。

1.5.3 专业共建-天融信班

随着网络安全行业的发展，学院越发重视网络安全人才的培养。在前期卓有成效的校企合作背景下，以及院领导对天融信教育西安分公司进行考察和调研后，决定从 2021 年起深化产教融合、拓展校企合作新模式，共同组建天融信班，秉承现代学徒制对学生以技能培养为主的现代人才培养模式，从 21 级计算机网络技术专业 200 多名学生中，遴选出学生组建天融信班。校企双方共同制定天融信班网络安全人才培养方案，第一学期以通识类课程为主，期间企业开展网络安全专项宣讲，加深学生对网络安全的认知，从第二学期至第四学期，校企承担开展核心专业课的教学，包括《网络攻防》《服务器系统安全》等，从第五学期开始，根据天融信科技集团及合作企业用人的需求，后期择优为学生推荐实习岗位，同时加强学生对网络安全核心的技术的掌握。



1.6 山西大学

1.6.1 山西大学校企合作“3+1”人才培养模式

学校和企业共同完成人才培养，四年制本科学生在校完前三年的学习任务， 最后一年到企业完成实践学习任务。 校企合作共同培养针对企业需要的人才是当今高校教育改革的新课题。

山西大学自动化与软件学院和北京天融信教育科技有限公司共

同开展的网络安全渗透测试方向实习实训把我校学生的教育与企业所需人才的实际需求相结合，根据学分安排和实践操作要求，在大四学年到北京天融信教育科技有限公司的实训基地进行实习实训，由企业的讲师进行授课，使学生们能学到最前沿、最实用的技术，通过理论和实践相结合的方式促进学生实践能力、创新能力和综合素质的培养，实现学校、企业和学生三赢的人才培养模式。

1.6.2 校企合作“3+1”人才培养模式的主要特征

（一）教师和学生的双重角色

在校企合作"3+1"人才培养模式中，教师不仅承担理论教学，而且指导学生的专业技能实践。教师不但要深入企业学习新的专业技能，而且要承担校外学生的实践指导和日常管理任务。学生进驻企业实习，必须以准员工的身份，参与企业所安排的各项工作，服从企业的管理，遵守企业的各项规章制度。不仅要按照学校的计划完成实习任务，而且要履行企业员工的岗位职责，在实践中培养职业技能和综合素质。

（二）高校和企业的协同育人

在校企合作"3+1"人才培养模式中，高校与企业签订合作协议后，人才培养由原先的高校独立培养模式转变为校企合作协同育人模式，教学内容要求理论与实践并重，学生需要通过企业的实战演练来完成实践课程的学习任务。在实践过程中，企业兼职指导教师和学校指导教师必须协同指导学生实践，指导教师和学生是师徒关系。学生在企业必须以准员工的身份参与工作，通过实践掌握工作的基本技能和基本规范，积累相关工作经验，为将来走向社会就业做好铺垫。

2. 网络安全学院建设

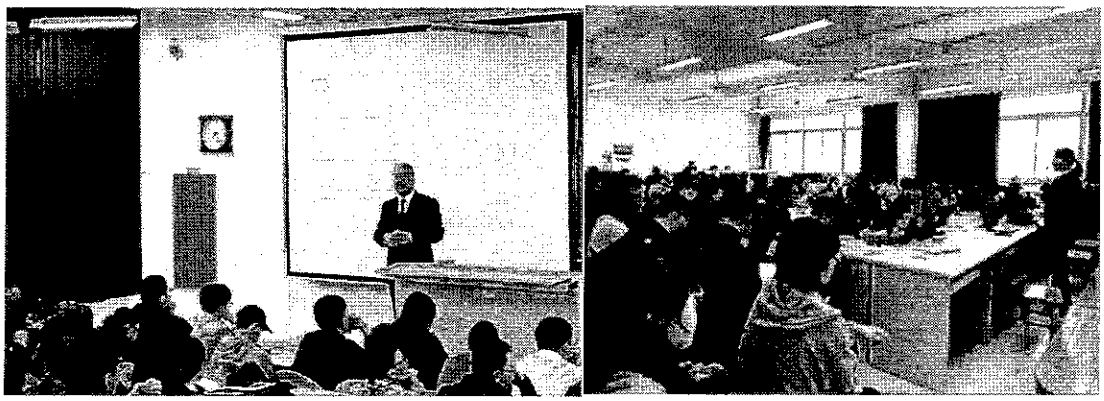
2.1 西安邮电大学

2019 年，西安邮电大学在原信息安全系的基础上，成立网络空间安全学院。也是从这一年起，天融信教育与学院确定了校企合作关系，从开始的举办网络安全宣讲、课程服务，到之后的师资培训、实习实训，再到横向产学协同育人项目合作。直至今日，通过深化产教融合，巩固校企合作，双方共同探讨校企合作新

模式。目前，天融信教育与网络空间安全学院已签署《校企合作框架协议》《校企共建实践中心协议》并完成相互授牌，同时院方聘任天融信工程师为实践中心导师。实践中心的建设将有助于高校引入企业资源与案例，提升高校技术类课程教学效果，促进高校专业学科建设。

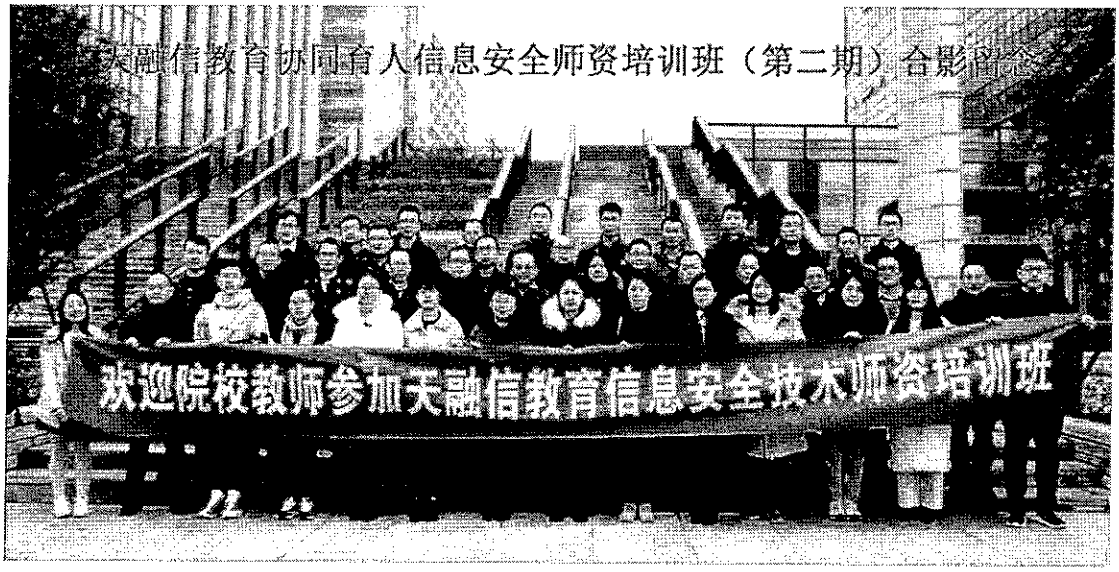
2.1.1 网络安全宣讲与课程服务

“天融信‘活力智行’网络安全校园行”活动，已对 16 级至 20 级信息安全专业和信息对抗专业学生开展不同主题的讲座，涵盖网络安全行业分享，技术演示和就业指导，通过讲座拉近与学生的距离，加强天融信品牌在学校的影响。同时，承接 19 级信息安全专业课程设计，将网络安全脱敏后的项目带给学生。



2.1.2 师资培训与实习实训

在 2019 年，学院委派两位实验室骨干教师参加天融信教育在南京举办的协同育人信息安全技术师资培训班。



从 2019 年开始，天融信教育分别承担了 15 级，17 级，18 级信息安全专业的生产实习，以及 19 级和 20 级信息安全专业的认知实习。

2.1.3 教育部产教融合协同育人项目合作

从 2019 年起，与学院积极开展教育部产学合作协同育人项目，通过师资培训项目，协助提升了一线教师的技术能力和课程建设；通过实践条件和实践基地建设项目的合作，促进了教学改革创新和学生实践能力的提升。

项目编号	项目类型	项目名称	项目负责人
201901048028	师资培训	师资培训项目	于海燕
201901048029	师资培训	师资培训项目	魏雅娟
201902039030	师资培训	师资培训项目	浩明
201902049031	师资培训	师资培训项目	刘意先
202002057024	实践条件和实践基地建设	网络空间安全实践条件与实践基地建设	刘意先

除此之外，天融信教育对接天融信科技集团用人需求，在学院开展天融信专场招聘会，同时学院积极组织老师和学生，参加 2021 一带一路暨金砖大赛之企业信息系统安全比赛。

3. 竞赛指导

3.1 武昌职业学院

2019 年至今，天融信与武昌职业学院从赛事合作（2021 年武汉市第二十二届职业院校网络安全技能大赛、2021 年一带一路暨金砖大赛之企业信息系统安全大赛）、学生实习实训（2019 年、2020 年国家护网行动项目）、组建校内网络安全项目工作室（工作室人员筛选、人员技能强化）、协同申报湖北省高技能人才基地等皆展开实质性的合作，2021 年 12 月 23 日下午，天融信与武昌职业学院电子信息工程学院领导在武昌职业学院 1 号报告厅举行共建产业学院签约仪式。

3.1.1 网络安全比赛合作

为进一步提高大学生网络安全技术水平、攻防实战能力，6 月 19 日上午，以“建党百年展风采 技能建功大武汉”为主题的武汉市第二十二届职业技能大赛在武昌职业学院拉开帷幕，武汉市三十余家职业院校的 800 多名学生同台竞技，天融信作为网络安全赛项技术支持）。

