安全牛
AQNIU.NET

（2025版）

新时期网络安全人才能力建设指南

新时期网络安全人才驱动的安全战略势在必行

版权声明

本报告为北京谷安天下科技有限公司（以下简称“本公司”）旗下媒体平台安全牛研究撰写，报告中所有文字、图片、表格均受有关商标和著作权的法律保护，部分文字和数据采集于公开信息，所有权为原著者所有。未经本公司书面许可，任何组织和个人不得将本报告内容作为诉讼、仲裁、传媒所引用之证明或依据，不得用于营利或用于未经允许的其他用途。任何未经授权的商业性使用本报告的行为均违反《中华人民共和国著作权法》及其他相关法律法规、国际条约。未经授权或违法使用者需自行承担由此引发的一切法律后果及相关责任，本公司将依法予以追究。

免责声明

本报告仅供本公司的客户或公司许可的特定用户使用。本公司不会因接收人收到本报告而视其为本公司的当然客户。任何非本公司发布的有关本报告的摘要或节选都不代表本报告正式完整的观点，一切须以本公司发布的本报告完整版本为准。

本报告中的行业数据主要为分析师市场调研、行业访谈及其他研究方法估算得来，仅供参考。因调研方法及样本、调查资料收集范围等的限制，本报告中的数据仅服务于当前报告。本公司以勤勉的态度、专业的研究方法，使用合法合规的信息，独立、客观地出具本报告，但不保证数据的准确性和完整性，本公司不对本报告的数据和观点承担任何法律责任。同时，本公司不保证本报告中的观点或陈述不会发生任何变更。在不同时期，本公司可发出与本报告所载资料、意见及推测不一致的报告。

本报告所包含的信息及观点不构成任何形式的投资建议或其他行为指引，亦未考虑特定用户的个性化需求或投资目标。用户应结合自身实际情况独立判断报告内容的适用性，必要时应寻求专业顾问意见。报告中涉及的评论、预测、图表、指标、理论等内容仅供市场参与者及用户参考，用户需对其自主决策行为负责。本公司不对因使用本报告全部或部分内容所产生的任何直接、间接、特殊及后果性损失承担任何责任，亦不对因资料不完整、不准确或存在任何重大遗漏所导致的任何损失负责。

引言

在“数字中国”战略的浪潮之下，数据作为核心生产要素，正深度融入实体经济、政务服务、科技创新等关键领域，其重要的战略地位愈发凸显。同时，近期人工智能（AI）为代表的新兴技术正以前所未有的速度渗透到各行各业，在赋能数据挖掘、智能决策提升效率发挥作用。在数字化发展的新时期，网络安全已然跃升为维系国家经济命脉、社会稳定和个人隐私安全的基石，国家高度重视网络安全，从《网络安全法》《数据安全法》到《个人信息保护法》，法律法规体系不断完善筑牢制度防线，网络安全成为企业抵御风险、保障持续运营的“生命线”。

但是，新型技术也带来了全新的攻击面和风险，AI 驱动的自动化攻击能突破传统防御壁垒，深度伪造技术可制造虚假信息引发信任危机，算法漏洞更可能导致数据泄露或决策失序，安全威胁态势呈现出“速度快、隐蔽性强、影响范围广”等快速演变特征。国家积极推动实战化攻防演练，倒逼企业打破“合规即安全”的传统认知，推动企业需要将安全能力体系升级到高强度实战化主动防御，以适配数字时代的安全需求。

在这样的背景下，国内企业在人才能力发展上普遍遭遇各种困境和挑战。一方面，安全领域技术迭代与攻防态势的快速演变，使得企业陷入人才能力管理盲区，“不知道需要什么能力的人才”，不清楚应对 AI 漏洞挖掘、数据溯源追踪等新兴需求应匹配何种知识结构与实战经验，也“不知道怎样管理人才”，缺乏适配安全人才成长规律的培养体系与激励机制，难以将零散的人才能力转化为系统性的实战的主动的战斗力。另一方面，国内企业长期存在的“重合规建设、轻运营”惯性思维，导致安全建设多聚焦于满足政策条文的硬性指标，资源多投向硬件采购与制度堆砌，忽视攻防实战所需的应急响应、威胁狩猎等核心能力培养，造成安全人才“纸上谈兵”者多、能打硬仗者少，能力与常态化攻防对抗需求严重脱节。更值得警惕的是，新兴技术带来的新难题持续放大人才缺口，如面对量子计算对加密体系的冲击、生成式 AI 带来的虚假攻击溯源等新挑战，已有的人才储备几乎无经验可循。这些问题构成了企业安全能力难以逾越的“鸿沟”，不仅让安全团队在实际攻防中屡屡陷入被动，更使企业数字化转型赖以支撑的安全基石出现致命短板，面临数据泄露、系统瘫痪等严峻风险。

针对这些痛点，本报告旨在提供新时期网络安全人才培养的清晰路径和行动指引，通过深入探讨新时期的网络安全人才的能力框架、治理管理，为企业、政府和行业者提供新时期网络安全人才培养的路径和行动指引，共同应对数字时代的安全挑战。

关键发现

- **新时期需要跨领域融合创新的π型复合人才。**新时期最需要的人才已不再是单一技能型人才，而是具备“一横”（宽广通用知识面）和“一竖”（深入专业技能）的 T 型人才，并演进为拥有多重深度、能够实现跨领域融合创新的π型复合人才。

- **人才是新时期安全战略的核心引擎。**在新时期背景下，人才驱动战略将使网络安全从单纯的成本中心转变为持续创造价值的战略投资。拥有创新思维和复合能力的π型人才，能够帮助企业驱动业务创新和可持续发展。网络安全思维应将人才视为战略资产，才能从根本上驱动安全能力的持续提升，应对复杂多变的威胁。

- **新时期人才通用需求的根本性转变。**新时期最需要的人才已不再是单一技能型人才，而是具备“一横”（宽广通用知识面）和“一竖”（深入专业技能）的 T 型人才，并进一步演进为拥有多重深度、能够实现跨领域融合创新的π型复合人才。

- **AI 的颠覆性影响。**从技术威胁到人才升级的契机。AI 发展带来的“知识平权”效应是一把双刃剑，淘汰了固守过往知识的人，但同时也为具备敏捷学习能力的“主动进化者”提供了升级为π型复合人才的重大机遇。

- **AI 训练师将成为 AI 时代的职业新赛道。**随着人工智能的快速发展，AI 的变革正在驱动职业角色从“AI 操作员”向“AI 训练师”新赛道升级转型。

- **国内现有人才能力框架的不足与挑战。**国家标准 GB/T42446-2023 等现有框架在应对新时期的挑战时存在明显不足，报告融合 GB 国标、NIST、ECSF 等框架优势，重构一个深度融入中国特有战略和技术需求的融合型人才能力框架。

- **人才能力发展应以治理为本。**人才治理是人才发展的系统化保障，应通过将人才战略纳入企业整体治理框架，确保人才培养有顶层设计、有资源保障、有持续改进机制。

- **人才能力的生态共赢。**协同解决人才困境问题需要政、产、学、研、用各方的深度协同。通过建立人才培养生态，加强企业与高校、厂商的合作，可以共同弥补人才供给的结构性短板，实现人才发展的可持续性。

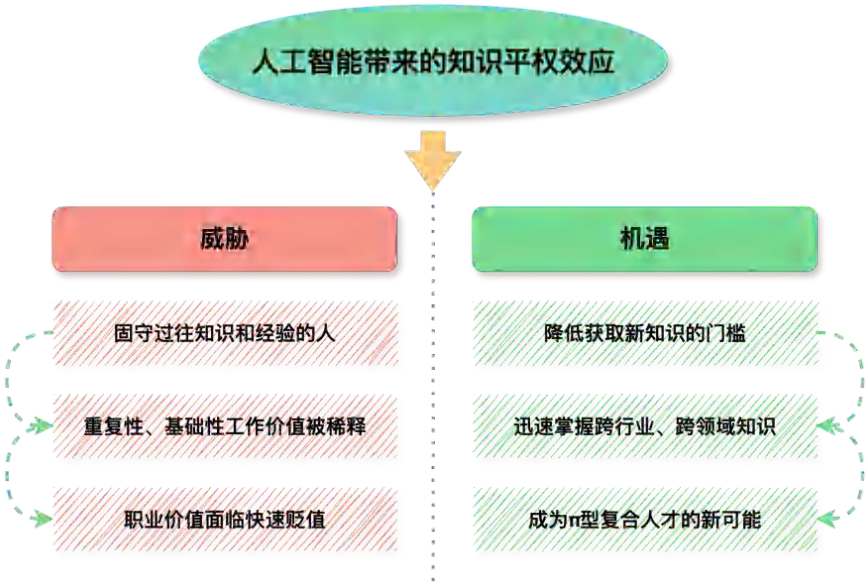
目 录

第一章 新时期的通用复合人才

新时期面临的是充满不确定性的数智化浪潮和日益复杂的经济环境，企业与个人都面临着前所未有的生存与发展考验。在数字中国战略、以数据作为核心生产要素和人工智能（AI）为代表的新兴技术的数智化背景下，AI、大数据等技术已不再是单纯的工具，而是驱动商业模式变革的核心力量，这种技术范式的大变革，使企业对人才的价值要求空前提高，迫使我们不得不重新审视传统的人才培养模式。

1.1 新时期数智化浪潮的人才抉择

数智化浪潮变革中，人工智能快速发展带来了“知识平权”效应，正像双刃剑一样深刻地重塑着人才的价值逻辑。人才需从被动适应转向主动进化，π型复合人才将成为企业数智化转型的核心驱动力，也是个人在 AI 时代实现价值提升的必然选择。



“知识平权”效应

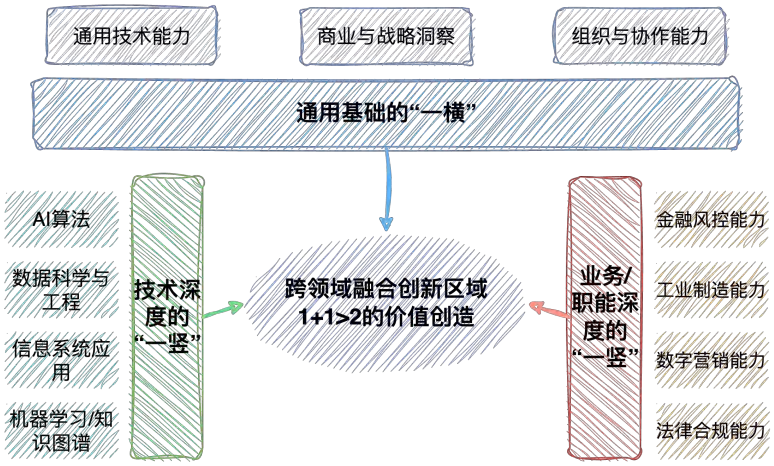
首先，对那些固守过往知识和经验、安于现状的人来说，AI 构成了巨大的“威胁”。AI 工具的普及让掌握知识变得唾手可得，使他们所依赖的重复性、基础性工作变得越来越不值钱，职业价值面临被快速稀释的风险。**同时，**AI 也极大地降低了获取新知识的门槛，为人才的“能力升级”提供了前所未有的机遇。使一部分人能够迅速掌握跨行业、跨领域的知识，为成为π型复合人才提供了新的可能。安全牛认为，未来 AI 将不再是简单的工具，而是能够赋能人才、加速学习、实现能力跃迁的“智能导师”。因此，在数智化浪潮中，人才的抉择已不再是“要不要学 AI”，而是“如何从被动适应，转向主动进化”。对

