PDF-XChange Editor
Click to BUY NOW!
www.tracker-software.com

指导委员会（排名不分先后）

郝志强　封化民　刘欣然　鲁　辉　谷红勋
谢　懿　苗春雨　段平霞　郭　盛　李　强

工作委员会（排名不分先后）

黄　惠　刘亚天　李海明　杜　妍　谭　念
王淑燕　于天娇　许斯欣　邱紫情　王一新
李小丽　李玉昭

序言
PREFACE

随着互联网的普及，我国数字经济规模不断扩大，网络安全问题也引起了越来越多人的关注。保障网络安全不仅事关个人信息安全，也涉及国家安全、社会稳定等多个层面。2021年底，中央网络安全和信息化委员会印发《“十四五”国家信息化规划》（以下简称《规划》），对我国“十四五”时期信息化发展作出部署安排。《规划》围绕确定的发展目标，部署了10项重大任务，其中明确提出要“培育先进安全的数字产业体系”。加强网络安全和信息化工作、建设网络强国势在必行，而人才便是这其中的关键一环。

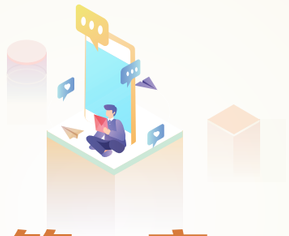
放眼中国乃至世界，政策法规、经济、技术、投资等多项驱动力共同推动着网络安全进入发展的黄金期，网络安全的人才培养力度也在不断加大，但依然尚未跟上产业的发展需求，国内外均面临着大规模的网络安全人才短缺。2023年伊始，以ChatGPT为代表的生成式人工智能爆发，对网络安全从业者的工作和在校生的专业学习与就业均带来了前所未有的挑战。

为深入研究网络安全人才的供需、培养与发展情况，工业和信息化部教育与考试中心、北京市海淀区互联网信息办公室、教育部高等学校网络空间安全专业教学指导委员会、中国网络空间安全人才教育论坛、安恒信息、智联招聘等单位集合各自优势资源，汇集在网络安全人才培养方面的研究成果，结合人才培养实践，进行高校走访、企业调研、专家咨询、策略分析，共同牵头编写《2023网络安全产业人才发展报告》，对我国网络安全人才发展进行了一次系统性的调研分析。本报告数据主要来自智联招聘平台大数据、问卷调研数据等。问卷调研分别面向网络安全从业者和在校生，覆盖北上广深、新一线城市、省会城市等全国重点城市的众多企事业单位和高等院校。

结合以上数据，本报告通过梳理国内外网络安全产业及人才概况，总结当前网络安全产业的人才从业与培养现状、人才供需结构等方面，结合当下人工智能技术的突破式应用、数据安全等热点话题，洞察网络安全产业人才培养与发展的新趋势，并提出了相关的人才发展建议。希望此份研究报告能够对政府部门、科研院校、用人单位及有志于从事网络安全工作的求职者，提供有价值的参考借鉴。

目录
CONTENTS

PDF-XChange Editor
Click to BUY NOW!
www.tracker-software.com



第一章

国内外网络安全产业及人才发展概况

8月1日，美国国家网络总监办公室发布《国家网络人才和教育战略》，标志着美国开启为期数年的系统性培养网络安全技能和能力计划。实际上，随着人们对互联网设备和技术依赖程度的提高，网络黑产有了滋长空间，网络漏洞变得更加普遍，网络安全的重要性不断上升。目前，网络安全问题主要来源于硬件、软件和网络使用管理及信息安全等方面。本章通过分析和对比欧美及国内网络安全产业及人才整体发展情况，为网络安全问题的解决提供思路及借鉴。

第一节 | 欧美等发达国家网络安全产业及人才发展概况

一、欧美网络安全领域立法不断加强

今年6月，美国众议院军事网络、信息技术和创新小组委员会发布《2024财年国防授权法案》（NDAA），以技术和网络为重点制定新战略，促进对五角大楼网络安全计划的更全面审查。美国证券交易委员会提出的网络安全和隐私规则草案将要求上市公司披露具有安全知识或经验的董事会成员。美国康涅狄格州发布《康涅狄格州数据隐私法》的相关指南，对大型科技公司提出了全面的隐私要求，还要求更广泛实体进行儿童隐私保护。

欧洲议会成员就《网络弹性法案》（Cyber Resilience Act）中有关制造商的义务以及如何适用于开源软件的条款进行了讨论。英国信息专员办公室（ICO）发布了对拟议的《数据保护和数字信息法案》（Data Protection and Digital Information Bill）的意见。荷兰政府宣布将各分散的网络安全机构融并为一个单独的国家机构。新西兰内政部（DIA）公布了一项提案，呼吁建立一个新的全行业监管机构，以保护新西兰人免受社交媒体和其他数字平台上的有害内容的侵害。

总体来说，欧美网络安全立法有不断加强的趋势，网络安全与国家安全、个人隐私、商业活动等紧密联系，欧美从各维度加强了对网络安全的监管。

二、全球网络安全产业稳步增长

根据IDC于2023年发布的《全球网络安全支出指南》，2022年全球网络安全总投资规模预计将达到1955.1亿美元，有望在2026年增至2979.1亿美元。另据Gartner《2021-2023年全球信息安全与风险管理细分市场终端用户支出报告》，2022年全球的信息安全与风险管理产品和服务支出1691亿美元，2023年预计将超过1883亿美元，增长11.3%。

近年来，全球网络安全行业创新风向标——美国RSAC大会创新沙盒竞赛的入围十强企业，主要集中在云安全、数据安全、软件供应链安全、身份安全四个热门赛道。2023年，受AI技术爆发的影响，智能化网络安全应用成为新热点。今年创新沙盒公布的十强企业中，有三家是通过智能技术应用来提升网络安全能力，应用方向分别为智能SOC、智能网络攻防和智能数据治理与隐私安全。在安全自动化赛道，来自美国和以色列的公司实现了自动化的事件分析和快速响应，以及与用户企业业务互动的工作流程。

今年3月，美国微软公司推出了基于GPT-4的网络安全助手Security Copilot，可帮助防御者识别网络入侵。该安全助手集成了OpenAI的GPT-4生成式人工智能和微软的安全专用模型，网络安全人员可输入文件、网址或代码片段进行网络安全分析、询问某个特定漏洞的概要或从其他安全工具中获取安全事件及警报信息。Security Copilot是第一个生成式人工智能安全产品，可服务于安全团队，以人工智能的速度和规模执行工作。

综合来看，无论从产业规模，还是技术应用落地来看，网络安全产业在全球都实现了快速发展。随着各行各业的数字化转型，网络安全产业还将具有长足的发展空间。

三、全球网络安全人才缺口较大

网络安全专业人才是数字经济下劳动力市场不可或缺的组成部分，但人才缺口较大，据相关数据调查，当前已有数以百万计的相关职位空缺有待填补。

例如，目前全球有340万网络安全职位正在招聘但未能找到相应人才。同时，美国也有超过70万的网络安全职位空缺，主要集中于那些能专职保护公司、客户和基础设施安全的人才。

据美国信息系统审计和控制协会（ISACA）的研究，网络安全的两个主要技能缺口是软技能和云计算知识。为了帮助建立网络安全劳动力职业路径并填补现今的空缺职位，需要来自各种不同背景的专业人员，把这些软技能带到网络安全前线。麦肯锡认为，企业可以拓宽潜在应聘者的寻找范围，识别并保留背景更多样的候选人。另外，还应该培养网络安全团队领导人合作解决问题的能力，帮助其重新审视团队内的职业发展策略，消除传统的职业发展障碍，建立更具包容性的工作场所文化。

为了更好防范安全威胁，企业除了引进软技能及云计算方面的技术人才外，还应加强全体员工的网络安全培训。一些安全事件往往由业务项目和网络钓鱼而起，通过改善各行业、各岗位的网络安全培训，企业可以推动建立安全第一的文化，让安全成为每个人的职责。例如，亚马逊正在帮助更多人认识到网络安全的重要性，联合美国国家网络安全防范联盟发起“保护和连接”网络安全意识宣传活动，并向全世界个人和企业免费提供网络安全意识培训。

结合全球网络安全人才现状，可以看出网络安全岗位需求与人才供给不匹配的矛盾仍然存在，全球网络人才缺口较大，领先的科技公司已经在培养发掘人才方面做出了表率。

第二节 | 我国网络安全产业概况及人才发展概况

一、我国网络安全领域政策规定不断完善

今年1月，《工业和信息化部等十六部门关于促进数据安全产业发展的指导意见》（以下简称《指导意见》）发布。《指导意见》聚焦数据安全保护及相关数据资源开发利用需求，提出促进数据安全产业发展的总体要求，并按2025年、2035年两个阶段提出产业发展目标。指导意见分两个层面明确促进数据安全产业发展的七项重点任务，明确了提升产业创新能力、壮大数据安全服务、推进标准体系建设和推广技术产品应用四项重点任务。

今年5月，国家互联网信息办公室发布《数字中国发展报告（2022年）》，要求强化数字中国关键能力。构筑自立自强的数字技术创新体系。筑牢可信可控的数字安全屏障。推动网络安全法律法规和政策体系持续完善，不断增强网络安全保障能力。

二、我国网络安全产业发展更加清晰明确

2022年我国全年国内生产总值（GDP）超121万亿元，其中数字经济规模达50.2万亿元，占GDP比重为41.5%。其中，典型网络安全产业规模达到900亿元，在数字经济中的占比达到0.18%。与2021年数字经济在GDP的占比（40.7%）及网络安全在数字经济中的占比（0.16%）相比，2022年均有显著提升。

根据《指导意见》的官方解读，数据安全产业聚焦数据全生命周期安全保护和开发利用的需求，支持相关技术、产品和服务的研究开发。网络安全产业主要从保护数据存储、处理、传输等载体的角度，实现对网络数据完整性、机密性、可用性保护，主要包含网络边界防护、计算环境防护等方面的技术、产品和服务。

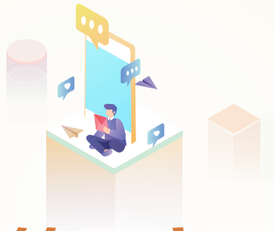
当前我国网络安全企业在学习国外先进技术的同时，国内需求侧对创新的驱动更为显著。数据安全在创新方面的比重已接近传统安全领域，我国网络安全重视攻防、安全运营、SOAR等更具实战化的赛道，工业安全、汽车安全、安全芯片等赛道符合我国新型行业对网络安全的需求。海外市场为我国网络安全企业带来新的机遇，网络安全国际市场、国家海外利益保护、中东/东南亚数字化加速带来的配套网络安全市场均是潜在增长点。

三、我国网络安全人才培养加快

目前，我国网络安全人才培养加快。截至2023年3月，国内已有80所高校开设网络空间安全专业，132所高校开设信息安全专业，2所高校开设保密技术专业，17所高校开设信息对抗技术专业，28所高校开设网络安全与执法专业。同时，我国各高校正在逐步加强网络安全高层次人才培养力度。

对于企业而言，当前网络安全业务份额越来越重，但是招到匹配和适合的网络安全技术人才却并不容易。从人才培养角度来看，深耕研究的定向人才十分缺乏，实战人才也处于供不应求的状态。日益增加的网络安全招聘岗位数，愈发精确地面向专业人才。

PDF-XChange Editor
Click to BUY NOW!
www.tracker-software.com



第二章

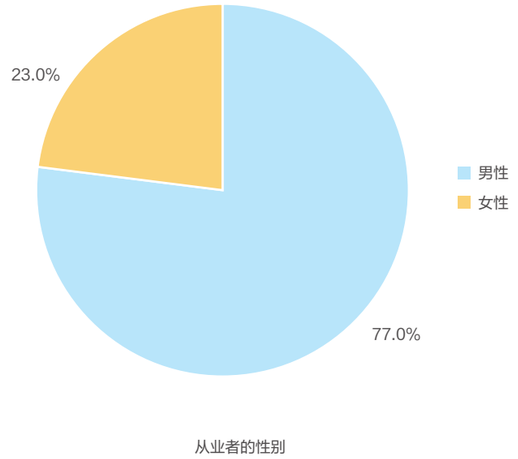
网络安全人才从业现状

随着网络安全产业的快速发展，网络安全人才的从业现状也引起业界关注。本章将通过分析面向网络安全从业者的问卷调研数据，从性别、年龄、专业等方面为网络安全人才画像，并观察当前网络安全从业者的工作岗位、企业/行业、城市等以及企业薪酬福利情况等，全面刻画网络安全人才的从业现状。

第一节 | 我国网络安全从业人才画像

一、男女比重为77：23

问卷调研数据显示，2023年，网络安全从业人才中，男性和女性分别占比77%、23%。一方面，从专业学习来看，就读于网络安全相关理工科专业的男性比重更高，因而在后续就业中的占比也高于女性；另一方面也表明在当前的网络安全领域，男性仍是产业劳动力的主体。

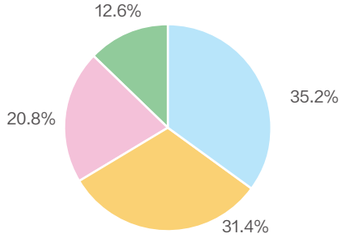


二、行业从业者逐渐年轻化

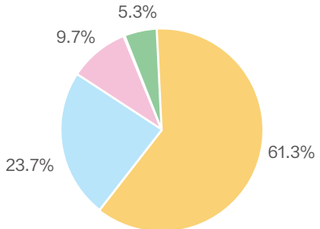
从年龄来看，2023年，31-40岁的网络安全从业者占比最高，达到35.2%，但低于2022年的50.8%和2021的59.7%，该年龄段从业者的占比呈逐年下降趋势。相比之下，18-25岁网络安全从业者的占比呈逐年上升趋势，2021年、2022年、2023年的占比依次为3.2%、11.2%、31.4%。另外，2023年26-30岁的从业者占比为20.8%，40岁以上占比12.6%。由此可见，网络安全从业者逐渐年轻化，更多的年轻从业者涌入该行业，为行业的未来发展注入了新鲜的活力。

三、本科毕业生占比超6成

从学历来看，2023年，本科毕业的网络安全从业者占比最高，达到61.3%。其次是高职高专和硕士研究生以上学历的从业者，分别占比23.7%、9.7%。本科学历从业者一直是网络安全领域的主要人才供给，在2022年、2021年的调研数据中，分别占比59.3%、63.9%。可见，网络安全从业者学历素质整体偏高。



从业者的年龄



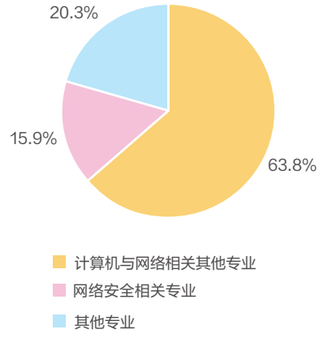
从业者的学历

四、6成以上网络安全从业者专业为计算机与网络

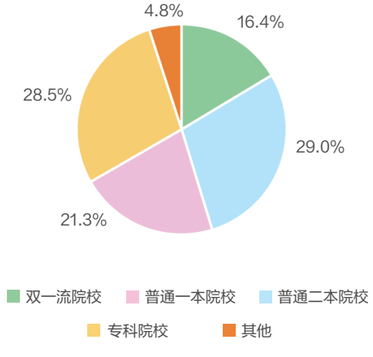
问卷调研结果显示，受访者中，63.8%的最高学历专业为计算机与网络相关专业，其次是网络安全相关专业，占比15.9%。可以看出6成以上网络安全从业者的业务领域与所学专业有所区分，一方面，网络安全一级学科和专业开设时间较晚，目前新一代科班毕业生刚刚进入网络安全产业，导致网络安全相关专业的从业者占比较低，另一方面，这也表明网络安全行业凭借行业优势及学科交叉特性，吸引了较多“跨专业”人才就业。

五、16%从业者来自双一流院校

调研数据显示，网络安全从业者中有16.4%毕业于双一流院校，占比较高，可见网络安全领域对名校毕业生较有吸引力。此外普通二本、普通一本、专科院校的占比分别为29%、21.3%、28.5%，分布较为均衡。网络安全人才队伍呈现层次化、多样化特点，人才发展注重应用导向和实战导向，因此网络安全从业者的毕业院校分布相对比较均衡。