金砖国家技能发展与技术创新大赛是 2017 年金砖国家最高领导人会晤筹备委员会认可、经中华人民共和国外交部同意、金砖国家工商理事会批准的国际大赛。11 月 26 日上午，2021 一带一路暨金砖国家技能发展与技术创新大赛之企业信息系统安全赛项的初赛顺利举行。网络安全赛项由天融信作为技术支撑，本

赛项为团体赛，设专科组、本科组。初赛吸引来自全国各地 70 所院校的 111 支队伍，共 400 余名参赛者进行精彩角逐。初赛为线上理论笔试，历时一个半小时。最终，河南警察学院的两支队伍高居榜首，湖北财税职业学院队伍位列第三。

3.1.2 HW 项目

培训加选拔学生参加 2021 公安部护网行动，武昌职共选出接近 30 人参加到各单位 hw 项目中。

3.1.3 学生实训以及师资培训

2021 年 20 级学生共 100 人参加天融信实习实训，由天融信的黄老师、王老师进行授课工作；以 web 安全渗透与攻防作为实训内容；学院对天融信教育致力于网络安全人才培养的专业性给予赞赏和认可。

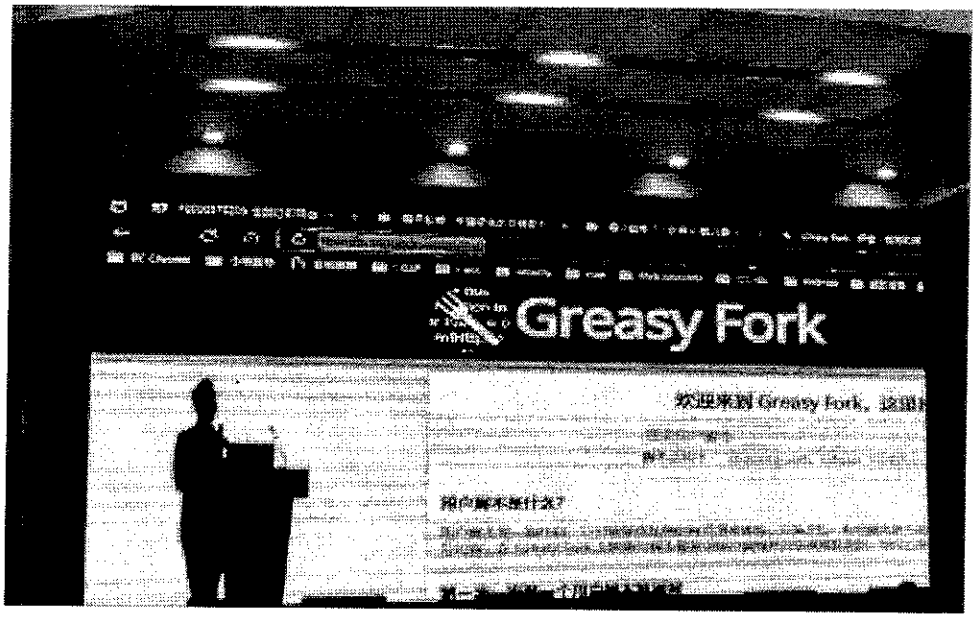
同时为了提高学校老师的实践教学能力，巫院长等三位老师参加天融信教育举办的“天融信 1+X 网络安全渗透测试职业技能等级证书试点院校师资培训”，通过 3 天的线上学习和考试，最终三位老师均获得《网络安全渗透测试职业技能等级证》讲师认证。

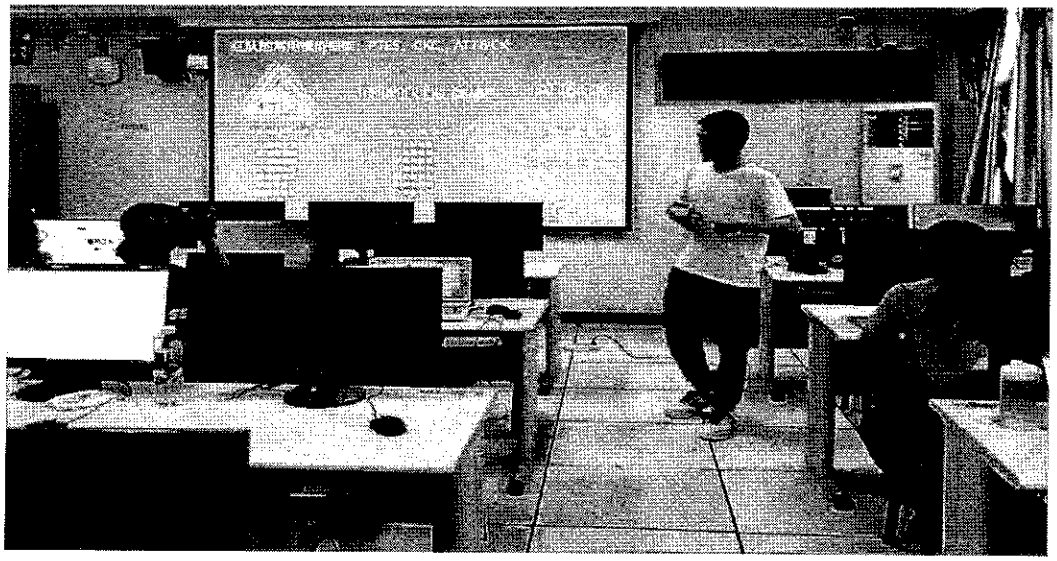
3.2 中南财经政法大学

为深化教育教学改革，深入实施产教融合协同育人，推动复合型人才培养体系建设，10 月 14 日，天融信与中南财经政法大学在中原楼三楼会议室举行校企合作签约授牌仪式。天融信向院校提供企业实战型导师资源、企业岗位实践资源、认证培训资源、实验室专业设备资源等。作为首批入驻国家网络安全人才与创新基地的网络安全企业，积极利用基地培训中心的便利条件，提供一站式服务，提高对师生服务的水平，提高对社会的服务能力，为数字校园发展建设贡献力量。

3.2.1 网络安全宣讲与课程服务

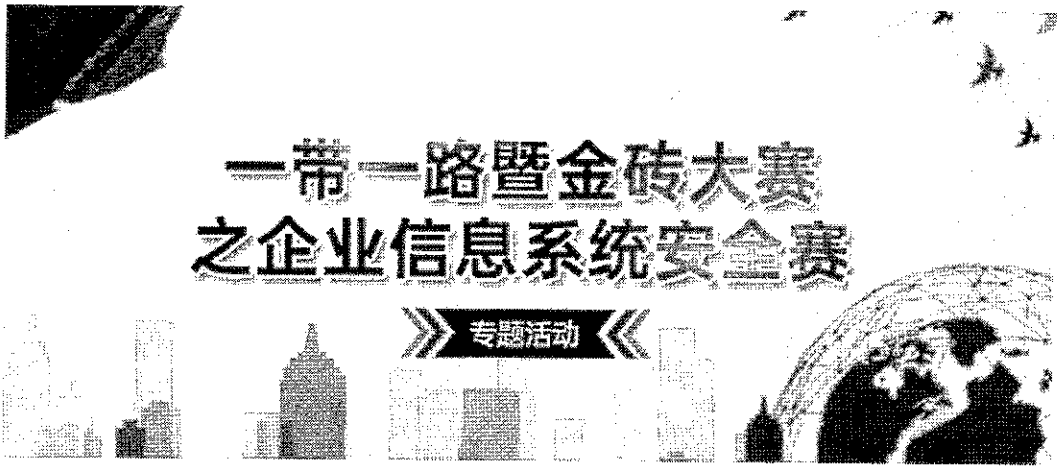
2021 年，开始开展网络安全行业认知学习以及校园招聘活动，同时。在课程服务方面，组织了信息安全管理、计算机科学与技术、大数据管理与应用的本科生以及研究生参与到网络安全实训活动中。





3.2.2 赛前培训及比赛参与

组织了学校学生参与到了金砖一带一路网络安全赛项中，并且赛前组织了两场培训，共四位学员参与其中。



3.3 陕西职业技术学院电子信息工程学院

电子信息工程学院成立于 1999 年，2016 年与上海智翔科技有限公司合作成立“鼎利产业学院”。学院坚持校企合作、产教融合的办学理念，以真实的产业项目、真实的产业工程师授课团队以及生产性的实训教学环境培养高素质的技术技能型人才。

从 2020 年开始，天融信教育与学院网络与信息安全产业团队开展校企合作。通过近两年的合作，现已开展网络安全宣讲，实习实训，师资培训和竞赛辅导等多项合作。鉴于前期校企合作的成果，在院领导和网络与信息安全产业团队到访天融信西安分公司参观和调研后，双方共同秉承“产教深度融合、校企全面合作”

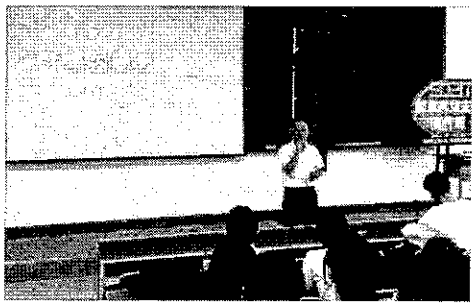
的发展理念，决定签署《校企合作框架协议》。同时，企业授予学院“天融信信息安全协同中心中心”的牌匾，学校授予企业“陕西职业技术学院电子信息工程学院校外实习基地”的牌匾，为后期双方开展校企深度合作奠定了基础。

1.3.1 网络安全宣讲与实习实训

从 2020 年开始，每逢国家网络安全宣传周，天融信教育都会派工程师为学院师生开展以网络安全为主题的系列讲座，同时也会为计算机网络技术专业学生开展网络安全技术分享讲座。同时，天融信教育与网络与信息安全产业团队经

过.