于企业而言，人才能力的主动进化是保障数智化转型的核心驱动力；对于个人而言，是在数智化时代变革中实现价值提升的必然选择。

在这样的背景下，安全牛提出了适合这场数智化浪潮的人才能力的变革新范式：π型复合人才，并将详细对π型复合人才的能力框架进行解构说明，同时为企业和个人提供了详细的解决方案，旨在帮助企业和个人在 AI 时代找到清晰的方向，将挑战转化为机遇，共同迎接数智化浪潮带来的全新未来。

1.2 新时期π型数智化人才的概述

在数智化时代，企业数字化转型需要跨领域、跨职能的业务能力，传统的单一技能型的“专业人才”已无法应对企业的需求，因此企业与个人都必须重新定义人才。π型数智化复合人才正是为解决这一困境而生的新范式。π型复合人才是指拥有两条深度“一竖”（技术深度+业务/职能深度）的复合型人才，包括通用基础的“一横”与技术深度和业务深度的“双竖”，实现跨领域融合创新，是数智化时代企业数字化转型的关键人才类型，实现企业数字化转型需要的跨领域融合创新能力。“梳子型人才”则被视为π型人才的进阶形态或多维复合型人才的代名词，属于最高阶的 L4 创新/领导层，本报告统一使用‘π型’作为标准术语。”



π型数智化人才模型

1）“一横”：数智化时代的通用基础

通用基础的“一横”代表所有π型复合人才必须具备的、宽广而坚实的通用基础能力。构成了人才的底层通用基础能力，是人才实现“主动进化”的根基。在 AI 的知识平权效应下，通用基础能力变得尤为关键，知识获取不再是简单的记忆，而是融会贯通、灵活应用的综合素养。

通用技术能力：通用技术不是要求成为技术专家，而是需要具备快速高效地理解能力。比如对 AI 算法、机器学习/知识图谱、大模型基础原理、数据分析方法、云计算基础架构和网络安全与数据治理基础的理解，这种能力使人才能够快速将技术融入业务决策。

商业与战略洞察：深入理解业务流程、商业模式和行业发展趋势，能够将技术能力与商业价值相匹配。人才需要跳出技术视角，从市场、用户和竞争的角度思考问题，确保技术创新能够转化为实际的商业成果。

组织与协作能力：具备卓越的沟通协调、领导力、创新思维和伦理判断能力。在跨职能、跨部门的协作中，π型复合人才需要扮演“翻译”和“粘合剂”的角色，确保团队能够高效协同，共同解决复杂问题。

2）“双竖”：实现价值突破的双重深度

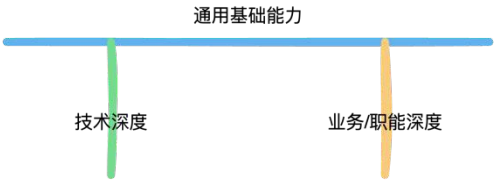
“双竖”是π型复合人才的核心价值所在，代表人才在两个或更多领域具备专家级深度，并能够实现创新性融合。多重深度能使人同时在多个业务领域中工作，推动业务创新，从而创造出 1+1>2 的价值。

- 技术深度的“一竖”：聚焦于核心技术领域的精深造诣。这是π型复合人才的硬核能力。例如：AI/机器学习算法能力，可设计、训练和优化复杂的 AI 模型。数据科学与工程能力，能够处理海量数据，进行深度分析，并构建数据管道。云原生架构能力，能够设计和管理基于容器、微服务的高弹性云架构。高级网络安全攻防能力，具备红队、蓝队或威胁狩猎的实战能力。

- 业务/职能深度的“一竖”：聚焦于特定业务领域或职能的专家级经验。这是π型复合人才的落地能力。例如：金融风控能力，熟悉金融业务流程，能够运用技术进行欺诈识别和信用评估。工业制造能力，深入了解工业生产线，能够运用技术优化生产效率和设备维护。数字营销能力，掌握营销策略和用户行为，能够运用技术进行精准营销。法律合规能力，精通法律法规，能够运用技术进行合规审计和风险管理。

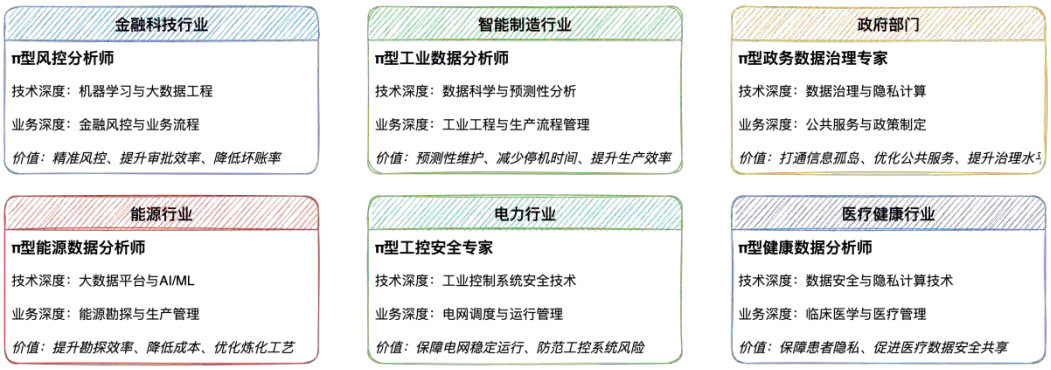
1.3 新时期π型数智化人才的设计

在数智化浪潮中，企业面临的挑战已不再是单纯的技术问题，而是技术与业务、技术与管理、技术与市场的深度交叉。π型复合人才正是应对这种“交叉性”挑战的最佳解法。



π型人才能力结构

π型复合人才能够以多维视角洞察问题，并以融合能力创造出颠覆性的解决方案,解决技术与业务、管理、市场的深度交叉挑战通过“一横一竖”的能力结构创造颠覆性解决方案。下面使用多个行业举例详细说明π型复合人才如何通过其独特的能力结构，为业务产生实际价值和深远影响。



π型人才在各行业的设计

1）金融科技行业：π型风控分析师

传统的金融风控专家懂业务但不懂技术，难以利用大数据进行精准风控；而传统的算法工程师懂技术但缺乏金融知识，导致开发的模型难以落地。**π型风控分析师**则能将“机器学习”与“金融风控”深度结合。自主设计并开发更精准的欺诈识别模型，预测和防范潜在的信贷风险，从而在保证业务安全的前提下，大幅提升信贷审批效率，降低企业的坏账率。通过跨领域的洞察，能够将技术创新转化为直接的商业价值，有效平衡风险与收益。

π型风控分析师能力包括：

π型风控分析师通用基础的“一横”包括具备强大的数据分析能力、商业伦理与合规意识，以及与业务、技术团队高效沟通的能力。

π型风控分析师技术深度的“一竖”包括掌握机器学习与大数据工程。精通各类风控模型（如欺诈识别、信用评分）的开发、训练与部署，能够处理银行、交易平台的海量数据。

π型风控分析师业务/职能深度的“一竖”包括掌握金融风控与业务流程。深入理解银行信贷、支付清算、反洗钱（AML）等金融业务的底层逻辑、监管要求和风控痛点。

2）智能制造行业：π型工业数据分析师

传统的生产工程师懂设备但不懂数据分析，难以从海量数据中提炼价值；而通用的数据分析师懂算法但缺乏工业知识，无法理解数据背后的物理意义。**π型工业数据分析师**则能将“数据科学”与“工业工程”无缝融合。可以基于设备运行数据，构建预测性维护模型，提前发现设备故障隐患，将停机时间减少。同时还能分析生产流程中的瓶颈，提出优化方案，大幅提升生产效率和产品质量，真正用数据驱动工业生产力的升级。

π型工业数据分析师人才能力包括：

π型工业数据分析师通用基础的“一横”包括具备数据科学基础、数智化管理理念、物联网（IoT）技术认知，以及与生产线工程师和 IT 团队协作的能力。

π型工业数据分析师技术深度的“一竖”包括掌握数据科学与预测性分析。能够处理并分析工业设备传感器产生的大规模时间序列数据，运用算法进行异常检测和故障预测。

π型工业数据分析师业务/职能深度的“一竖”包括掌握工业工程与生产流程管理。深入了解生产线的物理运行机制、设备工艺参数、供应链管理和质量控制标准。

3）政府部门：π型政务数据治理专家

传统的政府 IT 人员懂系统但不懂数据治理，难以保障政务数据的安全共享；而政策制定者懂法规但缺乏技术认知，难以设计可落地的数字政府方案。**π型政务数据治理专家**能将“数据治理技术”与“公共服务与政策制定”进行融合，在确保公民隐私数据安全的前提下，设计跨部门的数据共享平台，打通“信息孤岛”，从而优化公共服务流程，提升政府治理的智能化水平。使政府能够在法律合规与技术赋能之间找到最佳平衡，实现数据价值的最大化利用。

π型政务数据治理专家能力包括：

π型政务数据治理专家的通用基础的“一横”包括具备数据治理、隐私计算等技术认知，熟悉国家法律法规（如《数据安全法》）、公共管理与服务流程，以及与技术团队、政府各部门沟通协调的能力。

π型政务数据治理专家技术深度的“一竖”包括掌握数据治理与隐私计算。精通政务数据的分类分级、权限管理、数据脱敏等技术，能够设计和实施安全的数据共享平台和隐私计算方案。

π型政务数据治理专家业务/职能深度的“一竖”包括公共服务与政策制定。深入理解政务服务的核心流程、政策制定的逻辑以及公民对数据保护的诉求。

4）能源行业：π型能源数据分析师

传统的油气勘探专家懂地质但缺乏数据分析能力，难以从海量勘探数据中高效提取价值；而通用的数据科学家懂算法但缺乏能源行业的专业知识，难以将算法应用于实际问题。**π型能源数据分析师**能将“大数据与 AI 技术”与“能源勘探与生产”相结合。可以利用 AI 模型，从地质数据、地震波数据中快速识别油气储藏区域，大幅提升勘探效率，降低勘探成本。同时，还能通过分析生产数据，优化炼化工艺，预测设备维护周期，提高整体生产效益。