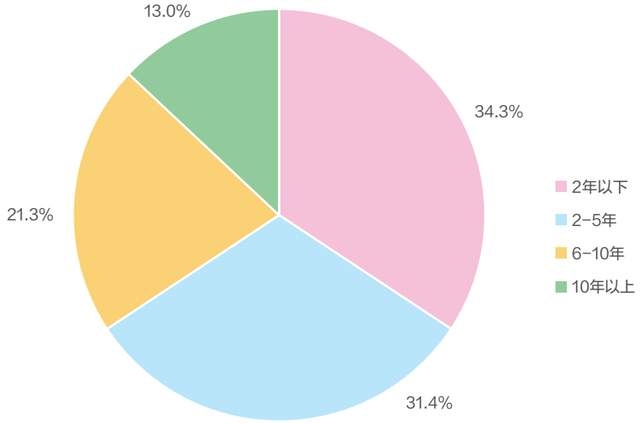
从业者最高学历专业



从业者最高学历的毕业院校

六、5年以下工作年限从业者占比超6成

从工作年限来看，34.3%的受访者工作2年以下，占比最高。其次是2-5年、6-10年工作者，占比分别为31.4%、21.3%。由于网络安全产业兴起时间不长，目前处于稳步上升阶段，从业者整体上也处于探索和成长阶段，拥有较长工作经验的从业者占比较低。

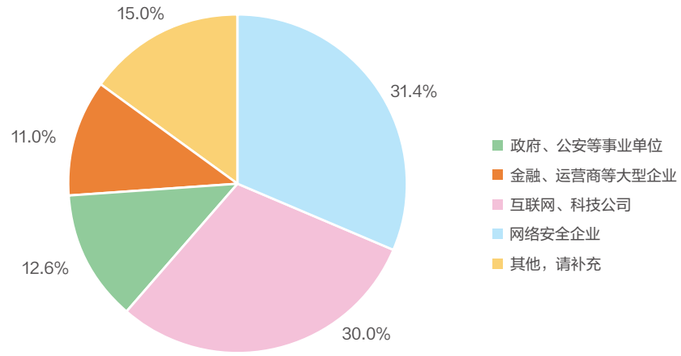


从业者的工作年限

第二节 | 网络安全产业人才的从业现状

一、网络安全企业和IT行业成产业人才汇聚地

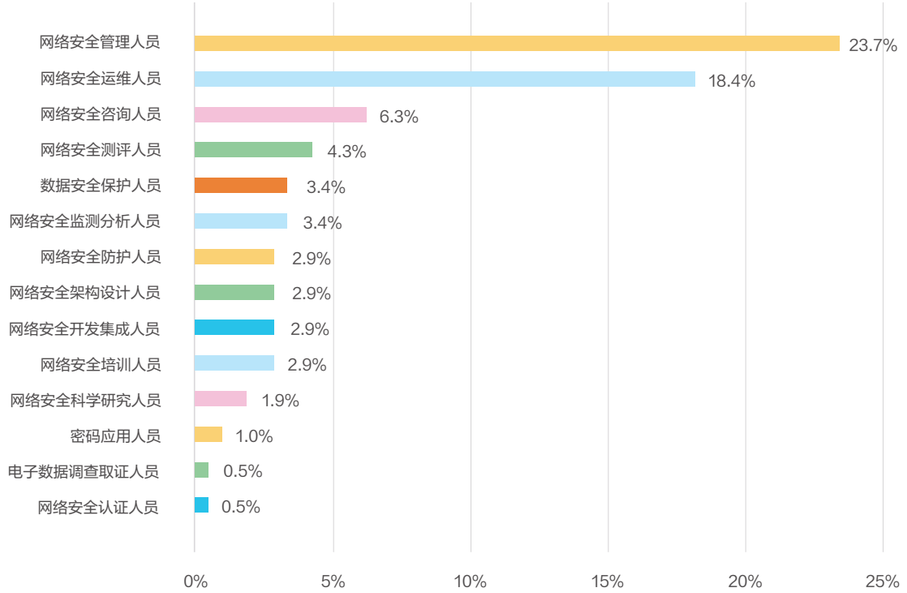
从问卷调研结果可以发现，网络安全企业是网络安全产业人才的主要聚集领域，占比31.4%，排名第一。其次是互联网、科技公司，占比30%。此外，政府、公安等事业单位，以及金融、运营商等大型企业，占比分别为12.6%、11%。可见，网络安全企业和IT行业是当前网络安全专业人才的主要汇聚地。



从业者所处的行业

二、安全管理和安全运维人员占比较高

从岗位来看，受访者中，从事网络安全管理工作的人才占比最高，达到23.7%。其次是网络安全运维人员，占比18.4%。而网络安全咨询、网络安全测评、数据安全保护等其他岗位的从业者占比均低于7%。在具体的工作中，管理及运维类职能范畴相对宽泛，是网络安全人才的两大主要就业领域。

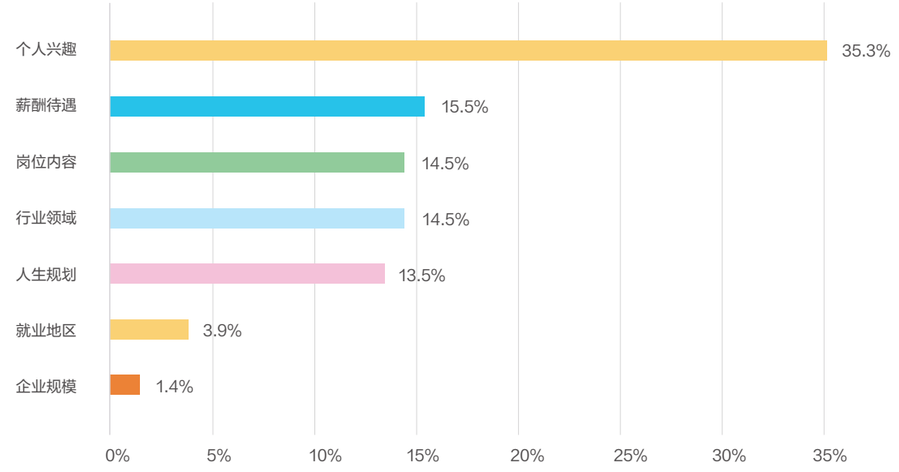


2023年从业者的工作岗位

三、3成以上人才因个人兴趣选择从事网络安全行业

调研数据显示，在今年的受访者中，35.3%表示因个人兴趣选择从事网络安全行业，高于选择薪酬待遇的15.5%，也高于2022年选择个人兴趣而入行的7.2%。

从年龄看，18-25岁受访者因个人兴趣而入行的占比最高，为46.2%，其次是26-30岁、40岁以上和31-40岁的从业者，选择该项的占比分别为34.9%、34.6%和26%。新一代年轻人更倾向于以热爱为激励，把个人兴趣与职业相结合。随着越来越多年轻人加入网络安全行业，与薪酬待遇等“身外物”相比，因“真爱”而入行网络安全也显得更为普遍。

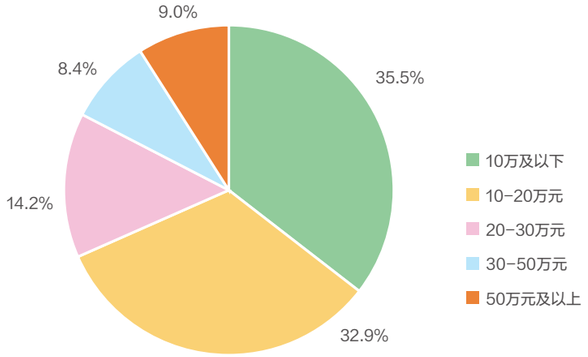


从事网络 安全工作的原因

第三节 | 网络安全产业人才的薪酬及福利待遇

一、近2成从业者税前年薪30万元以上

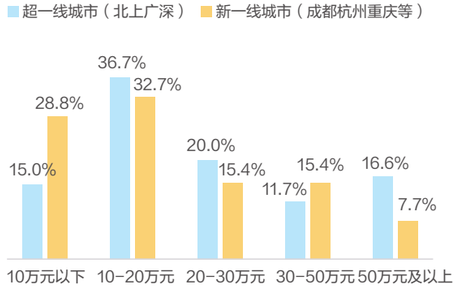
问卷调研结果显示，35.5%的受访者税前年薪不足10万元，但更多的从业者拥有较高的薪酬水平。其中，32.9%的从业者薪酬在10-20万元之间，14.2%的从业者税前年薪为20-30万元，8.4%从业者税前年薪为30-50万元，还有9.0%的从业者拥有50万元及以上的高薪。网络安全是一个快速发展的朝阳行业，对从事相关工作从业者的技能要求也较高，因此企业更愿意为保护系统和数据免受网络威胁的专业人员提供优厚的薪酬待遇，预计未来网络安全人才的薪酬及福利待遇也将稳步提升。



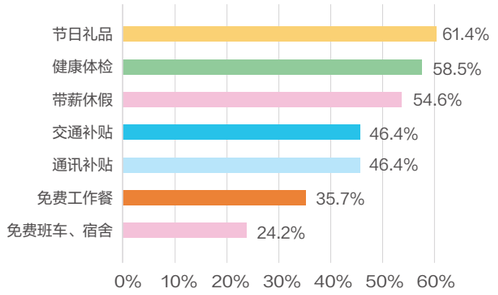
从业者的税前年薪水平

从城市看，36.7%的超一线城市（北上广深）网络安全从业者税前年薪在10-20万元之间，占比最高，且高于总体水平。其次，北上广深从业者的税前年薪水平在20-30万元、50万元及以上的占比分别为20%、16.6%。在新一线城市，32.7%的网络安全从业者税前年薪水平在10-20万元之间，占比最高，其次是10万元以下，占比是28.8%。可见，相比新一线城市，北上广深凭借多年来积累的雄厚经济实力，使网络安全从业者得以拥有更高的薪酬。2023年上半年，重庆、苏州、成都、杭州、武汉、南京等新一线城市在全国各大城市GDP排名中进入前十，且重庆超越广州，排名全国第四位。随着城市的崛起和经济的发展，未来新一线城市的网络安全从业者有望获得更高的薪酬。

从福利待遇来看，61.4%的受访者表示所在企业提供节日礼品，58.5%提供健康体检，54.6%提供带薪休假。拥有交通补贴、通讯补贴、免费工作餐、免费班车和宿舍等福利待遇的从业者，占比均在50%以内。可见，网络安全企业除了能提供优厚的薪酬待遇之外，在节日礼品、健康体检等软福利方面也有比较出色的表现，更能体现对从业者的人文关怀。



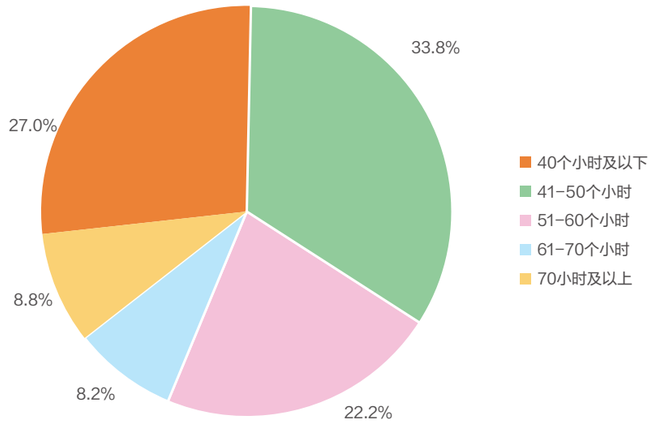
不同城市从业者的税前年薪水平



从业者所在企业提供的福利待遇

二、超7成从业者每周工作时长40小时以上

问卷调研数据显示，73%的网络安全从业者每周工作时间超40个小时。其中，33.8%的从业者每周工作41-50小时，22.2%每周工作51-60小时。因工作性质原因，网络安全从业者需要时刻保持警惕，随时应对可能或已经发生的网络安全漏洞和风险，因此工作强度较高，加班情况较为普遍。

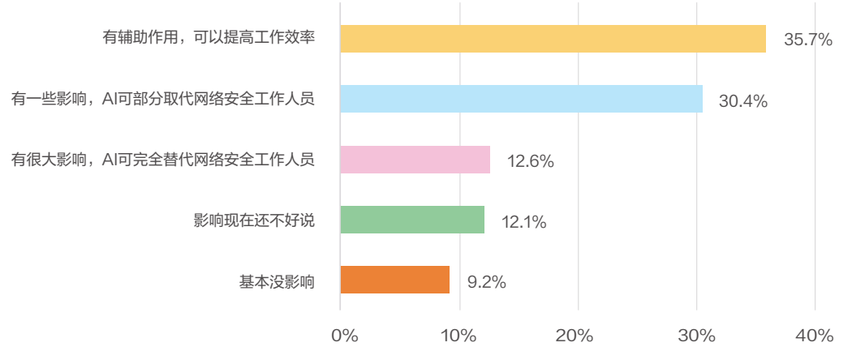


从业者的每周工作时长

第四节 | 网安人才的AI技术应用

一、超3成从业者认为5年内AI将对网络安全有辅助作用

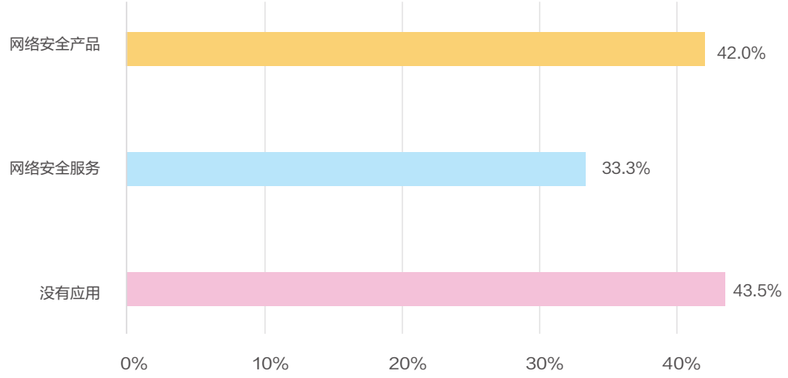
面对发展迅猛的AI技术，一些从业者担心被机器替代。调研问卷结果显示，35.7%的受访者认为，AI技术将在5年内对网络安全人才带来自动监测和分析等辅助作用，占比最高。也有30.4%的受访从业者较为保守，认为AI可部分替代网络安全人才。只有9.2%的从业者认为AI对网络安全人才几乎无影响。可见，网络安全人才对AI的辅助和替代作用都保持相对冷静客观态度，部分从业者对这项技术持乐观心态，认为可以提升当前工作效率；同时有相当一部分从业者对AI技术的行业影响保持观望且警惕的心态。



从业者对AI影响工作的看法

二、7成以上网络安全人才所在企业在产品或服务上运用AI技术

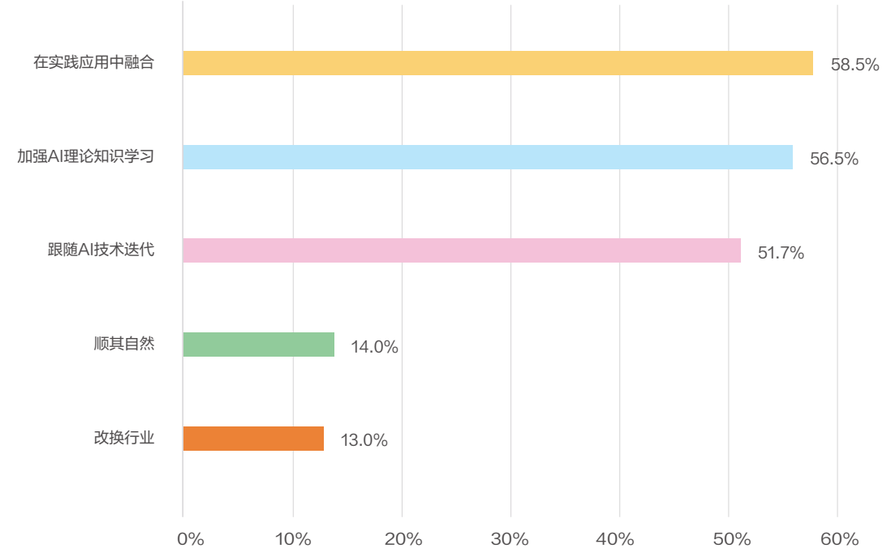
谈及所在企业对AI技术的应用，56.5%的受访者表示，所在企业应用了AI技术。具体到应用领域上，42.0%的受访者所在企业在网络安全产品上应用了AI技术；33.3%在网络安全服务方面应用了AI技术。这表明，目前AI技术在网络安全领域的应用较为广泛。就目前来看，虽然多数网络安全企业已经将AI技术应用于相关产品或服务，但更多是传统层面的AI技术，随着人工智能大语言模型突飞猛进式的发展，未来应用于网络安全产品和服务的AI技术也有望得到刷新。



所在企业应用AI技术的方面

三、近6成从业者将在实践应用中融合AI技术

为了应对AI技术的不断迭代，58.5%的受访者表示将在实践应用中融合AI技术，占比最高。其次是加强AI理论知识学习和跟随AI技术迭代，占比分别为56.5%、51.7%。AI技术的快速普及，让人们对AI的应用意识更加强烈，网络安全从业者愿意通过实践提升AI技术融合能力，并加强AI知识的更新换代。



