

# 三六零数字安全科技集团有限公司 参与高等职业教育人才培养年度报告 (2024)

北京信息职业技术学院



三六零数字安全科技集团有限公司



2024年12月



## 目 录

1 公司概况 .....	4
1.1 企业介绍 .....	4
1.2 核心优势 .....	4
1.2.1 技术创新 .....	5
1.2.2 安全大数据 .....	5
1.2.3 核心人才 .....	6
2 企业参与办学总体情况 .....	7
3 企业资源投入 .....	7
3.1 资金投入 .....	7
3.2 技术投入 .....	8
3.3 人力投入 .....	8
4 企业参与办学情况 .....	9
4.1 校企合作制度建设 .....	9
4.2 人才培养模式创新 .....	10
4.3 共同修订人培方案 .....	10
4.4 校企共建专业课程 .....	11
4.5 校企合作开发教材 .....	11
4.6 校企共建实践项目 .....	12
5 助推企业发展 .....	12
5.1 服务企业信息人才建设 .....	12
5.2 服务企业技术升级改造 .....	13
5.3 校企协同开发培训资源 .....	14
5.4 促进国际交流与合作 .....	15
6 问题与展望 .....	15
6.1 资源整合不充分，校企共享程度不高 .....	15
6.2 成果转化率不高，助力小微企业不足 .....	15
6.3 未来与展望 .....	16
6.3.1 校企协同，增强专业引领能力 .....	16

6.3.2 强化技能，助推人才生态建设 .....	16
6.3.3 产教融合，共建共享载体运营 .....	17

# 三六零数字安全科技集团有限公司参与高等职业教育人才培养

## 年度报告（2024 年）

### 1 公司概况

#### 1.1 企业介绍

360 数字安全集团(三六零数字安全科技集团有限公司)是数字安全的领导者，秉持“上山下海助小微”企业使命，确立安全和 AI 发展双主线。

在安全领域，为解决国家“看见”高级威胁的卡脖子问题探索形成一套以“看见”为核心的数字安全中国方案，并以“安全即服务”为核心发展理念全面升级 360 安全云，将近 20 多年被行业反复验证成功的数字安全运营体系框架，以云化、服务化方式赋能城市、大型企业、中小微企业，帮助其构建应对数字时代复杂威胁的安全能力。

在人工智能领域，360 在国家级安全能力基础上，基于类脑框架推出国内首个实现 AI 实战应用的安全行业大模型：360 安全大模型，并实现全线产品矩阵赋能，驱动企业数字安全体系提质增效。为解决大模型安全问题，360 提出“可靠、可信、向善、可控”安全四原则，打造“双轮驱动”的大模型安全解决方案框架，将 360 大模型安全核心能力输送给千行百业。

截至目前，360 累计捕获 54 个境外 APT 组织，监测到 6200 多次对我国 20000 多家重要机构单位的高级网络攻击事件；360 数字安全中国方案已落地超 20 个大中型城市，涵盖四大直辖市和部分省会城市，树立了标志性的城市级安全服务典范；同时，覆盖了超过 90%的中央部委、80%央企、95%大型金融机构和 100%的运营商，累计服务超 10000 家政企客户。

除此之外，360 已连续八年支撑国家级网络攻防实战演习，一直是国家重大政治、经济活动的核心网络安全保障力量。在两会、二十大、九三阅兵、“一带一路”峰会、G20、金砖会议、APEC、七十周年庆典、2022 年北京冬奥会等活动的重保工作，以及国家安全和国防安全相关工作中发挥了重要保障作用。

#### 1.2 核心优势

### 1.2.1 技术创新

360 累计申请专利超 1.5 万件，其中发明专利占 90%以上，是拥有专利数量最多的数字安全企业。在中国安全企业中，360 是安全投入最多的公司。我们的安全投入超过行业 top10 中第 2 名到第 10 名的总和，累计超过 200 亿。

360 建立了大数据时代的协同联动防御体系，全方位提升中国政企客户的安全防护能力和水平。360 网络安全大脑获得由科技部颁布的国家新一代人工智能开放创新平台，是网络安全领域唯一入选的公司，标致着 360 成为人工智能安全领域的领军企业。



