常州信息职业技术学院
CCIT CHANGZHOU COLLEGE OF INFORMATION TECHNOLOGY

北京神州绿盟科技有限公司
参与高等职业教育
人才培养年度报告（2022）
信息安全技术应用

二〇二一年十一月

目　录

1. 企业概况

绿盟科技集团股份有限公司（以下简称绿盟科技），成立于 2000 年 4 月，总部位于北京。公司于 2014 年 1 月 29 日在深圳证券交易所创业板上市，证券代码：300369。绿盟科技在国内设有 50 余个分支机构为政府、金融、运营商、能源、交通、科教文卫等行业用户与各类型企业用户，提供全线网络安全产品、全方位安全解决方案和体系化安全运营服务。公司在美国硅谷、日本东京、英国伦敦、新加坡及巴西圣保罗设立海外子公司和办事处，深入开展全球业务，打造全球网络安全行业的中国品牌。

绿盟科技高度重视安全研究和技术创新，致力于跟踪国内外最新网络安全攻防技术，星云、格物、伏影、天机、天枢、天元、平行、威胁情报八大实验室，分别专注于云安全、物联网安全、威胁感知与监测、漏洞挖掘与利用、数据智能、新型攻防对抗、网络空间安全战略、威胁情报八个领域，在基础安全研究和前沿安全领域进行积极的探索，为绿盟科技的核心竞争力的持续提升提供了有力的保障。

基于多年的安全研究，绿盟科技为政企用户提供安全检查与评估类、安全检测与防护类、认证与访问控制类、安全审计类、安全运营及管理类等 60 余款高品质安全产品。其中，抗拒绝服务攻击系统（ADS）、安全和漏洞管理（AIRO）、网络入侵防护系统（IDPS）、Web 应用防火墙（WAF）等多款产品获国际权威咨询机构推崇。

随着数字中国战略的推进，绿盟科技在云计算、大数据、物联网、工业互联网、新型基础设施建设、信息技术应用创新等多个领域，不断推出适应新场景的安全产品和解决方案。

依托人工智能、大数据分析和态势感知等专业技术，绿盟科技为用户提供安全态势感知、云安全资源池、下一代威胁防护、威胁和漏洞管理、网站安全监测和防护、智能安全运营等解决方案，帮助用户在研究成果中受益。

结合多年安全实践以及对未来发展的深度思考，绿盟科技提出智慧安

全 3.0 理念。该理念以体系化建设为指引，构建“全场景、可信任、实战化”的安全运营能力，达到“全面防护，智能分析，自动响应”的防护效果。智慧安全 3.0 理念的推出，标志着绿盟科技 P2SO（Products to Solution + Operations）战略计划迈入新的阶段，向“全能力，全运营”方向进化。

在保持自身高速发展的同时，绿盟科技时刻铭记社会责任。多年来为历年全国两会、全运会、进博会以及 2008 年奥运会、2010 年世博会、2016 年 G20 会议、2017 年金砖会议、2018 年上合峰会等重大活动提供网络安全保障技术支持，并成立了绿盟科技应急响应中心。此外，还与多家重点高校建立了紧密的校企合作关系，在网络空间安全学科建设、人才培养、前沿课题研究等领域进行深度合作，并设立“CCF-绿盟科技鲲鹏基金”，为高校和科研院所在网络空间安全前沿领域的研究提供资金支持，打造以企业为主体、市场为导向、产学研用深度融合的技术创新体系。

作为巨人背后的专家，绿盟科技将一如既往以创新精神、精湛技术、优质产品、专业服务，在全球范围内，提供基于自身核心竞争力的企业级网络安全产品、安全解决方案和安全运营服务，成为备受用户信赖的网络安全公司。

2. 参与办学

常州信息职业技术学院为国家示范性高职院校，注重技能型应用技术人才的培养，培训的特点是注重实践。

以地方经济建设需要为方向，以网络安全人才培养为建设目标，2020 年常州信息与绿盟科技联手共建网络空间安全专业工业互联网安全特色的重点实验室，用于支撑工业数据安全人才培养。

