湖北生物科技职业学院
Hubei Vocational College of Bio-Technology

天融信 TOPSEC

北京天融信教育科技有限公司

参与高等职业教育人才培养年度报告

（2024）

二〇二四年十二月

前言

企业的参与一直是职业教育发展的核心问题，随着《中华人民共和国职业教育法》（2022 年修订）的正式实施，我国职业教育迎来了全新的发展机遇。企业在职业教育中的作用已从合作伙伴、产教融合的重要主体发展为职业教育的重要办学主体，企业参与职业教育已从承担社会责任、获得经济利益，演变为履行法律责任与兼顾经济激励。天融信集团作为一家具有 29 年发展历程，专注于网络安全产品，网络安全服务及大数据与云服务，在网络安全领域极具的影响力的企业集团，有能力也有义务为地方区域经济发展作出贡献。天融信与湖北生物科技职业学院携手合作共建产业学院，不断创新教育模式，提高教育质量，为职业教育的发展注入新的活力；为企业发展提供技术支持、科研合作等服务，推动企业技术创新和转型升级；注重培养学生的职业素养、创新精神和实践能力，为学生的职业发展打下坚实的基础。

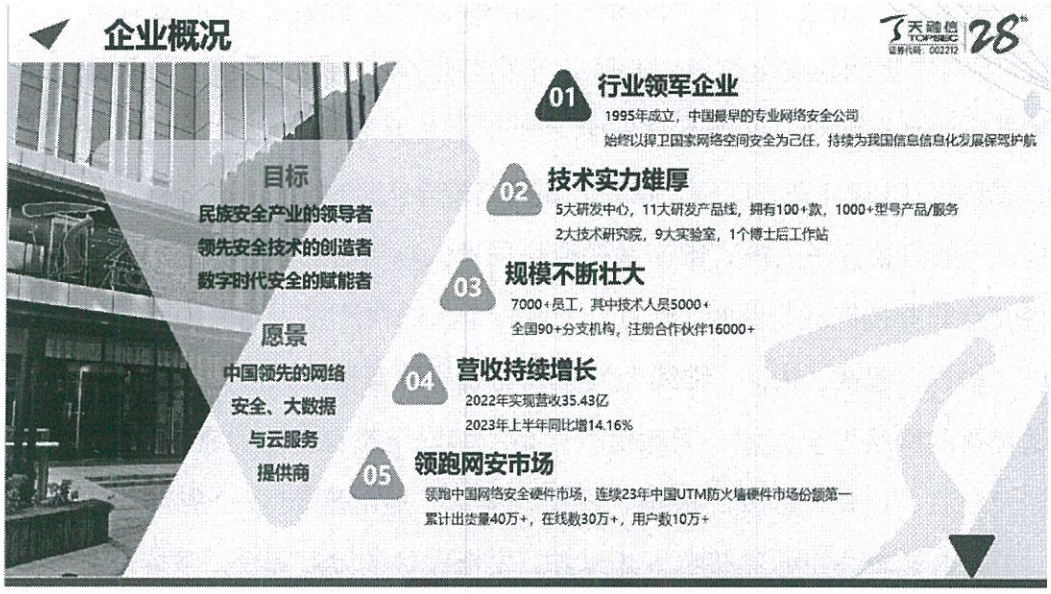
1 目录

1 、企业概况

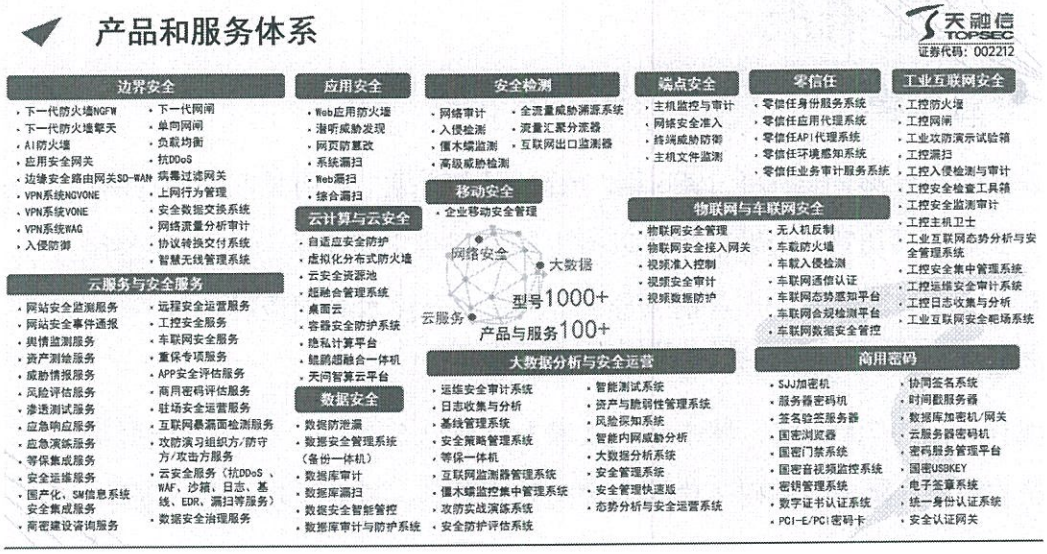
1.1 企业规模

天融信科技集团创始于 1995 年，风雨兼程 29 载，亲历见证了中国网络安全产业的发展历程。天融信始终以捍卫国家网络空间安全为己任，创新超越，致力于成为民族安全产业的领导者、领先安全技术的创造者和数字时代安全的赋能者。

现有员工约 7000+名，其中研发技术人员超过 3000 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。

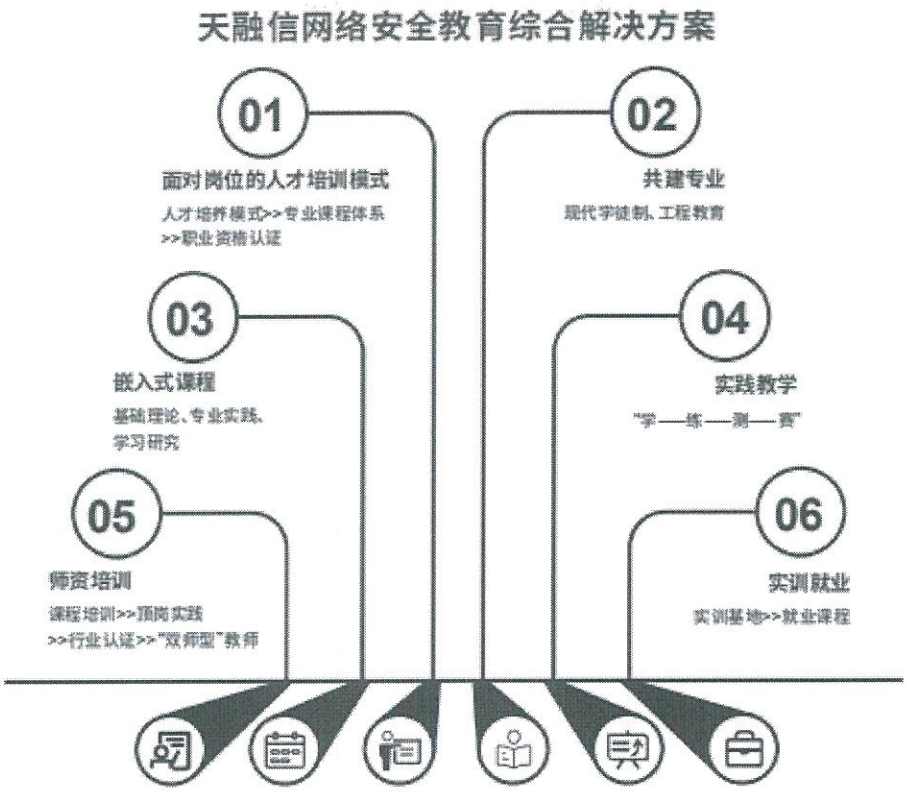


天融信拥有庞大且全面的产品体系，包括基础网络安全产品，应用安全产品、安全检测产品、端点安全产品、安全管理产品、数据安全产品、工业互联网安全产品、物联网安全产品以及车联网安全产品等等。



1.2 网络安全学院-天融信教育

北京天融信教育科技有限公司（简称天融信教育）是天融信集团旗下承担教育培训服务和人才生态建设的专业服务公司，依靠雄厚的技术实力和行业经验，研发出了先进、实用且最为权威的网络安全厂商认证 TCSP 系列培训课程，并与中国网络安全测评中心联合开发出业界首个针对数据安全治理方向的国家级认证培训——注册数据安全治理专业人员（CISP-DSG），同时是 CISSP、CISP、CISP-PTE、CCSK、CCSRP 等网络安全人才认证证书的授权培训机构。天融信教育作为教育部产教融合协同育人项目合作单位，打造完整的网络安全职业技能成长路径，致力于企业与个人的快速发展与能力 提升，通过以“培训、考试、认证、维续”为流程的新型教育模式为国家和社会持续输送优秀的网络安全人才。天融信教育是网络安全教育行业的领军企业，业务涉及北京、广州、西安、成都、武汉、南京、郑州等 60 多个省市分支机构。天融信教育公司始终坚持人才培养、安全守护的发展理念，坚持专业专注专心的服务特色，引领安全教育行业长足稳定发展。