图 1 安全大脑

### 1.2.2 安全大数据

360 通过安全领域十余年积累了大范围、长时间、多维度的全网安全大数据，汇集超 290 亿个恶意样本，22 万亿安全日志、80 亿域名信息、2EB 以上的安全大数据，为看见高级网络威胁奠定了基础。由 360 作为牵头单位的大数据协同安全技术国家工程实验室已由国家发改委批复的，联合复旦大学等相关单位共同建设，是国内唯一一个由民企牵头的国家工程实验室，是我国大数据安全领域的第一个国家级科研机构。

基于这个平台，校企双方可联合开展网络安全技术创新，共同承担国家课题。也可以搭建网络安全创新成果转化平台，推进网安创新成果转化。还可以吸引高端网络安全人才聚集，为校企合作提供有力的人才支撑和智力支持。



图 2 协同安全技术国家过程实验室

### 1.2.3 核心人才

高级别攻防专家在发现高级网络威胁中起决定性作用，360 拥有东半球最强“白帽子军团”，在对网络漏洞的挖掘和发现 APT 攻击方面达到全球领先水平。拥有超 200 人的安全精英团队，超 3800 人的安全专家团队。是亚太最大安全创新中心、具备世界级漏洞挖掘与攻防对抗能力。2022 年 9 月，入选网络安全威胁预警与监测处置领域技术支撑单位。获公安部授牌建设“国家大数据安全靶场”，提供特定的网络环境和靶场场景，提供护网支持、净网行动、网络攻防竞赛、网络攻防演练、实网攻防等服务。360 公司自 2016 年以来连续 6 年支撑国家级攻防演练，可为学校师生提供真实项目实践。360 成为唯一具有超过 15 年攻防实战经验的网安公司，丰富的实战经验为产学研合作赋能提供强力支撑。



图 3 国家大数据安全靶场



## 2 企业参与办学总体情况

三六零数字安全科技集团作为信息安全行业的头部企业，积极构建持续、健康、繁荣的产业人才生态环境。北京信息职业技术学院是教育部“双高计划”信息安全与管理专业群建设单位，北京市特色高水平专业群建设、北京市职业院校特色高水平实训基地(工程师学院、技术技能大师工作室)建设单位。2024 年三六零参与办学过程中，重点围绕信息安全应用技术专业群现场工程师项目，充分整合校企资源，发挥企业责任担当，以全国信息安全产教融合共同体为依托，创新产教融合机制，在专业课程建设、人才培养、师资队伍、技术服务方面与北京信息职业技术学院进行产教协同育人。

## 3 企业资源投入

### 3.1 资金投入

为开展实网攻防高质量人才培养，引入行业真实的攻防案例与前沿技术，让学生接触到实战化的场景与经验，提供价值 50 万元的软件及课程资源，模拟各类复杂网络环境与攻击场景，使学生在近似真实的情境中反复锤炼攻防技能。通过实战演练、项目挑战等方式检验学生的学习成果，确保培养出的人才具备扎实的技术功底、敏锐的风险洞察能力和高效的应急处置能力，满足日益增长的网络安全防护需求，为保障国家与企业的网络空间安全筑牢坚实的人才基石。