多次交流，制定了一系列产教融合培养网络安全人才的方案。从承接 20 级计算机网络技术专业 WEB 安全实训开始，拉开了校企合作的序幕，通过此次合作，学院对天融信教育致力于网络安全人才培养的专业性给予赞赏和认可。



3.3.2 师资培训和竞赛辅导

学院不仅重视学生专业技能的培养，更加重视“双师型”教师队伍的建设。在 2022 年初，网络与信息安全产业团队的三位老师参加了天融信教育举办的“天融信 1+X 网络安全渗透测试职业技能等级证书试点院校师资培训”，通过 3 天紧张的学习，最终三位老师通过考核获得《网络安全渗透测试职业技能等级证》讲师认证。同时，学院对职业技能大赛给予高度重视，因为大赛是检验学院教育教学水平的重要平台，是职业院校学生提升技能水平，强化素质的重要途径和方式。天融信教育与学院的理念相同，对学院参加陕西省职业技能大赛给予大力支持，在信息安全管理与评估赛项上提供赛前指导和专项训练。

3.4 陕西邮电职业技术学院信息工程学院

从 2019 年起，天融信教育与学院开展校企合作，鉴证了学院从计算机系发展成为信息工程学院的全过程，随着校企合作的深度发展，校企双方共同探索出新的合作模式。从 2019 年竞赛辅导开始，次年开展网络安全宣讲和专业课程实训，在 2021 年，校企合作达到新高度，共同开展天融信订单班合作，联合培养学生，提高学生就业质量。

1.3.2 竞赛辅导

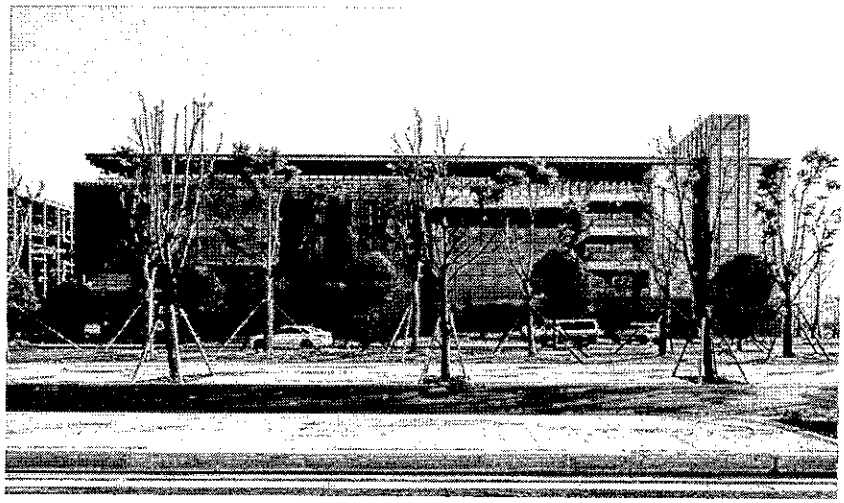
在 2019 年 11 月，学院组队参加“知行杯”中国通信服务职业教育联盟学生职业技能竞赛，得知学院需要赛前辅导后，天融信教育西安分公司领导给予大力支持，工程师对于赛项内容进行分析，对学生进行针对性的指导，最终，学院代表团荣获计算机网络与信息安全项目团体二等奖，其中两位学生荣获计算机网络与信息安全项目个人二等奖，两位学生荣获计算机网络与信息安全项目个人三等奖。通过此次合作，校企合作逐步开展。

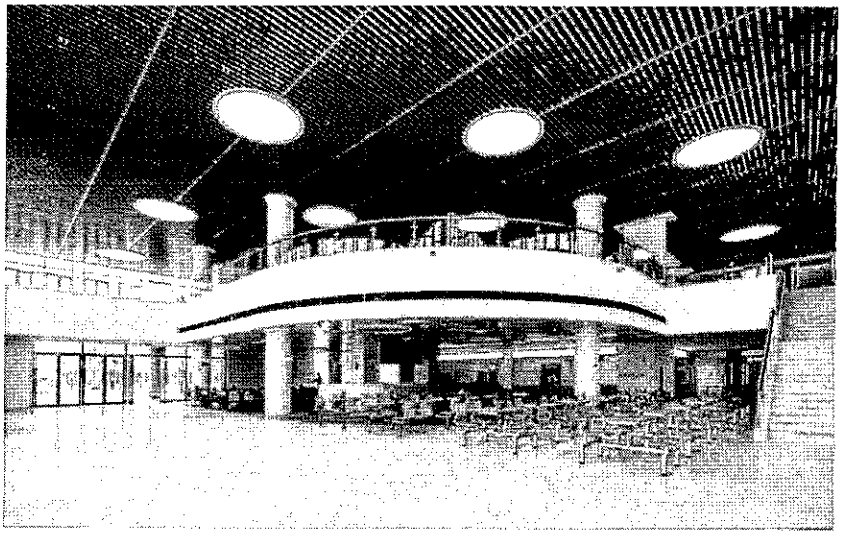
4. 学生培养

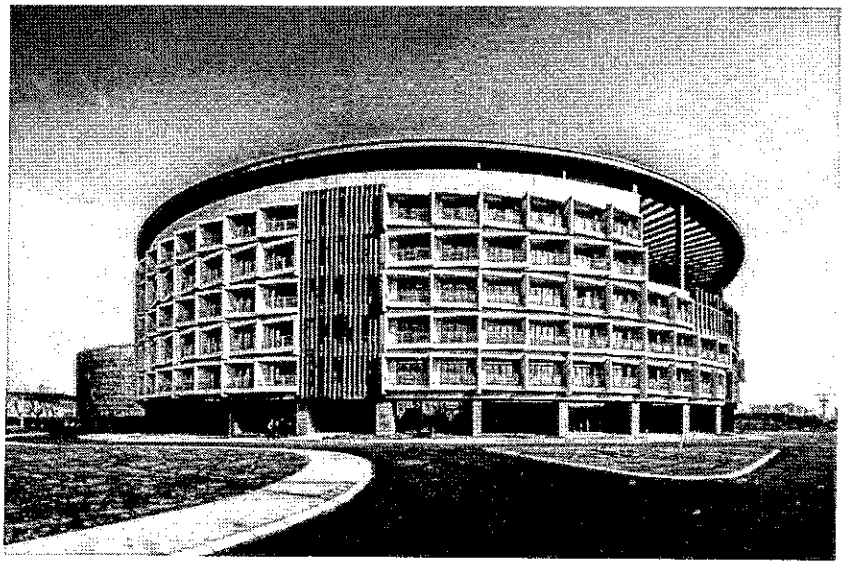
天融信教育每批学员固定分配到北京天融信网络安全技术有限公司，其余均分配到友商公司，如默安科技，奇安信、小米科技、金盾等。

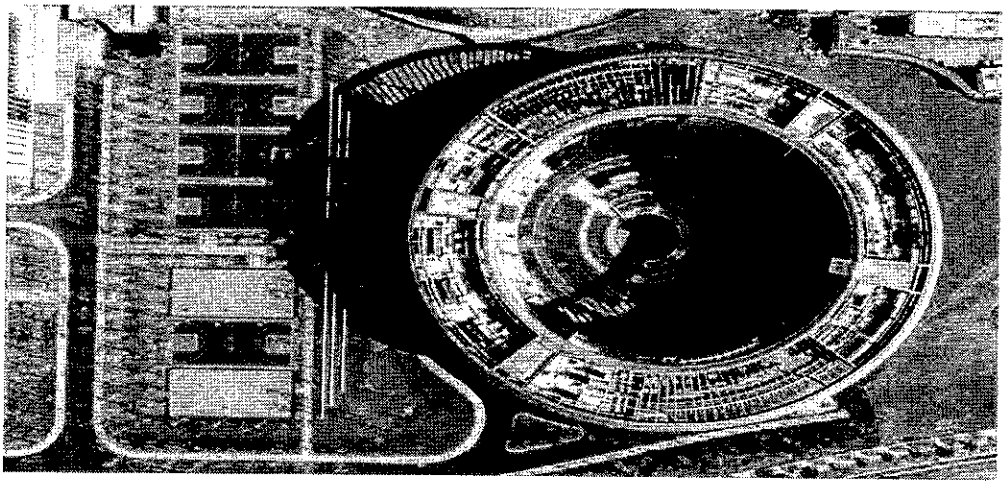
4.1 学生学习基地环境

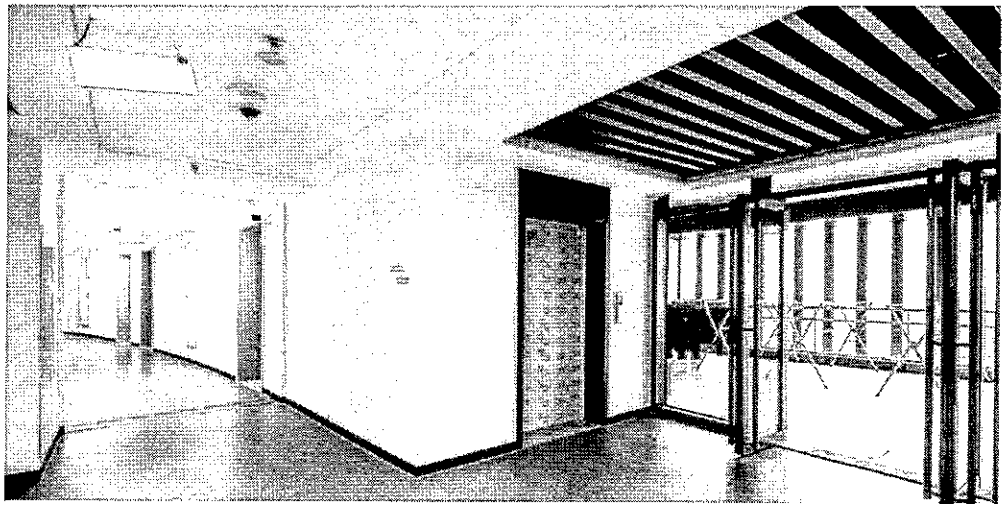
国家网络安全人才与创新基地位于武汉临空港经济技术开发区(东西湖区)。国家网安基地是在中央网信办的指导和支持下，由武汉市承接的我国网络安全领域的重点布局项目。