教学保障优势

天融信拥有专业的网络安全培训教室、网络安全试验室，为培训服务提供一流的教学设施。

为强化学习成果、增加学习成果转化率、提高学员考试通过率，天融信建立了一套完善的教学考试模拟系统。系统分为：分类练习模块和综合测试模块两个部分，内置大量模拟题。通过不断习、反复强化，达到强化学习成果的目标。

天融信组建专业的培训实施团队，培训前准备工作、收集资料、与学员、认证机构、讲师、客户沟通

培训安排；培训中解答学员问题，保障培训顺利实施；培训后整理学员资料，完成培训总结，以及后续成绩、发证跟进。

配套资源

为参加培训的所有学员提供高质量的培训课件、教材及考试学习手册、复习资料，全面配合参训 人员的学习。

学员自动成为天融信俱乐部的会员，获取网络安全行业前沿资讯及免费沙龙、主题研讨会等免费 参会资格。

在培训结束后，为了使参训人员能够长期有效地把知识转化到实际工作中，天融信将为参训人员定期发送《网络安全小贴士集锦（微信、QQ 图片）》，便于参训人员长期、有效地加深对安全的认识。

为参训人员在课后能够将学习内容更好地应用在日常生活与工作中提供极大的便利，使课程学习的良好效果能够更加明显和持久，使客户单位为员工安排的本次培训能够取得立竿见影且能长期保持的效果和收益。

天融信拥有业界最为丰富、实力最为雄厚的网络安全领域的师资力量。面授专家讲师团队 40 余人，远程直播教学专家讲师团队 100 余人，授课讲师均已取得相关网络安全讲师认证证书。区别于一般培训机构，天融信是老牌的安全厂商，讲师不仅能够教学授课，还有丰富的大型网络安全项目工程实施、审核、测评、管理等经验，能够结合项目实战，我们的讲师团队分为金牌、资深讲师，金牌讲师已有 15 年以上授课经验，资深讲师也有 8 年以上授课经验。为学生提供更完善更标准的体系化课程和虚拟化真实案例演示。依托于自身的强大师资力量，天融信研发出先进、实用且最为权威的网络安全厂商认证 TCSP 系列培训课程，并与中国网络安全测评中心联合开发出业界首个针对数据安全治理方向的国家级认证培训——注册数据安全治理专业人员（CISP-DSG）。同时是 CISSP、CISP、CISP-PTE、CCSK、CCSRP 等网络安全人才认证证书的授权培训机构。

李跃忠

中国信息安全测评中心CISI认证讲师
国家互联网应急中心CCSRP网络与信息安全认证讲师
TCSP信息安全行业认证讲师
注册数据安全治理专业人员CISP-DSG
国际云安全联盟C-CCSK
《计算机网络管理员——高级网络管理员》系列教材作者

吕延辉

北京信息安全等级保护专家组成员
曾参与公安部等级保护试点工作，国资委、国土资源部、工信部、新闻出版总署、山东高速（试点）、国家中医药管理局、政协、残联、计生委、气象局、中国中铁、国家林业局等单位的信息安全等级保护咨询、培训或实施工作

谢琴

20年的计算机网络领域工作经验
中国信息安全测评中心CISI认证讲师
信息系统安全专业认证 CISSP认证专家
曾负责国家发改委计算机网络改扩建工程、北京市农村商业银行信息安全体系建设项目、农信银资金清算中心网络安全项目等多个大型网络安全项目

苗春羽

中国信息安全测评中心CISI认证讲师
国家互联网应急中心CCSRP网络与信息安全认证讲师
注册数据安全治理专业人员CISP-DSG
思科认证CCIE
TCSP信息安全行业认证讲师

郝钢

全国高等教育教师资格，15年教育行业从业经验
国家互联网应急中心CCSRP网络与信息安全认证讲师
中国信息安全测评中心CISI认证讲师
注册数据安全治理专业人员CISP-DSG
TCSP信息安全行业认证讲师

王志航

国家互联网应急中心CCSRP网络与信息安全认证讲师
注册信息安全专业人员-渗透测试工程师CISP-PTE
注册数据安全治理专业人员CISP-DSG
TCSP信息安全行业认证讲师

-10-

1.3 企业文化

天融信秉承 “融天下英才、筑可信网络” 的人才理念，重视人才的引进与培养，建立了由近千名信息安全专业研发、技术与服务人员构成的强大服务团队，公司始终以捍卫国家网络空间安全为使命，坚持多年与国家各个漏洞库进行深度合作，向各个漏洞库输送高质量原创漏洞，协助漏洞库平台完成各项网络安全风险排查任务，为网络强国、数字中国建设贡献力量。

1.4 职教融入

天融信与湖北生物科技职业学院合作共同制定人才培养方案，提高学生的就业竞争力；共建实训基地，为学生提供实践机会，帮助学生更好地掌握实践技能；进行“双师型”人才培养，提高企校双方的教学水平与实际操作能力。产业学院合作申报获批，互联网安全产教融合基地合作申报获批，湖北省高水平专业群合作申报获批等标志性项目成果。

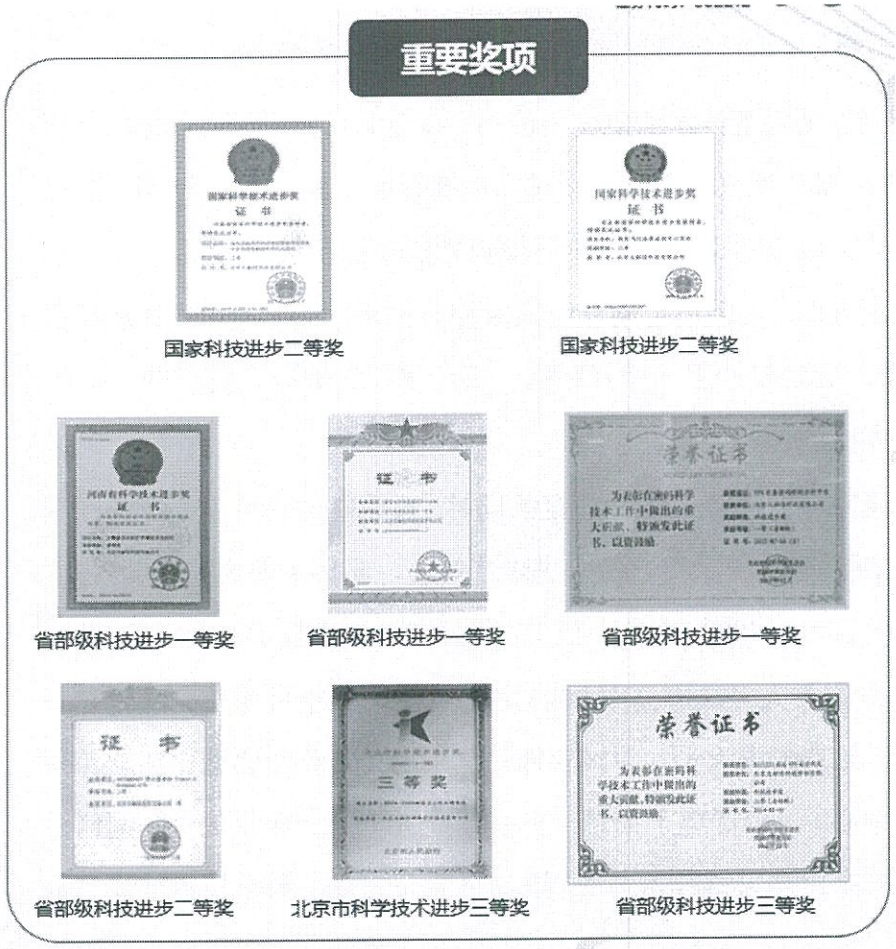
1.5 企业荣誉

天融信长期以来重视技术的研究与应用，在专利申请方面持续增长（累计申请 2630 件，累计授权 822 件。同时当前拥有超 410+项软著证明，产品资质证书 530+项，这也印证了天融信长期积累的知识产权能力。

在国家课题方面，天融信主动参与国家相关技术研究课题，累计承接国家课题 70 余个，拥有包括下一代互联网、云计算、大数据、物联网、工业互联网等诸多方面的课题成果。

积极参与国家课题和重大工程建设的同时，天融信也获得了丰厚的回报。2017、2018 年两次获得国家科学技术进步二等奖，是国家对天融信研发能力和创新能力的认可。2022 年，天融信荣获国家知识产权优势企业称号。

2024 年，北京市人民政府公布 2023 年度北京市科学技术奖励决定。天融信科技集团、北京邮电大学、中国软件评测中心（工业和信息化部软件与集成电路促进中心）、中国电子信息产业发展研究院联合申报的《关键信息基础设施数据安全治理关键技术与应用》项目荣获北京市科学技术进步二等奖。