绿盟科技积极和常州信息职业技术学院开展形式多样的人才培养和产教深度融合的合作活动。为了从根本上去解决教育人才培养和产业需求上存在的“两张皮”问题，双方开展以下相关工作：

（1）送企入校：学校学期中，派送“作战”经验丰富、技术能力资

深的企业技术专家进驻到学校，协助高校一起进行专业教学。提前把企业所需要的专业知识在高校对学生进行培训和传播。把企业对不同岗位人才的技术能力要求与综合能力标准要求传播到高校去，让学生更有针对性地对自我能力进行定向提升。

（2）请校入企：为了创建校企协同、实践育人的人才培养模式，解决课程内容与职业标准、教学过程与生产过程相对脱节问题，更好的将理论与实践相结合，企业请学校派遣优秀老师进到企业。派驻到企业的老师按照企业的各岗位真实需求，协作企业一起制定人才培养方案、专业教学标准、课程标准、实践标准。

（3）校企融合：结合常州当地产业情况与当地网络安全人才市场需求情况，校企以适应产业需求的网络安全人才培养为方向，共同制定了专业的课程与实验设计：

表 1　校企合作开发课程列表

序号	课程	内容	包含素材	备注
1	数据安全基础	1. 数据安全概述 2. 数据安全法律法规解读 3. 数据安全建设体系 4. 数据安全分级分类方法与实践	讲义+PPT	理论
2	数据资产测绘	1. 数据扫描发现 2. 数据分类分级 3. 数据分布地图	讲义+PPT+实验	理论+实践
3	数据安全风险评估	1. 数据环境漏洞发现 2. 数据环境配置核查 3. 大数据组件安全检查	讲义+PPT+实验	理论+实践
4	数据加密、备份与恢复	1. 数据加密 2. 数据备份 3. 数据恢复	讲义+PPT+实验	理论+实践
5	数据访问安全	1. 统一身份认证 2. 用户单点登录 3. 访问链路加密 4. 访问地址隐藏	讲义+实验	理论+实践
6	运维数据安全	1. 运维人员特权账号管理	讲义+PPT+实验	理论+实践

序号	课程	内容	包含素材	备注
		2.运维侧访问行为监控		
7	数据库安全监控	1.数据库访问行为审计 2.数据库应用关联审计 3.数据库返回结果内容过滤	讲义+PPT+实验	理论+实践
8	数据库防护安全	1.数据库攻击防御 2.SQL 语句黑白名单 3.数据库权限控制	讲义+实验	理论+实践
9	主机数据风险监控	1.主机数据入侵监测 2.主机数据泄露防护 3.主机数据加密使用	讲义+实验	理论+实践
10	数据安全异常事件分析	1.数据流转监测分析 2.数据安全事件分析 3.数据安全风险分析 4.数据安全溯源分析	讲义+PPT	理论
11	数据安全事件复现演练	1.数据安全异常事件复现 2.数据安全异常事件复现	讲义+PPT	理论
12	前沿技术研讨	1.数据脱敏技术研讨 2.个人隐私保护技术研讨 3.脱敏效果评估技术研讨	讲义+PPT	理论
14	漏洞检测与扫描技术	1.漏洞与扫描 2.RSAS 介绍和原理 3.RSAS 配置方法	讲义+实验+视频+PPT	理论+实践
15	WEB 安全防护技术	1.WEB 安全基础 2.常见攻击介绍 3.WAF 的介绍 4.WEB 安全防护策略 5.常见问题	讲义+实验+视频+指导手册	理论+实践
16	运维安全管理系统	1.堡垒机使用基础 2.运维流程 3.日常运维安全管理 4.常见问题	讲义+实验+PPT+指导手册	理论+实践

3. 资源投入

（1）校企双方共同投资共建工业数据安全实训室。为了更好支撑与保障学校的教学、科研、竞赛任务，体现常州信息职业技术学院的实训室建设与管理水平，神州绿盟科技有限公司投资 80.5 万，常州信息职业技术