π型能源数据分析师能力包括：

π型能源数据分析师的通用基础的“一横”包括具备数据科学基础、AI/ML 原理、大数据平台架构知识，以及对能源市场趋势和管理流程的洞察。

π型能源数据分析师技术深度的“一竖”包括掌握大数据平台与 AI/ML。精通海量数据存储、处理与分析技术，能够构建和部署复杂的 AI/ML 模型，用于油气勘探数据分析、设备故障预测等。

π型能源数据分析师业务/职能深度的“一竖”包括掌握能源勘探与生产管理。深入了解油气勘探的地质学原理、钻井技术、炼化工艺以及能源供应链的运作模式。

5）电力行业：π型工控安全专家

传统的 IT 安全专家懂 TCP/IP 但不了解各种电网设备，并无法理解电网工控系统的特殊性；而工控工程师懂设备但缺乏网络安全意识，可能成为安全事件的突破口。**π型工控安全专家**能将“工控安全技术”与“电网调度”完美融合，可以在保障电网稳定运行（B）的前提下，对关键工控系统进行安全加固，并能够发现并处置针对工业控制系统的恶意软件，防范物理设备被远程控制的风险，直接保障国家关键基础设施的安全，避免大面积停电等灾难性后果。

π型工控安全专家能力包括：

π型工控安全专家的通用基础的“一横”包括具备 IT 网络安全基础、风险管理、国家关键信息基础设施保护政策法规，以及与生产调度人员和 IT 人员协作的能力。

π型工控安全专家技术深度的“一竖”包括掌握工业控制系统（ICS）安全技术。精通工控协议、工业防火墙、工控系统漏洞评估与加固技术，能够设计并实施 IT 与 OT 深度融合环境下的安全防护体系。

π型工控安全专家业务/职能深度的“一竖”包括掌握电网调度与运行管理。深入理解电网调度规程、发电厂和变电站的运行流程、电力设备的物理特性和安全要求。

6）医疗健康行业：π型健康数据分析师

传统的 IT 安全人员懂技术但不懂医疗数据，难以保障数据在诊疗和科研中的合规使用；而医生懂业务但缺乏数据安全知识，可能无意中造成数据泄露。**π型健康数据分析师**则能将“数据安全技术”与“临床医学”进行融合。设计出既能确保患者隐私，又能让医院在多中心科研合作中安全地共享数据的系统，在加速新药研发和疾病诊疗的研究的同时，规避法律风险，并为医疗健康行业的创新提供了安全底座。

π型健康数据分析师能力包括：

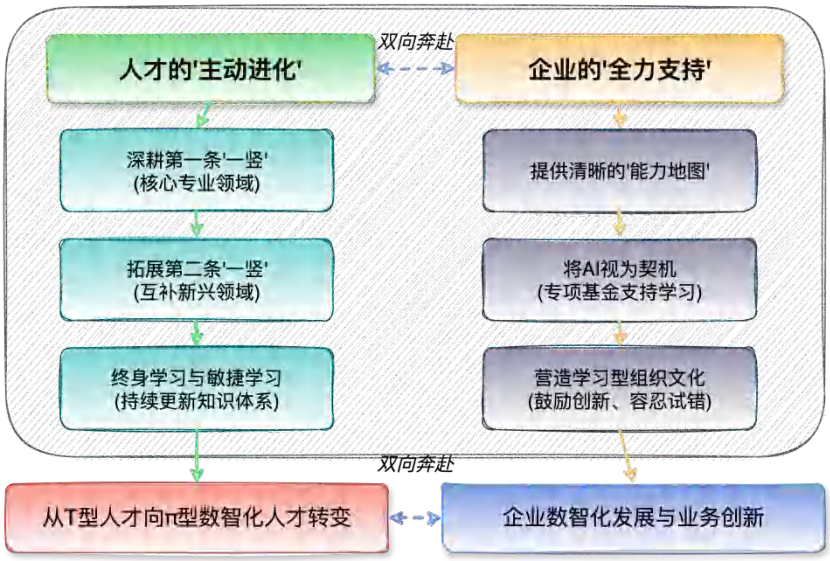
π型健康数据分析师通用基础的“一横”包括具备法律法规素养（如《数据安全法》）、数据治理基础、生物医疗伦理意识，以及与医生、IT 人员、患者等多方沟通的能力。

π型健康数据分析师技术深度的“一竖”包括掌握数据安全与隐私计算技术。精通数据加密、数据脱敏、联邦学习等隐私保护技术，能够设计符合监管要求和行业标准的健康数据安全架构。

π型健康数据分析师业务/职能深度的“一竖”包括掌握临床医学与医疗管理。深入理解医疗流程、患者诊疗数据（病例、影像）的特殊性，以及医院内部 IT 系统的运作方式。

1.4 新时期π型数智化人才的成长路径

π型数智化人才不仅是应对时代变革的生存之道，更是实现个人与企业价值共创的必由之路。π型数智化人才并非天生，是通过有意识地跨领域学习和实践培养而成，是个人的“主动进化”与企业“全力支持”的双向奔赴，企业和个人的共同目标是推动工作迈向新高度，保障企业数智化发展，实现从赋能业务创新的转型。



π型数智化人才成长是企业与个人共同责任

1）人才的“主动进化”是个人的成长责任

在 AI 的“知识平权”效应下，个人必须告别“被动适应”的旧思维，将终身学习内化为一种习惯。

个人应努力学习，从“T”主动进化成长到“π”型数智化人才：

- 首先，深耕第一条“一竖”：确保在某一核心领域（无论是技术还是业务）具备专家级的深度，这是建立业务能力立足点和信任基础的关键。

- 然后，有意识地拓展第二条“一竖”：基于第一条“一竖”，选择一个相邻或互补的新兴领域进行深度学习和实践。例如，一个具备数据科学深度的人，可以选择学习智能制造或数字营销的业务知识；一个具备网络安全深度的人，可以学习 AI 或云原生架构，利用 AI 工具作为快速学习新知识的强大助手。

- 最后，应终身学习与敏捷学习。在知识快速迭代的时代，应具备强大的自我驱动力和敏捷学习能力，不断更新知识体系，适应新的岗位要求和技术挑战。可通过跨部门轮岗、参与跨领域项目、获取新兴技术认证等方式，拓展自己的能力边界。

2）企业的“全力支持”：构建赋能人才的沃土

企业在人才进化中扮演着至关重要的“赋能者”角色。人才的成长是企业的责任，企业的全力支持能够极大地加速人才的转型，并最终转化为企业的核心竞争力。

企业应为人才提供清晰的“能力地图”：

- 构建路径：为员工提供清晰的π型复合人才画像和职业发展路径，让员工明确知道下一个进阶目标所需的具体知识、技能和能力水平。将人才画像具现化，形成企业内部的“人才能力地图”，并将其作为绩效考核和职业晋升的重要依据。

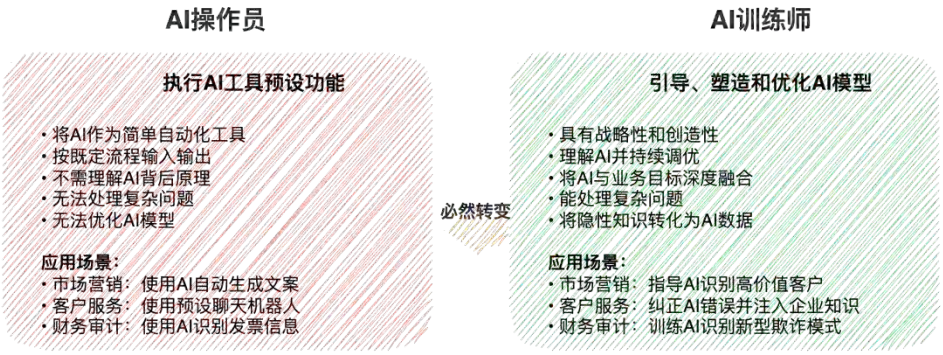
- 将 AI 视为契机，设立专项基金，鼓励员工学习 AI、隐私计算等新技能，并将其纳入绩效考核。

- 鼓励不同背景的员工（如技术与业务）组成创新小组，在实际项目中进行能力融合，创造新价值。

- 营造鼓励创新、容忍试错的学习型组织文化。

1.5 AI 时代的职业新赛道：从 AI 操作员到 AI 训练师

随着人工智能的快速发展，AI 应用将不再是可选项，AI 浪潮正在席卷每一个行业，重塑每一个岗位，无论是企业管理者、市场分析师、财务专家，还是客户服务经理。这场 AI 的变革正在驱动职业角色从简单的“AI 操作员”升级为战略性的“AI 训练师”，通过业务创新、降本增效与安全防护，将 AI 从工具转变为企业核心资产。



AI 时代的职业新赛道：从 AI 操作员到 AI 训练师

1）AI 操作员与 AI 训练师的区别

“AI 操作员”主要负责执行 AI 工具的预设功能，将 AI 作为一种简单的自动化工具来使用。但不需要理解 AI 背后的原理，只需按照既定流程进行输入和输出操作。例如：

- 市场营销：使用 AI 工具自动生成社交媒体文案，但不会分析文案的转化率并反哺模型。
- 客户服务：通过预设的聊天机器人回答用户常见问题，但无法处理复杂、个性化的问题，也无法对机器人进行优化。
- 财务审计：使用 AI 工具自动识别发票中的关键信息，但无法调整模型去适应新的发票格式或识别异常交易。

“AI 训练师”则更具战略性和创造性，需要引导、塑造和优化 AI 模型，使其更好地服务于业务。不仅要使用 AI，更要理解 AI，需要通过持续的反馈进行调优，将 AI 能力与业务目标深度融合。

- 市场营销：通过标注历史营销数据，指导 AI 模型识别高价值客户群体，并生成能显著提升转化率的个性化文案，从而实现业务创新。
- 客户服务：通过分析大量对话记录，纠正 AI 机器人的错误，并为其注入企业独特的知识库和语

气风格，使其能够处理更复杂的问题，提升客户满意度，实现降本增效。

- 财务审计：通过标注异常交易数据，训练 AI 模型去识别新型的欺诈模式，从而将审计工作从被动合规变为主动风险预警。

2）AI 操作员升级到 AI 训练师的必然性

从 AI 操作员到 AI 训练师的转变是企业在 AI 时代保持竞争力的必然选择。

- 从自动化到业务创新：AI 操作员只能利用 AI 实现简单的自动化，解决“效率”问题。而“AI 训练师”能够通过将业务的“隐性知识”转化为 AI 数据，指导 AI 去发现新的商业模式、预测市场趋势、优化产品设计，从而实现业务创新。