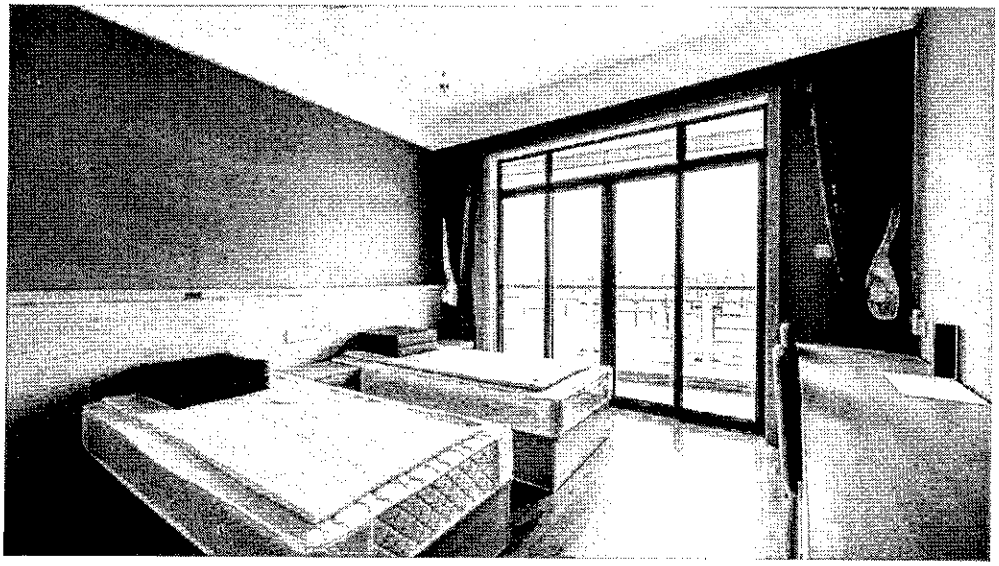












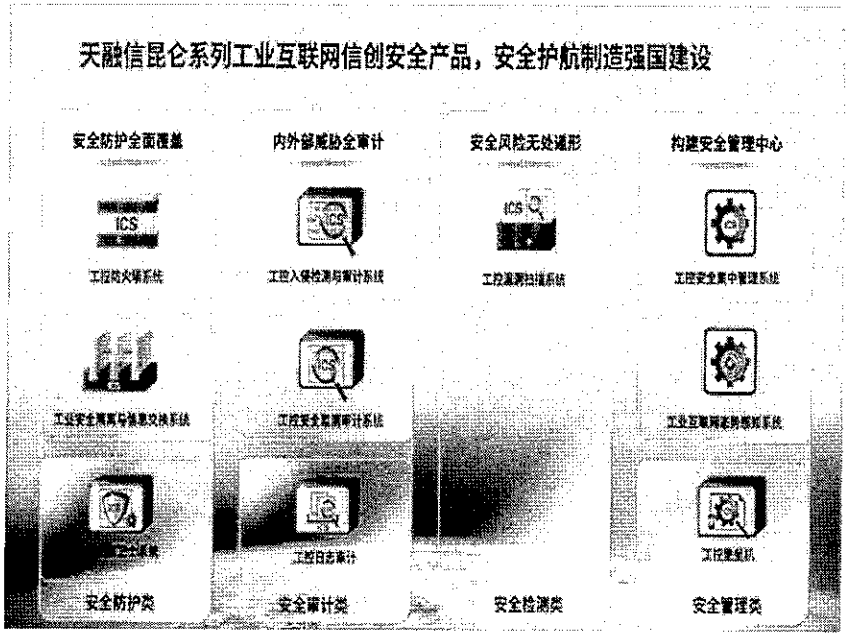
4.2 往期部分学生就业情况

王[illegible]燃	江苏安信息测评认证有限公司	8K	重庆工业建设职业学院	短训	安全服务工程师
金[illegible]辰	网捷信息科技有限公司	9K	宁波大学科技学院	专业共建	安全服务工程师
郭[illegible]昊	小米科技有限公司	20k	宁波大学科技学院	专业共建	安全服务工程师
王[illegible]美	杭州默安科技有限公司	10k	宁波大学科技学院	专业共建	安全服务工程师
陈[illegible]龙	天融信网络安全技术有限公司（杭州）	10k	宁波大学科技学院	专业共建	安全服务工程师
焦[illegible]铭	杭州迪普信息技术有限公司	16K	宁波大学科技学院	专业共建	安全服务工程师
丁[illegible]远	长城汽车	12k	宁波大学科技学院	专业共建	安全服务工程师
李[illegible]乐	杭州默安科技有限公司	10k	宁波大学科技学院	专业共建	安全服务工程师
夏[illegible]耀	杭州安恒信息信息技术有限公司	12k	宁波大学科技学院	专业共建	安全服务工程师
[illegible]曼	网统信息科技有限公司	9k	宁波大学科技学院	专业共建	安全服务工程师
潘[illegible]一民	奇安信科技集团股份有限公司	14k	宁波大学科技学院	专业共建	售前工程师
林[illegible]钧	浙江汇民网络公司	8k	宁波大学科技学院	专业共建	安全服务工程师
路[illegible]阳	北京天融信网络安全技术有限公司	12K-15K/月	哈尔滨信息工程学院	短训	渗透测试工程师
祝[illegible]华	北京天融信网络安全技术有限公司	12K-15K/月	哈尔滨信息工程学院	短训	渗透测试工程师
李[illegible]鹏	北京天融信网络安全技术有限公司	10k	哈尔滨信息工程学院	短训	售后工程师
郭[illegible]航	江苏金恒检测技术股份有限公司	10k	哈尔滨信息工程学院	短训	渗透测试工程师
宁[illegible]青	北京文人网络安全科技有限公司	10k	哈尔滨信息工程学院	短训	渗透测试工程师
赵[illegible]鹏	北京文人网络安全科技有限公司	13k	哈尔滨信息工程学院	短训	渗透测试工程师
梁[illegible]芝	北京文人网络安全科技有限公司	10k	哈尔滨信息工程学院	短训	渗透测试工程师
袁[illegible]芳	奇安信科技集团股份有限公司	9k	山西大学	3+1	售前工程师
李[illegible]蕾	绿盟科技集团股份有限公司	转正12k	山西大学	3+1	售前工程师
韩[illegible]奇	天融信科技集团股份有限公司	转正10k+	山西大学	3+1	安全运维工程师
张[illegible]林	远江盛邦(北京)网络安全科技股份有限公司	转正10-12k	山西大学	3+1	安全运维工程师
姜[illegible]东	远江盛邦(北京)网络安全科技股份有限公司	转正11.5k	山西大学	3+1	安全服务工程师
朱[illegible]雅	天融信科技集团股份有限公司	转正8-10k	山西大学	3+1	安全运营岗
任[illegible]涛	启明星辰信息技术集团股份有限公司	8k	山西大学	3+1	安全服务工程师
乔[illegible]平	信安世纪科技股份有限公司	10k	山西大学	3+1	安全服务工程师
彭[illegible]文	天融信科技集团股份有限公司	转正10k+	山西大学	3+1	安全运维工程师
郝[illegible]明	北京宇信科技集团股份有限公司	转正9-10k	山西大学	3+1	安全运维工程师
侯[illegible]坤	北京安博通科技股份有限公司	10k	山西大学	3+1	技术支持工程师
李[illegible]磊	北京宇信科技集团股份有限公司	转正9-10k	山西大学	3+1	安全运维工程师
李[illegible]雄	启明星辰信息技术集团股份有限公司	9k	山西大学	3+1	安全服务工程师
孟[illegible]磊	信安世纪科技股份有限公司	8k	山西大学	3+1	安全服务工程师
文[illegible]昌	北京安信天行科技有限公司	转正7500	山西大学	3+1	安全服务工程师
赖[illegible]宇	用友网络科技股份有限公司	薪资16k*14	山西大学	3+1	安全服务工程师
翟[illegible]龙	高伟达软件股份有限公司	8k	山西大学	3+1	安全运维工程师
乔[illegible]宏	实习金由云，毕业后去用友	用友15k	山西大学	3+1	安全服务工程师
郝[illegible]钢	上海弈橙科技有限公司	8k	山西大学	3+1	售前工程师
乔[illegible]阳	深信服科技股份有限公司	12000	西安石油大学	短训	安全服务工程师
唐[illegible]青	深信服科技股份有限公司	12000	西安石油大学	短训	安全研究员
贾[illegible]东	绿盟科技集团股份有限公司	9000	西安石油大学	短训	安全服务工程师
王[illegible]铭	绿盟科技集团股份有限公司	9000	西安石油大学	短训	安全服务工程师
李[illegible]星	绿盟科技集团股份有限公司	9000	西安石油大学	短训	安全服务工程师
黄[illegible]伟	绿盟科技集团股份有限公司	9000	西安石油大学	短训	安全服务工程师
刘[illegible]阳	中国电子科技集团有限公司	12000	西安邮电大学	短训	安全服务工程师
赵[illegible]洋	北京百家互联科技有限公司（限推荐）	17000	陕西科技大学	短训	安全运营工程师
赵[illegible]信	上海瀚都信息科技有限公司	10000	西安邮电大学	短训	渗透测试工程师
王[illegible]瀚	奇安信科技集团股份有限公司	9000	西安邮电大学	短训	渗透测试工程师
刘[illegible]江	华为	15000	西安邮电大学	短训	网络安全工程师
王[illegible]慢	中国电子科技集团有限公司	15700	西安邮电大学	短训	安全研究员
陈[illegible]加	深信服科技股份有限公司	12000	陕西科技大学	短训	安全服务工程师
康[illegible]飞	北京仁科互动网络技术有限公司	14000	西安邮电大学	短训	测试开发工程师
高[illegible]磊	中兴通讯股份有限公司	14000	西安邮电大学	短训	安全研究员
华[illegible]鑫	紫光软件系统有限公司	12000	西安欧亚学院	短训	安全技术服务工程师
王[illegible]洋	紫光软件系统有限公司	10500	西安欧亚学院	短训	售前工程师
闻[illegible]杰	紫光软件系统有限公司	10500	西安欧亚学院	短训	安全运营工程师
刘[illegible]宇	紫光软件系统有限公司	10500	西安欧亚学院	短训	售前工程师