<p><b>关于开展实网攻防高质量人才培养计划的通知</b></p> <p>各有关单位：</p> <p>为全面学习贯彻党的二十大精神，落实《教育部办公厅关于加快推进现代职业教育体系建设改革重点任务的通知》，深入推进校企协同育人，打通技术技能型人才成长通道，提升高技能人才培养质量，促进毕业生高质量充分就业。经研究，360 数字安全集团牵头全国信息安全行业产教融合共同体开展实网攻防高质量人才培养计划，凝聚力量共育网络安全高质量技能人才。现将有关事项通知如下。</p> <p><b>一、申报条件</b></p> <p>(1) 计算机、网络安全等相关专业开设 2 年以上，至少 2 名网络安全方向的专职师资，负责对接企业安排实训内容并指导学生完成相应的实训任务。学校已安排学生参加全国性网络安全攻防比赛或 360 公司主办或者承办的网络安全攻防比赛并获得二等奖以上名次。</p> <p>(2) 高校负责招生、教学、学籍管理，提供必要的场地等硬件条件支持，按时提供学生在校学习期间的详细情况，每年年底能够提供当年总结及下一年计划。</p> <p>(3) 同意企业参与相关课程和教学内容设置，以开放的态度共同研制培养计划和教学方案，为专业实训课程设计和职业能力</p>	<p>力培训提供必要的师资和专业支持。</p> <p><b>二、项目遴选及管理</b></p> <p>1. 拟申报本次培育项目的院校及相关单位组建符合上级部门相关要求、职称年龄结构合理、真抓实干的团队，填报《2024 年实网攻防高质量人才培养计划项目申报书》(见附件)；</p> <p>2. 项目申报人须在 2024 年 11 月 30 日 18:00 申报截止时间前将加盖高校校级主管部门公章的申报书形成 PDF 格式电子文档发送至邮箱 infosec@ttnetgroup.com，纸质材料一式三份，经申报单位签字盖章后报送；</p> <p>3. 组织专家进行项目评审，经评议符合立项要求的将进行立项并公示入选项目名单。</p> <p>4. 与项目申报负责人所在单位签署立项项目协议书。立项项目周期为 1 年，所有工作应在立项项目协议书约定的项目周期内完成。项目到期后，项目负责人通过项目平台提交结题报告及项目成果，共同体组织专家对项目进行验收。</p> <p><b>三、建设要求</b></p> <p>1. 根据产业用人需求，实施学科交叉融合，培养复合型人才，提供详细教学计划及课程大纲；</p> <p>2. 制定实训计划，配合企业开展“实网实兵实战”培训，线上或线下培训时间不少于 30 天；安排不少于 50 名学生前往企业至少见习 1 次，实实训时长至少 90 天，会同企业至少开发实</p> <p>— 2 —</p>
--	--

图 4 实网攻防高质量人才培养计划

### 3.2 技术投入

2024 年 4 月，三六零聚焦工业互联网安全领域人才培养需求，面向全国中、高职院校骨干教师以及企业一线技术员工，精心组织开展了“工业互联网安全运维及安全态势感知”实战班公益免费培训。此次培训旨在提升相关人员在工业互联网安全方面的专业素养与实践能力，以应对日益严峻的工业网络安全挑战。培训采用理论与实践紧密结合的教学模式，邀请了业内资深专家及技术精英进行授课，通过真实案例剖析、模拟场景演练等方式，让学员们在沉浸式的学习环境中深入理解工业互联网安全运维及态势感知的精髓，为工业互联网安全领域储备更多优秀人才奠定坚实基础。

关于举办“工业互联网安全运维及安全态势感知”  
实战班公益培训通知

各中高职院校、联盟企业：

为贯彻《国家职业教育改革实施方案》《现代产业学院建设指南（试行）》《关于加快推进现代职业教育体系建设改革重点任务的通知》等国家有关文件要求，全面落实职业院校实施学历教育与培训并举的法定职责，按照育训结合、长短结合、内外结合的要求，促进职业院校加强专业建设、深化课程改革、增强实训内容、提高师资水平和一线员工技能操作水平，促进产教融合，提升教育教学质量。

全国工业和信息化职业教育指导委员会计算机职业教育教学指导分委员会、中国教育学会职教分会、全国信息安全职业教育集团、全国信息安全产教融合共同体、北京新一代信息技术的产教联合体、京津冀信息安全产教联盟为指导单位，北京信息职业技术学院为承办单位，360 数字安全集团、神州数码集团为技术支撑单位。

拟定于 4 月 25、26、27 日（三天）举办“工业互联网安全运维及安全态势感知”实战班公益培训，现通知如下：

**一、培训目标**

通过 3 天的线上线下集中实战培训，针对工业互联网安全运维的知识点要求，做相关技能要求重点培训，参训后具备网络安全态势感知，掌握工业互联网基础和网络安全技能，能够对网络安全风险进行评估，对信息安全事件进行分析、总结和管理，掌握信息安全事件的分析能力。