2 企业参与办学情况

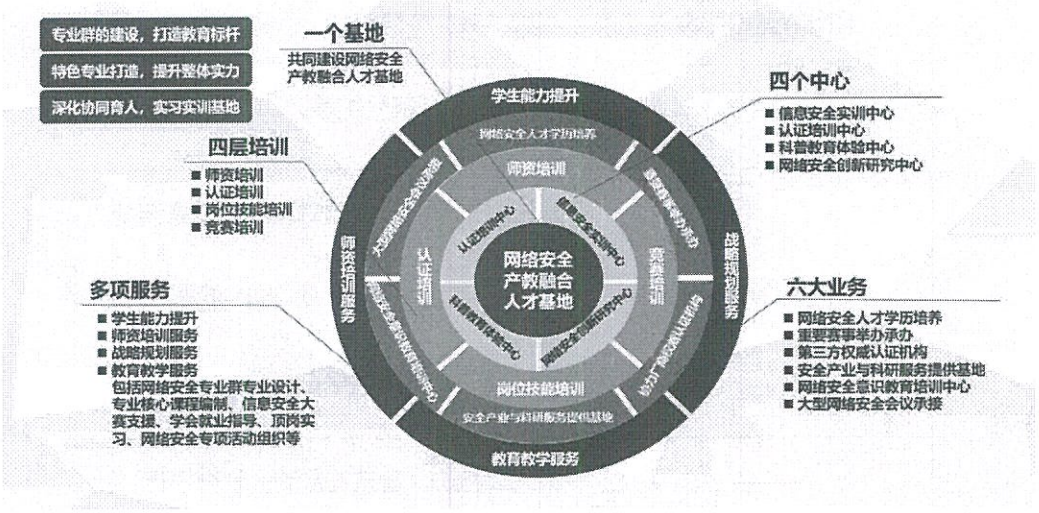
2.1 参与形式

2024 年 6 月，天融信与湖北生物科技职业技术学院本着“人才共育、过程共管、成果共享、责任共担 ”的原则，共建互联网安全产教融合基地，全力推进产教融合共同体建设与发展。

产教融合基地依托湖北生物科技职业学院信息安全专业，以信息安全专业为基础，创新校企合作人才培养模式，开展专业建设、学生职业能力培养、员工培训、现代学徒制试点、导师互聘双师共建、课程建设教材开发、实验实训基地建设、联合招生就业服务、资源共享及课题研究、项目开发、技术合作、专利申报、成果转化等方面的合作建设。产教融合基地自建立以来，校企双方全力推进产教深度融合，共同全面培养面向未来的网络安全行业的高技能人才，力争建成全国领先的产教融合示范基地。

2.2 发展规划

天融信网络安全技术有限公司凭借新一代协同防御体系和综合网络安全能力以及对教育行业多年来服务经验，探索出以“聚集人才、建立高地，输出人才、服务产业”为核心，学历教育与产业培训相结合的网络安全人才培养新模式，从湖北生物科技职业学院整体利益出发，整合现有资源与合作基础，规划提出“1 个学院，一个基地，4 个中心，4 层培训，6 大业务，多项服务”的人才培养目标，以此推动安全人才培养与产业合作的发展。



2.3 岗位实践

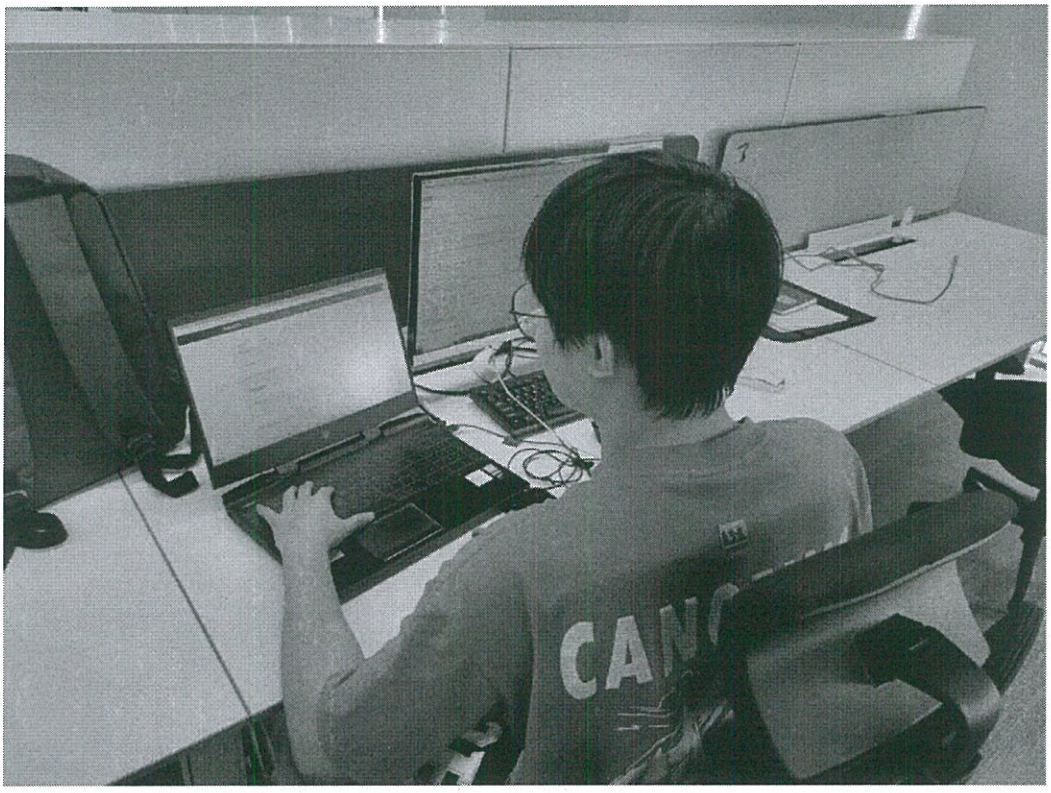
公司通过提供资金、设备、人员等方式，帮助学校改造校内外实训条件，丰富实践教学资源。同时，公司引入市场机制，使得教育资源的配置更加合理，提高了教育效率。通过公司的参与，湖北生物科技职业学院能够更好的与社会接轨，提升了教育的实用性和前瞻性。

安排学生进行岗位实践，实践地点在国家网络安全人才与创新基地、天融信企业大楼，开展具体的企业实践项目，实践内容主要包括涉网案件侦查、护网与重保网络安全服务，同时也会考察学生的沟通交流能力、文档输出能力以及应变能力。通过岗位实践的方式，了解企业实际工作环境及实际用人需求，对自身未来的发展具备更加清晰的规划。

2.3.1 涉网案件侦查

涉网案件支持服务是为国家及各省市公安机关提供专业高效的打击涉网犯罪的情报甄别、深度溯源、 取证支撑、技术攻坚、信息关联等技术支撑，帮助公安机关分析涉网案件流程，甄别情报可用性，快速定位涉案人员。

时间	实践类型	实践内容
全年	涉网新型犯罪案件支撑	博彩网站、博彩 APP、赌博游戏、 非法棋牌游戏、色情网站、色情 APP、色情直播、 毒品销售网络等。
	网络诈骗案件支撑	杀猪盘诈骗、投资理财诈骗、贷款诈骗、信用卡诈骗、游戏充值诈骗、兼职刷单诈骗、消费返利诈骗等。
	电信诈骗案件支撑	冒充公检法、冒充运营商、冒充银行、冒充电商平台、冒充快递公司、冒充政府职能部门、冒充医院医保等。
	涉众经济犯罪案件支撑	网络传销、网络集资、P2P、投资理财、消费返利、金融互助、虚拟货币、非法洗储、非法经营证券等。



2.3.2 护网行动

护网行动是由公安部牵头的网络安全攻防实战演习，旨在评估并提高企事业单位的网络安全防范能力。

护网行动的具体实施过程包括公安部组织攻防两方，进攻方（红队）在一个月内对防守方（蓝队）发动网络攻击，以检测出防守方存在的安全漏洞。

红队：在国家及各省市护网行动期间，为攻击队提供有效的红队专家服务，挖掘高危风险，挫败目标单位防护能力，获取系统权限并取得护网成绩。

蓝队：在国家及各省市护网行动期间，为防守单位提供有效的蓝队专家服务，通过流量监控、 研判分析、应急处置、溯源反制等防守战术提升复杂对抗能力，保证防守单位目标不被失陷。

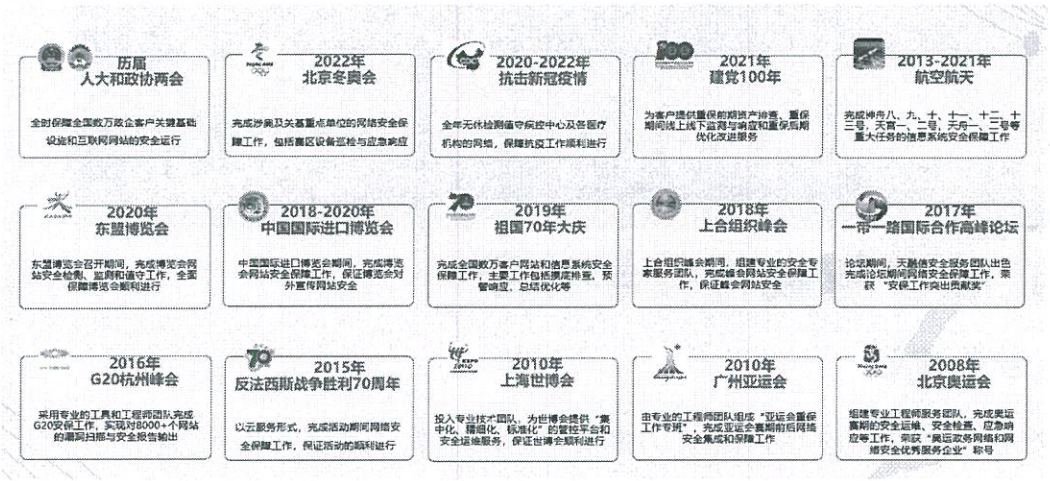
时间	实践类别	实践内容
6月～10月	红队	1. 侦察 2. 初始访问 OR 建立据点 3. 权限维持 4. 特权提升 5. 内部侦察 6. 横向运动 7. 数据分析 8. 渗透并完成任务
	蓝队	监控组：负责实时汇报监控平台上的高危告警。 研判组：负责实时研究判断监控组反馈的高危告警是否为误报。 处置组：负责应急处置研判组反馈的真实攻击告警事件。 溯源组：负责溯源攻击告警事件以及攻