五、助推企业发展

5.1 天融信昆仑系列信创网络安全产品体系---加速推进工业国产化

随着《关键信息基础设施网络安全保护基本要求》的发布，以及信创“2+8+N”应用体系需求的全面开展，信创步伐在电力、烟草、石油石化、水利、智能制造、国防科技等领域持续迈进，相关领域的安全保护措施应当与关键信息基础设施同步规划、建设和使用。在国家政策的指引下，天融信以加速推进工业企业数字化转型升级为目标，全面推进全系列工业互联网安全产品实现自主可控、安全可靠，发布安全防护类、安全审计类、安全检测类、安全管理类等 4 大类 10+款国产化工业互联网安全产品。践行功能安全与信息安全深度融合的技术理念，天融信从嵌入式底层技术的整合应用、通信过程行为识别技术的整合应用、安全分析与管理下的融合应用等多个维度，为工业互联网企业构建“双安融合”下的工业互联网安全协同防护体系，形成了覆盖工业企业全场景国产化工业信息安全防护所需的产品体系，真正解决工业企业深层次的网络安全问题，助力数字中国高质量发展。



国家“十四五”时期，信创发展进入加速发展阶段，而建设高质量生态体系是发展的核心和关键。为满足工业企业自主可控安全需求，天融信不断加强与产业链上下游的合作，在基础软件和基础硬件方面共同进行技术、产品、服务的研发和落地，形成合力共同打造国产自主创新生态圈，加速推进工业信息安全自主创新生态建设，共同打造以“中国芯”为底层支撑的系列整机产品与行业解决方案。

天融信昆仑系列信创网络安全产品体系已累计发布 61 类 203 款产品，打造出业界品类最全、数量最多的信创网络安全与云计算产品图谱，并与国产 CPU、操作系统、数据库、浏览器、中间件等生态伙伴积极开展合作，取得 1600+兼容性认证。此外，在工业互联网安全体系新赛道中，天融信始终走在信创网络安全技术应用创新与生态建设的最前沿，打造出满足等保、关保要求且适用于工业全场景的国产化工业互联网安全产品及方案，为国家关键基础设施保驾护航。

公司基于国产软硬件的天融信昆仑系列国产化产品已有 53 款 168 个型号，在信创产品入围中保持品类与型号数量领先，目前产品与解决方案已在党政、金融、能源、交通等 23 个行业实现规模化应用。

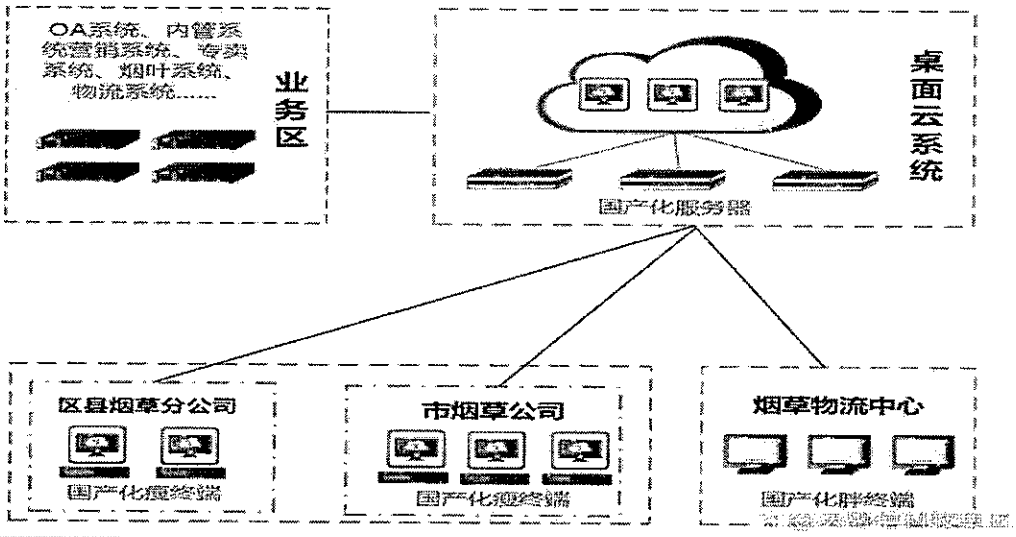
5.2 天融信定制开发地市烟草公司办公网桌面云系统解决方案

当前，数字经济蓬勃发展，数字技术推动千行百业重塑升级，各种新产业、新模式、新业态快速增长。国家政府历来高度重视烟草行业的信息化发展和数字化转型进程，以期进一步提升行业的运营和管理效率，全面适应即将到来的数字经济时代的建设和发展需求。

烟草企业数字化转型，可进一步推动实体经济和数字经济融合发展，加快形成以创新为引领和支撑的数字经济。经过前期调研，天融信发现地市级烟草公司、物流中心存在地理位置分散、终端系统老旧、数据存储混乱等多种安全问题。

针对地市级烟草公司、物流中心业务现状和安全需求，天融信定制开发地市烟草公司办公网桌面云系统解决方案，采用业界主流的 VDI+VOI 复合桌面

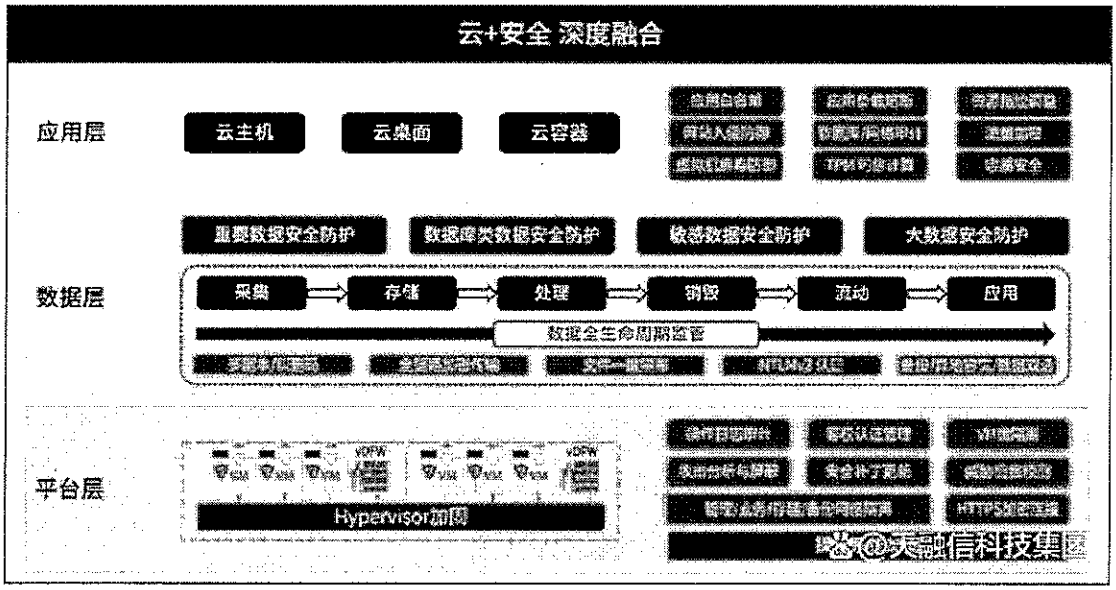
云架构模式，在地市烟草公司建立桌面云统一管控中心进行云桌面资源的集中分配和管控，在办公场所使用瘦终端进行网络接入和桌面资源调用；在物流中心使用胖终端进行模板统一管理和状态监控，以达到各云桌面的统一管理需求。



5.3 天融信太行云解决方案

物流中心涉及工业控制网络使用环境，对网络可用性及稳定性要求极高。因此，该场景更适用于 VOI 架构，将计算级存储资源置于本地，即使出现网络中断的极端情况，仍能保障云桌面的正常使用。同时，采用桌面云管理系统对终端机进行远程管理和维护，降低工作人员现场运维的工作量及时间成本。

云数融合”是大数据应用的发展趋势，越来越多的企业选择数据上云，利用云作为平台支撑，以实现更优的性能扩展与系统维护。天融信将云计算、大数据应用和安全深度融合，基于“太行云内生安全防护体系”，推出天融信太行云解决方案，从平台层、数据层、应用层为客户业务上线即安全提供全面支撑和保障，实现云+安全一体化交付。