从业者计划应对AI技术的方式

第三章

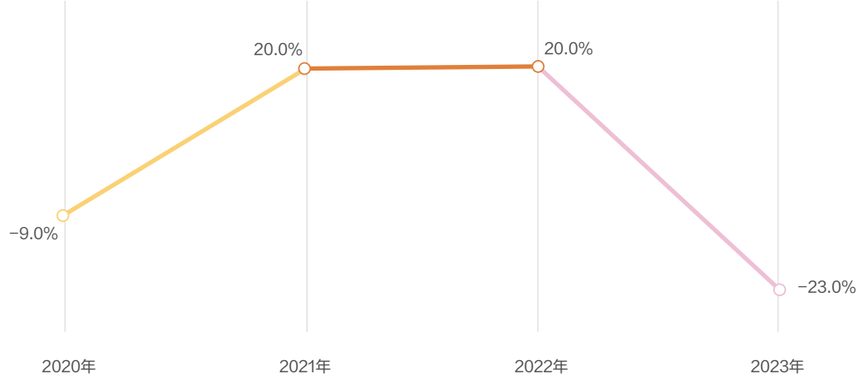
网络安全产业人才供需分析

网络安全产业的发展推动了人才招聘需求的增长，也激活了相关领域的就业，带动了人才供给。本章将以智联招聘的平台数据为依据，从网络安全产业人才的供需两个维度出发，盘点人才供需情况。

第一节 | 网络安全产业人才需求

一、网络安全产业招聘职位数呈现波动

从网络安全人才需求来看，该产业招聘职位数呈现波动趋势。智联招聘平台数据显示，2021和2022年网络安全相关岗位招聘数量分别同比增长20.0%，2023年则有所下降。考虑到每年平台数据统计周期为上一年7月至今年6月，而2022年下半年疫情较严重，同时受国内外经济波动影响，部分行业在投资、拓展业务等方面有所收缩，企业人员增速放缓，同时内部推荐选才比例有所上升，因而网络安全产业招聘职位需求呈现出波动状态。

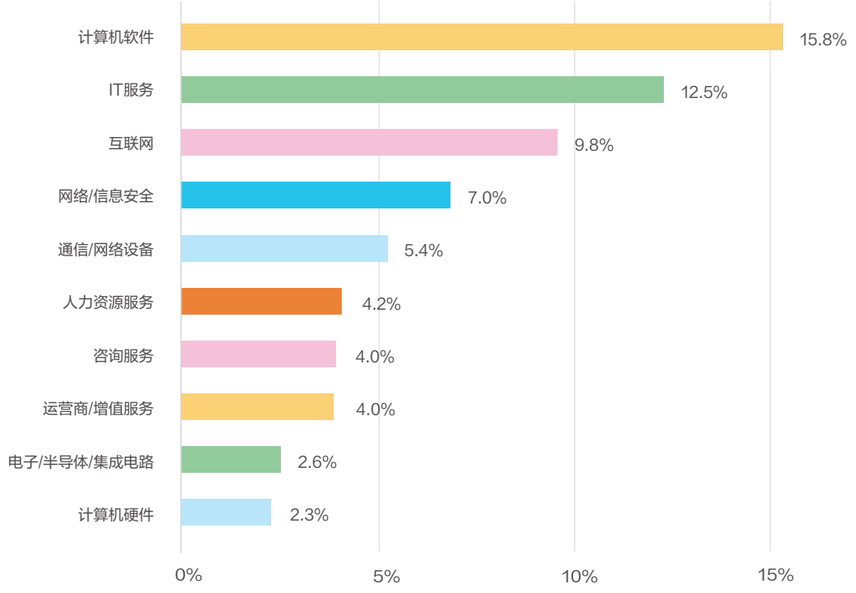


网络安全人才需求同比增速

数据来自智联招聘

二、计算机软件、IT服务、互联网招聘需求排名前三

从招聘职位所在行业分布来看，2023年招聘网络安全岗位数量最多的是计算机软件行业，占比15.8%。其次是IT服务和互联网行业，招聘职位数占比分别为12.5%和9.8%。此外，网络/信息安全、通信/网络设备、人力资源服务、咨询服务等行业，也对网络安全人才有较大需求。

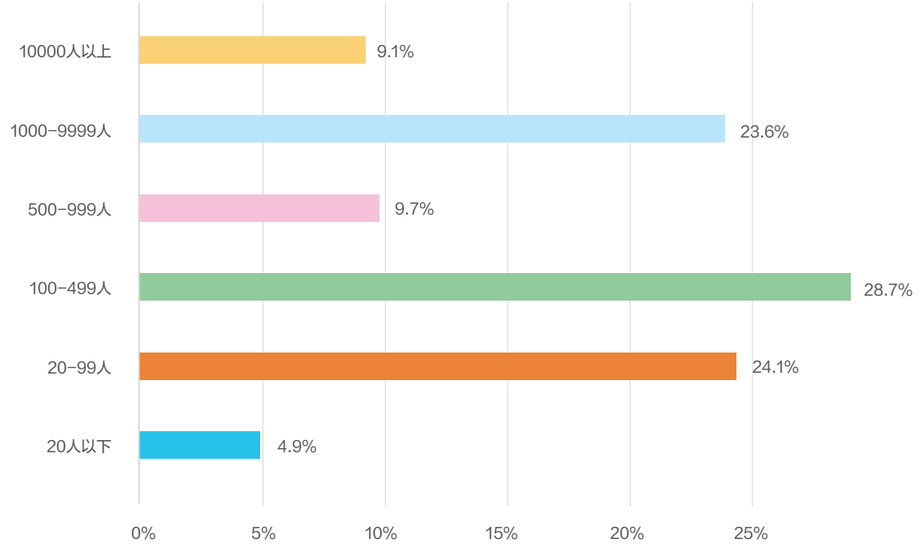


2023年招聘网络安全岗位数占比TOP10行业

数据来自智联招聘

三、中小型企业对网络安全人才招聘需求更高

从企业规模看，2023年，招聘网络安全岗位数量最多的是100-499人企业，招聘职位数占比达28.7%。其次是20-99人企业、1000-9999人企业，分别占比24.1%、23.6%。在全球网络安全人才短缺的背景下，中小型企业普遍进入数字化转型阶段，网络安全业务处于成长期，因而网络安全人才需求相对更加旺盛，有志于在网络安全领域发展的求职者可以重点投递中小型企业，积累经验迅速成长。



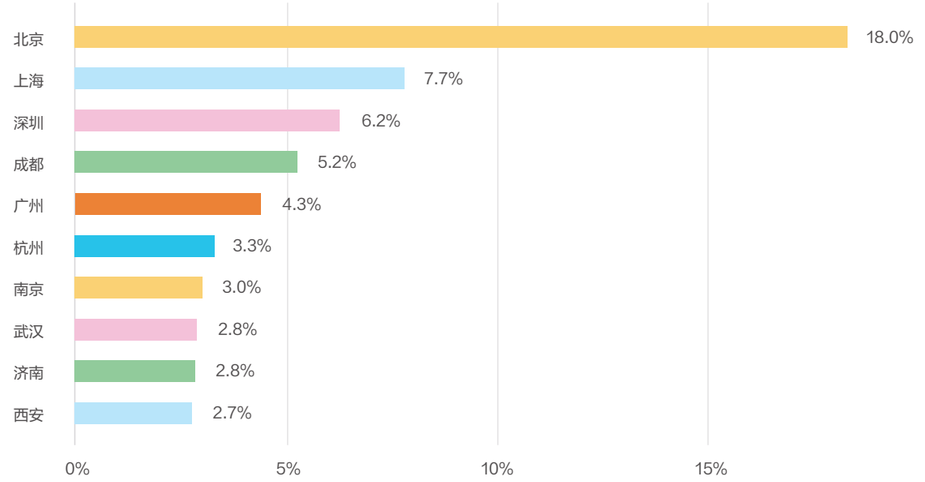
2023年不同规模企业招聘网络安全岗位数量占比

数据来自智联招聘

四、一线城市对网络安全人才招聘需求大

从城市来看，一线城市是对网络安全人才需求最大的城市，2023年北京市招聘网络安全岗位数量占比为18%，排名各城市之首，数字安全产业正逐渐成为支撑首都数字经济发展的重要领域之一。其次是上海、深圳、成都，招聘职位数占比均超5%。

总体来看，除了一线城市，网络安全人才需求主要集中在信息技术、智能制造等新兴产业布局广、数字化程度高的新一线城市。作为唯一进入前十的二线城市，济南高新区入选全国首批国家网络安全教育技术产业融合发展试验区，牢筑网络安全根基，人才需求也相对较大。



2023年招聘网络安全岗位数量占比TOP10城市

数据来自智联招聘

五、网络安全运营岗位招聘职位数占比29%

从岗位分布来看，网络安全运营的招聘职位数占比最高，达到29%。其次是网络安全建设、网络安全管理、数据安全类职位，分别占比18.6%、17.7%和10.2%。从典型职位上看，安全运维工程师的招聘职位数占比最高，达到15.2%。数据安全是网络安全中极为重要的内容，从招聘职位数占比来看，数据安全招聘需求呈现出“少而精”的趋势。

一级职能	二级职能	典型职位	招聘职位数占比
网络安全运营（29.0%）	网络安全运维	安全运维工程师	15.2%
	网络安全集成	集成方案解决师	7.6%
	网络安全应急响应	网络安全应急响应工程师	6.1%
网络安全建设（18.6%）	网络安全开发	网络安全开发师	11.5%
	网络安全架构	安全系统架构师	6.6%
	个人信息保护	——	0.3%
	供应链安全	供应链安全管理	0.1%
网络安全管理（17.7%）	网络安全测试	安全测试工程师	8.3%
	网络安全合规	安全合规工程师	3.5%
	网络安全咨询	安全咨询工程师	2.7%
	网络安全规划	安全规划师	1.9%
	网络安全防护	安全等级保护测评师	1.3%
数据安全（10.2%）	数据安全体系	数据安全体系工程师	3.2%
	数据安全管理	数据管理师	3.2%
	数据安全评估	数据安全评估师	2.6%
	数据安全保护	数据安全保护工程师	1.0%
	电子数据取证	电子数据取证师	0.3%
网络安全审计和评估（8.8%）	网络安全分析	渗透测试/漏洞挖掘工程师	5.9%
	网络安全评估	网络安全评估师	2.5%
	网络安全认证	安全认证工程师	0.4%

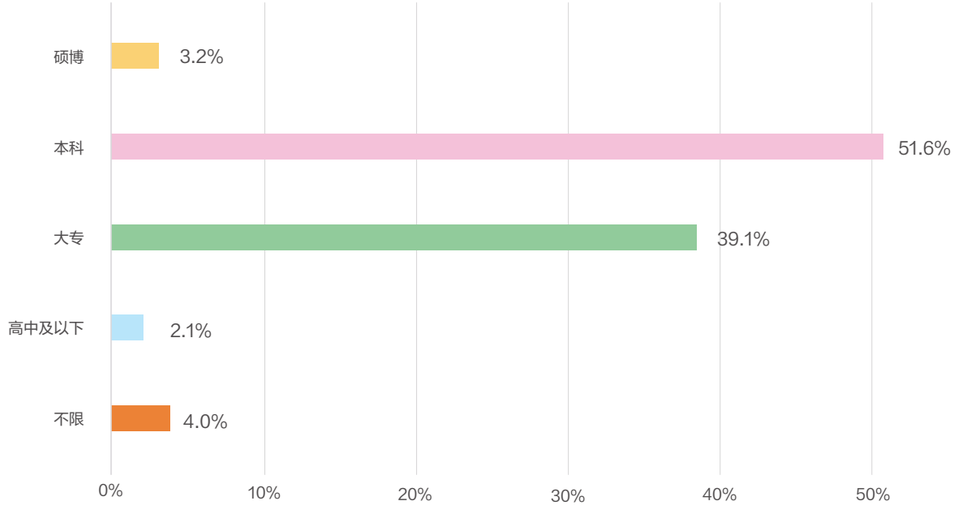
2023年网络安全岗位招聘数量分布

数据来自智联招聘

数据来自智联招聘

六、本科、硕博学历的网络安全人才需求呈上升趋势

从学历要求来看，2023年本科、大专学历网络安全人才的招聘需求较高，招聘职位数占比分别为51.6%、 39.1%。其中要求本科学历的招聘职位数占比较2022年提升了2.8个百分点，要求硕博学历的招聘职位数占比较2022年提升了1.3个百分点。总体来看，网络安全企业对本科和硕博人才的需求有所提升，越来越青睐高学历人才。网络安全行业本身是知识密集型行业，对底层知识的“门槛”要求和更新换代需求较高，高学历人才能更好地适应行业需求，因此受到青睐。

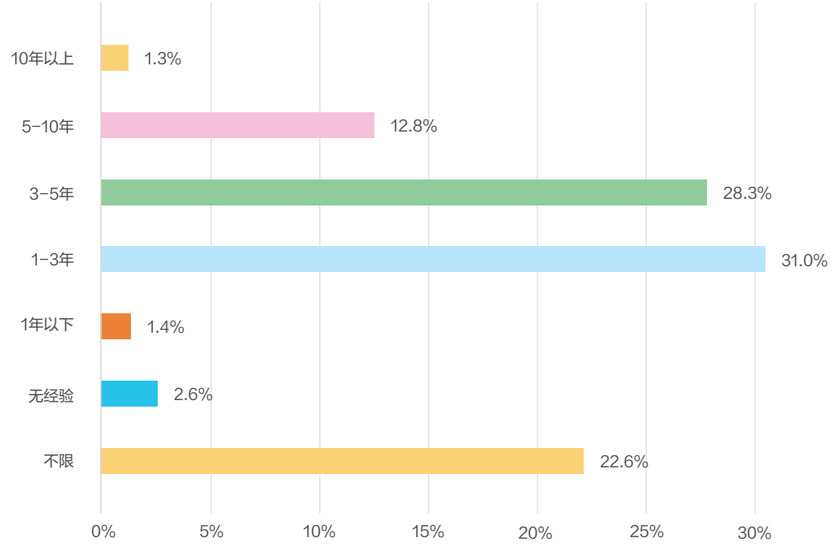


2023年网络安全岗位的学历要求分布

数据来自智联招聘

七、要求1-3年工作年限的招聘职位数占比最高

从工作年限要求来看，2023年，网络安全领域要求1-3年工作年限的招聘职位数占比为31%，排名当年第一。其次是要求3-5年工作年限、不限工作年限的，招聘职位数占比分别为28.3%和22.6%。网络安全行业经常需对网络“盯梢”，年轻人体力精力更为旺盛，有利于工作目标达成。因此行业对年轻人才招聘需求较高。



2023年网络安全岗位的工作年限要求分布

数据来自智联招聘

八、Linux、Java、Windows等技能需求大

考虑到安全研发人员和安全服务人员对攻防技术方面的关注和以往无明显区别，因而本报告中增加了安全研发方面的技能供需分析。从需求端来看，在各种针对研发人员的技能中，Linux、Java、Windows等技能的招聘需求最高，排名招聘要求技能榜TOP3。Linux是一种自由和开放源码的类Unix操作系统，在安全领域的应用非常广泛，如网络维护、系统管理等；Java是一门面向对象的编程语言，具有跨平台性，因此可以在不同的操作系统和硬件上运行。这一特点使得Java语言成为开发网络安全应用的理想选择，因此招聘需求也相对较大。其次，招聘企业对Python、MySQL、TCP/IP协议等技能的需求也比较高。可见，掌握系统编程和面向对象的编程技术人才，在网络安全领域更受企业青睐。

排名	技能
1	Linux
2	Java
3	Windows
4	Python
5	MySQL
6	TCP/IP协议
7	C++
8	CCNP
9	Oracle
10	SQL

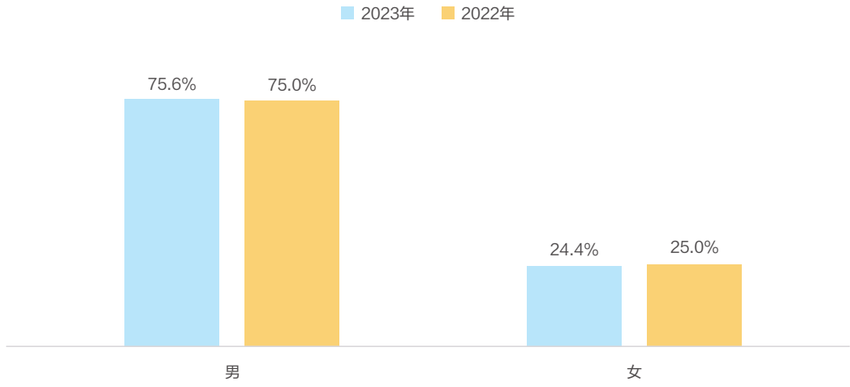
2023年网络安全岗位需求的专业技能TOP10

数据来自智联招聘

第二节 | 网络安全产业人才供给

一、男性求职者占比超7成

智联招聘平台数据显示，2023年向网络安全岗位求职的人才中，男性占比75.6%，女性占比24.4%。2022年，男性占比75%，女性占比25%。性别结构较为稳定。由于网络安全属于理工科，就读相关专业的男性更多，而该工作对技术升级迭代、工作时间的要求较高，需要持续学习和加班工作，相比之下男性更适应这样的工作要求，因此男性求职者比重持续处于高位，属于绝对的求职主体。