**二、培训对象**

全国中、高职院校骨干教师、企业一线技术员工

**三、培训时间及地点**

1. 培训时间：2024 年 4 月 25、26、27 日（三天）

2. 报到及培训地点：线上腾讯会议

线下北京信息职业技术学院东校区 产业互联网学院

**四、培训费用**

1. 收费标准：公益培训免费，如因培训产生食宿交通费请自理。

图 5 工业互联网安全运维实战班公益培训

### 3.3 人力投入

为推进学徒制模式，开展校企“双导师”制教学。三六零集团依托高水平产教融合平台，投入企业高级工程师 3 名，进行企业导师、学校导师教学协同分工教学。企业导师参与专业人才培养方案修订、课程标准制定、课程资源建设；参与专周实训、生产性实训、顶岗实习等实践教学，融入产业新标准、新技术、新规范；校内导师完成专业基础课程、专业核心课程教学、毕业设计等教学环节。校企双导师共同承担学生职业素养、企业文化、工匠精神、工程创新能力的培养。



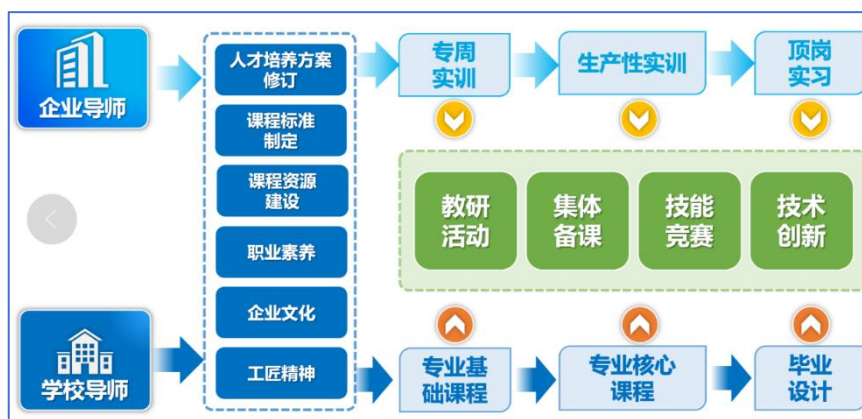


图6 校企“双导师”制教学

## 4 企业参与办学情况

### 4.1 校企合作制度建设

在推进现场工程师联合培养项目过程中，学院始终将制度和机制建设摆在首位。精心构建了涵盖项目全流程的管理体系，从招生选拔制度明确生源标准与流程，保障优质生源输入到项目中；构建课程共建机制，联合企业共同设计贴合实际需求的教学大纲与课程内容，确保理论与实践紧密结合。同时，依托学院教学资源激励制度、专任教师顶岗实践制度、横向课题管理办法，激励团队教师开发具有现场工程师特色的课程资源，鼓励教师积极参与企业技术升级改造，服务中小微企业；通过“金课名师”计划，培养高水平双师教学团队，形成校企“双导师”协同育人格局；建立严格的岗位工程师能力标准，制定现成工程师项目考核制度，通过定期课堂评估、企业反馈评价以及学生成绩分析，保证培养质量。