- 从工具使用者到核心资产管理者：AI 应用的安全风险日益凸显，数据投毒、隐私泄露、提示词注入等问题层出不穷。“AI 训练师”可将 AI 应用安全纳入日常管理，通过安全性标注等手段，确保模型的完整性、合规性和可信赖性，将 AI 从潜在的风险点转化为可信的核心资产。

3）AI 训练师的新技能

AI 训练师的角色要求混合型新技能：

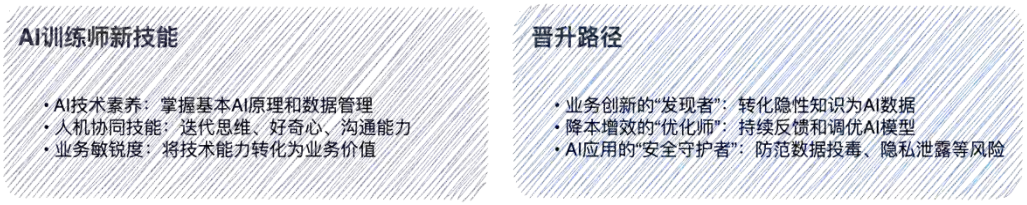
- AI 技术素养：并不要求你成为 AI 科学家，而是要求掌握基本的 AI 原理、数据管理技术以及数据分析工具。

- 人机协同技能：相比技术本身，更重要的是与 AI 协作的能力，包括迭代思维、强烈的好奇心、优秀的沟通能力以及道德判断力。

- 业务敏锐度：将 AI 技术能力转化为业务能力，并形成可量化的财务指标，让 AI 的技术优势转化为商业价值，驱动企业战略决策，提高投资回报率（ROI）。

4）如何从 AI 操作员晋升到 AI 训练师

那么，职业角色如何从“AI 操作员”升级为“AI 训练师”呢？当 AI 接管了重复性任务后，人类的价值便得到了前所未有的放大。新角色应不再是简单地使用 AI 工具，而是成为 AI 系统的导师、塑造者和守护者。这是一种全新的、共生共荣的协作模式。



AI 操作员晋升到 AI 训练师

AI 训练师的核心职责应紧密围绕业务创新、降本增效与安全防护这三大目标展开：

业务创新的“发现者”：AI 训练师是企业的“隐性知识”策展人。“AI 训练师”将这些基于经验的智慧系统地转化为 AI 可以学习的结构化数据。例如，通过标注历史销售数据，让 AI 识别出新的客户群体或市场趋势，从而指导业务部门进行新产品的开发或市场扩张。

降本增效的“优化师”：AI 模型并非“开箱即用”的完美工具，需要持续的反馈和调优。当 AI 的销售预测模型出现偏差时，“AI 训练师”需要像一位导师一样，纠正它的错误，并提供明确的反馈，使其更好地适应公司的业务流程和市场变化。这种持续的调优能显著提升模型的精准度，降低运营成本。

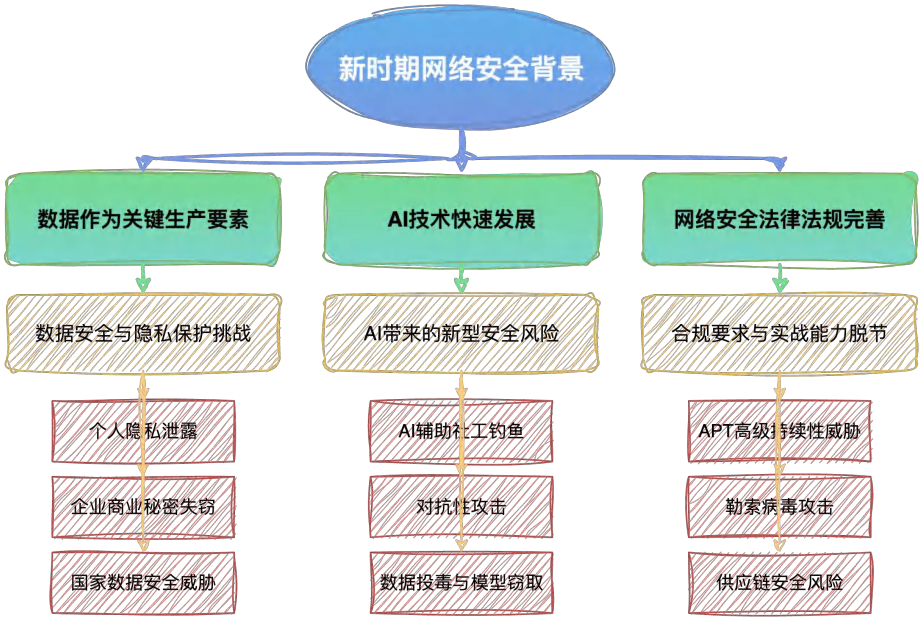
AI 应用的“安全守护者”：这是至关重要的职责。AI 模型在训练过程中可能面临数据投毒、隐私泄露、提示词注入等独特的安全风险。“AI 训练师”必须在模型训练前，对所有数据进行严格的质量验证和不良数据检测，防止恶意数据投毒；并且，专门为 AI 提供安全性标注，教会它如何识别并安全处理包含安全风险的输入，如恶意提示词或有害内容；同时审计 AI 的决策逻辑，识别并纠正任何可能导致不公平或歧视性对待的模式。

第二章 新时期的网络安全复合人才

在全球数字化浪潮的席卷下，中国正高速迈向“数字中国”的宏伟目标，中国以数据作为核心生产要素，开展 5G、工业互联网、物联网络、云计算为代表的“新基建”，大力发展数字经济。新时期背景的主要特点是数据作为核心生产要素、以人工智能（AI）作为新质生产力，同时面临快速演变的网络安全、数据安全、AI 安全的威胁风险，企业需要向智能化和实战化主动防御升级的背景下，人才能力提升成为新时期安全战略升级的驱动。

2.1 新时期的网络安全背景

在数据与 AI 驱动的新时期，网络安全已成为国家战略基石，企业需转变安全思维，从合规导向转向实战能力建设，应建立“先敌发现、先敌打击”的主动防御体系。



新时期网络安全背景

在数据作为关键的生产要素，依托 AI 等先进的技术实现新质生产力的数字化发展新时期，网络安全跃升为国家维系经济命脉、社会稳定和公民隐私安全的战略基石。同时数据在为经济社会发展注入强大动力的同时，也为网络安全带来了颠覆性的挑战。同时，人工智能（AI）的火热与大数据技术在国内快速发展。以大语言模型（LLM）为代表的生成式 AI 技术，带动智能体应用快速落地，正以极快速度渗透到各行各业。尤其是随着国务院发布《关于深入实施“人工智能+”行动的意见》，我国正式全面启动“人

工智能+”新时代，将利用人工智能（AI）技术以前所未有的速度渗透到各行各业，涵盖科学技术、产业发展、消费提质、民生福祉等各个领域，未来我国将以更快的速度改变着社会生产和生活方式。

在新技术带来效率提高和商业价值的同时，也带来了全新的攻击面和风险。例如，攻击者利用 AI 进行更精准的社工钓鱼、自动化挖掘漏洞，甚至生成高度仿真的欺骗信息进行欺诈。AI 系统本身也成为攻击目标，例如对抗性攻击能导致 AI 模型识别错误，数据投毒能污染 AI 数据从而影响决策，模型窃取和提示词注入则可能直接引发核心算法泄露、数据解密和内容安全等风险。

同时，在数字化发展的新时期，网络安全已然跃升为维系国家经济命脉、社会稳定和个人隐私安全的基石，国家高度重视网络安全，从《网络安全法》发布以来，法律法规体系不断完善筑牢制度防线，网络安全成为企业抵御风险、保障持续运营的“生命线”。而且，数据作为新质生产力的核心要素的战略地位。国内近年来出台了《数据安全法》《个人信息保护法》等一系列法律法规，明确了数据分类分级保护、数据跨境传输、个人信息处理规则等合规要求，并正在积极探索数据要素市场化配置机制，数据安全合规管理成为企业运营的生命线，任何数据泄露、丢失等，都可能给企业带来名誉、经济等巨大损失。数据的海量汇聚、高速流动和深度，使数据安全和保护面临空前挑战，从个人隐私泄露、企业商业秘密失窃，到国家数据面临严重威胁，一旦数据安全防线失守，国家后果不堪设想，直接威胁到安全和经济稳定。

此外，随着国际地缘政治和激烈的网络空间竞争，高级持续性威胁（APT）攻击、勒索病毒攻击、供应链攻击等已成为常态，这类攻击具有目标明确、手段广泛、持续时间长、破坏性强等特点，使传统防御体系难以抵御。面对人工智能、数据安全和复杂的高级威胁，传统安全防御能力难以有效应对，在技术飞速发展和法律监管收紧的新时代背景下，企业的安全能力建设陷入了方向迷失的困境，数字化转型的基石面临崩塌的风险。

另外，我国积极组织网络安全攻防演练，网络安全实战对抗趋于常态化、高强度化，这不仅要求企业具备识别和阻止攻击能力，更要具备主动发现、追踪、反制威胁的能力，甚至需要具备“先敌发现、先敌打击”的战略思维。然而，由于许多企业长期过度关注合规，将安全重点放在采购设备和通过合规检查，导致“重合规建设、轻运营”，安全投入未能真正转化为实战能力，与真实的威胁脱节，使企业在“护网行动”、不断变化的 APT 高级威胁等高强度实战中，面临着严峻的安全实战人才和能力不足，难以有效抵御和响应高级持续性威胁，安全防线不堪一击，业务连续性面临可危，甚至可能引发系统性风险。

2.2 新时期网络安全人才的战略

面对新时期网络安全的严峻态势，网络安全人才的培养已不再是企业“可有可无”的选择，而是关

乎国家安全、企业生存与发展的战略。企业必须将安全思维提升到全新的高度：以人才为核心，构建人才驱动的新时期网络安全战略。

人才驱动的新时期网络安全战略

国家安全与数字经济的基石。在复杂多变的国际地缘政治背景下，网络空间安全已成为国家安全的核心组成部分。拥有高素质的网络安全人才队伍，是维护国家网络空间主权、实现关键信息基础设施自主可控的根本保障。特别是具备人工智能和数据安全能力的专业人才，是保障数据新质生产力健康发展、数据要素价值安全流动的关键力量。既是《数据安全法》《个人信息保护法》等国家法律法规得以落地实施的执行者，也是数据主权保障和数字经济安全发展的守护者。没有足够、顶尖的复合型人才，国家数字化战略的推进将面临无法承受的风险，数字经济的支撑发展也将失去安全基础。