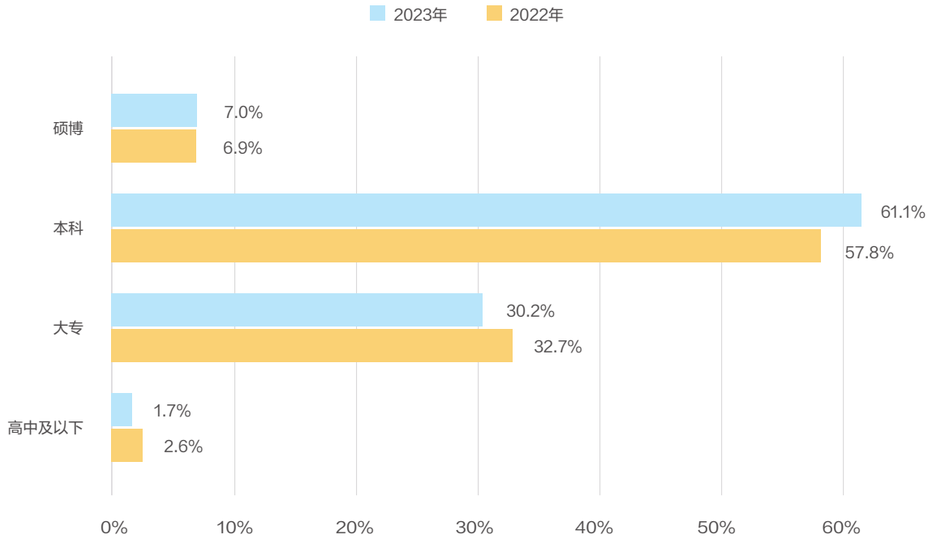


网络安全求职者的性别分布

数据来自智联招聘

二、本科学历求职者占比较高，且呈上升趋势

从学历来看，2023年本科学历的网络安全求职者占比最高，达到61.1%，相比2022年的57.8%，提升了3.3个百分点。其次是大专学历，求职者占比30.2%，比2022年的32.7%下降了2.5个百分点。随着学历教育的普遍提升以及网络安全行业的知识密集特性，网络安全行业本科求职者在增多。

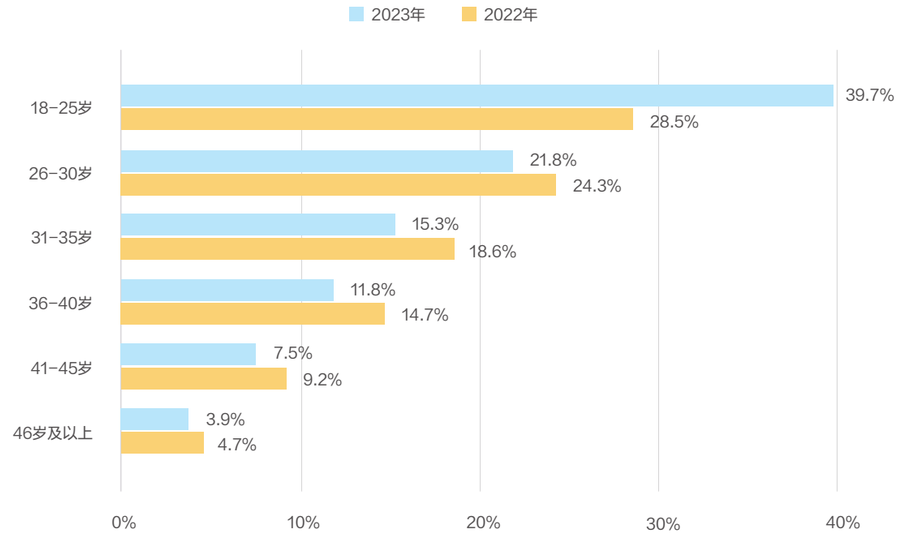


网络安全求职者的学历分布

数据来自智联招聘

三、18-25岁人才求职者占比排名第一

从年龄来看，2023年，网络安全领域18-25岁人才求职者占比39.7%，排名第一，而且相比2022年的28.5%，提高了11.2个百分点。其次是26-30岁、31-35岁求职者，占比分别为21.8%和15.3%，但相比2022年均有所下降。可见年轻人普遍看好我国网络安全行业这一蓝海市场的发展前景，未来网络安全行业将受到更多求职者的青睐。



网络安全求职者的年龄分布

数据来自智联招聘

四、北京是网络安全人才聚集“大本营”

从网络安全求职人才的居住城市来看，2023年，20.8%的求职者居住在北京，排名各城市之首，稍高于2022年的20.3%。其次，5.3%的网络安全求职者居住在成都，略低于去年的5.8%，且超过深圳、上海、广州等一线城市，位居新一线城市首位。作为成都万亿级电子信息产业最具优势的赛道之一，成都的网络安全产业基础实力雄厚、政策环境优越，因此超越部分一线城市位居第二。

值得一提的是，除了一线城市之外，新一线城市和省会城市也汇聚了大量的网络安全求职者。

排名	2023居住城市	占比	排名	2022居住城市	占比
1	北京	20.8%	1	北京	20.3%
2	成都	5.3%	2	成都	5.8%
3	深圳	5.1%	3	深圳	4.7%
4	上海	4.6%	4	广州	4.0%
5	广州	4.0%	5	上海	3.6%
6	西安	3.5%	6	西安	3.5%
7	郑州	3.2%	7	天津	3.1%
8	重庆	3.0%	8	郑州	3.0%
9	天津	2.7%	9	重庆	2.8%
10	济南	2.3%	10	武汉	2.2%
11	南京	2.3%	11	济南	2.1%
12	武汉	2.2%	12	长沙	2.1%
13	长沙	2.0%	13	南京	2.0%
14	杭州	1.9%	14	沈阳	2.0%
15	沈阳	1.8%	15	杭州	1.7%
16	石家庄	1.5%	16	石家庄	1.6%
17	贵阳	1.4%	17	贵阳	1.5%
18	合肥	1.2%	18	青岛	1.3%
19	青岛	1.1%	19	合肥	1.2%
20	长春	1.0%	20	长春	1.1%

网络安全求职者的居住城市TOP20

数据来自智联招聘

五、计算机科学与技术专业求职者占比最高

从专业分布来看，2023年，计算机科学与技术专业毕业的求职者占比最高，达11.8%，且高于2022年的9.5%。其次是软件工程、计算机网络技术和工商管理，2023年的占比分别为4.3%、3.3%和3.1%。计算机科学与技术专业学生具有较强的专业优势，网络安全产业的学科交叉特性也鼓励着具有专业优势的技术人才跨界求职。

排名	2023专业	占比	排名	2022专业	占比
1	计算机科学与技术	11.8%	1	计算机科学与技术	9.5%
2	软件工程	4.3%	2	工商管理	3.3%
3	计算机网络技术	3.3%	3	计算机网络技术	3.3%
4	工商管理	3.1%	4	软件工程	3.0%
5	网络工程	3.0%	5	网络工程	2.9%
6	计算机应用技术	3.0%	6	计算机应用技术	2.8%
7	通信工程	2.6%	7	通信工程	2.7%
8	电子信息工程	2.0%	8	电子信息工程	2.1%
9	信息管理与信息系统	1.6%	9	会计学	1.7%
10	软件技术	1.5%	10	信息管理与信息系统	1.7%
11	会计学	1.3%	11	市场营销	1.5%
12	土木工程	1.3%	12	电子信息科学与技术	1.3%
13	市场营销	1.2%	13	电气工程及其自动化	1.3%
14	物联网工程	1.2%	14	土木工程	1.1%
15	电气工程及其自动化	1.2%	15	软件技术	1.1%

网络安全求职者的专业TOP15

数据来自智联招聘

六、北京理工大学、电子科技大学等理工类院校的求职者为主体

从求职者毕业的院校来看，2023年北京理工大学上升为“投递大户”，其次是电子科技大学、北京邮电大学、郑州大学。而2022年，电子科技大学、吉林大学、北京理工大学、郑州大学等高校投递网络安全领域的人才占比较高。

整体来看，受行业工作性质影响，网络安全领域的求职者主要来自于理工类院校。结合招聘需求来看，网络安全产业的招聘需求主要集中于北京，导致北京院校人才对网络安全行业投递热情更高，但随着产业发展，预计未来网络安全产业也将在更多城市排布，吸引更多更广泛的求职人才。

排名	2023院校	排名	2022院校
1	北京理工大学	1	电子科技大学
2	电子科技大学	2	吉林大学
3	北京邮电大学	3	北京理工大学
4	郑州大学	4	郑州大学
5	吉林大学	5	北京邮电大学
6	北京交通大学	6	中国人民大学
7	中国人民大学	7	北京交通大学
8	天津理工大学	8	北京航空航天大学
9	郑州科技学院	9	西南科技大学
10	北京航空航天大学	10	西安电子科技大学
11	西安电子科技大学	11	东北大学
12	西南科技大学	12	北京科技大学
13	东北大学	13	四川大学
14	河北科技学院	14	天津大学
15	北京联合大学	15	天津理工大学

网络安全求职者的毕业院校TOP15

数据来自智联招聘

七、MySQL是网络安全求职者掌握最多的技能

从求职者具备的技能看，在各种针对研发人员的技能中，求职者具备的前三项技能分别是MySQL、Java、Linux。其次是SQL、SpringBoot、Python等技能，求职者具备多元化技能，不同技术人才都希望在网络安全领域找到用武之地。对比求职者技能和职位所需技能，MySQL是时下最流行的关系型数据库管理系统之一，学习者众多，因此这项技能的供给更加充足。

排名	技能
1	MySQL
2	Java
3	Linux
4	SQL
5	SpringBoot
6	Python
7	Windows
8	Vue
9	CAD
10	SpringCloud

网络安全求职者具备的技能TOP10

数据来自智联招聘

第三节 | 数据安全人才供需分析

一、网络安全与数据安全技能、岗位均存在差异

从岗位分布来看，网络安全与数据安全不同，数据安全主要涉及数据的安全性，防止数据泄露和损害丢失，因此数据安全的典型岗位有电子数据取证师、数据安全保护工程师、数据管理师、数据安全评估师、数据安全体系工程师等，可以达到数据加密、数据脱敏、数据去标识化等目标，为非联网下的数据保障安全。

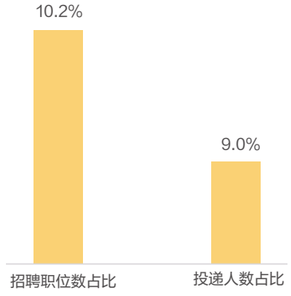
而网络安全主要涉及计算机网络的安全性，为防止黑客攻击、网络漏洞，设置的岗位主要涉及安全运维、应急响应、安全规划、渗透测试、漏洞挖掘、安全评估等。

从技能来看，网络安全工作主要是保障系统不被攻击、网络不中断、系统正常运行，数据安全工作主要是对数据资产安全的保护。二者工作的侧重点有所区别，技能也有所差别。网络安全人才应当了解网络系统，掌握JavaScript和HTML等常用代码框架，以及Python编程语言。还要熟悉MacOS、Windows和Linux等系统。数据安全则需掌握SQL访问、区块链、隐私计算等技术。

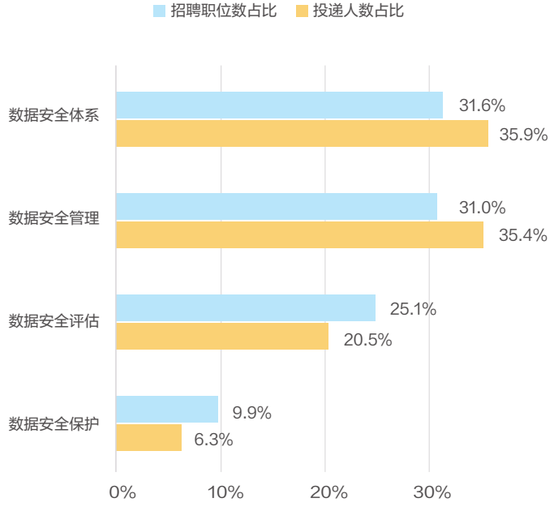
二、数据安全人才供需两旺，更受高学历人才欢迎

智联招聘平台数据显示，2023年，数据安全相关的招聘职位数在网络安全整体中占比10.2%，投递人数占比9%。可见数据安全领域整体招聘求职情况火热。

数据安全细分岗位中，数据安全体系招聘职位数占比最高，达到31.6%，投递人数占比也排名各细分行业之首，达到35.9%。其次是数据安全管理，招聘职位数占比31%，投递人数占比35.4%。数据安全评估和数据安全保护岗位的招聘需求占比则高于求职占比。



数据安全领域人才供需情况

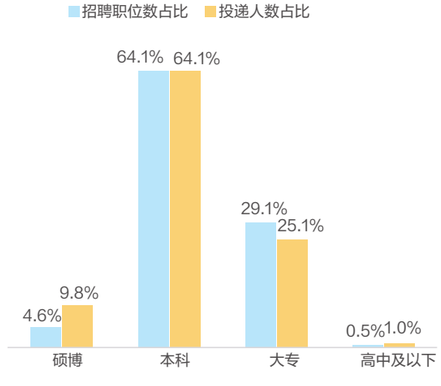


数据安全领域各细分岗位人才供需分布

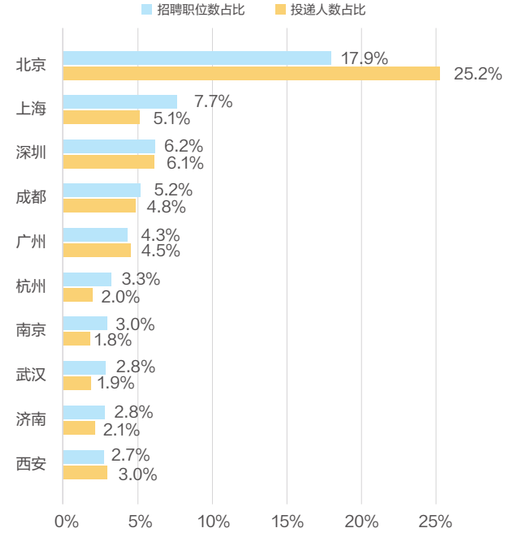
数据来自智联招聘

从人才的学历供需来看，数据安全领域的招聘职位中，本科人才需求与投递占比均为64.1%，二者均为最高，且相对匹配。要求大专和高中及以下学历的招聘职位数占比共为29.6%，而该学历阶段的投递人数总占比为26.1%。与此同时，要求硕博学历的招聘职位数占比4.6%，而同等学历的投递人数占比达9.8%。可见，数据安全岗位吸引更多高学历的人才投递。

从人才供需的城市来看，北京成为数据安全领域招聘职位数占比和投递人数占比最高的城市，分别为17.9%、25.2%，整体供大于求。上海、深圳、成都、杭州等网络安全产业发展较好的城市，则呈现出人才供不应求的现象，这对人才而言是极大的就业机会。