学院投资 200 万联合共建工业数据安全实训室。实训室建设清单如下：

表 2　工业数据安全实训室信息表

项目名称	面积	工位数	主要实训模块	实训项目或实训内容	技术要求
工业数据安全课程教学与综合实训	90㎡	57	数据安全基础	数据安全概述 数据安全法律法规解读 数据安全建设体系 数据安全分级分类方法与实践	
			数据资产测绘	数据扫描发现 数据分类分级 数据分布地图	
			数据安全风险评估	数据环境漏洞发现 数据环境配置核查 大数据组件安全评估	
			数据容灾	数据加密 数据备份 数据恢复	
			数据访问安全	统一身份认证 用户单点登录 访问链路加密 访问地址隐藏	
			运维数据安全	特权账号管理 访问行为监控	
			数据库安全监控	数据库访问行为审计 数据库应用关联审计 数据库返回结果内容过滤	需要具备数据库基础理论知识
			数据库防护安全	数据库攻击防御 SQL 语句黑白名单 数据库权限控制	
			主机数据风险监控	主机数据入侵监测 主机数据泄露防护 主机数据加密使用	
			数据安全事件分析	数据流转监测分析 数据安全事件分析 数据安全风险分析 数据安全溯源分析	

项目名称	面积	工位数	主要实训模块	实训项目或实训内容	技术要求
			数据安全事件实战	数据安全异常事件复现 数据安全异常事件演练	
			前沿技术研讨	数据脱敏技术 个人隐私保护技术 脱敏效果评估技术研讨	
			漏洞检测技术	漏洞与扫描简介 原理介绍 使用与配置方法	
			WEB 防护技术	WEB 安全基础 常见攻击介绍 WAF 的介绍 WEB 安全防护策略 常见问题	
			运维安全管理系统	堡垒机使用基础 运维流程 日常运维安全管理 常见问题。	
仿真化工业场景建立	90㎡	57	工业化场景构建	配电（西门子 PLC 虚拟机，OPC 环境；施耐德 PLC 虚拟机，环境，上位 citect，win xp，win 7 32 位）。	
				水务（AB，上位组态王，kinscada，Win xp,xin7 32 位，server2000）。	
				水处理（施耐德 340，580，）	
				轨交	
				风电（倍福，上位组态王，kinscada，Win xp,xin7 32 位，server2000）	
				智能制造（三菱）	

序号	资源名称	资源建设内容
1	网络空间防御演练平台-基础平台	资源及网络管理系统：对底层资源的细粒度操作进行封装，向上提供对宿主机、虚拟机、虚拟网络的管理，支持通过安全能力编排配置虚拟安全设备，并提供向导模式便捷构建靶场实验环境，自带配套教学器材。
2	网络空间防御演练平台-实训子系统	应用于工业数据安全仿真实验教学，技能研究方向。具有完善的课程模块，用户模块，资源管理模块，知识库模块，试题模块，成绩统计模块，将教学与实验进行一体化承载。
3	网络空间防御演练平台-竞赛子系统	基于工业场景下，着重于攻防两端实战演练，竞赛课题编排，网安赛事的支撑子平台。
4	工业数据资产扫描工具	对接收的工业流量进行内容解析审计，包含数据访问者、数据访问时间、数据分类、数据分级等。并记录传输数据的审计日志，包含数据访问账号、数据访问时间、数据类型、数据分类、数据分级。对敏感数据检测。
5	数据安全运维工具	数据安全运维实训课程工具，对管理员与运维使用者进行权限分配，对于工业数据安全操作进行完整的记录，分析与数据安全事件溯源。
6	工业数据安全防护工具	对于工业数据库元件进行安全防护配置教学实训。包含场景化中的数据安全访问策略，数据安全防护级别设定，数据安全防护规则制定。
7	主机数据风险监控工具	用于工业主机，元器件的数据入侵监测，主机数据泄露防护，主机数据加密使用。
8	工业数据安全风险评估工具	对于工业数据进行风险评估与漏洞审查，发现收集工业虚拟资产，针对虚拟资产的基础合规监测，工业风险评定以及脆弱性检查。
9	工业数据库安全监控工具	用于全局工业化场景主要数据节点监控。对全局数据安全进行流量行为的复盘。
10	集中授权管理	工业实训设备与工业数据安全设备统一激活认证。
11	机房管理系统	可通过移动设备通过网页方式对机房进行远程管理，包括远程开关机、时间同步、系统切换、消息广播等操作，对 Ubuntu、Redhat、Centos、Fedora 等系统的立即还原和 ip 地址自动分配，在电脑本地硬盘操作系统；（win7\win8\win10\linux）的立即还原和还原点瞬间创建，支持 MBR 分区系统和 GPT 分区系统混合安装,可支持 60 个以上的不同操作系统。
12	支撑资源	3 台服务器配置为：双 CPU，10 核 20 线程，内存 256g，硬盘 4t 以上（4 块硬盘以上做 raid5），双网卡千兆、双电源。 48 口千兆交换器。 10U 物理机柜空间。