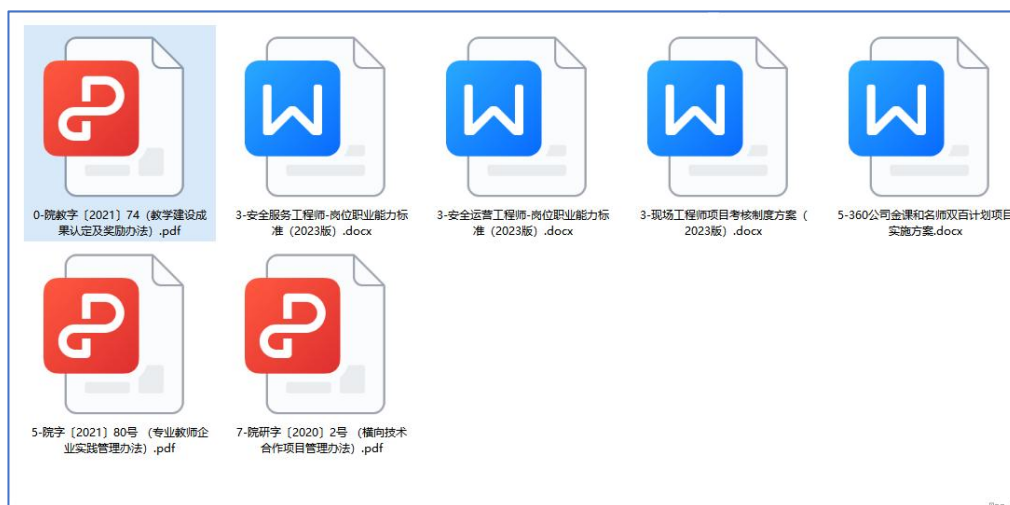


图7 校企合作制度建设

## 4.2 人才培养模式创新

三六零在推进校企协同育人过程中，充分调动“政行企校”四方面积极因素，凝练“双导师、工程化、递进式”人才培养模式。“双导师”是指充分发挥学校和企业教师两种身份优势，既塑造学生的专业知识体系，又培养学生解决问题的是能力。“工程化”是指将网络安全工程实践贯穿于人才培养的全过程。通过引入实际工程项目，让学生在真实的工程环境中学习和成长。“递进式”培养则遵循学生的认知规律和成长阶段，按照单元项目、课程项目、综合项目、岗位项目分层次、逐步推进人才培养进程。

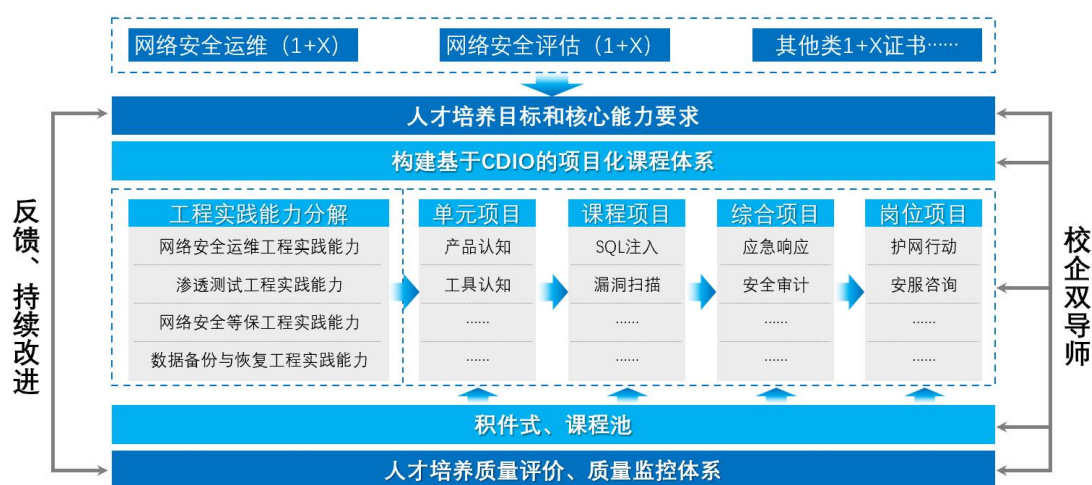


图8 “双导师、工程化、递进式”人才培养模式

## 4.3 共同修订人培方案

在推进现场工程师建设过程中，网络安全产业发展呈现新的趋势。一方面，随着网络安全与人工智能的深度融合，零信任安全、统一安全平台等新技术的出现，产业的发展趋势出现了新的变化；另一方面，伴随产业的发展，特别是网络安全产业与人工智能、大数据、物联网等技术的融合不断加深，要求网络安全人才具备多领域的技术知识和融合应用能力，特别是攻防实战的能力。在此基础上，校企双方围绕现场工程师网络安全系统部署与实施、现场维护与巡检、故障排除与应急响应主要工作场景，修订人才培养方案1次。



图9 专业动态调整机制

#### 4.4 校企共建专业课程

以产教融合为引领，以产业发展需求为导向，以提高学生就业竞争力为目标，对标信息安全主流工程实战能力，以网络安全运维工程实践能力、渗透测试工程实践能力、网络安全等保工程实践能力、数据备份与恢复工程实践能力为驱动，构建单元项目、课程项目、综合项目、岗位项目的工程化实战项目；充分发挥现场工程师紧密联系产业，技能人才储备丰富的优势，校企合作开发6门专业核心课程，对接信息安全新标准、新工艺、新规范；持续建设北京市级信息安全专业教学资源库1项、北京市级精品课程2门；实现全部课程资源上线，开展线上线下混合教学。