		击者相关信息。 反制组：负责反制钓鱼邮件中的钓鱼网站或者通过社工的方法反制红队。

2.3.3 重大活动保障

重要时期安全保障是指在国家重要会议或重大活动期间协助客户保障网络基础设施、重点网站和业务系统的安全，通过明确的职责分工与协作，能快速应对各种网络安全事件，使重要会议或重大活动期间的客户业务系统安全平稳运行。

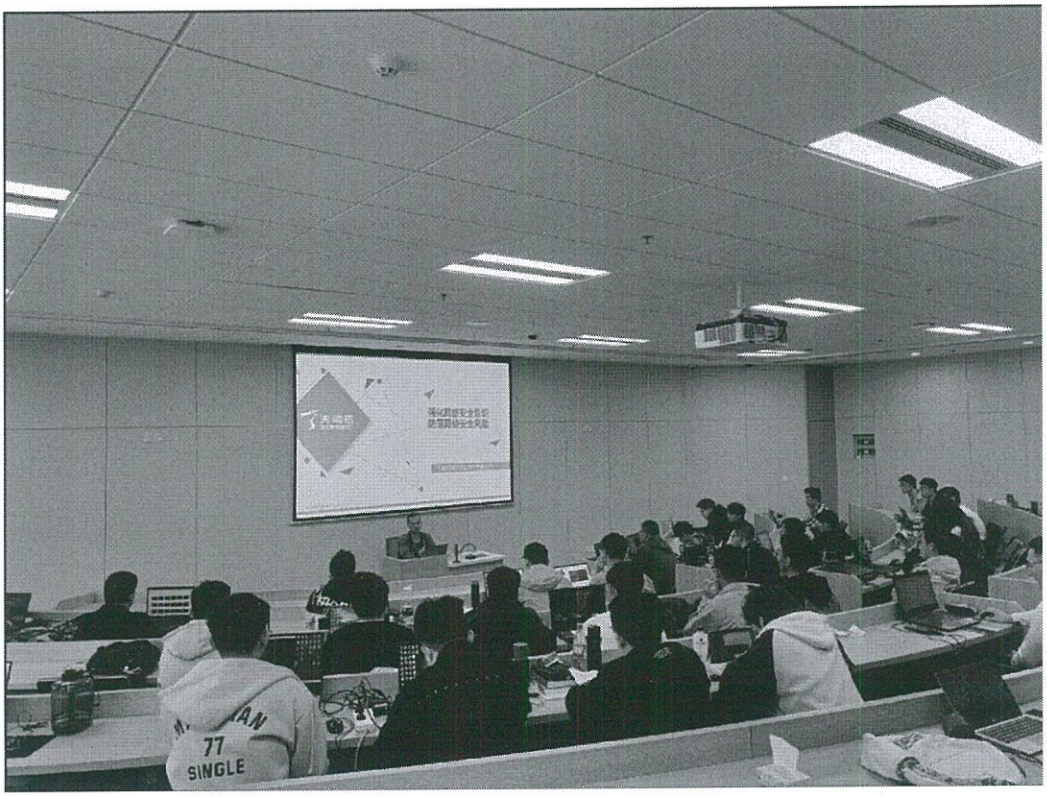
时间	实践类别	实践内容
3月～4月或大型活动举办	现场值守	设备监控预警 威胁检测分析 事件快速响应
	云端技术支持	疑难问题研判 威胁情报共享 远程技术检测



3 企业资源投入

企业安排 3-4 位企业导师，与学校老师共同构建专业核心课程体系，联合研制人才培养方案，创新校企协同育人机制，创新考核评价方式，明确企业导师教学职责，强化学校导师实践能力，制定双导师管理制度，促进交叉学科研究。

每年安排教师到天融信或国家网络安全人才与创新基地参加新技术培训，统一进行安全技术、安全理论、安全产品、实验室使用、教学技巧等方面内容的培训。内容从人才培养核心技术、理论到实验操作、使用，再到课程答疑等方面，保障高校各教职工教学任务的开展。



4 企业参与教育教学改革

4.1 专业建设

产教融合基地发展的初期着力建设“扩大内需，打造教育的业务标杆”，根据湖北生物科技职业学院的现状、合作资源的条件成熟度、技术难度等综合因素评估情况，动态调整专业结构，深化专业供给侧改革，完善网络安全专业群应具有健全专业动态调整机制，做好存量升级、增量优化、余量消减，

以学生就业为主导，以培养学生能力为中心，强调专业与产业、行业技术领域发展的相关性和适应性，专业群内资源具有可共享、可复用的特点。

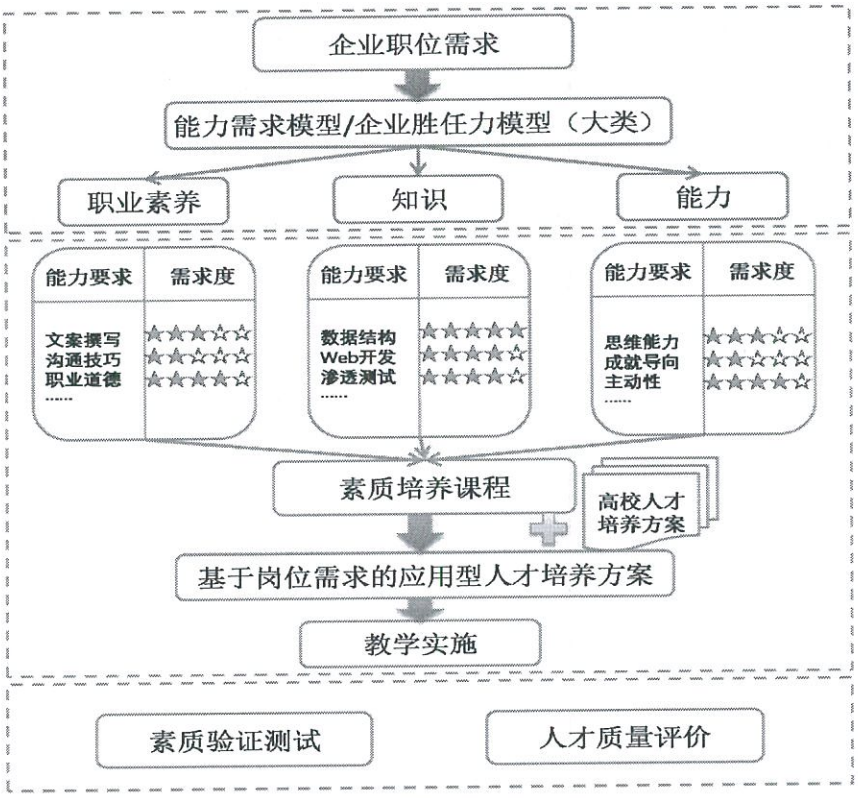
由 3-5 个安全方向专业组成，以信息安全专业为核心，配套的网络安全培训中心（实验室）、网络安全认证中心、科普教育中心拓展企业和高校多元化办学模式，扩大需求，推动高校形成就业与招生计划、人才培养的联动机制，打造教育业务新标杆。

推进现代信息技术与教育教学深度融合，打造网络安全特色优势专业，不断深化开展校企合作以聚集人才，提高专业建设质量，人才培养适应新时代对人才的多样化需求，推动高校及时调整专业人才培养方案，定期更新教学大纲，适时修订专业教材，科学构建课程体系。进一步加强专业质量建设，提高学生和社会的满意度，优化专业布局，结合内高校学科专业特色和优势，加强专业布局顶层设计，培育特色优势专业集群，提高教育办学质量，向应用型院校看齐。

深化协同育人机制。建立与社会用人部门合作更加紧密的人才培养机制，与相关部门联合制订人才培养标准，对人才培养进行协同管理，培养真正适应经济社会发展需要的高素质专门人才。

加强学习实训基地的建设。综合运用校内外资源，建设满足实践教学需要的实验实习实训基地，满足学生顶岗实习、就业实训需求，为学生实习实践提供服务。依托学习实训基地和学校科技成果，搭建学生科学实践和创新创业平台，推动高质量师生共创，增强学生创新精神和科研能力。

基于岗位需求的应用型人才培养体系



所属部门	职位名称	岗位职责	技能需求
产品	产品经理助理	1、研究网络安全技术，跟踪技术发展趋势； 2、负责产品的需求分析，定义产品的功能，监控产品的研发； 3、研究、制定网络安全标准，编写产品的市场材料，进行产品促销设计，对销售体系相关人员进行培训。	1、熟悉信息安全领域的现况和发展趋势； 2、跟踪国内外最新攻击技术及防护技术； 3、熟悉信息安全知识体系，深入理解信息安全技术体系知识能； 4、熟悉防火墙、VPN、IDS/IPS、UTM、安全审计、SOC等主流安全产品的原理。
售前	信息安全售前工程师	1、配合销售完成项目投标、完成投标过程； 2、与客户现场交流，挖掘用户需求并设计撰写解决方案、方案讲解、技术建议等； 3、负责产品的安装/试用和售前的产品讲解。	1、掌握Subtopic技术； 2、熟悉主流数据库技术； 3、熟悉Windows/linux/Unix操作系统的管理与应用； 4、熟悉主流安全产品原理与配置，防火墙、IDS、IPS、WAF、审计等； 5、熟悉信息系统安全等级保护知识体系和网络安全服务体系； 6、良好的文档能力及沟通表达能力。
销售	1安全产品销售经理 2安全产品区域销售经理 3安全产品行业销售经理	1、负责辖区域产品和行业的销售工作； 2、负责辖区域产品和行业的客户关系建设、维系，提升客户忠诚度； 3、负责辖区域产品和行业市场信息的采集、反馈，信息的分析	1、熟悉行业客户需求；具有某行业知识背景；有一定行业经验客户资源； 2、具有成熟市场和良好客户关系 3、具有很强的沟通协调能力