13	实训室环境	建设工业化网络安全场景实验室，突显校企合作的信安人才培养主题。 对于墙面涂绘，地面，吊顶，大屏进行改造。

4. 参与教学

结合地方产业特色与学校办学专业特色，如何针对企业需求制定专业的知识体系、课程体系、人才培养方案和课程大纲，成为校企合作的核心内容与关键节点。在不断的探索、实践、总结、迭代过程中，摸索出了校企共建、协同育人的可持续模式：

（1）基于应用场景，结合产教融合，构建符合地方发展需求的网络安全人才培养体系。

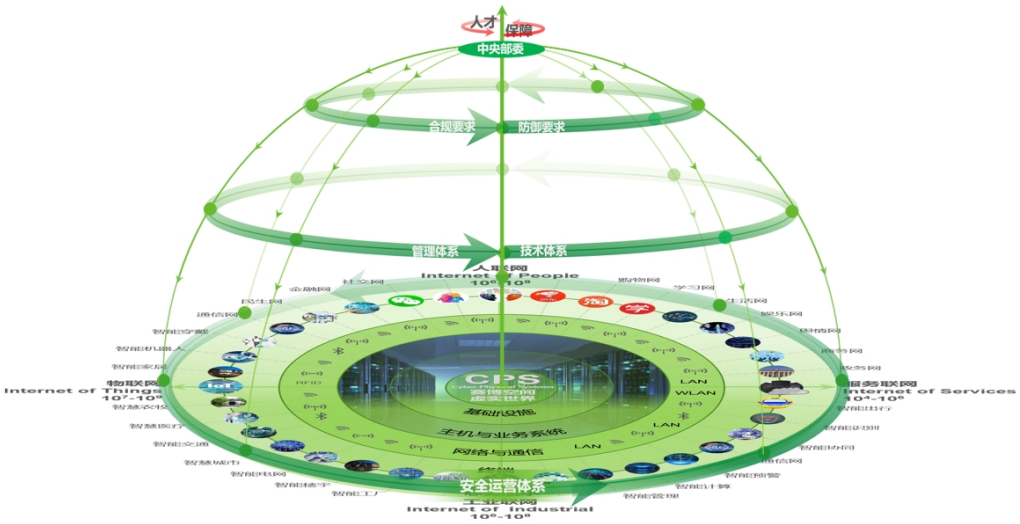

图 1　人才培养设计思路

（2）从角色岗位定位着手，引导学生如何成为各行业领域专家

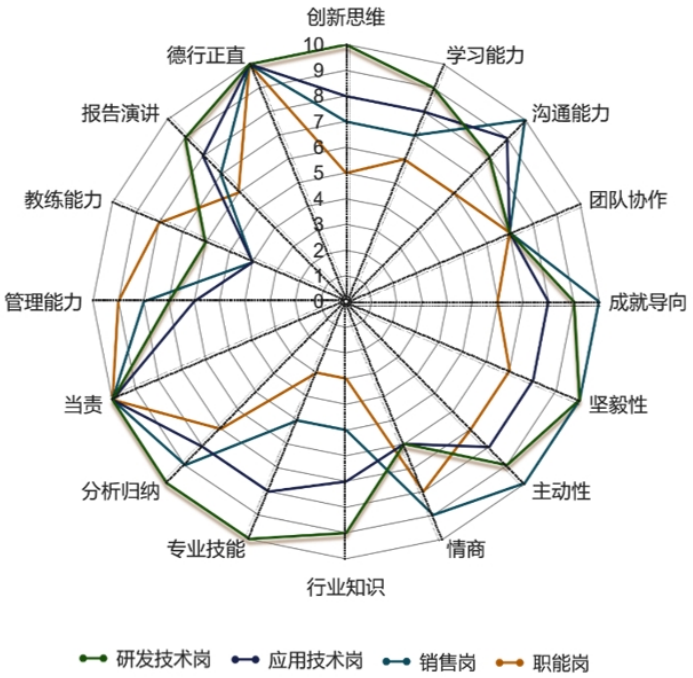

图 2 设定能力框架与毕业要求