人才驱动提升实战和主动防御。在不断演变的 APT 攻击、日益频繁的“护网行动”等实战攻防的背景下，传统的合规建设、被动响应和合规驱动模式已无法满足企业需求，企业急需填补日益扩大的能力鸿沟，实战人才成为提升实际防御能力的关键，更是避免“黑天鹅”事件而导致的业务瘫痪、品牌损失的重要途径。未来，缺乏高水平人才将使企业面临被攻击的风险，最终可能被市场无情淘汰。

人才驱动的 AI 安全和数据安全：利用 AI 技术的数字化转型是新质生产力发展的核心驱动力，人才则是保障其安全运行和价值创造的关键要素。具备 AI 安全能力的复合型人才，能够帮助企业从源头评估和规避 AI 模型自身的风险（如对抗性攻击、数据投毒），确保 AI 技术在为业务赋能的同时，保证 AI 的安全。而数据作为 AI 应用的核心，企业要保障数据的安全流通，不仅需要懂数据治理，更要掌握隐私计算

等前沿技术，才能保障 AI 在应用中的数据安全。

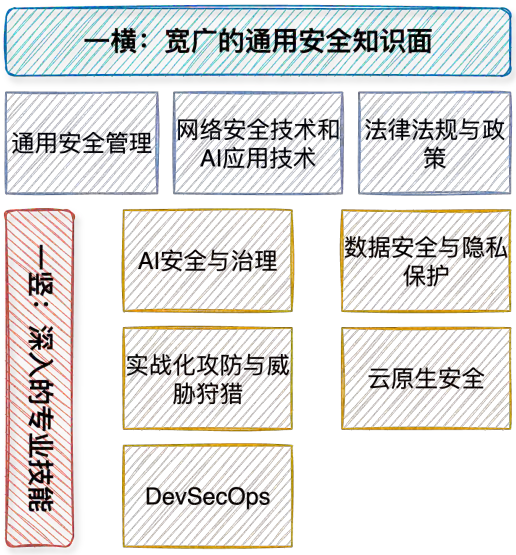
人才驱动核心竞争力的提升：在同质化竞争激烈的市场环境中，强大的网络安全能力可以使企业拥有差异化的独特竞争优势。拥有创新思维、安全和业务能力的复合型人才，能够帮助企业实现“业务安全左移”，产品和服务的安全能够赢得客户的信任，驱动业务创新和可持续发展，使企业在数字经济时代处于领先地位，成为行业内的安全标杆。

2.3 新时期的π型网络安全人才

面对复杂多变、技术日新月异的网络安全威胁，新时期对网络安全人才的要求不再是传统的单一技能体系，而是需要具备跨领域、复合型、高素质的特征，并需要更进一步的多维复合型人才。

1）T 型网络安全人才

“T 型人才”理念是指具备宽广的通用安全知识面（“一横”）和深入的领域专业技能融合（“一纵”）的人才。



T 型网络安全人才

1）“一横”：宽广的通用安全知识面

“一横”代表网络安全从业者必须具备的宽广通用知识面，是专业技能的根基。企业在培养“一横”时，应注重系统性、全面性和合规性。以下是“一横”的典型能力：

- 通用安全管理：了解风险管理（识别、评估、处置）、应急管理（预案编制、演练）、漏洞管

理（发现、修复、跟踪）、安全运营基础（监控、分析、响应），以及 DevSecOps 基本理念和数据治理基础，是所有安全职能的通用语言和方法论。

- 网络安全技术和 AI 应用技术：掌握网络体系、操作系统、数据库、密码学基础、PKI/CA 体系等传统技术原理，并拓展至云原生（容器、微服务、K8s）基础、大数据平台安全基础，**特别是应该掌握** AI 基础模型等新兴技术的工作原理。

- 法律法规与政策：理解《网络安全法》《数据安全法》《个人信息保护法》《关键信息基础设施安全保护条例》等国家法律法规，以及人工智能伦理规范、数据跨境传输规定等最新政策。通过案例分析、合规演练，确保员工不仅知法守法，更能将法规要求转化为实际的安全控制措施。

2）“一竖”：一个或多个领域的深入专业技能

“一竖”是网络安全人才在特定领域的专业深度，是解决复杂安全问题的关键。企业应根据自身业务特点和战略需求，引导员工在关键领域进行深耕。以下是“一竖”的典型能力：

- AI 安全与治理：深入学习 AI 模型攻防原理（对抗性攻击、数据投毒、模型盗窃）、可信 AI（鲁棒性、可解释性、公平性）、大模型安全（提示词注入防御、内容安全）。培养 AI 系统安全架构设计、评估和加固的能力。

- 数据安全与隐私保护：精通数据分类分级、全生命周期管理、隐私计算技术（如联邦学习、同态加密）的实施，以及数据要素安全流通的。

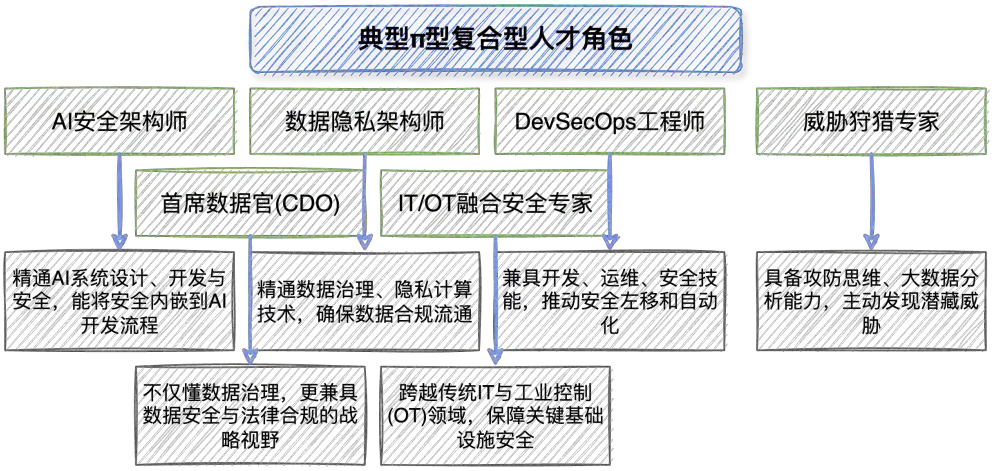
- 实战化攻防与威胁狩猎：具备高级渗透测试（0 日挖掘、绕过免杀）、红蓝对抗、威胁狩猎、APT 攻击溯源与占领等实战能力。

- 云原生安全：掌握容器、微服务、K8s 等云原生环境下的安全架构、开发和运维能力。

- DevSecOps：能够将安全实践“左移”到软件开发全生命周期，实现自动化安全集成与测试。

2）π型复合型网络安全人才

π型复合人才是指在“T 型人才”的基础上，进一步升级为拥有多个一竖的“π型”的复合人才。新时期对π型复合型人才的需求迫切，是在多个相关领域较深的造诣的梳子型知识结构的多维复合型人才。例如，既是 AI 又懂数据隐私保护的专家，又或者既是实战攻防高手又熟悉云架构的安全架构师。π型复合人才的崛起，是面对高度集成化、复杂化数字环境的必然结果。



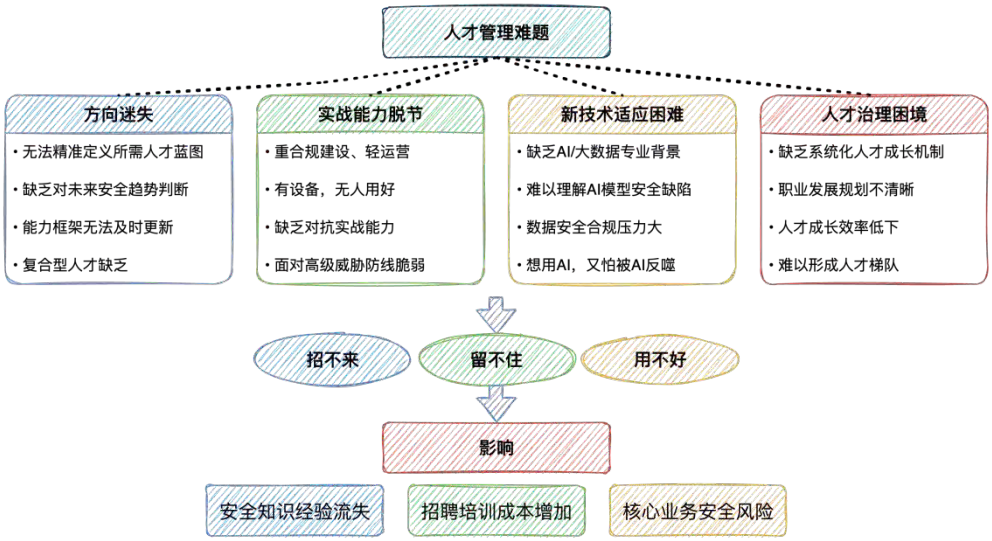
典型π型复合型人才角色

例如，典型π型复合型人才角色：

- AI 安全架构师：精通 AI 系统设计、开发与安全，能够将安全内嵌到 AI 开发流程。
- 数据隐私架构师：精通数据治理、隐私计算技术，能确保数据合规流通。
- DevSecOps 工程师：兼具开发、运维、安全技能，推动安全左移和自动化。
- 威胁狩猎专家：具备攻防思维防御、大数据分析能力，能够主动发现潜藏威胁。
- 首席数据官（CDO）：不仅懂数据治理，更需兼具数据安全与法律合规的战略视野。
- IT/OT 融合安全专家：跨越传统 IT 与工业控制（OT）领域，关键基础设施安全。

2.4 企业网络安全人才的能力困境鸿沟

在新时期的背景下，企业的网络安全能力需要从传统的主动防御、合规驱动，转向高强度实战能力的主动防御体系转型。然而，尽管驱动明确且紧迫，但是国内企业在网络安全人才能力管理方面普遍面临方向迷失、实战脱节、新技术适应与人才治理等多重困境。



企业网络安全人才的能力困境鸿沟

方向迷失，即“不知道需要什么能力的人”。这是国内企业最普遍、最核心的困惑，也是众多人才困境的关键。企业由于无法精准定义所需网络安全人才蓝图，导致面对瞬息万变的网络安全威胁（如变异勒索病毒、认知 APT）和技术前沿（如 AI 生成式对抗、量子计算威胁），往往缺乏对未来安全发展趋势的准确判断，导致安全投入往往事倍功半的困境。现有的人才能力框架无法及时更新，无法有效整合人工智能安全、数据安全合规、云安全等新兴领域的这种方向上的模糊，导致具备实战经验、跨领域知识的复合型人才，特别是能够应对 AI、数据安全合规、云基础等新兴技术专家的缺乏。