		利用； 4、能准确把握客户心理，及时抓住客户需求和商机； 5、负责开拓市场及协调客户资源。	
研发	信息安全研究人员	1、负责安全攻防相关技术研究； 2、负责各类漏洞挖掘与分析； 3、研究各类攻击特征及特征分析； 4、负责处理紧急安全事件应急响应； 5、负责重要信息系统渗透测试。	1、具备全面安全能力，并在某一领域有深入研究； 2、熟悉Web安全、移动安全、物联网安全、云安全、系统安全、网络安全等方面的常用安全技术； 3、掌握恶意代码的诊断和评估技术。
售后	1售后基础支持工程师 2信息安全技术支持工程师	1、负责公司售后设备的备件及维护维保推广销售工作； 2、负责公司客户项目安全巡检工作； 3、总结收集产品问题信息，为后端研发提供参考意见； 4、收集一线用户意见，对公司营销策略、产品方案、等提出参考意见； 5、与客户保持良好沟通，及时响应用户需求；维护公司老客户关系。	1、熟悉路由交换原理； 2、熟悉主流服务器原理与配置； 3、熟悉安全设备（fw\ips\ids\waf\审计等）原理与配置； 4、熟悉所销售产品的维护、升级、备机管理流程； 5、熟悉主流硬件平台及底层硬件问题分析能力。
实施	信息安全实施工程师	1、负责安全工程类项目实施方案的编写工作； 2、负责安全工程类项目实施，完成安全设备的上架、测试调试工作。	1、熟悉TCP/IP网络协议；熟悉路由交换技术，并熟悉主流厂商设备配置； 2、熟悉主流攻防技术原理与防御方法； 3、精通windows、Linux操作系统及各类服务器（DNS\WEB\DHCP\MAIL等）搭建与安全加固； 4、熟悉主流厂商安全设备原理（FW、IDS、IPS、WAF、负载均衡、审计、VPN等）及配置； 6、熟悉主流数据库（mssql、mysql、Oracle）的安装与安全加固； 7、熟悉主流web服务器及中间件（IIS、Apache、tomcat、weblogic、nginx...）的配置与安全加固。
	1信息安全咨询顾问 2信息安全服务工程师	1、收集、调研、分析和总结对应行业的客户市场安全基本情况和需求； 2、了解客户的业务安全需要并协助参与信息安全解决方案的设计； 3、负责协助信息安全高级工程师完成风险评估、等级保护、信息安全管理体系建设、信息安全规划服务等信息安全咨询类服务项目的售前工作。	1、具备扎实的计算机网络、通信技术、系统、网络、应用安全技术基础； 2、熟悉网络安全的专业技术知识、标准和相关安全产品（如FW、IDS、IPS、WAF、审计等）； 3、熟悉信息安全等级保护的标准规范和实施流程； 4、熟悉风险评估相关项目标准规范和实施流程； 5、熟悉ISO27000系列信息安全管理体系相关标准。
测试	1信息安全测试工程师	1、负责网络、系统进行渗透测试、安全评估和安全加固。 2、出现网络攻击或安全事件时，	1、精通TCP/IP网络协议；熟练掌握至少一门编程语言c/java/php/Python； 2、熟练使用linux，深入理解linux用户、权限管理

	2渗透测试工程师 3安全测试工程师 4应用安全测试工程师	提供应急响应服务，协助恢复系统及调查取证 3、跟踪国内外的安全动态，及时掌握最新的攻防技术和趋势	等安全机制；了解linux系统常见漏洞与利用方法； 3、熟练使用windows，深入理解windows安全机制、常见漏洞与利用方法； 4、熟悉主流服务器原理与脆弱性（DNS、web、mail、DHCP）； 5、深入理解系统扫描技术（端口、服务、系统、漏洞扫描原理），并熟练使用主流扫描工具（Nmap、nessus、openvas...）； 6、精通各类主机层面远程攻击技术及工具使用（口令爆破、远程溢出、数据库利用、Metasploit平台使用）； 7、精通各类网络攻击原理与利用技术（udpflood、synflood、icmpflood、arp欺骗、dns欺骗、网络嗅探）； 8、精通各类web应用漏洞利用技术，SQL Inject 、XSS、会话劫持、文件上传、文件包含、变量覆盖）； 9、熟练使用基于webshell各种途径提权技术（基于系统漏洞exp、第三方应用、数据库等）； 10、熟悉主流web服务器、中间件、开发框架或组件的漏洞与利用（Apache、tomcat、nginx、struts2、openssl）； 11、掌握内网渗透技术（基于内网反弹或代理技术、扫描内网、应用口令爆破、欺骗、流量嗅探）。
运维	1信息安全工程师 2网络安全工程师 3数据库安全工程师 4系统安全工程师 5云存储安全工程师 6安全运维工程师	1、制定和完善开发、运维相关安全规范； 2、参与信息安全评估工作和安全加固工作； 3、负责信息系统安全事件的分析、应急处理及上报； 4、负责日常安全漏洞扫描、渗透分析和入侵检测，及时发现安全隐患，并采取有效措施进行修复。	1、精通TCP/IP网络协议； 2、精通路由交换技术，对vlan、无线、路由设计、VPN、负载均衡深入理解，并熟悉主流厂商设备配置； 3、精通主流服务器原理与及安全配置（DNS\WEB\DHCP\MAIL等）； 4、熟悉dos及DDOS攻击原理，并能通过dos防护策略，实现防护； 5、熟悉主流网络攻击原理，精通安全防护产品原理与配置（fw、IDS、IPS、网关防病毒、日志审计），能够分析还原攻击，并通过策略调整，防护攻击； 6、熟悉web应用层攻击原理，WAF原理，能够熟练使用WAF进行web安全防护； 7、熟悉数据库操作配置，熟练使用数据库审计产品。

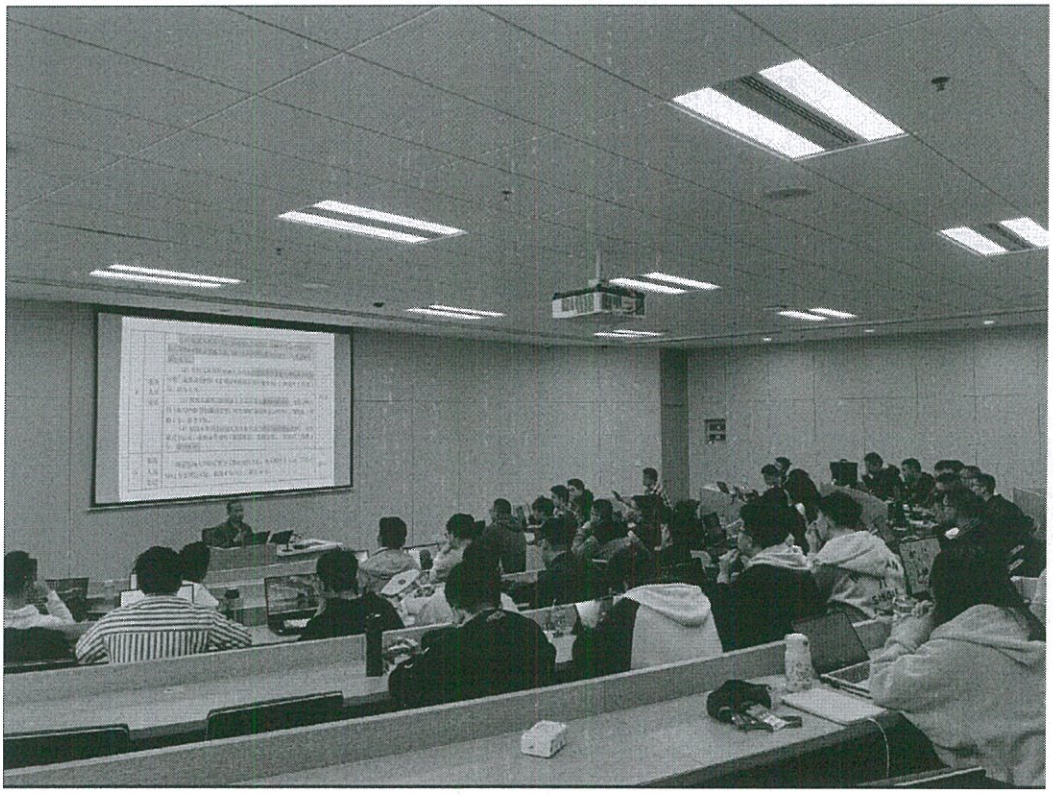
4.2 人才培养

公司在参与办学的过程中，注重创新人才培养模式，培养学生的职业素养， 如团队协作、沟通能力、责任心等。通过组织各种实践活动和培训课程，帮助学生提高职业素养，更好地适应未来的职业生涯。这种职业素养的