2021 年参与《工业数据安全》课程教学，累计 3 班次，192 课时。

5. 助推企业发展

校企深度合作推动学科专业建设与产业转型升级相适应，企业以自身能力为基础助力学科建设，高校以人才培养与科学研究为己任，为企业与社会提供优质的安全人才与高质量的科研成果转化。

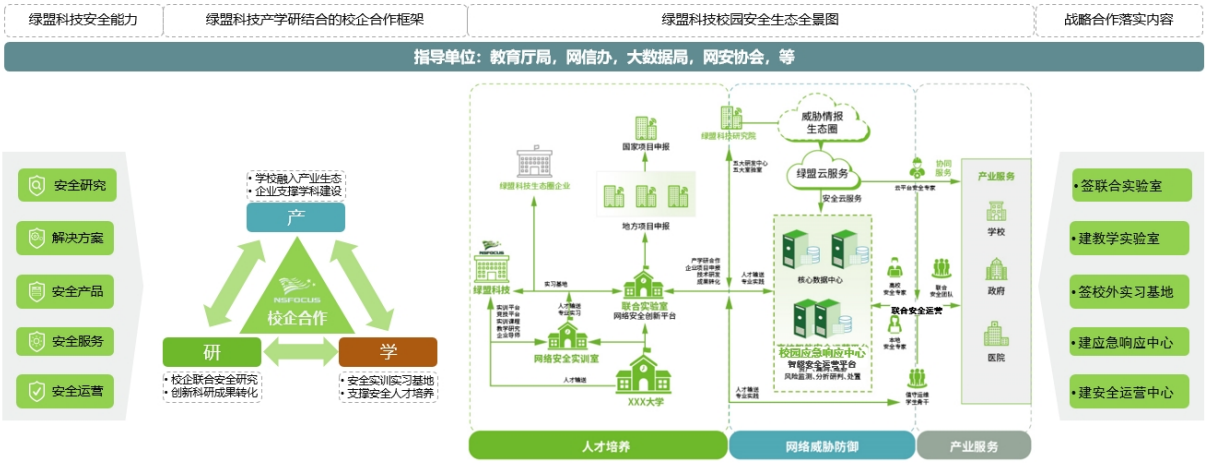

图 3 校企深度合作体系图

（1）校企联合共同进行人才培养，解决企业专业人才需求。校企共同进行工业数据安全领域人才培养，以满足技术水平发展需求与地方产业发展需要。当下我国网络安全人才缺口巨大，企业同样面临网络安全人才供不应求的问题。2020 年合作至今，累计储备网络安全人才 50 余人，且储备梳理仍在持续增长，逐步满足市场对网络安全人才的数量需求。不仅解决了社会对网络安全专业人才需求、又能解决学生就业问题，同时企业也扩大了商业市场。