实战能力脱节，缺少实战人才。企业在安全建设时，普遍重合规建设、轻运营。许多国内企业在网络安全建设目标主要是为了应对合规检查，虽然投入巨资采购安全产品，但是缺乏将产品能力真正利用起来的专业人才，导致企业面临“有设备，无人用好”的情况。并且，由于缺乏网络安全对抗实战能力的安全团队，企业面临难以有效抵御和响应 APT 等高级持续性威胁，在 APT 高级威胁或“护网行动”实战中往往安全防线不堪一击，业务连续性处于危险之中，甚至可能引发系统性风险。合规建设安全的困境，让企业在巨大的投入面前陷入深深的无力与焦虑。

AI 等新技术的应用带来的新困惑。尽管企业普遍认识到 AI 和数据的重要性，并纷纷尝试开展业务和安全防护，但带来了新的安全挑战，现有安全团队往往缺乏 AI/大数据原理和攻防实践的专业背景，难以理解 AI 模型固有的安全缺陷（如对抗性攻击、数据投毒），也难以有效利用 AI 工具进行高级威胁分析。此外，数据安全合规要求压力巨大，缺乏此类综合型人才，导致企业在冲击新技术的过程中，由于新的安全风险和人才能力鸿沟，常常面临“想用 AI，却又怕被 AI 反噬”的矛盾。

人才治理的困境，不知道如何构建安全人才管理体系。大多数企业缺乏系统化的人才成长机制，人才培养路径，职业发展规划缺乏清晰的线索。缺乏人才治理和管理体系，使企业的安全人员在职业发展

中迷茫，难以实现能力的循序渐进提升，导致人才成长效率低下，难以形成持续、有竞争力的人才梯队。治理乏力的困境使企业在不断变化的安全挑战面前，人才始终捉襟见肘，无法为核心业务提供持续的安全支撑。

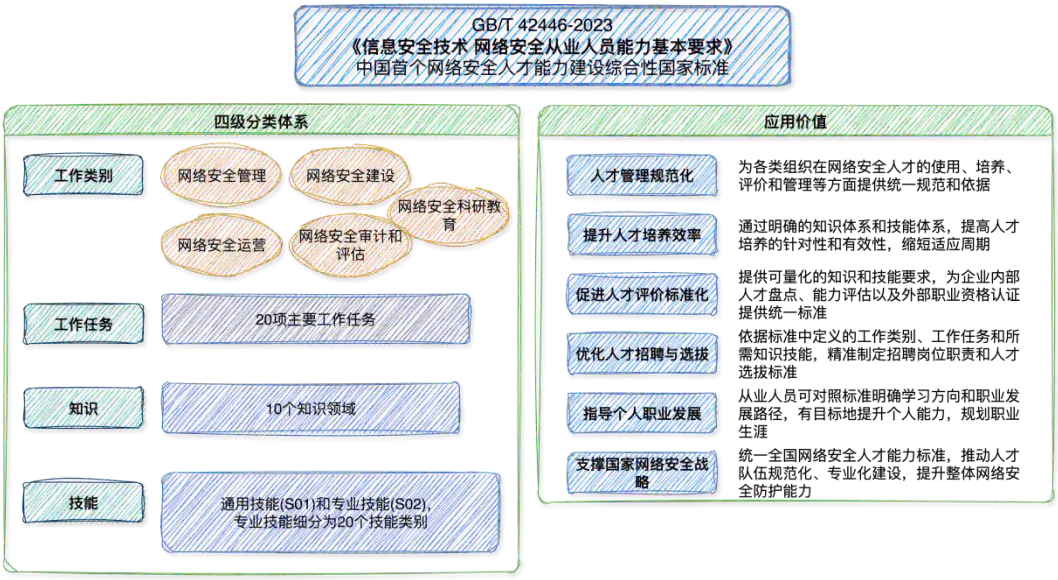
人才管理难题，招引留用难，招不来、留不住。根据《2024 年网络安全产业人才发展报告》，国内网络安全人才缺口不断扩大，对实战和复合型人才需求更加紧迫。但由于企业人才能力的治理和管理能力匮乏，缺乏人才职业发展空间、不够充分的刺激机制等，造成企业人才流失，造成，影响安全知识和经验积累，以及安全人才梯队的能力建设，使组织的人才招聘和培训成本的增加，甚至及其核心业务的持续发展。

第三章 网络安全人才能力框架挑战

安全牛以国家标准 GB/T42446-2023《网络安全人员能力要求》的框架为基础，与国外框架进行对比分析，在发现国内网络安全人才能力框架应对新时期的不足，同时引发我们对新时期的网络安全人才能力框架需求的思考，并进一步探索新的框架方向设想。

3.1 中国网络安全人才能力框架

国家市场监督管理总局和国家标准化管理委员会 2023 年 3 月发布国家标准 GB/T42446-2023《信息安全技术网络安全从业人员能力基本要求》（以下简称“《网络安全人员能力要求》”）作为中国网络安全人才领域的国家标准，不仅为网络安全行业提供了基础性的规范和指导，并明确了网络安全从业人员分类，规定各类从业人员具备的知识和技能要求，该标准是理解、定义、培养和评估网络安全人才的重要工具。



1）《网络安全从业人员能力基本要求》概述

《网络安全人员能力要求》为各类组织对网络安全从业人员的使用、培养、评价和管理提供了规范性参考。主要应用价值包括：

- 统一认知：弥合业务、技术、管理和人力资源部门对人才需求的理解差异。
- 精准识别：明确每个岗位所需的具体知识、技能和能力，指导招聘和选拔。

- 科学培养：为人才培训和发展提供路线图，确保培养内容的有效和有效。
- 初步评估：建立初步评估标准，减缓人才能力的提升和发展成熟度。
- 优化资源：确保有限的人力资源能够投向最关键、最急需的安全能力建设。

2）《网络安全人员能力要求》的结构体系和优点

- **《网络安全人员能力要求》的结构体系**

《网络安全人员能力要求》建立了网络安全四级分类体系，明确了从业人员应具备的知识和技能要求，为人才培养、评价和管理提供了统一规范。

- 工作类别：宏观层面，将网络安全工作划分为 5 类（网络安全管理、网络安全建设、网络安全运营、网络安全审计和评估、网络安全科研教育）。
- 工作任务：细化每个工作类别下需要执行 20 项具体工作活动和内容。
- 知识：完成工作任务所需的知识领域和知识单元。
- 技能：完成工作任务所需的技能类别和具体技能描述。

- **《网络安全人员能力要求》的优点**

《网络安全人员能力要求》的优点包括其作为国家标准的指导性、国情适配、涵盖面广和系统化体系结构等。

- 权威性：《网络安全从业人员能力基本要求》是由国家市场监督管理总局和国家标准化管理委员会发布的，作为国家标准，具有官方性和权威性，为国内网络安全人才能力评价和培养提供了依据和指导。
- 国情适配性：该标准紧密结合中国的法律法规和国家战略，明确了与国内实际的工作职责高度匹配的网络安全从业人员分类，规定了网络安全从业人员应具备的知识和技能要求，为各类组织对网络安全从业人员的使用、培养、评价和管理提供了规范性参考。
- 涵盖通用与专业要求：标准不仅给出了网络安全从业人员应具备的通用知识和通用技能要求，并且详细列出了承担工作类别的从业人员应具备的基本专业知识和技能要求。
- 系统化的分类体系：提供了清晰的“工作类别—工作任务—知识—技能”的自上而下的四级分

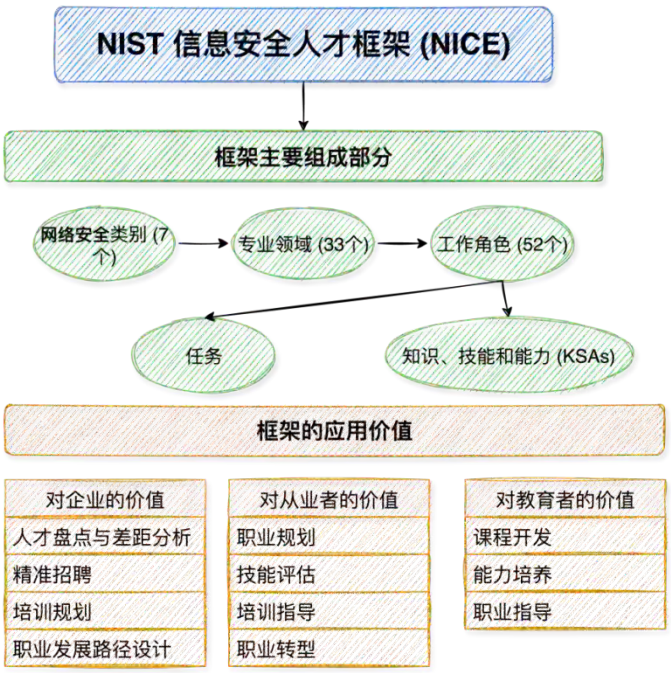
类体系，为各类组织建立人才能力体系、评估人员能力、规划职业发展路径提供了初步且规范性的参考，统一了网络安全人才评估体系，提升了人才管理的专业化水平。

3.2 国际网络安全人才能力框架

美国国家标准与技术研究院（NIST）和欧盟网络与信息安全局（ENISA）发布了较为成熟的网络安全人才能力框架，引领我们展望中国国家标准的改进方向。

1）NIST 网络安全人才能力框架（NICE）

NIST 网络安全人才能力框架（NICEFramework），是由美国国家标准与技术研究院（NIST）发布，为美国政府和企业网络安全建设提供结构化方法管理网络安全人才的参考框架，以建立通用语言，并解决人才短缺挑战。



NIST 网络安全人才能力框架

NICE 框架是网络安全工作解构为构建的语言，旨在促进对网络安全人才需求体系的共同理解、评估。将网络安全工作划分为 7 个类别（Categories）、33 个专业领域（Specialty）Areas）和 52 个工作角色（WorkRoles），并为每个工作角色详细定义了所需的任务（Tasks）、知识（Knowledge）、技能（Skills）和能力（Abilities，简称 KSA）。

NICE 的特点包括：

- 结构化与普适性：NICEFramework 提供了高度结构化的框架，细致的 KSAs 定义为网络安全工作的解构和人才需求分析提供了通用语言。标准化和解构能力在全球范围内被广泛采用，并被许多国家和企业所借鉴，成为理解和描述网络安全人才的标准。