提升，不仅有助于学生在未来的工作中更好地发挥自己的能力，也有助于提高企业的整体工作效率。

4.2.1 实习实训

2024 年 10 月 26 日至 11 月 9 日，根据天融信集团职业岗位结构和职业能力要求，在企业专家指导下，对接行业需求，以工作过程为线索，制订符合主要技能和职业态度、职业素养要求的模块化实习实训，明确各模块的实训目标、实训计划、实训教学环节和实训教学方法，形成分模块的训练与考核标准；根据职业技能形成的内在规律，科学划分实习实训阶段，制定不同阶段实习实训教学计划，建立实施方案与阶段计划有机结合、阶段计划又相对独立的实习实训体系。



4.2.2 赛事指导

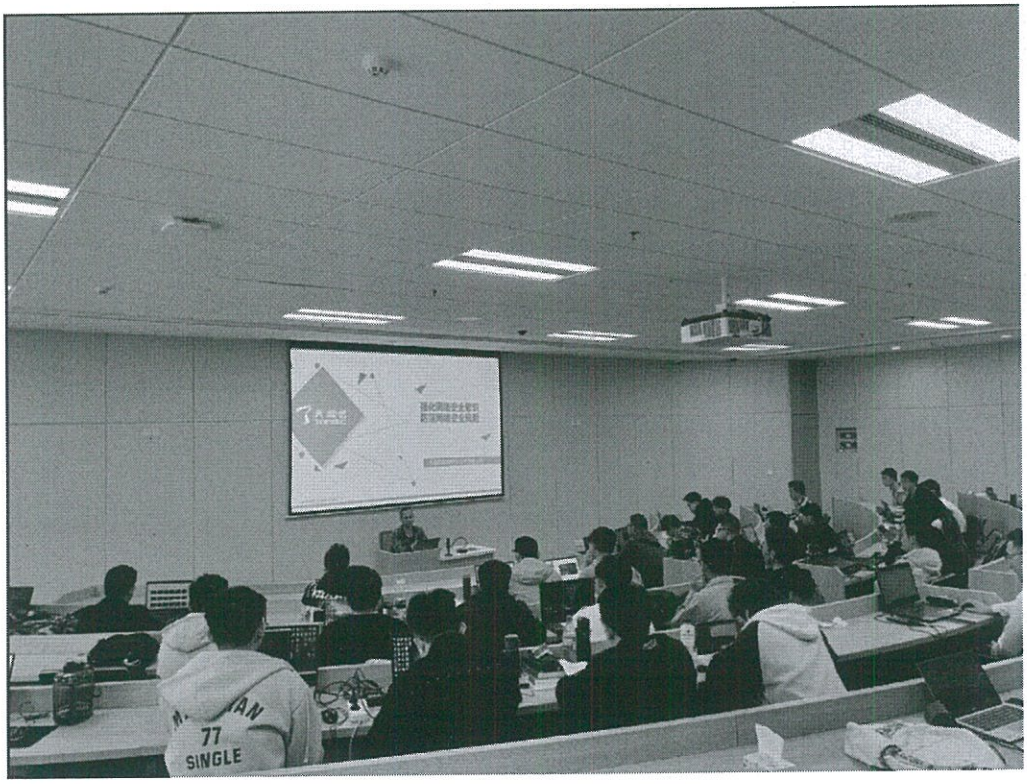
天融信科技提供竞赛能力提升培训，通过培训针对性的提升指导教师和战队队员的安全对抗能力，在校内营造以赛促学、以赛代练的良好氛围，增加学校指导教师、战队的综合网络安全对抗能力。

维护网络空间安全，筑牢人才根基是关键。为了培养更多的网络安全技术人才，天融信教育于 11 月 16 日至 11 月 17 日，在国家网络安全人才与创新基地成功举办了 2024 年天融信教育杯 CTF 赛事。本次竞赛以个人赛形式进行，CTF 模式（夺旗赛）为竞赛带来了更多挑战和刺激，天融信教育武汉网安基地共 100 余名实习实训学生参与了本次竞赛。本届 CTF 赛事亮点之一就是竞赛题型丰富，覆盖 MISC、CRYPTO、REVERSE、WEB 四大方向，旨在通过攻防对抗、程序分析等方式全方面展示和考察参赛选手的个人信息安全综合能力和实战水平。这些题型紧扣实际网络安全场景，让参赛选手们在比赛中学习的同时，也能更好地理解和应用所学知识。

4.2.3 网络安全宣传周

2014 年以来，中央网信办等部门连续多年在全国范围内举办国家网络安全宣传周活动。

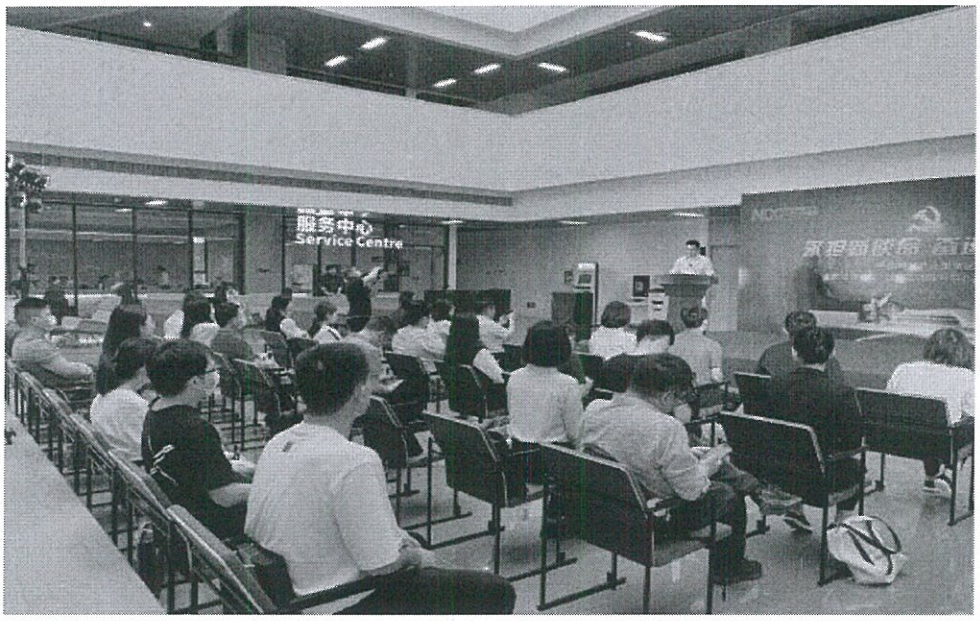
2024 年 9 月 15 日，通过线上线下相结合的方式，以通俗易懂、百姓喜闻乐见的形式，宣传网络安全理念、普及网络安全知识、推广网络安全技能，有力地推动了全社会网络安全意识和防护技能的提升。



4.2.4 网络安全科普教育

开展网络安全科普教育活动，走进学校、社区、企业等，向不同群体普及网络安全知识。通过举办讲座、培训等活动，提高公众对网络安全的认识和重视程度，增强公众的网络安全防范意识。

11 月 9 日，联动国家网安基地产业办党支部、天融信党支部助推学生党组织活动。参加学生在基地期间应邀参加国家网络安全人才培养与创新基地“临空港中部数谷产业集聚区江城红领驿站·党群活动服务中心”启动仪式，参观党群活动服务中心，组织党员参加由武汉大学国家网络安全学院刘芹教授主讲的“网安大讲堂”教育讲座。



4.3 课程建设

核心课程

课程类别	课程名称	课程内容
计算机网络技术	OSI 与 TCP/IP 协议	OSI 模型
		TCP/IP 协议族
		数据封装与解封装过程
		Wireshark 抓包分析
	ARP 协议	ARP 协议概述与原理
		ICMP 协议分析
	TCP 与 UDP 协议分析	TCP 与 UDP 报文分析
		TCP 三次握手与四次握手
		Wireshark 抓包分析
		DDOS 攻击与防御
程序设计基础	shell 脚本	Shell 基本功能
		Linux 变量类型
		流程控制
		服务探测脚本
		主机扫描脚本编写
		用户批量安全管理
		服务自动化脚本编写

	Python-Web 爬虫	Web 网页信息获取
		Web 爬虫编写
		Web 网页信息获取
		正则表达式
	Python-Socket 后门编程	C/S 架构与套接字
		socket 函数应用
		木马与后门编写
	Python 安全开发	Python 扫描主机工具编写
		Python 扫描端口工具编写
		Python 子域名探测工具编写
		延时注入 exp 编写
		布尔盲注 exp 编写
		Sea CMS RCE 利用工具编写
		FTP 弱口令检测工具编写
		Telnet 弱口令扫描
		SSH 弱口令检测工具编写
网络数据库技术与应用	MySQL	MySQL 数据库结构
		sql 语言增删改查
	SQL 注入	MySQL 数据库特性及风险分析
		SQL 注入漏洞概述
		SQL 基础语句
		SQL 常用语句和函数
		四大基本手法
		SQL 注入漏洞防御
	数据库安全风险分析	SQL 注入神器-SQLmap
		SQL 注入读写文件
		ACCESS 风险分析
WEB 应用开发	WEB 架构安全分析	Web 服务器环境搭建
		Web 工作机制
		http 请求头、响应头、状态码 Web 会话与 cookie
	HTML 语言	Web 服务器搭建
		HTML 基本结构