截至目前，天融信太行云全力保障电子政务、企业应用、桌面办公、云原生应用等业务的高效稳定运行，已广泛应用于政府、烟草、医疗、卫生、教育、企业、交通等多个行业，为客户持续提供有效、可靠的云+安全的平台。

未来，天融信将基于自身在网络安全领域的深厚积累，持续将云和安全深度融合，提供高性能、高可靠、高安全的云+安全一体化交付能力，从"技术、安全、方案、服务"四个维度打造值得信赖的云专家，赋能各行业数字化转型。

公司自 2019 年发布云计算产品以来，产品与解决方案持续完善，行业客户实现快速覆盖。报告期内，公司持续加大分布式存储、服务器虚拟化、云容器、桌面虚拟化等核心技术研发，发布了多云融合的"天融信太行云"2.0、支持双栈融合的超融合 2.0、VDI+VOI+WDI 三引擎合一的桌面云 3.0 以及国产化桌面云产品，并与腾讯深度合作联合发布太行云一体机，为客户提供集 IaaS、PaaS 于一体的综合私有云解决方案，为客户业务安全上云、数字化转型、敏捷交付奠定基础，现已在政府、医疗、教育、企业、运营商等 10 余个行业形成规模化应用。同时，公司进一步将自身安全基因融入云计算产品

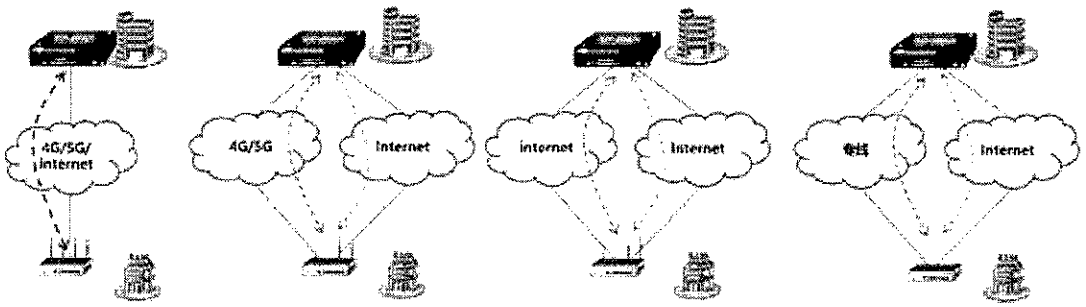
体系，在云计算平台上新发布包括下一代防火墙、安全审计、漏洞扫描、基线管理、安全策略管理等 11 种安全网元，保障云上业务安全运行。报告期内，公司作为核心成员单位参与《面向云计算的超融合系统技术要求》等 4 项云计算相关标准制定。截至报告期末，公司已拥有云计算专利 34 项，参与 9 项国家标准、行业标准、白皮书编制，牵头或参与多项国家项目攻关。在国产化生态建设方面，公司云计算产品全面支持国内外主流服务器、操作系统、数据库、中间件等，目前已取得兼容性认证 60 余项。

5.4 天融信安全 SD-WAN 解决方案

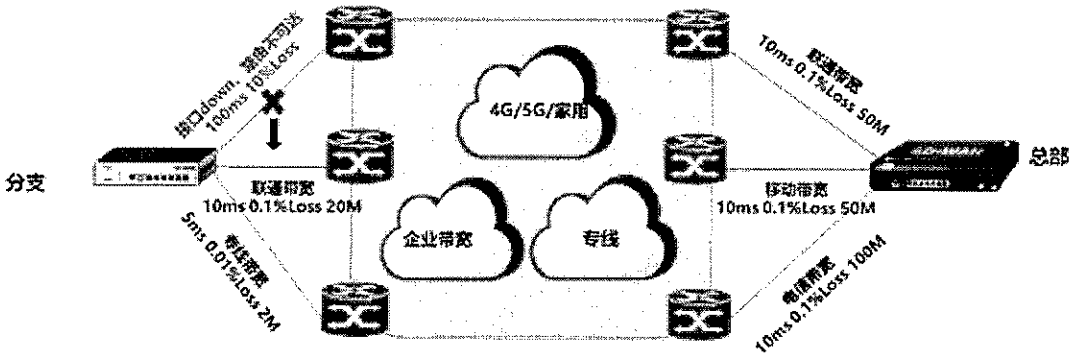
伴随云计算、物联网、虚拟化、5G 等一系列新技术、新场景的快速应用，企业广域网接入需求也在不断提高，而传统静态方式的多分支广域网接入解决方案往往因为成本高、体验差、运维难以及安全性低等问题，成为制约企业实现数字化转型的重要因素之一。

天融信安全 SD-WAN 解决方案根植于安全底层，结合 SDN 技术与广域网优化技术，具备惠智接入、智能路由、安全防护、极简运维四大核心能力，为企业带来高性能、高安全且与实际业务更加贴合的安全组网体验。

惠智接入---天融信安全 SD-WAN 解决方案使客户在使用企业带宽或 ADSL 等廉价宽带接入互联时，大幅度提升业务体验效果，为企业节省了大量的宽带建设成本和时间成本。同时，将 5G 带入总分互联的解决方案中，利用高速率，大容量，低延迟的 5G 技术，帮助客户构建无线融通的组网方案。

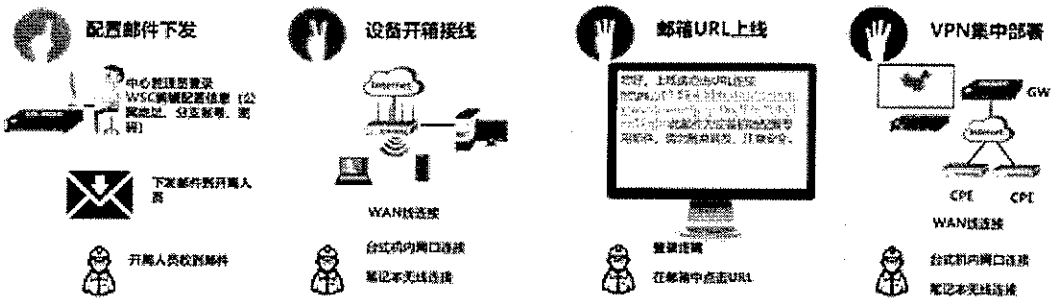


智能路由---近年来随着高带宽应用大量出现，单纯提升带宽容量并不能长时间给企业带来良好的体验，天融信安全 SD-WAN 结合现有的基于链路和数据包两种优化方案，以应用识别与链路实时状态检查为基准，将关键应用引导到状态最好的链路上进行优先转发，并且针对 HTTP 等业务能够在数据包侧进行业务访问加速，达到优化业务访问体验的目的。



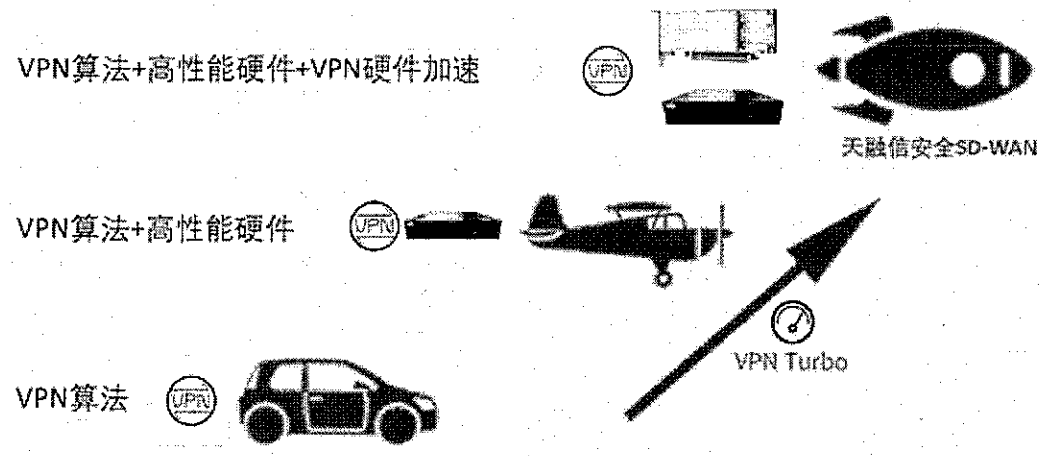
安全防护---天融信安全 SD-WAN 解决方案基于公司底层安全架构设计，从设备层面，保护设备本身的安全与可靠;从入侵攻击防护层面，保障内网业务服务安全;从数据传输层面，保障数据传输途中不被窃取关键信息，实现链路安全;从管控层面，保障管理数据可靠，实现管理安全。从而实现四位一体的安全防护。

极简运维---2018 年，新零售兴起，发展速度快、门店增设多、业务覆盖广对于 IT 业务部署与运维来说，是一个巨大的挑战。天融信安全 SD-WAN 解决方案借鉴 SDN 架构，实现分支设备零配置上线及统一管理。



高性能 VPN---VPN 作为逻辑层面的链路，如同血管一样为各个分支输送数据，承载着关键业务，其性能和稳定性逐步成为影响企业业务体验的关键因素。天融信安全 SD-WAN 解决方案团队高度重视 VPN 性能及稳定性问题，综合自身经验采用专用加速芯片，将 SD-WAN 的核心指标提升数倍，达到国内行业