图10 课程开发思路

#### 4.5 校企合作开发教材

在推进现场工程师项目建设过程中，以职业教育“金教材”为标准，以产教融合为路径，以岗位需求为遵循，坚持跟岗挖掘，坚持思政育人，加强企业调研，确保教材的实用性、针对性，不断优化教材结构，丰富教材内容，创新教材形式。主持教育部新一代信息

技术领域职业教育专业课程改革试点《网络技术架构与实践》数字化教材开发 1 项，编写教育部“十四五”规划教材 1 本。



图 11 校企合作开发教材

4.6 校企共建实践项目

校企共同建立基础技能、综合技能、工程应用实训的层次化、递进式实训体系。融入人工智能、大数据等新一代信息技术，紧密贴合一线需求，还原典型业务场景，构建真项目；映射典型业务操作环境，理解业务生产逻辑，应用真设备；对接企业岗位的业务技能要求，采用真要求；具备丰富的行业实践经验，完成实践教学，要求真双师，开发校级生产性实践项目 3 项。

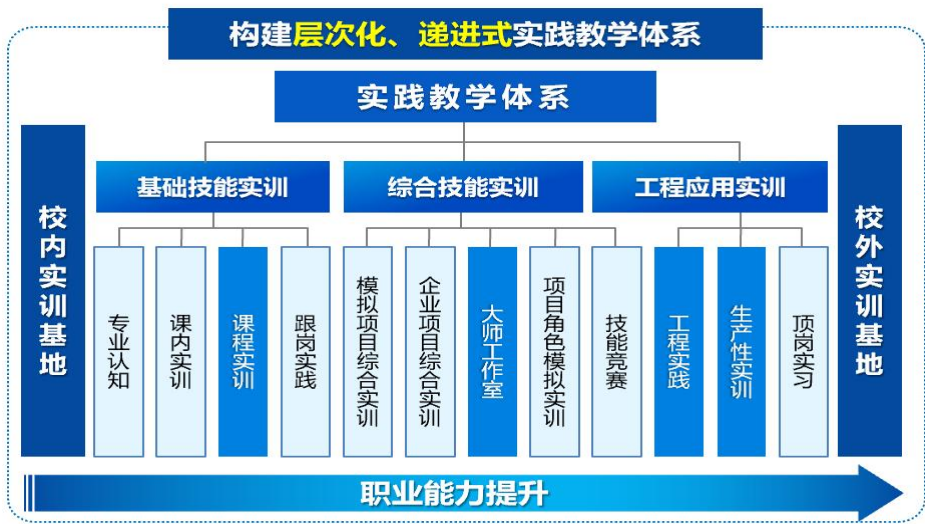


图 12 “层次化、递进式”实践教学体系

5 助推企业发展

5.1 服务企业信息人才建设



在参与北京信息职业技术学院办学过程中，企业充分依托神州泰岳信息安全工程师学院、全国信息安全产教融合共同体等高水平产教融合平台，深度挖掘并共享校企优质资源。聚焦新一代信息技术领域中小微企业在信息安全方面的需求痛点，积极开展网络架构与技术实施、超融合技术与虚拟化实施、工业互联网安全运维及安全态势感知技术系列新一代信息技术培养项目，吸引了来自不同中小微企业的众多员工参与，惠及企业员工达 318 人日，有效提升了企业整体的信息安全防护水平，为企业在数字化转型进程中的信息安全保障奠定了坚实基础。



## 5.2 服务企业技术升级改造

依托神州泰岳信息安全工程师学院以及现场工程师校企合作平台，充分发挥双方在人力资源、技术平台和研发创新等领域的协同优势，深度聚焦中小微企业的数字化转型、信息安全测评与网络安全运维需求。在科研方面成果丰硕，成功立项市级科研课题 1 项、校级科研课题 4 项；积极推动技术成果转化，顺利完成技术转让 3 项，并且与企业携手开展横向课题 3 项，在合作过程中充分结合企业实际场景，将理论研究落地应用。此外，积极致力于知识产权保护与创新驱动，申请发明专利 2 项，通过这一系列的举措，不仅有效攻克了中小微企业在数字化进程中的诸多关键痛点，还进一步提升了校企合作的深度与广度，为行业发展提供了有益的借鉴与示范。