		HTML 基本标签
		HTML 表格
		HTML 表单
	层叠样式脚本 CSS	内嵌框架
		CSS
	JavaScript	JavaScript 基础
		JavaScript 函数
	PHP 基础	PHP 概述
		PHP 变量与变量类型
		PHP 运算符
		PHP 流程控制
		PHP 函数与数组
信息安全标准与法律法规	网络安全法	网络安全内容简介
		网络安全法背景及概况
		网络安全法历程
		网络安全法内容解读
	密码法	密码法内容简介
		密码法内容解读
信息安全管理务实	信息安全管理	信息安全管理概述
	等保政策解读	网络安全概述及网络安全大事件
		网络安全产品
		等级保护相关法律法规
Linux 操作系统	Linux 操作系统	linux 基础命令
		linux 用户和组内容讲解
		linux 文件系统和权限讲解
		linux 网络配置及 ssh 服务和 apahce 基础配置
操作系统安全	windows 系统安全	windows 系统安全概述
		文件加密
		解密
		数据使用安全
		账号和组
		系统密码破解

	linux 系统安全	linux 账号安全
		配置安全
		文件系统
		进程服务
		ssh 安全
		网络访问控制
	中间件安全	Apache
		Nginx
		IIS
		Tomcat
		Weblogic
		Websphere
		Jboss
网络设备配置与安全	数据链路层分析	数据链路层与帧结构
		交换机工作原理与基本命令配置
	IP 协议分析与路由原理	IP 协议分析与静态路由
		默认路由
		动态路由
	VLAN 与 Trunk	虚拟局域网 VLAN
		Trunk
		端口聚合技术
	三层交换技术	三层交换技术原理
		三层端口技术
		DHCP 中继
	ACL 包过滤技术	ACL 技术原理
	NAT 与内网穿透	NAT 技术
		SNAT
		DNAT
		内网穿透
信息安全产品配置与应用	防火墙	防火墙概述
		防火墙配置与应用
	入侵防御	入侵防御概述
		入侵防御配置与应用

	上网行为管理	上网行为管理概述
		上网行为管理配置与应用
	VPN	VPN 概述
		VPN 配置与应用
	WEB 应用防火墙	WEB 应用防火墙概述
		WEB 应用防火墙配置与应用
数据存储与容灾	数据存储与容灾	数据恢复概述
		数据存储原理
		数据备份
WEB 应用安全与防护	SSRF 漏洞利用与防护	SSRF 基础
		SSRF 漏洞挖掘
		SSRF 漏洞利用与防护
	文件包含	文件包含概述
		本地文件包含
		日志包含
		协议
		远程文件包含
	XXE 利用与防护	XML 基础
		XXE 基础
		XXE 漏洞利用案例
		XXE 漏洞利用与防护
	web 提权	web 提权概念
		前端 js+MIME 类型绕过
		特殊后缀+.htaccess 文件绕过
		user.ini 文件+大小写绕过
		加点和空格绕过
		数据流+点空格点+双写绕过
		web 中间件提权
		redis 未授权
		常见 cms 提权
		数据库 web 提权
	内网渗透	内网渗透-认识域
		内网渗透-域权限解读

	内网渗透-chisel 端口转发
	内网渗透-chisel 之 socks 代理
	内网渗透-Frp 的使用
Pwn-栈溢出基础	栈溢出原理
	基础栈溢出-静态分析
	基础栈溢出-动态调试
	基础栈溢出-代码编写
ARM-Pwn	arm 基础
	arm-pwn 栈溢出基础
Pwn-堆溢出利用与防护	Pwn-FastbinAttack
Pwn-堆溢出基础	堆基础
Pwn-格式化字符串漏洞	格式化字符串基础
	格式化字符串劫持返回地址
	got 表劫持
Pwn-漏洞缓解措施	漏洞缓解措施
	ret2lib_x32
	ret2lib_x64
IOT 漏洞挖掘与利用	嵌入式架构
	工具
	固件分析
恶意代码分析	概述
	分析方式介绍
	反向 shell
服务器提权	服务器提权简介
	Rsync 提权
	Redis 提权
	基本反弹命令介绍
	Linux 内核提权
	suid 和 sudo 提权
	mysql 的 udf 提权
	windows 提权简介
	windows 提权辅助工具
	windows 溢出提权

		MSSQL 提权
	日志分析	windows 日志分析
		linux 日志分析
		web 日志分析
	脱壳原理	壳原理
		脱壳示例
	Pwn-shellcode	shellcode 原理
		shellcode 示例
	Pwn-数组越界和整数溢出	整数溢出
		数组越界
信息安全风险评估	风险评估基础	风险评估技术概况
		渗透测试技术介绍
		常见安全威胁和法律了解
渗透测试常用工具	渗透测试常用工具	nmap 介绍
		nmap 使用
		burpsuite 介绍和使用
		burpsuite 实战
		sqlmap 介绍
		sqlmap 实战
		御剑
		webshell
		菜刀、蚁剑、冰蝎
		渗透工具-初识 metasploit
		渗透工具-metasploit 之 search
		渗透工具-ms17-010 攻击示例
		渗透工具-metasploit 之 meterpreter
服务器配置与管理	应急响应基础	安全事件分类
		事件分级
		应急响应作用
		应急响应基础
	windows 应急响应	windows 账号检查
		windows 端口进程检查
		自动运行程序检查
		webshell 及后门
		其他检查
	linux 应急响应	账号与命令历史
		文件分析
		端口进程检查
		自动运行程序

		恶意程序

4.4 师资建设

依托学院优质师资资源，通过校企合作共建，内培外引，基地形成一支数量足够、相对稳定的“双师型”实习实训指导教师与培训师队伍，培育一支专兼结合、具有较高的政治素质和道德修养水平、有较强的课程开发能力和专业实践教学能力的指导教师团队，实现实训课堂与生产岗位的无缝对接。

制定师资队伍建设模式，按照“加强校企合作、引聘技术专家、培养教师骨干”的原则，通过内部培养、生产实践、同行交流、企业引进等方式，构建人才培养基地教师双向交流机制，建立兼职教师资源库，加强实训指导教师实践能力培养力度，严格骨干教师考核评价，建立实训教学监控体系，培育一支专兼结合的校企一体化人才培养指导教师团队。

2024 年 8 月 15 日，组织了产学协同育人项目天融信网络安全师资培训班，对校内老师的专业知识技能进行了提升，本次活动圆满完成。

4.5 实训基地建设

加强学习实训基地的建设。综合运用校内外资源，建设满足实践教学需要的实验实习实训基地，满足学生顶岗实习、就业实训需求，为学生实习实

践提供服务。依托学习实训基地和学校科技成果，搭建学生科学实践和创新创业平台，推动高质量师生共创，增强学生创新精神和科研能力。

2024 年 6 月，网络安全实训基地投入使用，主要包括网络安全实战能力提升的实训环境和实训设备，搭载用于网络安全实践教学的软硬件设施，为中心人员和社会人员提供网络安全实践的学习环境。

实验室占地面积不小于 100 ㎡，每间教室至少可容纳 50 人。实验室针对每门安全专业实践课会对应一种网络安全设备，每组默认配备一套网络安全设备共 6 人使用，根据实际教学的课时/学生/班级/教学计划可计算安排实验室使用率。