- 灵活性：NICEFramework 鼓励组织根据自身需求进行裁剪和调整，使其能够适应不同企业和行业的具体需求，而不是一刀切。

- 促进沟通：通过提供一套共同的术语和定义，NICEFramework 有助于弥合不同利益相关者，如企业、教育机构、政策制定者、求职者之间在网络安全人才需求理解上的差距，促进更有效的沟通和协作。

- 赋能人才管理：该框架为企业进行人才招聘、岗位描述、员工能力评估、培训课程设计以及职业发展规划提供了明确的参考依据，有助于构建科学的人力资源管理体系。

- 持续更新：NICEFramework 作为 NIST 的一项倡议，持续得到维护和更新，以适应网络安全领域不断演进的威胁和技术。拥有活跃的社区和生态系统支持，确保与行业发展保持同步。

2）欧洲网络安全技能框架（ECSF）

《欧洲网络安全技能框架》（ECSF）由欧盟网络与信息安全局（ENISA）发布。旨在为欧盟成员国提供一个统一的网络安全技能参考体系，以应对日益增长的网络安全威胁和人才短缺问题，并促进网络安全专业人员在欧洲范围内的自由流动和技能认可。

欧洲网络安全技能框架

ECSF 框架以角色为中心，将网络安全专业人员的职责细化为 12 个网络安全典型专业角色，并为每个角色提供了详细的描述和所需的能力、技能、知识，旨在促进人才市场对网络安全人才需求的理解。

ECSF 的特点包括：

- 以角色为中心且实用性强：ECSF 的最大特点是其以 12 个典型角色为核心，而不是抽象的能力领域。这种设计使框架非常直观和实用，企业能够根据其组织架构和招聘需求，直接找到对应的角色定义，从而促进人才市场对网络安全人才需求的清晰理解，并为求职者提供清晰的职业路径。

- 多方利益相关者受益：框架旨在为所有利益相关者（包括 IT 组织、学习提供者、个人专业人士、政策制定者和专业协会）带来益处。例如，它帮助组织进行人力资源规划和职位规范，帮助学习机构设计课程，帮助个人规划职业生涯。

- 促进通用语言和协作：ECSF 提供了一种通用的语言，用于描述网络安全领域的角色、能力、技能和知识。有助于消除不同部门、不同机构甚至不同国家之间在人才需求理解上的差异，加速协作流程。

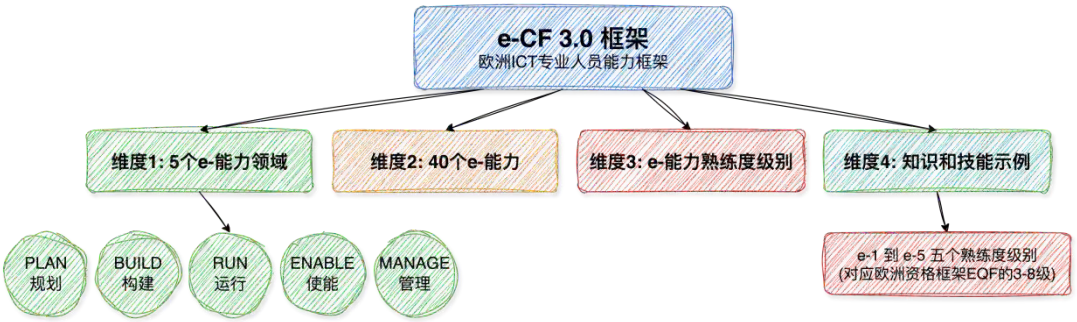
- 支持技能识别和培训设计：框架明确支持网络安全技能的识别和网络安全相关培训项目的设计。它提供了具体的步骤指南（如“五步指南”）来应用框架进行组织内的人才识别、技能提升和职业规划。

- 灵活性和可扩展性：ECSF 被设计为简单、灵活、全面、开放、欧洲化、公正、可扩展，可以在保持核心不变的同时，根据具体需求进行调整和扩展，以适应不断变化的网络安全环境和新兴技术。

- 政策和法律导向：ECSF 紧密结合欧盟的数据保护法规和人才市场特点，强调实用性和可操作性。这确保了框架的内容与欧盟地区的实际合规要求和行业需求紧密相关，并得到了欧盟委员会的政治支持。

3) 欧洲通用人才框架(e-CF)

《e-CF-E-CompetencesFramework3.0》（以下简称 e-CF3.0）是由欧洲标准化委员会（CEN）的 ICT 技能工作坊发布的通用欧洲框架。旨在为所有行业领域的 ICT（信息与通信技术）专业人员提供一套通用的能力描述标准。e-CF3.0 是欧洲 ICT 领域多方利益相关者持续 8 年努力的成果，其目标是为整个欧洲的 ICT 工作场所所需的能力、技能和能力水平提供一个通用的参考语言，以促进相互理解和透明化。



欧洲通用人才框架

e-CF3.0 框架基于其“四个维度”来构建 ICT 能力，宏观职能划分为 5 个 e－能力领域、定义了 40 个 e－能力，以及从 e-1 到 e-5 的五个熟练度级别，提供了在整个欧洲范围内对能力水平进行一致解释的参考。

特点和优势

- 通用性和互操作性：e-CF3.0 是一个“通用的欧洲框架”，为 ICT 专业人员提供了一个共同的语言，使其能力、技能和能力水平可以在欧洲范围内被理解和使用，促进了欧洲人才市场的透明度和人员流动。

- 实践导向与多方适用：关注 ICT 工作场所所需的能力，设计应用于 ICT 服务、用户和供应公司，以及管理者、人力资源部门、教育机构、培训机构、政策制定者等公共和私营部门的各类组织和个人。这非常实用和灵活。

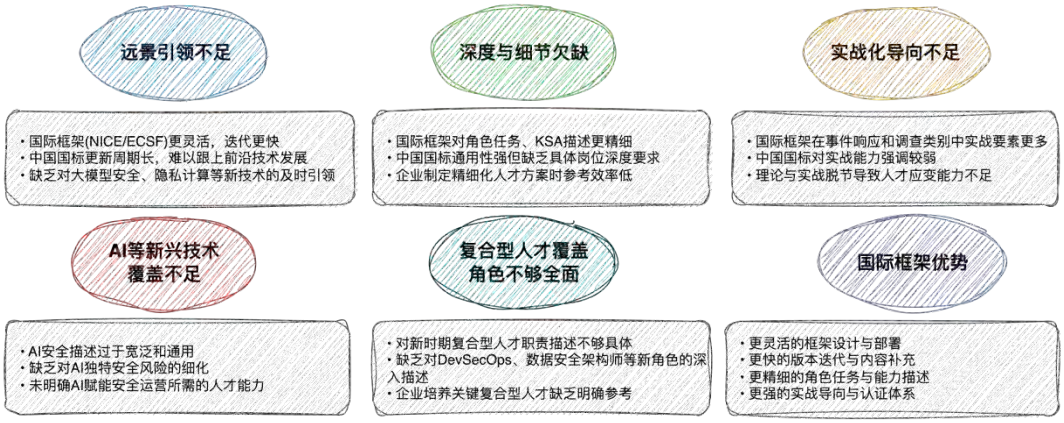
- 能力定义全面且持续演进：e-CF 将能力定义为一个整体概念：“能力是运用知识、技能和态度以实现可观察结果的示范能力”。框架本身具有“耐用性”，虽然技术变化迅速，但核心能力概念保持相对稳定，大约每三年进行一次维护更新以保持相关性。

- 与欧洲资格框架（EQF）的关联：作为欧洲资格框架的首个行业特定实施案例，e-CF 的能力级别与 EQF 级别之间建立了系统且合理的关联。这有助于在欧洲范围内对 ICT 专业资格进行比较和认可。

- 政策支持：e-CF 是欧盟“21 世纪 e－技能”长期战略的重要组成部分，并支持“数字就业大联盟”等关键政策目标。这为其推广和应用提供了强大的政治支持。

3.3 国内外网络安全人才能力框架对比分析

通过与国际主流框架的对比，结合新时期背景的运用，中国网络安全人才框架需要更加灵活、深入、实战化，并加强对新兴技术和复合型人才的覆盖，在前瞻性、深度细节、实战导向、新兴技术覆盖及复合型人才培养方面进行完善，以适应新时代网络安全挑战和快速发展的需求。



国内外网络安全人才能力框架对比分析

主要不足之处包括：

- 远景引领不足：NICE 和 ECSF 框架设计更加灵活和部署，能够更快地进行版本迭代和内容补充。中国国家标准周期相对较长，在应对“新质生产力”带来的前沿技术（如大模型安全、隐私计算、量子计算威胁）时，其更新可能速度无法完全匹配产业的快速发展。这使国内企业在未来挑战时，缺乏官方且权威与时俱进的引领。

- 深度与细节欠缺：国际框架在对特定角色的任务、知识、技能描述上较为精细，例如 NICE 为每个工作角色定义了详细的 KSA，为企业提供了更具体的指导。中国国家标准在通用性上表现出色，但在对具体岗位的深度要求上，结束了提升空间。这种深度上的不足，使企业在制定精细化的人才方案和能力评估标准时，不得不自行摸索，参考效率低下，也难以有效的网络安全能力基站业务基础。

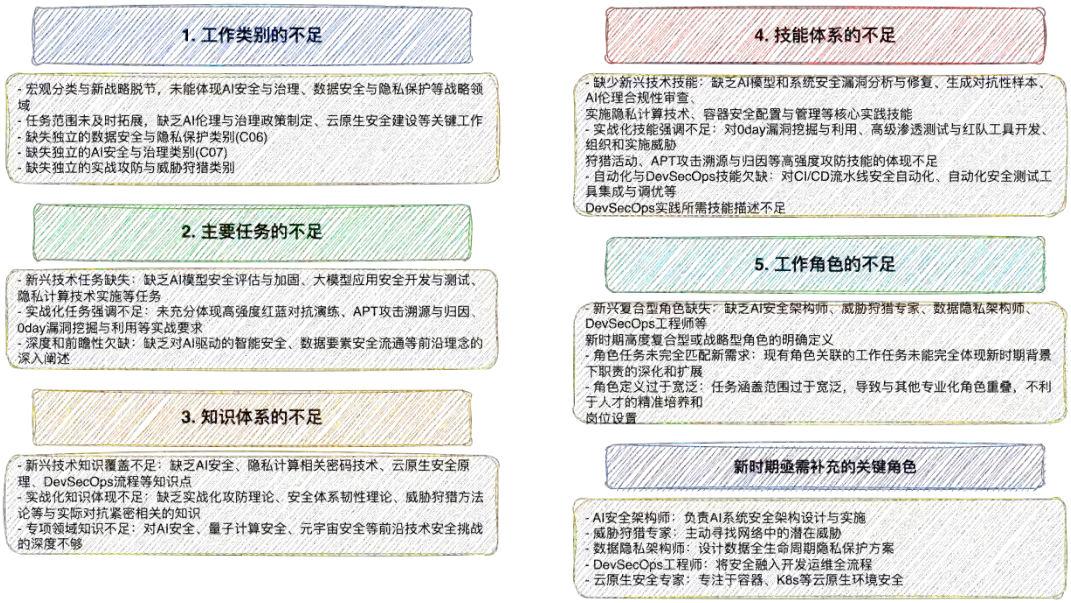
- 实战化导向不足：国际框架，尤其是在“事件响应”和“调查”等类别中，有更多实战化要素，