图 14 服务企业技术升级改造

### 5.3 校企协同开发培训资源

为切实提高服务企业培训质量，精准聚焦于提升企业信息安全水平，校企双方充分发挥各自优势，携手打造网络安全运维培训包，其涵盖网络设备维护、系统监控与应急处理等全面知识与技能；开发渗透测试培训包，深入剖析攻击手段与防御策略，助力企业提前防范风险；精心构建信息安全等保测评培训包，详细解读相关政策法规与测评指标体系。通过整合学校的教育资源与企业的实战经验，培训包将理论教学与实际案例紧密结合，为企业员工提供系统且具深度的学习内容，全方位增强企业在信息安全运维、风险监测以及合规测评等多方面的能力，为企业筑牢信息安全的坚固防线。



图 15 校企协同开发培训资源



#### 5.4 促进国际交流与合作

现场工程师项目依托埃中应用技术学院海外办学条件，将信息安全专业群部分课程进行深度优化与整合，结合当地信息产业特色与实际需求，定制开发出更具针对性和实用性的课程体系，培养出具备跨文化交流能力和国际竞争力学习者；2024 年 10 月，校企双方与埃及军事学院进行深度交流，以现场工程师课程体系为样本，设计现代通信技术课程体系，为中埃信息产业发展输送高技能人才。



图 16 埃中应用技术学院师生交流

### 6 问题与展望

#### 6.1 资源整合不充分，校企共享程度不高

校企双方在人力资源共享、设备共享方面的合作程度不够深化。具体表现在学校专业教师目前还无法深度参与企业的新产品、新工艺、新流程的技术开发，还不能完全融入企业生产、组织的全过程。因此校企双方在后续建设中，将化解企业技术难点、提供智力支持、深度参与企业项目运营作为今后校企合作建设的重点。

#### 6.2 成果转化率不高，助力小微企业不足

在校企合作办学期间，产生了一批优质的科研和技术服务成果，但在成果转化方面还有存在短板。在后续的建设过程中，制定科研和技术服务成果转化方案，促进批发明、专利、软著等科研成果的转化落地，助力中小微企业发展。

### 6.3 未来与展望

360 作为数字安全的领导者，未来将以更大的力度、更多的举措、更强的技术与北京信息职业技术学院开展深度的校企合作，将企业的典型案例、解决方案、生态伙伴等资源源源不断的注入到校企双元育人中，助力职业教育良性发展，培养数以千计、万计的高素质信息安全高能人才，不断繁荣产业人才生态，构筑起大国网安的人才屏障。

#### 6.3.1 校企协同，增强专业引领能力

建立政府专家、行业专家、企业专家、学校专家 40 人规模的共同体智库。为构建与产业链相衔接的专业体系、与岗位群相衔接的专业教学标准体系、与岗位工作内容相衔接的课程体系、与岗位人才需求相衔接的评价体系提供咨询、决策、智力支撑，研制《信息安全实战化人才培养标准》、编制《2025 年网络安全人才发展报告》。



图 17 共同体发展智库

#### 6.3.2 强化技能，助推人才生态建设

校企联合举办网络安全师资技能大赛与 ISC 网络安全创新赛，建立网络安全特殊人才培养机制，通过国际、国内、政府、企业等大赛锤炼网络安全高精尖人才，通过竞赛发现和挖掘从事网络安全的“奇才”、“偏才”、“怪才”，打破网络安全人才使用的学历、年龄、专业限制，做到人尽其才，吸引更多人才投身网络安全领域，为产业人才生态注入源源不断的活力与创造力。



图 18 “一会、两赛”人才生态建设

### 6.3.3 产教融合，共建共享载体运营

校企双方以全国信息安全行业产教融合共同体为依托，通过成立现场工程师学院、安全运营中心为支撑的高水平校企合作建设载体，进行产教供需精准对接、360 特色创新班创新引岗入校、以岗育人协同育人机制；建立中小企业数字安全运营服务中心，助力中小企业解决数字化办公带来的问题。



图 19 共同体常态化运营

三六零数字安全科技集团有限公司

北京信息职业技术学院 产业互联网学院

2024 年 12 月 31 日