数据安全领域人才学历供需状况



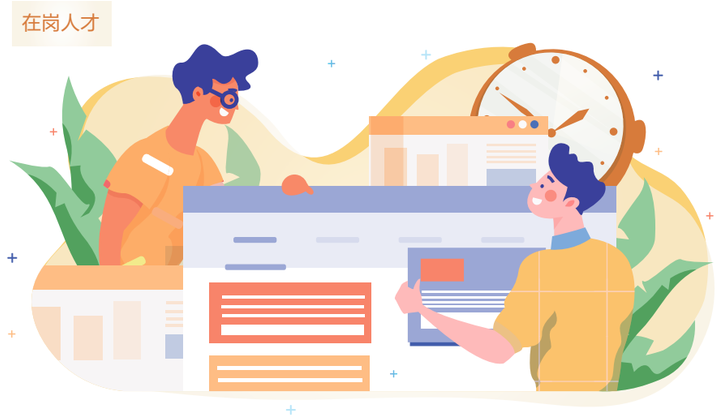
重点城市的数据安全领域人才供需情况

数据来自智联招聘

第四章

网络安全产业人才培养

网络安全产业的蓬勃发展，亟需高素质、高技能人才支撑。本章从在岗人才和在校人才两个维度，结合问卷调研数据结果，分析网络安全产业人才培养现状。

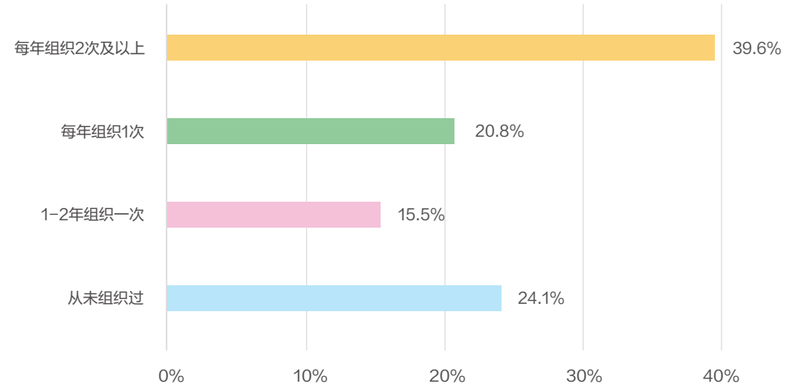


第一节 | 在岗人才培养

（一）用人单位人才能力建设

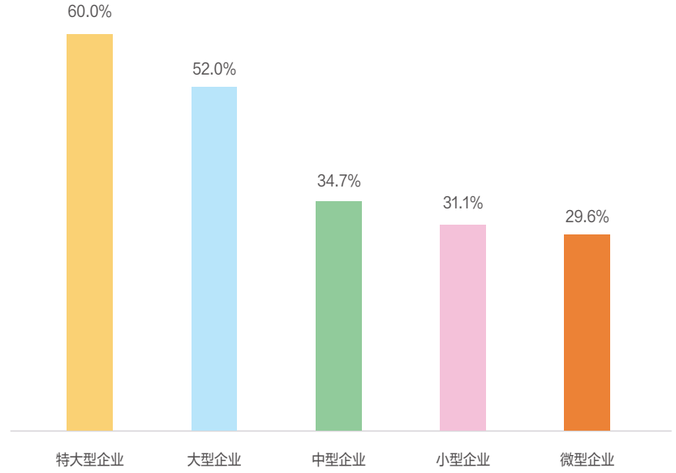
一、近4成从业者所在企业每年组织2次及以上网络安全培训

问卷调研结果显示，39.6%的网络安全从业者所在企业每年组织2次及以上培训，占比最高。其次是从未组织过培训的，占比24.2%。每年组织1次培训的，占比20.8%。可见，网络安全从业者所在企业组织培训呈现“两极分化”，培训频率较高和从未培训的企业同时存在。



从业者所在企业组织培训的频率

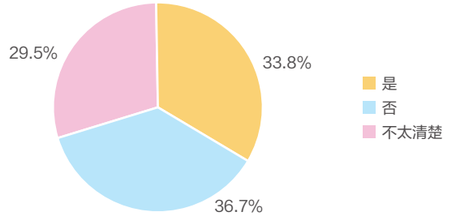
其中，每年组织2次以上培训的特大型企业占比60%，高于大型企业的52%、中型企业的34.7%、小型企业的31.1%和微型企业的29.6%。可见企业规模越大，对于培训就越重视，开展培训活动也更加频繁。微型企业受制于人手和经费所限，对网络安全相关培训的组织力度相对更弱。



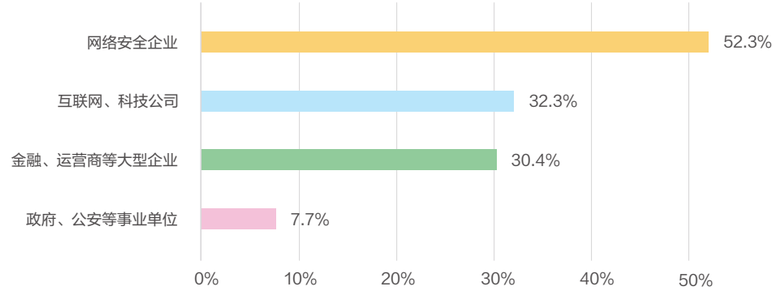
各规模企业每年组织2次及以上网络安全相关培训的比例

二、过半网络安全企业已建成或在建网络安全实训平台

目前，33.8%的受访网络安全从业者所在企业已建成或在建网络安全实训平台或实验室，而未建成的占比高达36.7%。从不同领域来看，已建成或在建网络安全实训平台或实验室的网络安全企业占比最高，达到52.3%，超过互联网、科技公司，金融、运营商等大型企业，政府、公安等事业单位。



企业是否已建成或在建网络安全实训平台或实验室

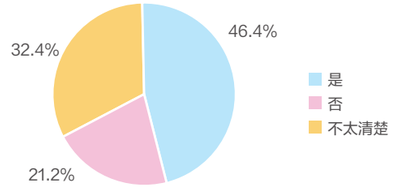


各领域企业已建成或在建网络安全实训平台或实验室的比例

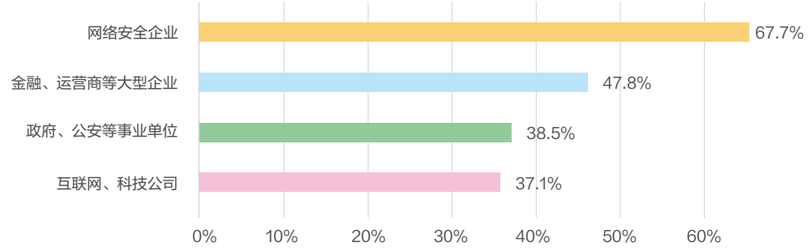
（二）用人单位人才体系建设

一、近7成网络安全企业建立任职标准

从任职标准来看，46.4%的受访网络安全从业者所在企业发布了能力评价、等级认证等任职标准。不过，也有21.2%的从业者所在企业未建立这项标准。具体来看，网络安全企业的从业者中，有67.7%表示所在企业建立了任职标准，占比高于金融、运营商等大型企业（47.8%），政府、公安等事业单位（38.5%），以及互联网、科技等公司（37.1%）。



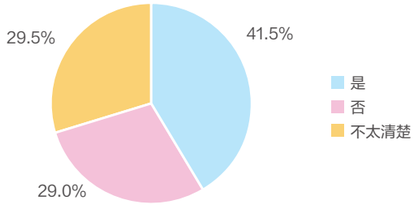
从业者所在企业发布网络安全从业人员任职标准的比例



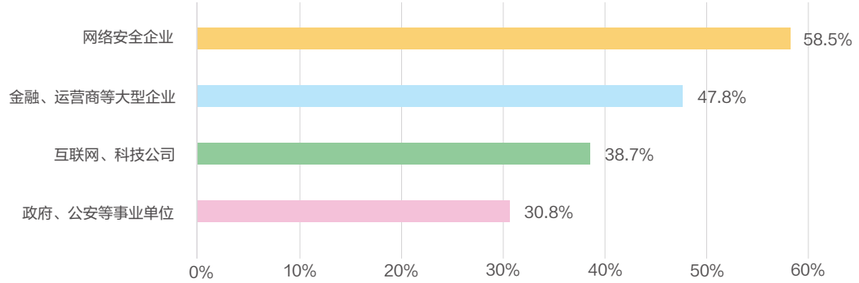
各领域企业发布网络安全从业人员任职标准的比例

二、4成从业者所在企业建立网络安全领域用人机制

专业人才的引入、选拔、培养对于网络安全领域专业人才至关重要，41.5%的受访从业者表示所在企业建立了网络安全领域用人机制。不过，也有29%的从业者所在企业未建立这项机制。具体来看，网络安全企业的用人机制构建最为完善，有58.5%的从业者所在企业建立了用人机制，超过金融、运营商等大型企业（47.8%），互联网、科技公司（38.7%），政府、公安等事业单位（30.8%）。



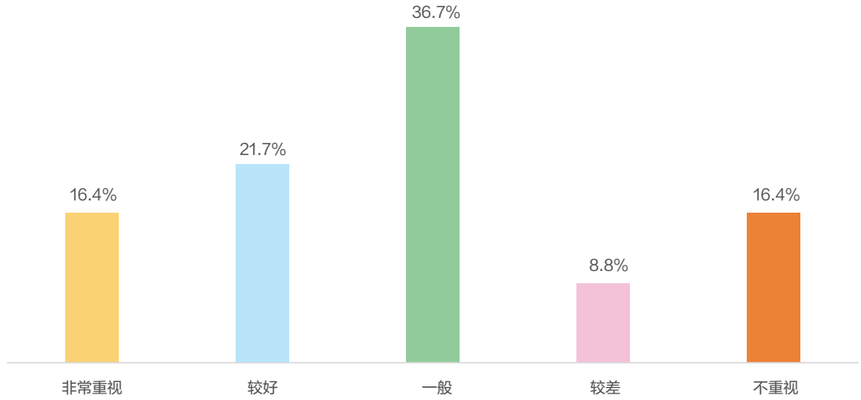
从业者所在企业建立网络安全专业人才用人机制的比例



各领域企业建立网络安全专业人才用人机制的比例

三、近4成从业者所属公司重视人才建设

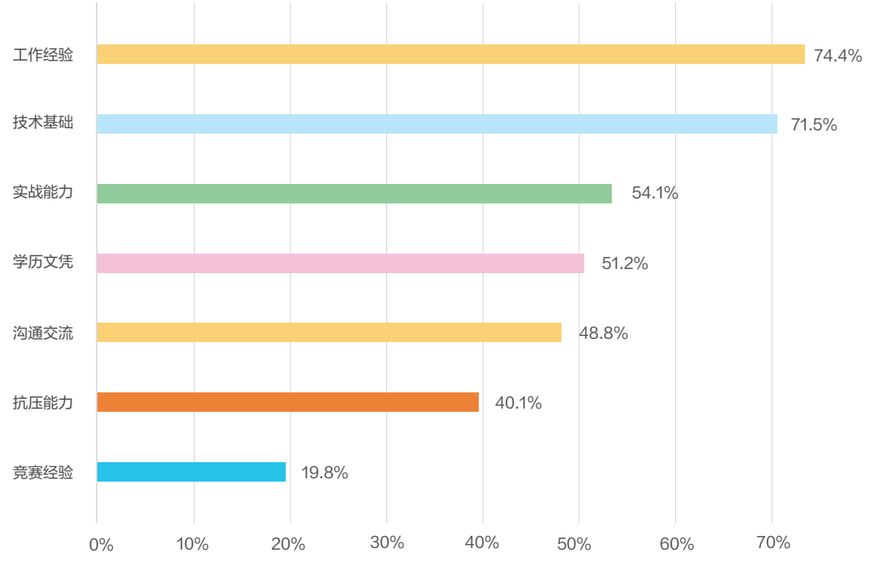
调研结果显示，分别有16.4%和21.7%的从业者所属企业对网络安全人才建设“非常重视”或“较好”。不过，36.7%的从业者认为企业对人才建设的重视程度“一般”。可见，网络安全人才所在公司对人才建设的重视程度仍有待提高。



企业对网络安全人才建设的重视程度

四、7成以上网络安全从业者所在用人单位重视工作经验

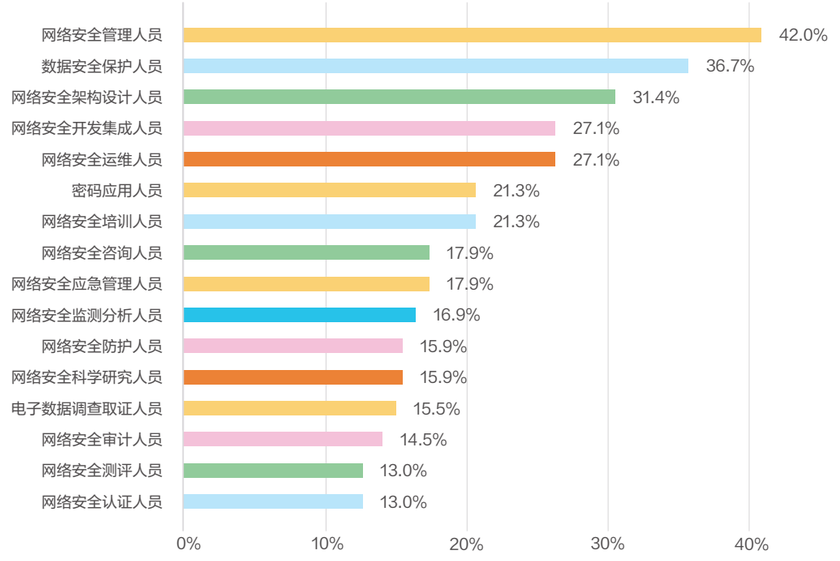
从用人单位在选才时注重的条件来看，74.4%的受访从业者表示所在企业重视工作经验，占比排名第一。其次是技术基础、实战能力、学历文凭，分别占比71.5%、54.1%、51.2%。可见，学历是网络安全人才选拔的关键一环，但不是唯一一环。工作经验和技术能力，才是用人单位更看重的因素。



企业选择人才看重的条件

五、超4成从业者认为公司应当增加网络安全管理人才

根据企业业务发展需求，42%的网络安全从业者认为，企业应当增加网络安全管理人员，其次是数据安全保护人员，占比36.7%，也有31.4%的从业者认为应当增加网络安全架构设计人员。此外，网络安全开发集成人员、网络安全运维人员、密码应用人员、网络安全培训人员的需求也排名前列。可见，管理人员和技术人员是目前行业较为缺乏人才的岗位。

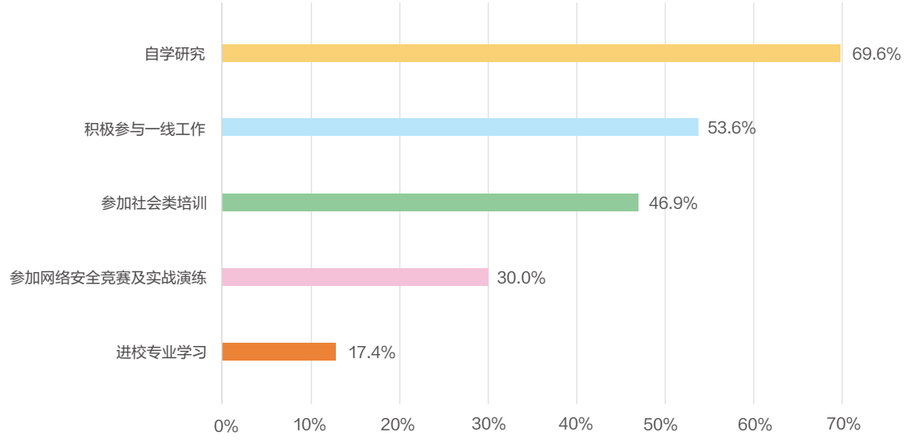


企业当前缺乏或应增加的岗位人员

（三）在岗人才能力提升

一、自学研究是从业者能力提升的主要方式

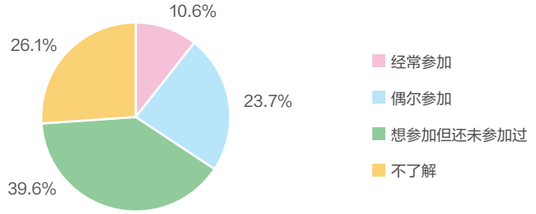
在提升能力的方法中，69.6%的网络安全从业者选择“自学研究”，其次是“积极参与一线工作”“参加社会类培训”，分别占比53.6%、46.9%。此外，“参加网络安全竞赛及实战演练”“进校专业学习”，也是从业者提高网络安全领域能力的方式。



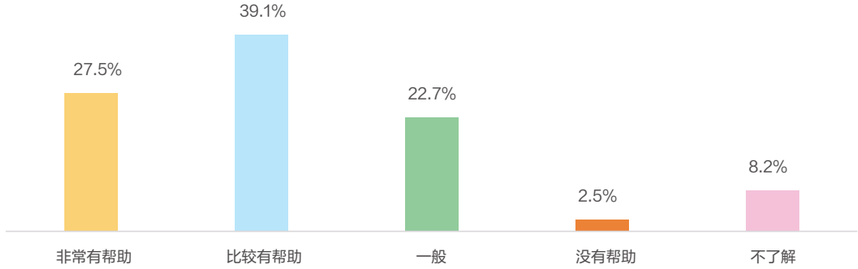
从业者进行能力提升的方式

二、34%从业者参加过网络安全竞赛，6成以上认为有助于提高专业能力

问卷调研显示，分别有10.6%、23.7%的从业者经常参加和偶尔参加竞赛，39.6%的从业者想参加但还未参加过网络安全竞赛。对于竞赛提高专业能力方面的作用，从业者普遍反映较好。其中，27.5%认为“非常有帮助”，39.1%认为“比较有帮助”，共计有66.6%的从业者认为有帮助。