（2）校企联合开展“新领域”学科共建，拓展企业产品推广及应用。在校企合作过程中，企业提供在工控领域内安全能力，校企共同完成产学研用的相关转化。经过高校转化的课程内容，更适合投入教学；经过实践过的课程内容，对人才培养更具针对性；经过实际市场需求优化过的企业产品，对市场更具推广及应用性。

（3）助力企业横向开拓教育市场。借助校企深度合作的契机，学校积极辅导和鼓励企业横向推广合作成果。学校团队指导企业讲师开展教学的基本技巧和教学理念，引导企业产品适应市场发展方向。以点建面，以面塑体，扩大成果使用群体，牵动区域院校共同开展“新领域”研究，共同优化人才培养体系，完善人才培养内容。

6. 服务地方

常州的十大支柱产业中大多数为国家制造发展的重点领域，并且有一半以上的产业涉及到工业互联网领域。工业互联网战略的发展对地方经济转型意义深远。《常州市关于深化“互联网+先进制造业”发展工业互联网的实施意见》，又进一步明确了围绕工业互联网发展新经济的工作思路与目标。结合当下工业互联网数据安全发展态势，专业人才培养与储备已迫在眉睫。

2020 年 6 月校企双方达成了合作共识，在国家战略与社会需求的大背景下，工业数据安全实训室正式成立。成立至今已专业网安人才储备已接近百人，且目前尚处于初期探索阶段，当模式成熟之后考虑扩大人才培养规模。

7. 保障体系

（1）组织保障

在企业与单位领导高度重视下，基于学术委员会和督导组的监督和指导，成立由校二级学院\系主任为领导核心和企业技术总监、教研室主任、专业带头人、企业技术骨干广泛参与的专业建设团队，对专业建设规划、实施过程、效果进行监控管理。共同组建工作小组，按照“产、学、研”的功能定位，设置组织及负责人，由企业和高校学院协同完成其职能。

（2）政策保障

完善专业建设中涉及教学资源、师资队伍等方面的管理考评方法。实行负责制、专人专管、专款专用，加强过程控制，实施科学管理等，保障专业建设各项工作顺利进行。

（3）经费管理

统筹安排使用由不同渠道下达或筹集的专项资金，并对建设项目的实施和资金的投向及资金年度调度安排实行全过程管理，确保预期建设目标的实现；学院财务处是专项资金的具体管理部门，负责专项资金的财务管理和核算工作；专项资金按财政国库管理制度的有关规定办理支付，设置单独账户进行核算，专款专用、专账管理。

8. 问题与展望

我们将围绕贯彻落实《教育信息化 2.0 行动计划》、《中国教育现代化 2035》，以及《关于深化产教融合的若干意见》等发展战略，顺应网络安全新方向的发展潮流，探讨人才培养改革创新的理论与实践，适应和引领网络安全技术发展新常态，培养具有国际竞争力的高素质创新型技术型人才；我们将基于新培养的双师型专家团队，积极探索为常州本地的工业制造行业提供可靠的安全运营服务、应急响应服务、安全咨询服务等；为学生赋予安全建设规划的能力、安全事件处理能力、以及安全运维能力。同时我们将基于产学研用的合作模式，共同推进工业数据安全领域的高速发

展。

构建校企统筹融合发展格局，坚持以需求为导向的人才培养模式，促进教育与企业联动发展。积极转化合作成果，将产学研用的可持续性发展循环运作起来。将优质的人才源源不断的输入到社会当中去，将行业领域内的新技术注入到人才培养过程中、反哺到产品功能开发中。

校企合作过程中，企业与学校保持需紧密合作。绿盟科技将作为“巨人背后的专家”与常州信息职业技术学院携手长期开展网络空间安全领域的人才培养与安全技术研究。