领先水平。



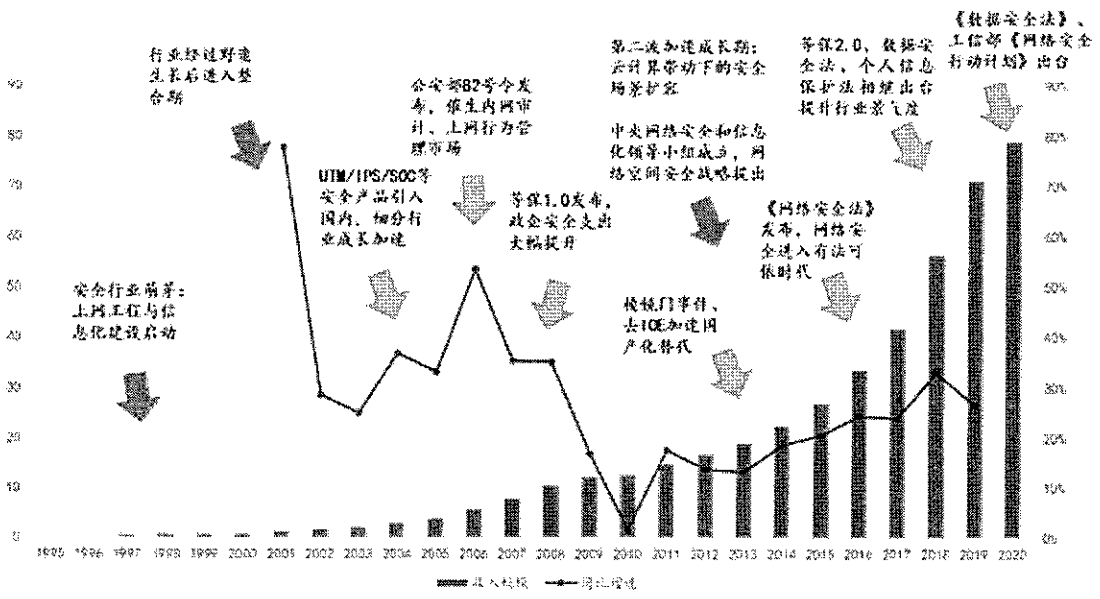
天融信始终坚持技术自主创新，不断攻破技术壁垒研发新产品。天融信安全 SD-WAN 解决方案的发布再一次向业界展示了天融信的技术创新能力和对网络安全的深刻理解。未来，天融信将再接再厉，在瞬息万变的数字化时代为客户不断创造更多价值。

六、问题与展望

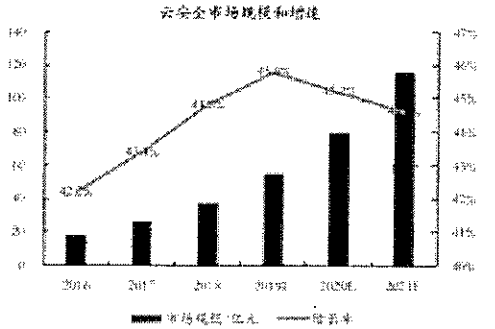
问题

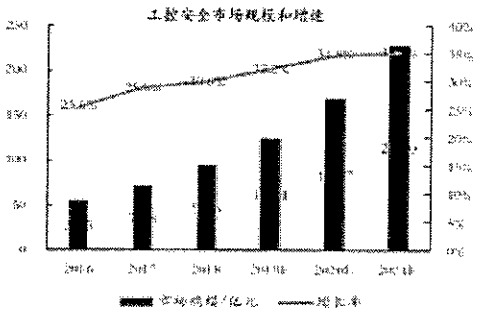
6.1 数据作为第四大资源重要性日益凸显

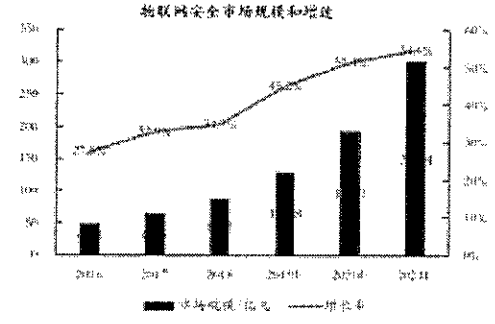
数据是继能源、资源、信息之后的第四大资源，随着各国实施数字化战略，数据资产的重要性日益凸显，数据也被视为国家主权。泄露数据，不仅仅是个人信息、商业机密，更是国家安全问题。从数据安全到国家安全，都是一场无形的战争。2021 年下半年，《数据安全法》正式实施，《汽车数据安全管理若干规定》开始试行，《工业和信息化数据安全管理办法征求意见稿》也开始起草。

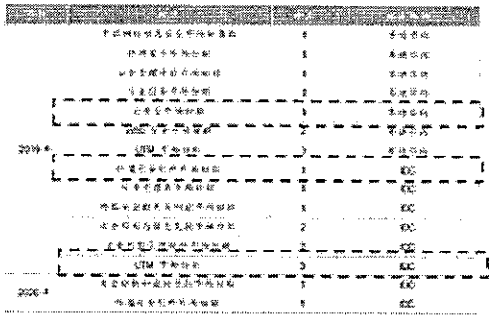


从投资角度来看，建设数据安全离不开网络安全厂商，所以现在网络安全行业处于兵马未动、粮草先行的阶段。原因有很多，一是法规出台到正式实施都需要一定的缓冲期；二是数据安全方面的解决方案还处于摸索阶段，需要时间打磨成熟，目前还不现实；其三，从建设方的角度来看，2021 年网安投入主要来自去年的预算，真正想看到在数据安全大规模的投入，仍需等到今年的预算规模。









所以，从投资的角度来看，投资者更应该选择在数据安全产品上有前瞻

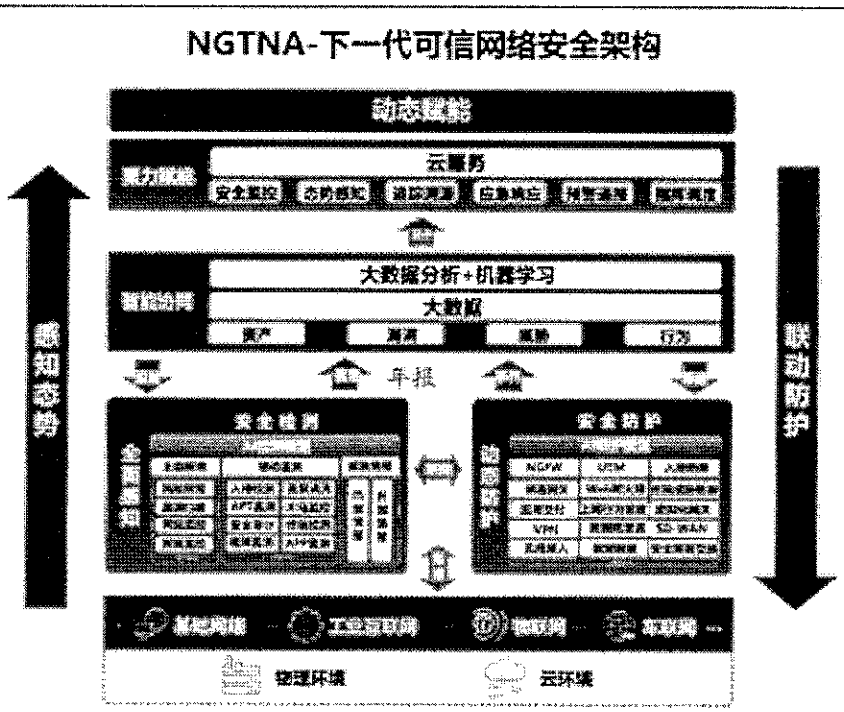
性布局的公司或者与数据安全协同性较强的公司。当然，对于网安行业的前景，2022 年 Q1 大概率是拐点，因为 2020 年疫情的影响，2021Q1 的网安行业普遍呈现出高增长态势，如果 2022Q1 继续保持较高的基数，那就意味着网安行业将迎来一个新的转折点，至此还需要努力。

6.2 数据安全时代即将到来，积极推动新产品研发

2021 年是公司从电线电缆业务剥离后专注于网络安全业务的完整财年，公司营收和订单均保持高增长，新业务表现抢眼，国产化业务增势迅猛。

剔除电缆业务及同天科技后，公司网络安全单体业务收入达 33.13 亿元，同比增长 36.42%。新方向新场景已形成先发优势，数据安全、工业互联网、信创、大数据、安全云服务、云计算等新赛道产品营业收入实现高速增长。

公司进一步加大投入，研发费用同比增加 47.35%，研发费用主要用于夯实基础网络安全业务，布局及完善数据安全、云计算、云安全与安全云服务、态势感知等新方向和工业互联网、车联网、物联网等新兴场景业务的技术及产品。销售费用同比增加 33.56%，主要用于行业深耕、地市下沉和渠道拓展，销售人员数量增幅为 15.89%，渠道销售人员数量在销售人员数量中占比为 10.91%，为进一步实现市场覆盖打下较好基础。



公司提出下一代可信网络安全架构

数据安全是大数据未来发展的基础。因为数据量越大，安全越重要。随着政策的出台，数据安全时代即将到来，天融信通过深耕政府行业、积极推动销售渠道改革、大力投入研发，布局新产品有望充分受益。

6.3 大数据安全与发展并重，行业化安全业务应用场景加速落地

数据是新时代重要的生产要素，是国家基础性战略资源。2021 年 11 月 30 日，工信部发布《十四五"大数据产业发展规划》，提出"产业保持高速增长"的发展目标，到 2025 年底，大数据产业测算规模突破 3 万亿元，年均复合增长率保持在 25%左右，创新力强、附加值高、自主可控的现代化大数据产业体系基本形成。《规划》将"发挥大数据特性优势"列为主要任务，着力于推进数据"大体量"汇聚、"多样性"处理、"时效性"流动、"高质量"治理、"高价值"转化等关键环