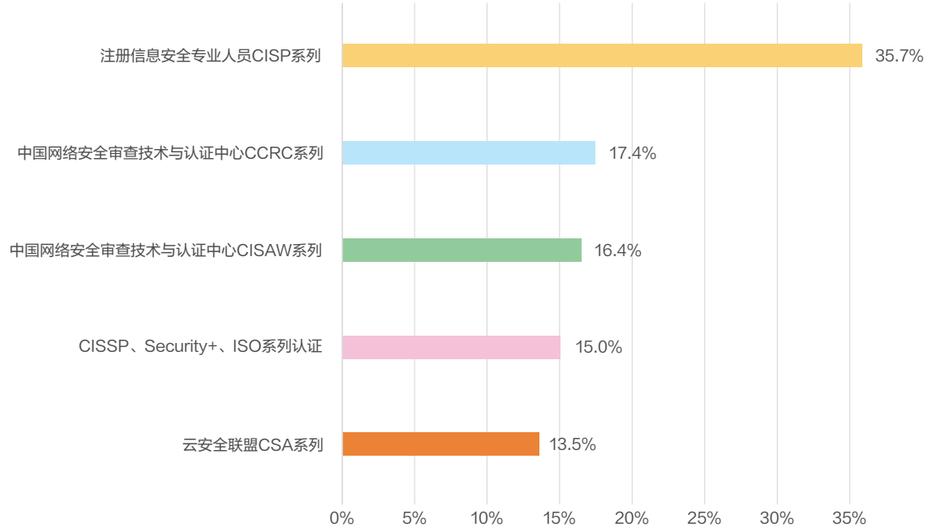
从业者参加过网络安全竞赛情况



从业者对参加竞赛提高专业能力的看法

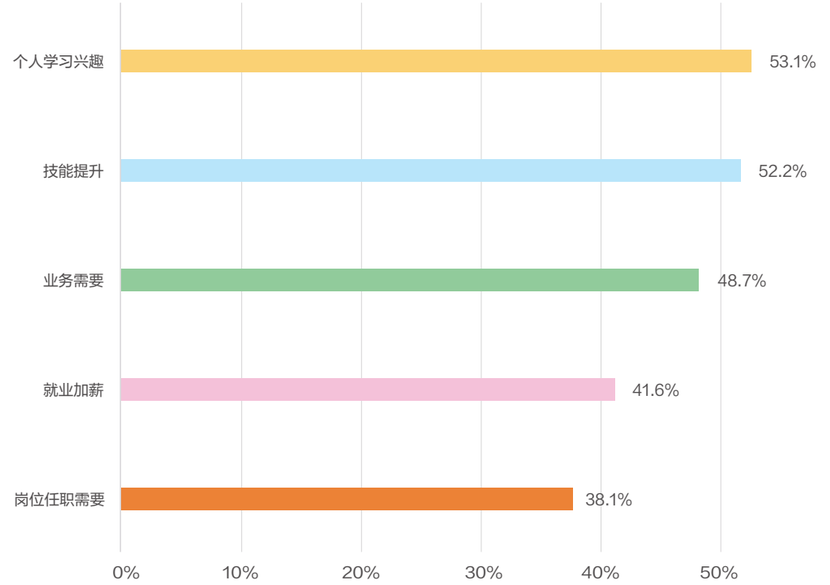
三、兴趣、技能、业务是考证的主要驱动力

在认证方面，目前拥有注册信息安全专业人员CISP系列认证的从业者占比最高，达到35.7%。其次是中国网络安全审查技术与认证中心CCRC系列，中国网络安全审查技术与认证中心CISAW系列，CISSP、Security+、ISO系列认证，占比均超过15%。



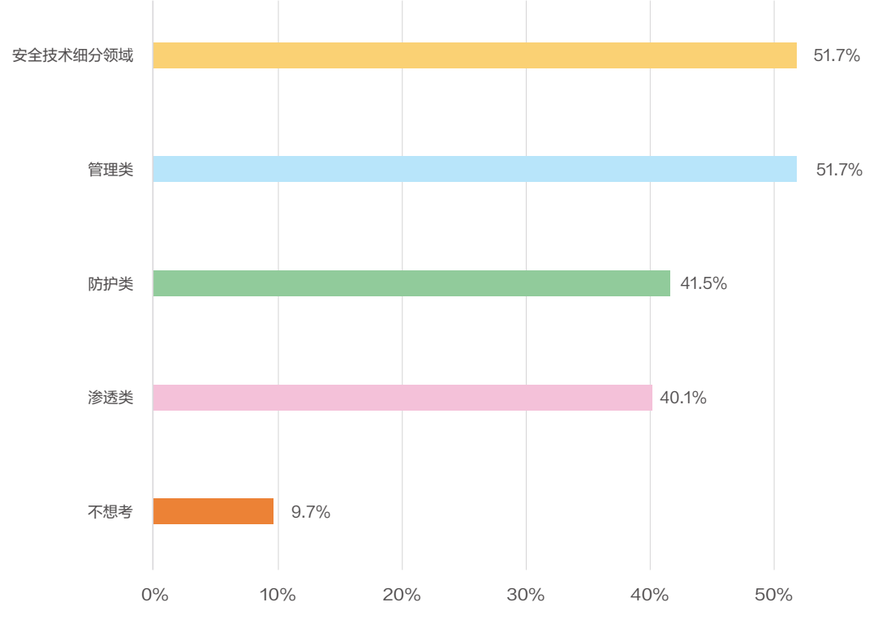
从业者拥有的网络安全相关认证

从考证驱动力来看，有53.1%的从业者考证是出于个人学习兴趣，也有52.2%和48.7%的从业者因为技能提升和业务需要而考证。也有41.6%的从业者奔着“就业加薪”目标，这些国家级或国际级认证，是从业者求职和升职加薪的重要“助攻”。



从业者考取认证的原因

从业者希望考取的认证类型中，安全技术细分领域、管理类为主要类别，占比均为51.7%。同时也有41.5%、40.1%的从业者分别选择防护类、渗透类认证。



从业者希望考取的认证类型

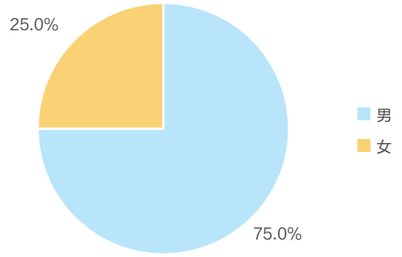
第二节 | 在校人才培养

网络安全人才的主要来源，是高等院校经历过专业教育的在校人才。基于针对网络安全在校生的问卷调研数据，本节将从在校生基本特征、专业建设情况、在校生就业规划等维度，从性别、学历、满意度等细分内容出发，对网络安全专业在校人才的培养进行分析。

（一）在校生基本特征

一、网络安全专业男生为女生的3倍

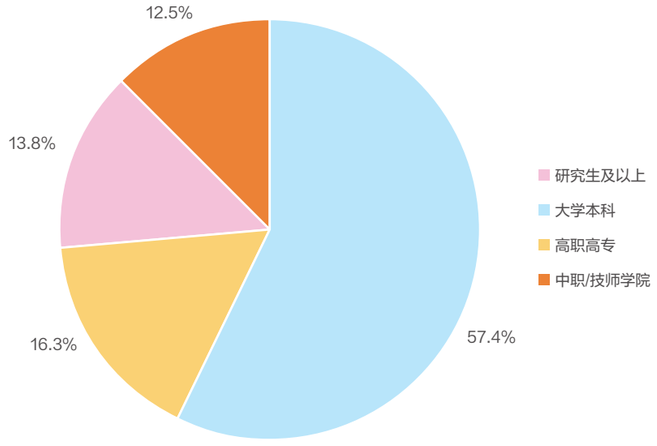
据问卷调研数据显示，从性别来看，网络安全专业在校生中，男生人数是女生人数的3倍。在校生男女性别分布，与2023年应聘网络安全岗位求职者男女分布（男性占比75.6%，女性占比24.4%）一致，网络安全专业男女比例保持稳定。



网络安全专业在校生的性别

二、网络安全在校生学历呈提高趋势

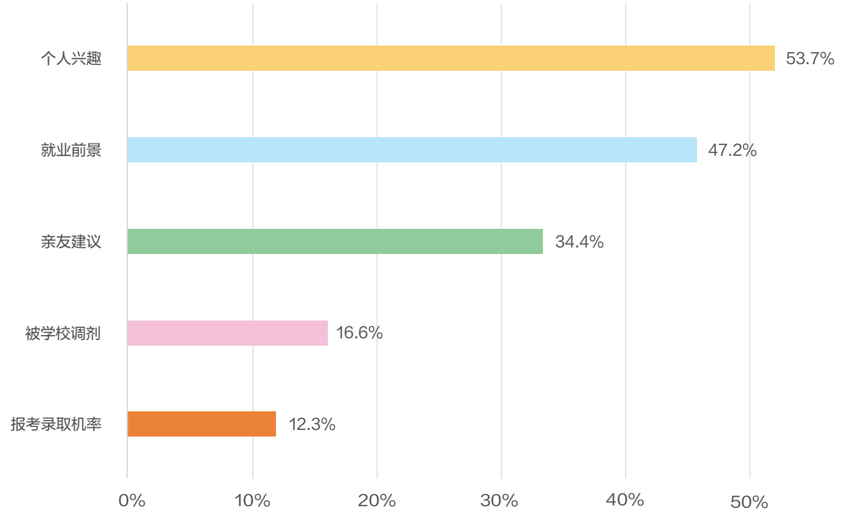
从学历来看，网络安全的大学本科在校生占比57.4%，占比最高；其次是高职高专、研究生及以上、中职/技师学院在校生，占比分别为16.3%、13.8%、12.5%。而2022年在校生主要以大学本科和高职高专学历为主，占比分别为45.3%和42.8%；其次是研究生及以上、中职/技师学历，占比分别为7.1%和4.9%。与2022年相比，今年网络安全在校生的学历中，研究生和本科生占比有明显提高，随着教育水平的提升，高学历成为越来越多网络安全人才的“标配”。



在校生的学历层次

三、过半因个人兴趣选择网络安全专业，就业前景排名第二

在选择网络安全专业的原因上，53.7%的受访在校生选择个人兴趣，排名第一。其次是就业前景，占比47.2%。也有部分受访在校生被动选择了网络安全专业，因亲友建议、被调剂和报考录取机率选择本专业的占比分别为34.4%、16.6%、12.3%。可见，在校生更关注自己的内心需求和未来成长，当前兴趣爱好和前景是他们选择网络安全专业的主要因素。

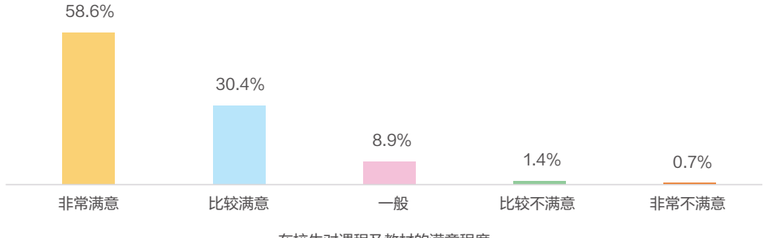


在校生选择本专业的理由

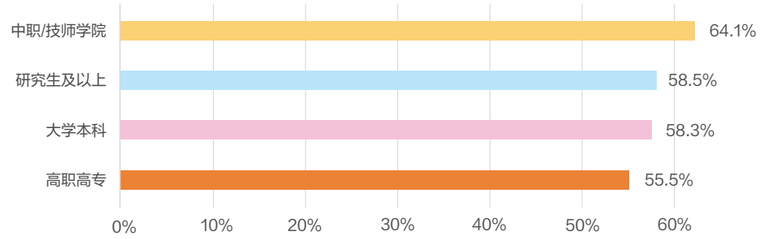
（二）专业建设情况

一、近9成在校生对课程及教材满意，8成以上满意实训环境

校园里的课程设置、教材安排和实践实训内容，都对网络安全学生的专业素质培养具有重要意义。从问卷数据统计结果来看，对于网络安全专业的课程及教材，58.6%的在校生非常满意、30.4%比较满意，共有89%的在校生对此表示满意。其中，中职/技师学历在校生认为非常满意的占比最高，为64.1%，其次是研究生及以上学历和大学本科学历在校生，占比分别为58.5%和58.3%。

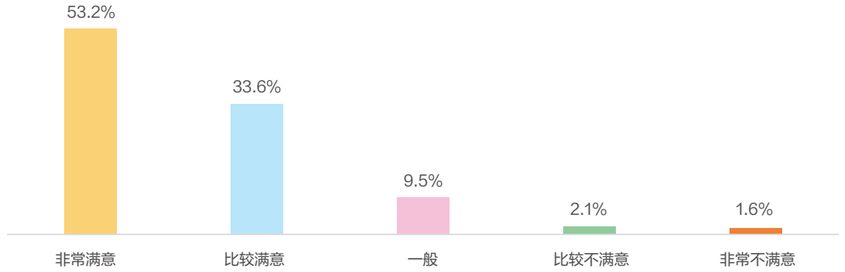


在校生对课程及教材的满意程度



不同学历在校生对课程及教材非常满意的占比

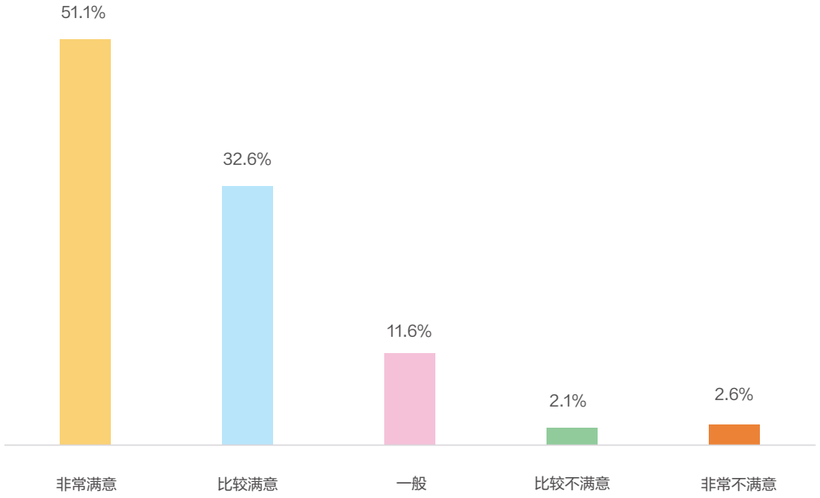
从师资水平来看，53.2%的受访网络安全专业在校生对师资水平非常满意、33.6%比较满意，共有86.8%的在校生对此满意。绝大部分在校生满意师资水平，为网络安全专业教师打出高分。其中，网络安全相关专业在校生对师资非常满意的占比60.3%，高于计算机与网络相关专业的51%。



在校生对师资水平的满意程度

不同专业在校生对师资水平非常满意的占比

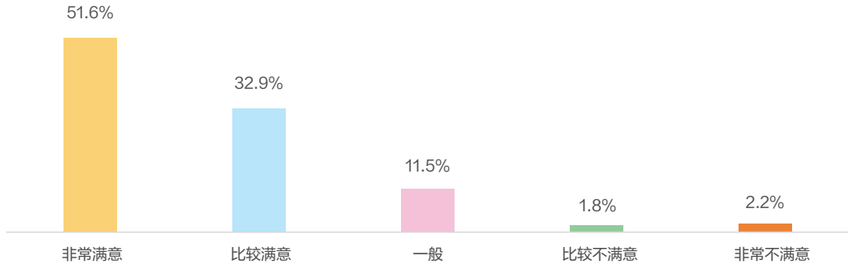
从网络安全专业的教学实践条件来看，51.1%的受访在校生非常满意、32.6%比较满意，共有83.7%表示满意，但也有4.7%不满意。



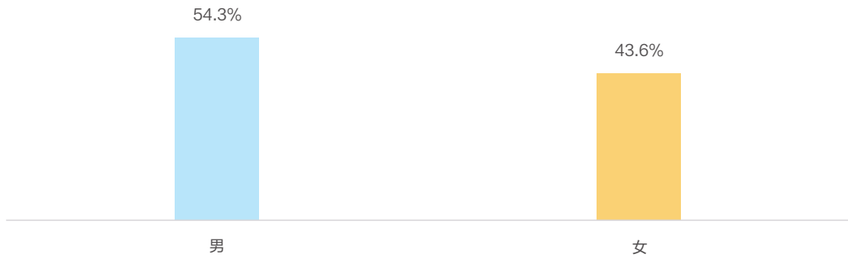
在校生对实践条件的满意程度

总体来看，受访在校生认为网络安全专业实训环境比实践条件更好。对该专业的实训环境，51.6%的在校生非常满意、32.9%比较满意，共有84.5%表示满意，但也有4%不满意。