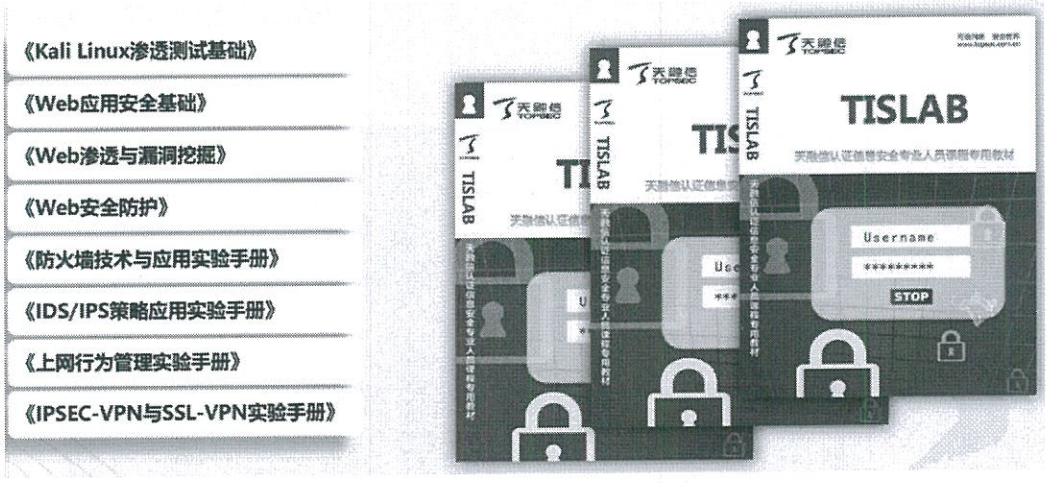
4.6 教材建设

2024 年 6 月，由基地专职教师与企业专家共同参与，建成集纸质、电子、媒体、静态、动态、书本、网络资源于一体的立体化教学资源库，内容包括：

① 教学标准子库：内含专业人才培养规格、岗位能力分析表、学习领域、课程标准、实习实训指导、实训评价表等要素。

② 教学素材子库：包括专业主干课程的资料图片、录像、专业教学案例及专业资料网站等。

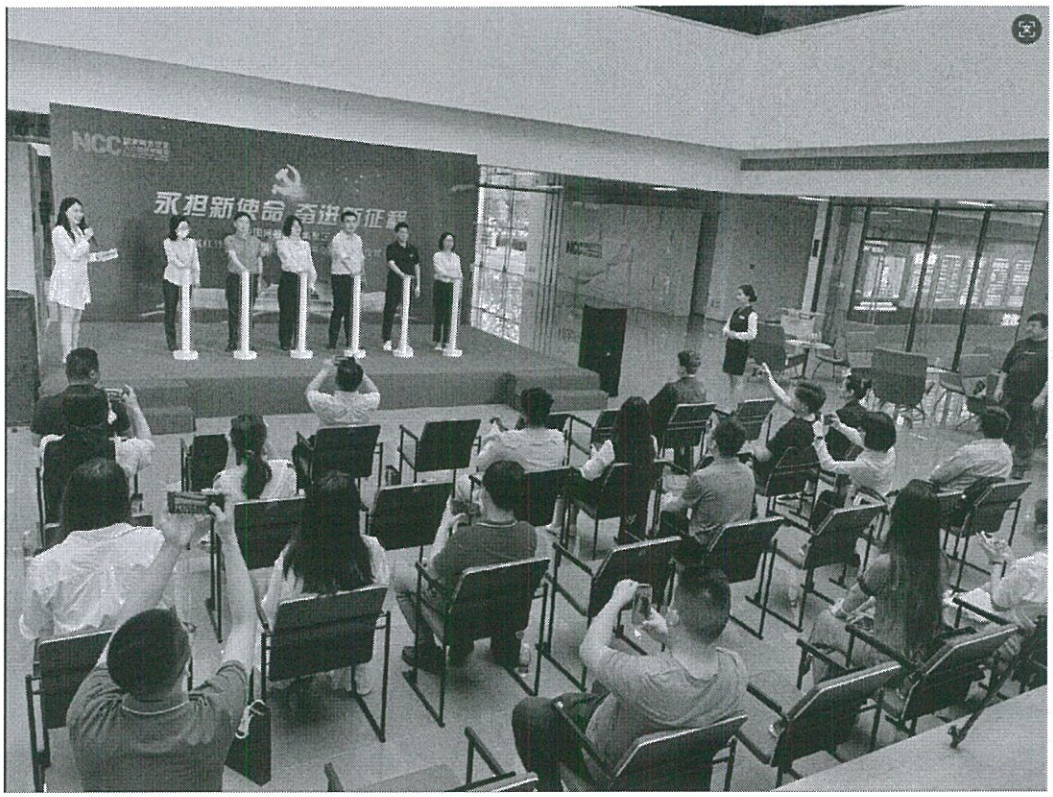
③ 自主学习型课程子库：建成包括《数据运营管理》、《数据安全治理》、《网络安全综合实训》等核心课程的学习课程。每门网络课程包含：网络教材、多媒体课件、电子教案、实训范例、试题库、以及在线答疑、网络测试、在线论坛等。



5 助推企业发展

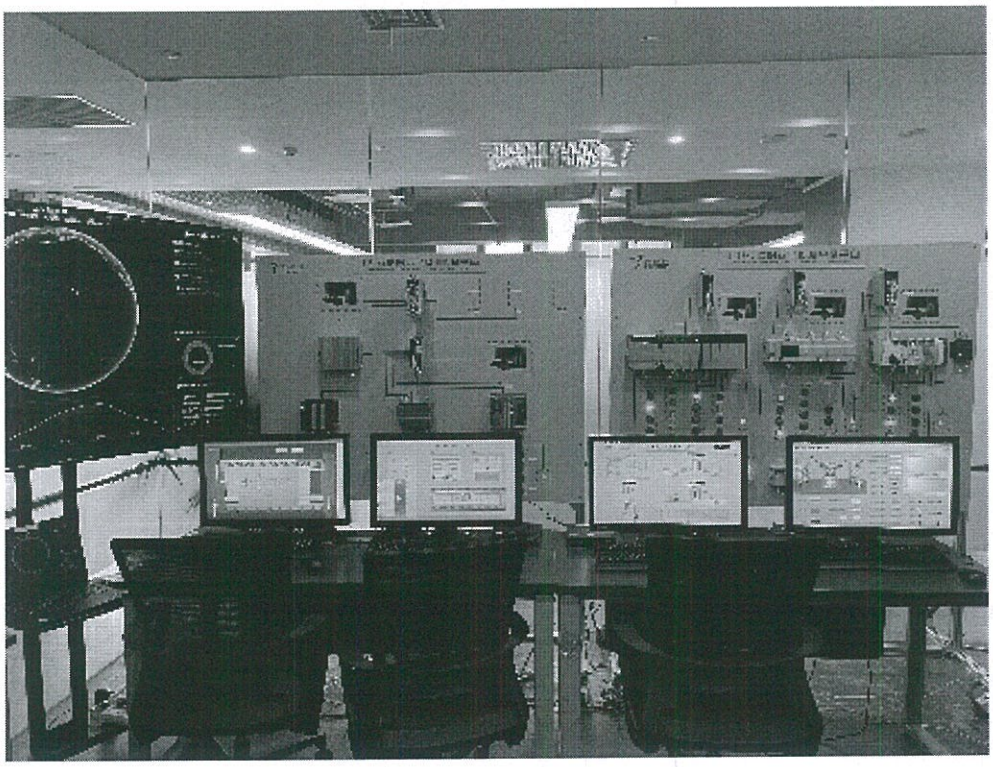
5.1 党建领航

2024 年，产教融合企业及校方积极组织党员、职工参加学习教育、 主题教育，学习系列重要讲话精神、党的各项路线方针政策、市场经济知识及法 律法规等内容，传达党的声音。严肃党员队伍管理，及时批评指出党员职工违反 劳动纪律和企业规章制度的行为，积极开展“双强六好 ”，“党员五亮 ”等活动， 促使党员发挥先锋模范作用，发挥党建沟通功能，既反映员工心声，维护员工合法权益，又传递企业决策部署，维护企业正当权利，促进企业管理层与员工的沟 通理解。同时，积极壮大党员队伍，努力把企业骨干培养成党员、把党员培养成企业骨干，不断提升党员、职工队伍整体素质，不断提高企业工作效率和管理水平。



5.2 科研合作

2024 年，面向工控互联网安全创新研究，建立健全协同创新机制，校企联合打造科研攻关团队，深入生产一线，瞄准产业需求，调研征集企业实际面临的生产性和技术性难题，支持职业学校在关键共性技术攻关中发挥“中试车间”的作用。后续共同体建设单位加强经费投入，共建技术创新中心、产学研用协同创新平台等，产出一批前沿领域的创新成果，服务行业企业技术改造、工艺改进、产品升级，提升服务水平。



6 问题与展望

6.1 挑战与机遇

网络安全领域的技术发展日新月异，新的攻击手段、防护技术不断涌现。产教融合基地需要紧跟技术前沿，及时更新教学内容和实训设备，以确保学生所学知识与实际工作需求相匹配。例如，随着人工智能技术在网络安全中的应用逐渐广泛，基地需要增加相关课程和实践项目，让学生掌握基于人工智能的威胁检测、漏洞分析等技术。

网络安全市场对人才的需求呈现出多样化、专业化的特点，不仅需要掌握扎实技术的专业人才，还需要具备良好沟通能力、团队协作能力和创新思维的复合型人才。产教融合基地在人才培养过程中，可能存在教学模式单一、实践环节不足等问题，需要根据市场实际需求调整教学内容与教学模式。

伴随着各项挑战，机遇也呈现于眼前，国家高度重视网络安全和产教融合工作，出台了一系列政策文件，如《关于深化现代职业教育体系建设改革的意见》《关于促进数据安全产业发展的指导意见》等，为网络安全产教融

合基地的建设提供了政策保障和发展方向。政府鼓励企业参与产教融合，支持学校与企业共建实训基地、联合培养人才等，为基地的发展创造了良好的政策环境。

6.2 措施与展望

建立动态更新机制：密切关注网络安全领域的技术动态，如人工智能在网络安全中的应用、零信任架构等，定期评估教学内容的时效性，及时将新的知识、技术和案例纳入教学体系。

加强与企业合作：与网络安全企业建立深度合作关系，借助企业的技术资源和实践经验，共同更新实训设备和教学软件，确保学生能够接触到行业内最新的工具和技术平台。

构建实践教学体系：增加实践教学比重，设计涵盖网络安全攻防演练、漏洞挖掘与修复、安全运维等多个方面的实践项目，让学生在实际操作中提高解决问题的能力。

开展校企联合培养：与企业共同制定人才培养方案，根据企业的岗位需求设置课程体系和教学内容，采用 “订单式” 培养模式，为企业定向输送符合其特定需求的网络安全人才。

随着网络安全产教融合基地的不断发展和完善，将为社会培养出大量既具备扎实理论知识，又拥有丰富实践经验的高素质网络安全人才，有效缓解我国网络安全人才短缺的现状，为网络安全产业的发展提供有力的人才支撑。产教融合基地将成为网络安全技术创新的重要平台，通过校企合作开展科研项目和技术研发，加速网络安全技术的成果转化和应用推广，推动网络安全产业的升级和发展，提高我国网络安全产业的核心竞争力。

未来，网络安全产教融合基地将进一步深化教育链与产业链的融合，形成教育与产业协同发展的良好局面。学校将更加紧密地围绕产业需求开展教学活动，企业也将更加积极地参与人才培养过程，实现教育与产业的无缝对接，共同构建网络安全教育、技术、产业融合发展的生态系统。