节协同联动发展，推动大数据产业发展和数据要素价值释放。

公司大数据业务覆盖大数据分析与态势感知、网络安全管理、数据安全管理、主动防御管理等四个方面，以安全数据中台为基础，形成了安全管理、态势感知、数据安全、零信任、工控安全等纵深一体化安全运营中心建设方案。报告期内，公司在核心技术研究、安全运营能力构建、先进产品研发与应用实践等方面持续突破，深化 AI 分析、用户行为分析（UEBA）、安全响应编排（SOAR）等关键技术在网络安全大数据中的应用，提升大数据安全整体技术水平。同时，《大数据安全防护关键技术及应用》荣获省部级科学技术进步一等奖，态势感知系统入选《IDC MarketScape：中国态势感知解决方案市场厂商评估》领导者行列。在落地实践方面，报告期内，公司产品与解决方案新增航天、人社、水利、医疗、国资集团、城投、电子政务 7 个行业的应用实践。

截至报告期末，公司大数据产品获得国家科技进步二等奖 1 项、省部级科技进步一等奖 2 项，参与编写政府、运营商、金融等行业的国家、行业相关标准 13 项，并在运营商、能源、税务、医疗、教育、金融等领域的 37 个行业化安全业务应用场景中落地实践。

6.4 产业数字化发展带动网络安全发展，行业化场景加速覆盖

产业数字化带动了工业互联网、物联网和车联网等新兴领域出现和发展，网络安全是这些新兴领域发展的前提和基础。随着新一代信息技术加速向工业领域渗透，国家围绕工业互联网大力推进工业企业进行数字化转型升级，未来三年是工业互联网的快速成长期。《2020 年中国互联网安全报告》指出，对能源、轨

道交通等关键信息基础设施在线安全巡检中发现，20%的生产管理系统存在高危安全漏洞，并且工业控制系统已成为黑客攻击利用的重要对象，安全是工业互联网高质量发展的重要前提和保障。

在工业互联网领域，公司持续拓展产品品类、丰富产品功能，形成覆盖工业控制系统信息安全建设、监管、运营与能力提升的 12 款工业领域的专用安全产品与服务。

在工业互联网安全能力方面，公司凭借广泛的技术覆盖与实践能力打造了支持工业互联网平台、工业数据安全、工业互联网标识解析系统等 21 个业务场景的完整解决方案，产品与方案在电力、石油、轨道交通、冶金、煤炭、机械制造等 32 个行业广泛落地实践。

同时，公司提出“基于 IPDRR 的工业互联网安全解决方案”，从识别、防护、检测、响应与恢复方面落实安全能力的全面覆盖，并以此为基础向工业互联网数据安全、工业互联网应用安全持续拓展与实践。结合工业领域数字化发展与整体安全需求，公司率先提出将功能安全与信息安全充分融合的“双安融合”理念。面向工业互联网全业务流程，公司围绕设备、控制、网络、标识、平台、数据安全防护需求进一步提升了工业互联网场景化安全防护能力。在标准建设方面，报告期内，公司重点参与 10 余项工业互联网领域标准制定，涉及工业企业安全数据分类分级、工业防火墙、工业网络安全隔离与交换系统等方向。

在物联网安全领域，报告期内，公司在边缘计算、视频流量处理、行业物联协议深度分析三个方向持续发力，推出了物联网边缘计算网关、物联网视频上云安全网关，与公安、能源等专用行业物联网协议广泛适配并通过专业测评；并推出覆盖智慧社区、智慧灯杆、智慧屏幕、智慧安防、智慧电桩等 9 大场景的

行业化解决方案，为北京、安徽和浙江等近万个小区以及广州、江苏等多地海关提供了高可靠的网络安全保障。同时，公司进入公共安全社会视频资源安全、公安视频图像信息系统安全的新市场，配合相关部门开展相关工作。在标准建设方面，公司重点参与了信安标委、公安部、信通院、CSA 等组织的物联网安全标准，为国家、行业、联盟的物联网安全标准制定持续做出贡献。在人才培养方面，公司与中国网络安全审查技术与认证中心联合推出《ISTE 物联网安全技术工程师》认证，独家负责课程体系开发，持续为国家培养和输出物联网安全专业人才。

6.5 以数据为中心的安全保障体系成为网络安全建设的重要内容

数据安全是“十四五”期间网络安全数字化建设的核心内容，2021 年《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》《关键信息基础设施安全保护条例》《网络安全审查办法》等系列政策法规相继出台与施行，强化了数据安全的法制基础。同时，数据作为核心生产要素，是推动企业数字化转型以及数字经济发展的新动力，随着数据安全系列政策的陆续实施，数据安全建设成为各行业数字化转型下合规的刚需。据 Risk Based Security（RBS）《Data Breach Report:2021 Year End》显示，2021 年全球公开披露的数据泄露事件 4145 起，共导致超 220 亿条数据泄露。在风险控制需求与合规建设需求双重推动下，数据安全产业将迎来高速发展阶段。

伴随客户业务、安全需求以及数据安全技术的发展，数据安全建设已逐步进入体系化、工程化阶段。基于“自上而下、分域管控、持续运营”的整体数据安全防护理念，报告期内公司推出涵盖数据安全治理评估、数据安全组织结构

建设、数据安全管理制度建设、数据安全技术保护体系建设、数据安全运营管控建设及数据安全监管建设的“六步走”数据安全治理体系，在政府、运营商、能源、金融、教育等 10 余个行业大型客户中规模化实践落地，同时，项目覆盖范围已延展到工业互联网、车联网等领域。在数据安全标准建设方面，公司累计主导或参编数据安全相关国家/行业标准 35 项，申请专利 50 余项，报告期内重点参与运营商及互联网行业，以及车联网、工业互联网领域相关标准编撰，在重点领域持续深耕。

展望

6.6 产品、技术布局

（1）技术产品化

公司持续跟进新技术，并与客户业务相融合、适配，不断研究、应用到新产品、新版本中。紧跟信息化、数字化的不断发展，公司在工业互联网、数据安全、大数据、云计算、边缘计算、国产化、物联网、车联网、人工智能等新领域、新技术方向不断加大研究和研发投入，快速实现这些新技术在产品中的应用。

（2）产品场景化

公司在强化基础网络安全场景研究基础上，不断深入了解工业互联网、物联网、车联网、数据安全、云计算、大数据、国产化等新应用场景，通过提前了解场景、

熟悉业务、梳理需求，对产品进行场景化适配和改进，使产品与解决方案更适应客户应用场景、适配客户实际需要。

（3）服务平台化

公司不断积累服务所需的安全知识、安全工具，并进行平台化。通过服务平台化，既能实现服务在全行业、全场景的标准化，又能实现服务提供的快速规模化。目前公司已将安全漏洞、威胁情报、指纹特征、安全工具等进行整合，构建了云服务平台、威胁情报平台、安全知识平台，借助这些平台，公司服务团队面向全行业全区域提供高质量安全服务。

（4）攻防技术专业化

网络安全攻防技术是网络安全公司的核心能力之一，攻防技术涉及多个方向，公司建立了阿尔法实验室、听风者实验室、赤霄实验室、网空安全对抗中心等在内的多个攻防技术研究团队，专注于漏洞挖掘、恶意代码分析、前沿攻防技术研究、威胁情报分析、威胁狩猎、APT 追踪、前瞻性攻防工具研究等方向，实现攻防技术主要专业方向的人才培养、能力积累。

6.7 人才布局

网络安全行业的竞争本质是人才的竞争，同时行业人才市场的供给和需求始终存在较大差距，行业内人才争夺加剧，因此公司始终将人才引进、人才培养工

作放在首位，“融天下英才，筑可信网络”是公司的人才建设坚持的基本理念。

（1）公司多渠道推动外部人才的引进：根据公司战略和业务发展规划，公司通过人才搜寻、高校合作、校园招聘、各类竞赛等多种渠道广纳贤才，在营销、研发、运营等体系补充人才，优化人才结构，完善人才队伍。

a)跨界人才引入：基于数字化的广泛应用及多技术的融合的背景，公司加大了工业互联网、物联网、车联网、云计算等相关专业人才的引进，以提升了技术革新和创新能力，形成更好满足客户需求变化的能力。

b)中高级业务人才引入：基于公司区域业务下沉、行业规模化等策略，公司在中高级销售管理人员，售前售后及安全服务高级人才的引入，以更好支撑业务拓展。

c)优秀基础人才的引入：通过高校合作、校园招聘等方式持续招聘优秀应届毕业生补充到各业务体系，达到提升人才质量、优化人才结构，保持人才队伍年轻化等人才管理目标。

（2）建立体系化的人才培养体系，形成人才自我造血机制，提升组织能力。公司针对新员工，营销、研发和工程技术专业序列员工，管理干部等不同群体设计了针对性的培养方案和计划，构建能力发展的学习地图，以实现人才培养的批量复制能力。建立内部讲师、内部导师、专业认证及管理、天融信学苑等人才培养的支撑系统。

6.8 生态布局

（1）战略投资：公司投资了 20 余家具有核心技术的企业，在工业互联网安全、物联网安全、智慧安防、自然资源大数据、EDR（Endpoint Detection and Response，端点检测与响应）、量子通信、人工智能、非结构化数据智能管理、网络安全人才培养等多个领域进行产品、技术布局。

（2）战略合作：公司不断引入战略合作伙伴，与行业主管机构和相关头部企业深度战略合作，强强联合、协同发展、安全赋能，共同为客户提供更优质服务；与上下游细分领域厂商在产品、技术领域深入合作，持续完善公司 NGTNA 架构，提升公司产品、技术和解决方案竞争力。