其中，对实训环境非常满意的男生占比54.3%，女生占比43.6%，可见男生对实训环境本身没有那么在意，满意度比女生更高。



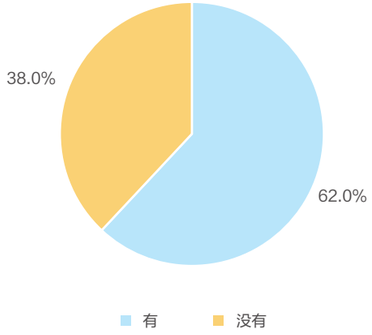
在校生对实训环境的满意程度



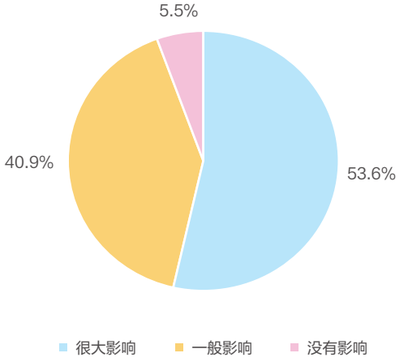
不同性别在校生对实训环境非常满意的占比

二、超6成学生被安排实习，半数以上深受影响

与此同时，62%的受访网络安全专业在校生表示学校安排了实习，38%的在校生未接到实习通知。这表明，大部分网络安全专业在校生从学校得到了实习机会。其中，53.6%的在校生认为实习经历对未来有很大影响，40.9%认为有一般影响，5.5%认为没有影响。



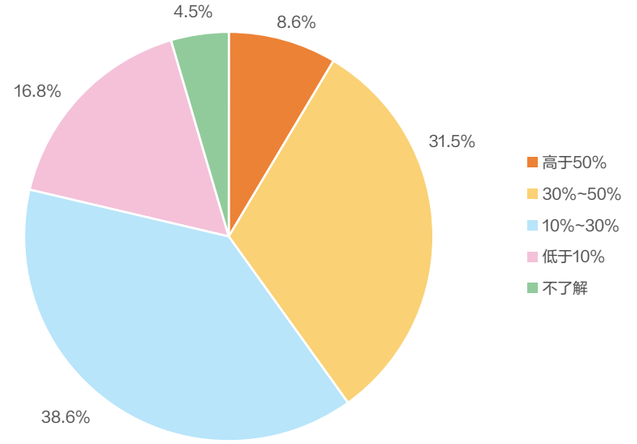
学校安排实习的在校生占比



在校生对实习影响从业的看法

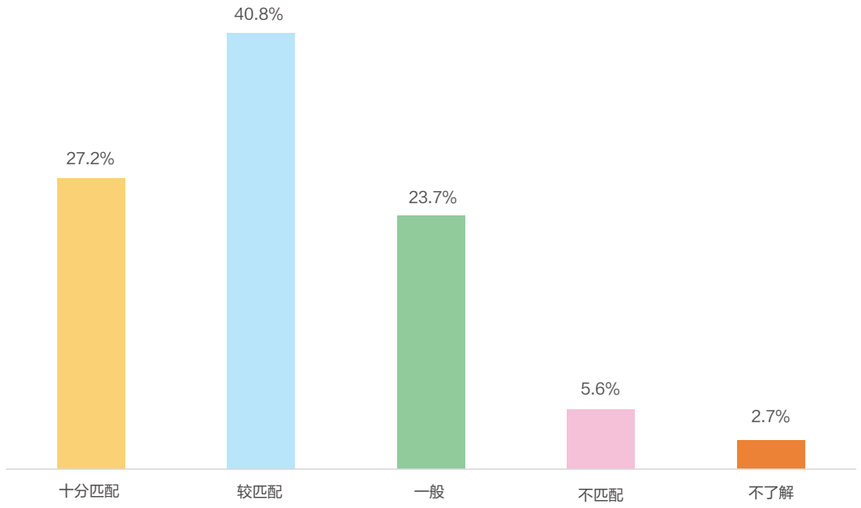
三、7成在校生表示实习实践内容偏少，但大部分认为授课与实习要求匹配

在被问及实习实践内容在网络安全专业中的占比时，共有70.1%的受访在校生表示，实习实践内容占比10-50%，而占比高于50%的在校生仅占8.6%。



在校生实习实践内容在专业中的占比

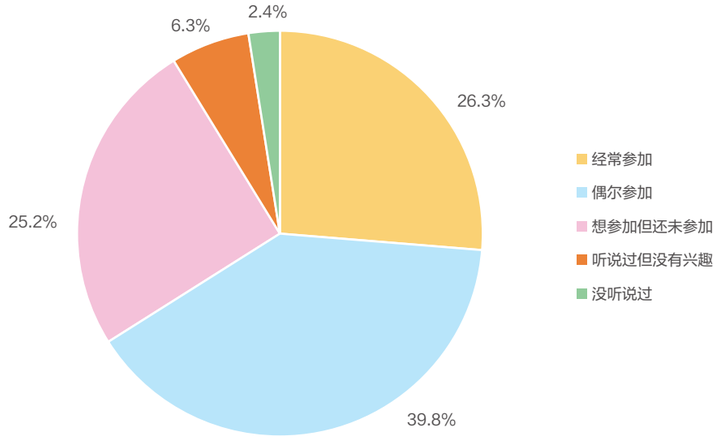
从实习与授课的匹配度来看，40.8%的在校生认为实习岗位知识技能要求与专业授课较匹配，占比最高；27.2%的在校生认为十分匹配，也有23.7%认为一般。这表明，大部分在校生都认为授课与实习要求能有效衔接。



实习岗位知识技能与专业授课匹配程度

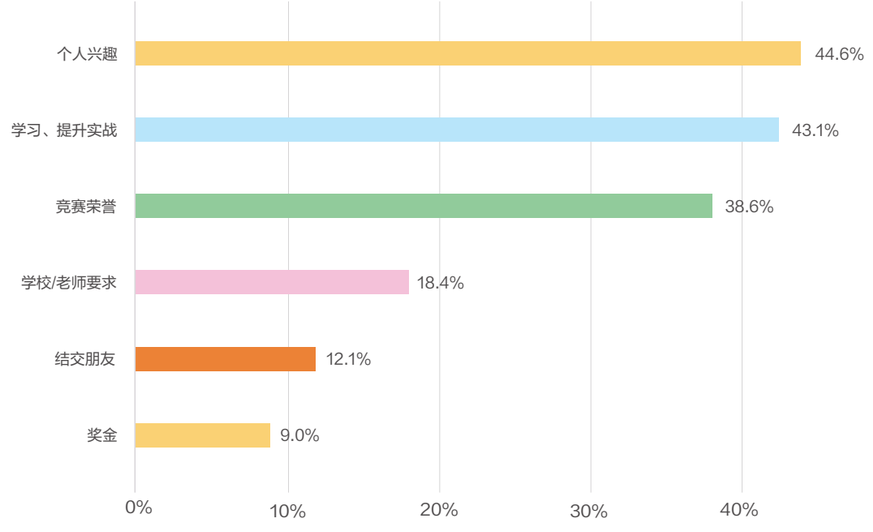
四、6成以上在校生参加过网安竞赛，兴趣和能力提升是主导

从参加的学科竞赛来看，26.3%的受访在校生经常参加专业相关竞赛，39.8%偶尔参加，共有66.1%的在校生参加过本学科竞赛。但也有25.2%的在校生想参加但未参加，2.4%的在校生根本没听说过。可见，在校生参加专业竞赛较为普遍，但普及度还有待加强。



在校生参加专业竞赛情况

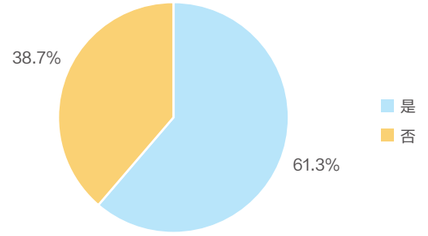
从参加竞赛的目的来看，44.6%的受访在校生表示，他们是出于个人兴趣参加网络安全竞赛。其次，43.1%是为了学习和提升实战能力而参加专业竞赛。可见，在选择网络安全专业时，兴趣就是促进选择的最重要因素，在参加竞赛方面，兴趣和能力提升更是在校生参赛最好的助推器。此外，也有在校生为了获得竞赛荣誉、应学校老师要求、结交朋友、获得奖金而参赛。



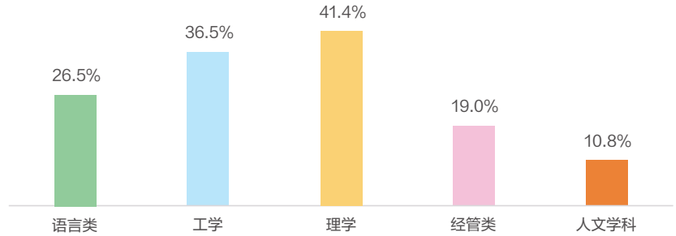
在校生参加专业竞赛的目的

五、超6成在校生辅修其他专业，理工类为主体

网络安全专业在校生普遍有辅修其他专业的需求，调研数据显示，61.3%的受访在校生辅修了其他专业。在选择辅修的在校生中，分别有41.4%、36.5%选择理学和工学，以富有技术含量的学科来加持网络安全主修专业。也有26.5%、19%的受访在校生选择语言类、经管类专业辅修，而选择与网络安全专业“跨度”最大的人文学科在校生最少，仅占10.8%。



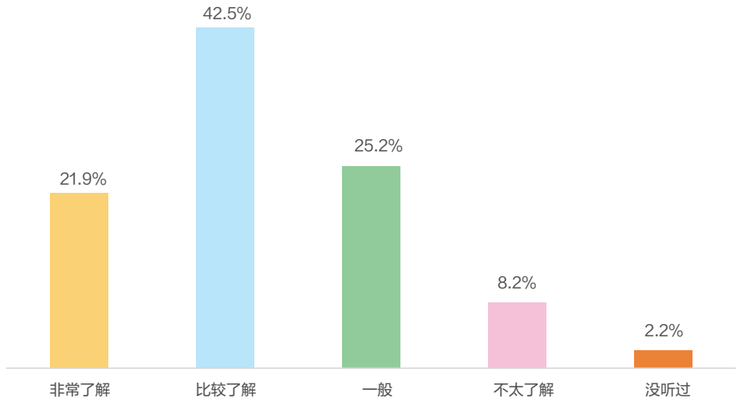
在校生辅修专业情况



在校生选择辅修的专业

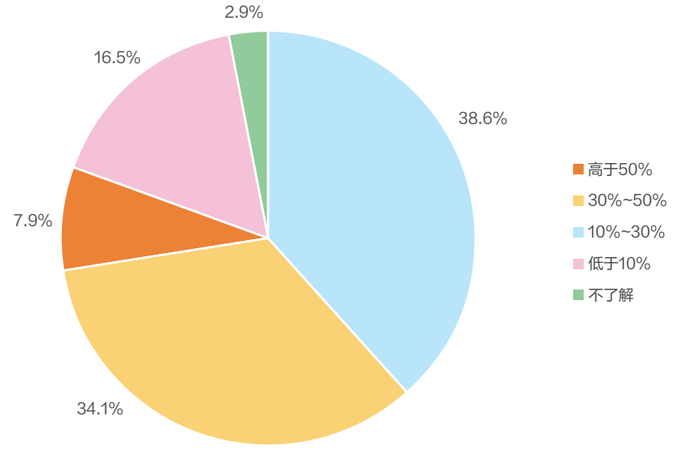
六、仅2成在校生非常了解AI的网络安全应用，AI技术迭代对专业学习影响大

随着以AIGC为代表的生成式AI技术迅猛发展，大语言模型在众多领域得到推广，在校生加强了对AI技术的学习。不过，非常了解AI在网络安全领域应用的受访在校生仅占21.9%，比较了解的占比42.5%，只有2.2%没听过相关应用情况。



在校生对AI应用的认知程度

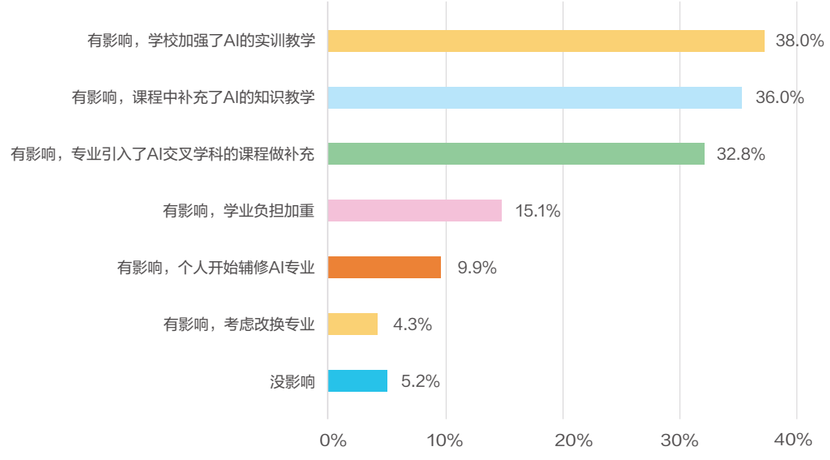
在受访的网络安全专业在校生中，学习AI知识占10%-30%的在校生占比最高，为38.6%。其次是学习AI知识占30%-50%的在校生，占比34.1%。而学习AI知识占比高于50%的在校生仅占7.9%。总体来看，AI技术于在校生专业知识中的比重合理，未来将更进一步提高。



在校生所学AI知识的占比

七、近4成在校生表示学校加强了AI的实训教学

在谈到AI对专业学习的影响问题时，超9成在校生认为AI对自己的专业学习产生了影响。其中，38%的受访在校生表示，受AI技术迭代的影响，学校加强了AI的实训教学，占比最高；36%表示，学校在课程中补充了AI的知识教学，32.8%认为，学校在专业中引入了AI交叉学科的课程作为补充。在面对AI技术冲击带来的专业知识调整时，受访在校生也体现出学习的主动性，9.9%开始辅修AI专业，也有4.3%考虑改换专业应对技术冲击。

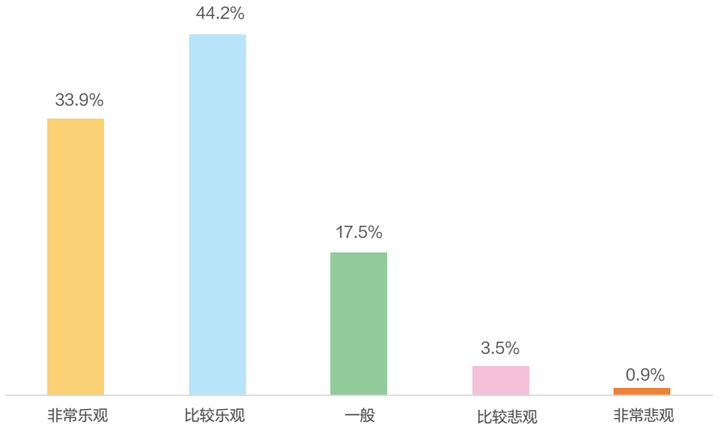


在校生对AI影响专业学习的看法

（三）在校生就业规划

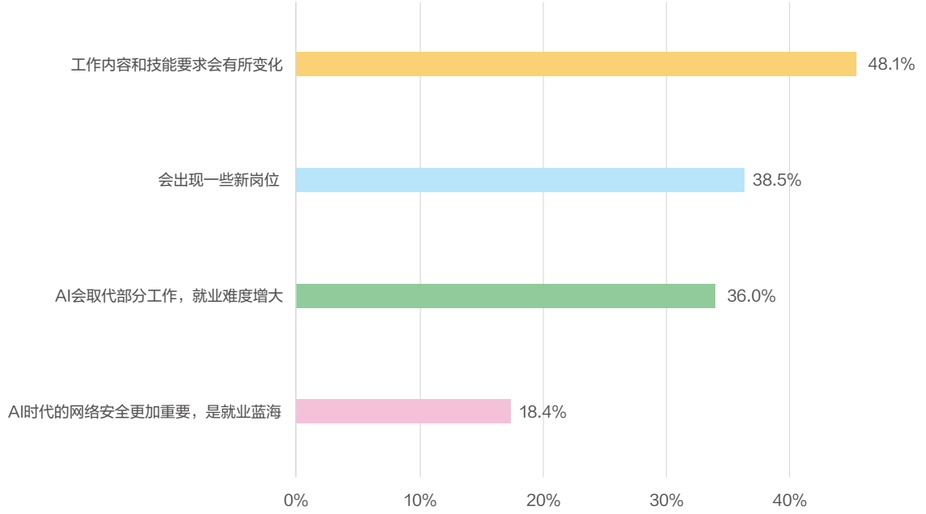
一、近8成在校生对就业表示乐观，正视工作技能要求变化

对于未来就业趋势，网络安全专业在校生普遍比较乐观。有33.9%的受访在校生非常乐观、44.2%比较乐观，共有78.1%表示出乐观情绪。也有17.5%的受访在校生认为未来趋势一般，保持冷静观望的态度。



在校生对未来就业趋势的态度

同时，在校生也普遍展现出对AI技术影响就业话题的关注，48.1%的受访在校生认为在AI技术影响下，工作内容和技能要求会有所变化，38.5%认为会出现一些新岗位，36%认为AI会取代部分工作并加大就业难度。此外，也有18.4%的受访在校生对AI的影响持乐观态度，认为AI时代的网络安全工作更加重要，是就业蓝海。

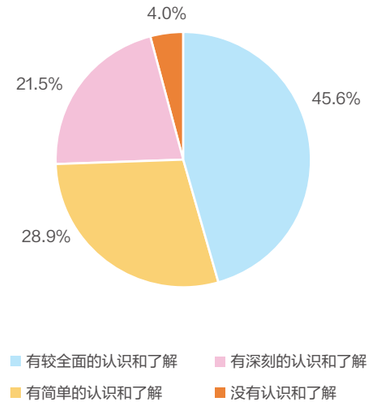


在校生对AI影响就业的看法

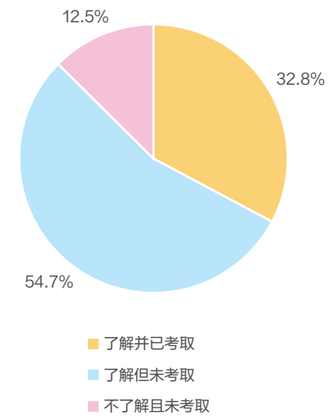
二、在校生对网络安全岗位普遍较为了解，超3成考取网安证书

学习网络安全专业的受访在校生中，45.6%对岗位要求有较全面的认识和了解，占比最高。其次，对相关专业有简单或深刻的认识和了解的在校生分别占比28.9%和21.5%。可见，共有67.1%的在校生对网络安全岗位的要求有比较深刻或全面的认识和了解。

不少在校生未雨绸缪，通过考证积蓄找工作的优势。32.8%的网络安全专业受访在校生考取了网络安全证书，也有54.7%的在校生了解这一考试但暂未考取相关职业证书。



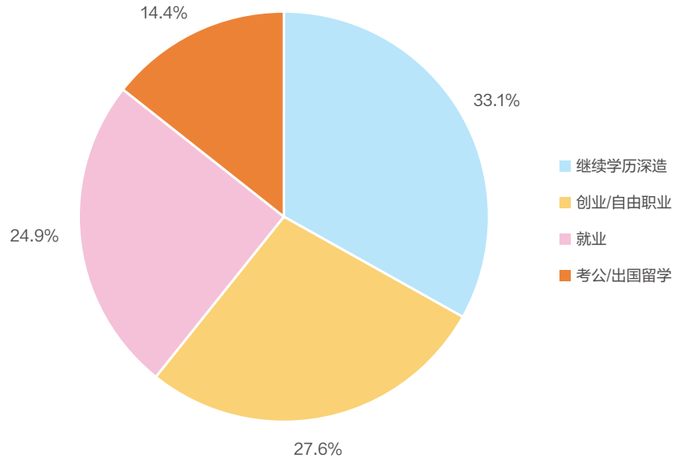
在校生对岗位要求的了解程度



在校生职业证书考取情况

三、学历深造是毕业生首选，不到25%选择就业

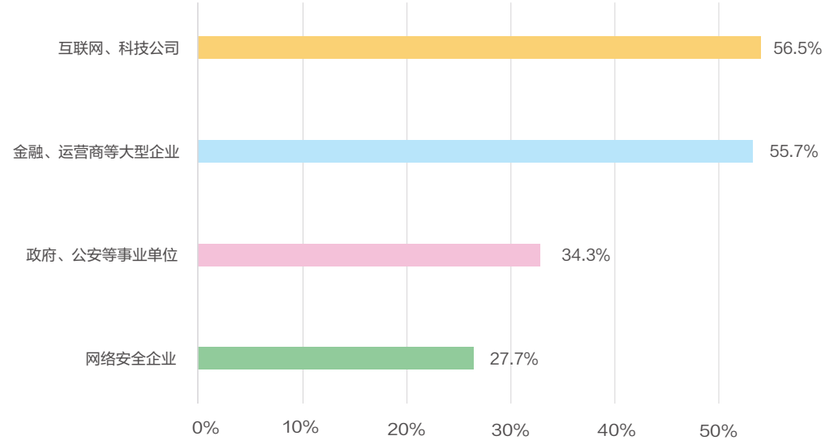
在被问及毕业后的去向时，33.1%的受访在校生表示将继续进行学历深造，占比排名首位。其次是创业/自由职业、就业，占比分别为27.6%、24.9%。也有14.4%的受访在校生准备考公或出国留学。可见网络安全专业在校生在就业去向的选择上更加多样，对继续深造的偏好明显，同时对创业/自由职业的接受度较高。



在校生毕业计划去向

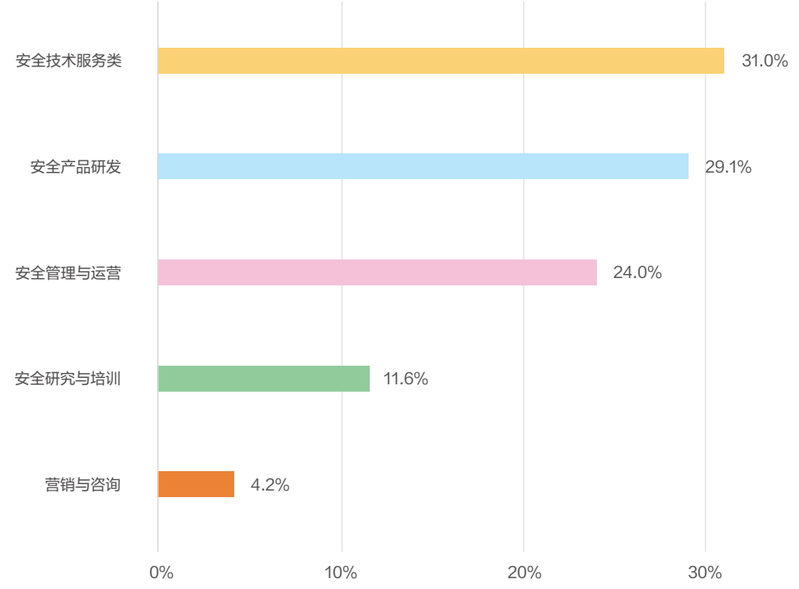
四、IT和金融是就业首选，安全技术服务与产品研发岗位受欢迎

问卷调研数据显示，对于网络安全在校生而言，互联网、科技公司是最向往的企业/行业，占比56.5%。其次是金融、运营商等大型企业，占比55.7%。IT、金融、运营商行业收入较高、福利待遇较好、前景广阔，是大多在校生向往的行业。此外，也有34.3%的受访在校生倾向于“求稳”，选择去政府、公安等事业单位工作，选择网络安全企业的仅占27.7%，这可能是因为网络安全领域正处于成长期，企业数量及规模仍在发展，对于在校生来说就业机会较少，预计未来随着网络安全产业的稳步发展，该领域可以为在校生提供更多的就业机会。



在校生意向的就业企业/行业

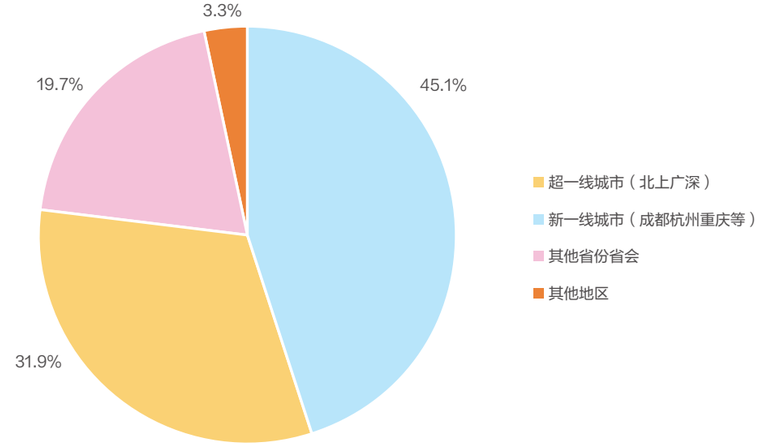
从岗位来看，安全技术服务类岗位最受在校生欢迎，占比31%。其次是安全产品研发，占比29.1%。而管理、运营、培训、营销、咨询等岗位的受欢迎程度位居其后，总体来看，网络安全在校生更倾向于到技术研发类岗位工作。



在校生计划从事的岗位方向

五、新一线城市更吸引网安毕业生

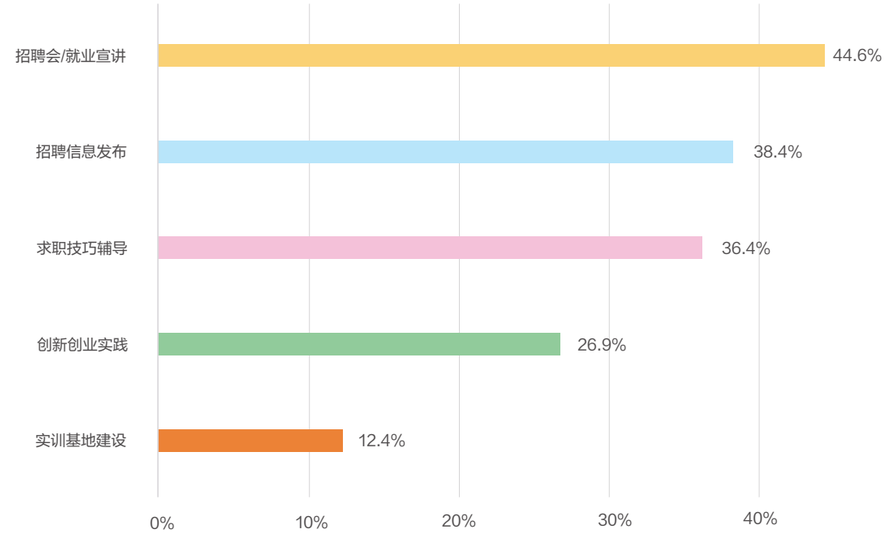
从城市来看，受访的网络安全专业在校生最愿意选择新一线城市就业，占比45.1%。其次是北上广深等超一线城市，占比31.9%。新一线城市成为毕业生的首要偏好，一方面与网络安全产业在新一线城市逐步成长有关，另一方面也与毕业生“一线城市情结”减弱有关。在校生对新一线的明显青睐，有助于弥补新一线城市与一线城市的人才差距，为新一线城市未来发展提供强有力支持。



在校生优先选择的就业城市

六、超4成网安生所在院校推出招聘会，校园招聘信息是求职最常用渠道

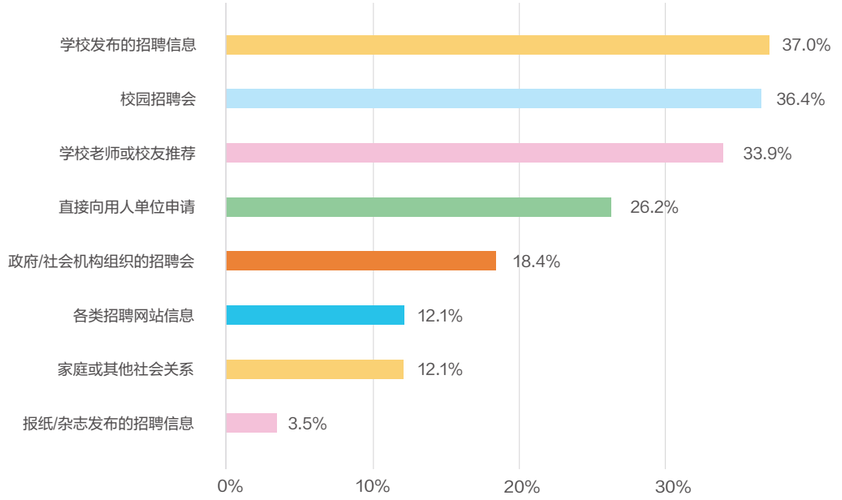
对于在校生来说，校园招聘会是求职的主要途径，网络安全专业在校生所在院校也会提供多种就业指导与就业服务。调研数据显示，44.6%的受访在校生所在学校会举办招聘会/就业宣讲，38.4%的学校会发布招聘信息，36.4%提供求职技巧辅导，26.9%提供创新创业实践。



院校就业指导与服务

目前，在校生获取求职信息最常用的渠道是校园网站或海报，37%的受访在校生通过学校了解招聘信息。其次是校园招聘会、老师或校友介绍，分别占比36.4%、33.9%。

这表明，在校生在获得就业信息方面有较为明显的校园路径依赖，企业可以通过学校发布招聘信息，提高招聘网络安全专业学生的效率。



在校生获取求职信息的渠道

第五章

网络安全产业人才发展建议

一、加强学科建设，以专业知识筑牢“防火墙”

从学科建设上看，近9成在校生对网络安全课程及教材满意，8成以上满意实训环境，可见目前高校网络安全学科建设较为成熟。不过，仍然要筑牢专业知识的防火墙，为学生上好Linux、SQL、Java等技术课程。与此同时，根据25.2%的在校生想参加但未参加网络安全竞赛、2.4%的在校生根本没听说过，高校可将竞赛纳入到网络安全专业学科建设中，提高人才的专业意识、解决问题的实践能力。此外，高校还应针对招聘企业及岗位需求，帮助网络安全专业学生进行辅修，了解AIGC等前沿技术，打造复合型跨领域人才。

二、实施产教融合，以实习基地下好“一盘棋”

从调研情况看，44.4%的在校生认为实践实习经历是未来求职的竞争力。高校应当实施产教融合，与各地园区建立实习实训基地，在助力在校生迅速成长的同时，也为网络安全企业储备人才。高校应与企业加强合作，搭建网络安全产教协同创新平台，推动网络安全“新工科”应用型人才培养，促进网络安全教育资源协同整合，为国家网络强国建设提供人才支撑。

三、增进区域交流，以互动学习夯实“护城河”

北京、上海、深圳、成都等地，是网络安全产业、人才需求、人才供给充分发展的区域。除了区域间的合作交流，其他城市也应从“先发者”经验中找到灵感，对网络安全、数据安全、云计算领域所形成的产品、方案进行深入了解，加强区域互动学习合作。除了区域交流，行业间的对话合作也很关键，可以通过行业协会等第三方组织牵线搭桥，增进网络安全细分专业领域的交流与合作，促进网络安全发展水平在互动交流中不断得到提升。

四、培养实战能力，使人岗匹配实现“无缝隙”

目前，我国网络人才需求与供给之间存在较大缺口。除了数量上的不匹配，网络安全人才的专业技能有时也无法满足企业需求，主要体现为缺乏实践、经验不足。应当鼓励和为高校人才提供实战机会，帮助在校人才掌握防火墙、网络交换机等设备配置能力以及企业在实际业务中亟需的其他行业技能。平衡理论与实践课程设置、师资配比，警惕教学投入过度。可适当减少专业能力的理论性投入，将更多资源投入到培养人才实践能力上，使人岗无缝匹配。

五、强化政策引领，为产业发展按下“快进键”

在数字中国建设过程中，网络安全产业是不可或缺的重要一环。应当加强政策引领，以政策指导各地布局网络安全、数字安全产业，构筑自立自强的数字技术创新体系。筑牢可信可控的数字安全屏障，切实维护网络安全，完善网络安全法律法规和政策体系，增强数据安全保障能力，建立数据分类分级保护机制，健全网络安全监测预警和应急处置工作体系，为产业发展按下“快进键”。

附录：2018-2023网络安全产业人才需求及相关情况

年份	招聘需求最高岗位	用人单位能力要求	招聘需求最高区域	从业人员能力提升主要方向
2018	安全运维	信息安全相关工作成功经历	北京、广东、上海	大数据安全
2019	技术服务	具备较强技术能力	北京、广东、上海	云安全
2020	技术服务	沟通交流能力好	北京、上海、深圳	安全工具
2021	安全研究	工作经验	北京、深圳、杭州	攻防渗透
2022	安全应急与防御	工作经验	北京、上海、深圳	大数据安全
2023	网络安全运营	高学历、高技能	北京、上海、深圳	AI技术

《网络安全产业人才发展报告》已连续发布6年，综观6年来的人才需求情况，企业对毕业生、高技能人才的招聘需求保持较高水平，但基于技术快速迭代、行业热点转化，企业对人才的经验要求有所下降，招聘需求最高岗位也从安全运维、应急防御等，转换到安全运营等。

从招聘企业类型上看，民营企业是网络安全招聘的主要需求方。而随着各行各业加快数字化转型，除了千人以上大型企业，中小企业对网络安全岗位招聘需求也与日俱增。从地域来看，北上广深等一线城市保持着网络安全招聘需求的热度，杭州异军突起，在2021年成为唯一跻身三甲的新一线城市。

网络安全从业人员普遍希望提升技术能力，从大数据安全、云安全，到攻防渗透、AI技术，技术学习需求与当下技术热点紧密挂钩。可见，技术升级对人才专业基础和知识结构提出了更多考验，在理论与实践中知行合一，是网络安全从业者奔赴更广阔未来的必由之路。

PDF-XChange Editor
Click to BUY NOW!
www.tracker-software.com