并有专门的认证体系支撑实战能力的培养。而中国国标对此的强调仍较弱，未能充分体现实战人才，网络安全已进入“背景实战对抗”时代的背景，这种理论与实战的脱节，导致国内培养的人才面对真实威胁时，往往实操能力和应变能力不足，无法满足攻防演练等高强度对抗的需求。

- AI 等新兴技术覆盖不足：《网络安全从业人员能力基本要求》在“新技术新应用安全”（K10-001）中包括了 AI，但其描述不够宽泛和通用。应深入细化 AI 系统自身所面临的独特安全风险（如对抗性攻击、大模型安全、模型盗取、数据投毒）以及如何防御这些风险此外，对于利用 AI 技术赋能安全运营（如 AI 驱动的威胁检测与响应、自动化编排）所需的具体人才能力，也缺乏明确阐述。使企业在培养 AI 安全人才时，缺乏明确的指引，层次上有 AI 业务，却不知如何安全保障的困境。

- 复合型人才覆盖角色不够全面：《网络安全从业人员能力基本要求》划分了 20 项工作任务和 5 类工作类别，但对于 DevSecOps 工程师、数据安全架构师（尤其是隐私计算）、AI 安全科学家、供应链安全专家、IT/OT 融合安全专家等新时期高度复合型或战略型人才的职责描述和能力，不够具体和深入。使企业在寻找或培养这些关键复合型人才时，缺乏明确的参考依据。

《网络安全从业人员能力基本要求》在工作类别、任务、知识体系、技能和工作角色等方面亟需更新与完善，如未能充分适应 AI 安全与治理、数据安全与隐私保护、实战攻防与威胁狩猎等新兴领域的发展需求，在工作类别、任务定义、知识体系、技能要求和角色设置：



网络安全人员能力框架的新时期不足分析

1）工作类别的不足

国内网络安全人才能力框架在工作类别方面的不足主要体现在：一是宏观分类与新战略脱节。工作类别划分为 5 类（管理、建设、运营、审计评估、科研教育），在新时期未能充分体现 AI 安全与治理、

数据安全与隐私保护（特别是数据要素化背景）、实战攻防与威胁狩猎等具有战略意义和独立性的新兴领域。二是任务范围未及时拓展。在每个工作类别下，国标的宏观任务定义未能涵盖如 AI 伦理与治理政策制定、AI 系统安全架构设计、云原生安全建设、威胁狩猎实践等新时期涌现的关键工作。

工作类别	工作任务	不足之处（新时期视角）
网络安全管理	网络安全需求分析，网络安全规划和管理，网络数据安全保护，个人信息保护，密码技术应用，网络安全咨询	缺乏对 AI 安全治理、数据要素安全规划的明确要求。未充分体现高层安全治理的战略性，多侧重于日常管理。
网络安全建设	网络安全需求分析，网络安全架构设计，网络安全开发，供应链安全管理，网络安全集成实施，网络数据安全保护，个人信息应用，密码技术应用	对云原生、AI 系统安全架构等新兴技术领域的建设任务覆盖不足。未明确 DevSecOps 等安全左移理念下的开发安全任务。
网络安全运营	网络安全运维，网络安全监测和分析，网络安全应急管理，网络数据安全保护，个人信息保护，密码技术应用	缺乏对 AI 驱动的智能运营、威胁狩猎等主动性运营任务的体现。对自动化、编排等提升运营效率的关键实践描述不足。
网络安全审计和评估	网络安全审计，网络安全测试，网络安全评估，网络安全认证，电子数据取证	对新兴技术（如 AI 系统、云原生）的审计评估任务缺失。缺乏对实战化攻防演练评估的明确要求。
网络安全科研教育	网络安全研究，网络安全培训和评价	对 AI 安全、量子计算安全等前沿新兴技术研究的强调不足。未明确实战化人才培养和评价的具体要求。
数据安全与隐私保护类（C06）	缺失	未独立将数据安全和隐私保护提升到核心工作类别，难以适应《数据安全法》和《个人信息保护法》的高强度要求。
AI 安全与治理类（C07）	缺失	缺乏对 AI 系统自身安全（SecurityofAI）的专门定义和任务，难以应对 AI 带来的全新攻击面和治理挑战。
实战攻防与威胁狩猎类	缺失	缺乏对实战化攻防和威胁狩猎等主动性、对抗性安全能力和任务的明确定义。

2）主要任务的不足

国内网络安全人才能力框架在任务描述方面的不足主要体现在：一是新兴技术任务缺失。20 项主要工作任务中，缺乏针对 AI 模型安全评估与加固、大模型应用安全开发与测试、隐私计算技术实施等 AI 和数据安全核心任务的明确描述。二是实战化任务强调不足。对于网络安全测试、应急管理等任务的描述，未能充分体现高强度红蓝对抗演练、APT 攻击溯源与归因、0day 漏洞挖掘与利用等实战化要求。三是深度和前瞻性欠缺。现有任务描述较为通用，缺乏对 AI 驱动的智能安全、数据要素安全流通等前沿理念的深入阐述。

序号	工作任务	工作任务描述	不足之处（新时期视角）
1	网络安全规划和管理	指导、制定、监督和执行网络安全战略规划、策略制度和体制机制。综合协调相关人员，采取各类网络安全控制措施，降低并缓解系统安全风险。	缺乏对 AI 安全治理、数据要素安全规划的明确要求。未能充分体现网络安全作为企业战略组成部分的需求。
2	网络数据安全保护	针对网络数据收集、存储、使用、加工、传输、提供、公开等环节，采取措施保障网络数据安全。	缺乏对数据要素化背景下的数据流通安全、AI 训练/推理数据安全，以及隐私计算等新兴技术应用的具体描述。
3	个人信息保护	针对个人信息收集、存储、使用、加工、传输、提供、公开、删除等环节，采取措施保障个人信息安全。	未明确个人信息跨境传输合规、个人信息匿名化/去标识化，以及 AI 模型中个人信息隐私保护的具体要求。
4	密码技术应用	运用密码技术，进行信息系统安全密码保障的架构设计、系统集成、检测评估、运维管理、密码咨询等。	缺乏对隐私计算（如联邦学习、同态加密）等新兴密码技术在数据安全和 AI 安全中的应用描述。
5	网络安全需求分析	依据法律法规、政策标准及业务流程要求，开展符合性需求分析、业务所依赖的信息通信技术（ICT）持续运行需求分析、数据安全需求分析等，定期或在遇到重大网络安全事件时对组织网络安全需求进行复审。	缺乏对 AI 系统和云原生环境的安全需求分析，以及数据要素流动对安全需求的洞察。
6	网络安全架构设计	依据网络安全需求分析、ICT 基础设施现状，组织环境和业务特点等，从物理环境、通信网络、计算环境、区域边界等方面进行网络安全架构设计，形成网络安全架构实施方案。	对云原生安全架构、零信任架构、AI 系统安全架构等新时期主流架构设计缺乏明确描述。
7	网络安全开发	实现软件、硬件安全架构及功能开发，并对其进行测试、更新和维护。	未明确 DevSecOps 等安全左移理念下的开发安全任务，以及云原生应用、AI 应用的开发安全要求。
8	供应链安全管理	运用供应链安全管理的方法、工具和技术，控制供应链安全风险，管理供应商及网络安全和信息化相关产品和服务的采购。	缺乏对软件物料清单（SBOM）分析与管理、开源组件安全管理等新兴实践的强调。

9	网络安全集成实施	网络安全项目管理，信息系统安全集成过程中软硬件设备与系统的安装、调试、测试、配置、故障处理和工程实施，以及配合验收交付。	对云安全产品、XDR、SOAR 等新型安全产品集成缺乏明确描述。
10	网络安全运维	利用网络安全技术/工具，根据网络安全相关标准和制度流程，操作、运行、维护和管理信息系统。	对云原生环境（容器、K8s）运维、工业控制系统（ICS）/运营技术（OT）运维安全缺乏明确描述。
11	网络安全监测和分析	利用相关技术、工具和情报信息等对目标系统进行安全监测、分析和预警，并提出应对威胁的措施和改进建议。	缺乏对威胁狩猎、AI 驱动的智能监测分析等主动性、智能化监测手段的体现。
12	网络安全应急管理	组织编制网络安全事件应急预案，实施网络安全应急演练，在应对突发/重大网络安全事件时，采取必要的应急处置措施将信息系统和业务恢复到正常状态，并进行事件溯源和调查取证。	缺乏对实战化攻防演练的组织与执行，以及 AI 驱动的自动化应急响应等高强度实践的描述。
13	网络安全审计	依据审计依据，在规定的审计范围内，监督和评价网络安全控制措施的设计有效性和执行有效性，确定被审计对象满足审计依据的程度，并提出网络安全工作改进的意见和建议。	对 AI 系统审计、云环境审计，以及针对数据流动的合规审计缺乏明确要求。
14	网络安全测试	对目标系统的脆弱性和防御机制有效性进行验证，发现安全问题并提出改进建议；根据测试依据，识别并测试系统和产品的安全性。	对自动化应用安全测试（SAST/DAST/IAST）、容器安全扫描、AI 系统安全测试（鲁棒性、偏见性、公平性测试）缺乏明确描述。
15	网络安全评估	评估信息系统、业务及相关网络数据等的符合性和面临的网络安全风险，对风险进行识别、分析、评价，提出改进建议。	对 AI 系统风险评估、云原生环境风险评估，以及供应链安全风险评估缺乏明确要求。
16	网络安全认证	对网络安全管理体系、服务、产品等开展认证与审核。	对数据安全认证、AI 安全认证体系缺乏明确描述。
17	电子数据取证	对电子数据进行提取、固定、恢复、分析等工作。	对云环境取证、容器取证、AI 系统取证，以及针对高级持续性威胁（APT）的深度取证缺乏明确描述。

18	网络安全咨询	根据组织的安全目标，提供安全规划、设计、实施、运维、管理等方面的政策法规和技术咨询服务。	对 AI 安全、数据要素安全、工业互联网安全等新兴领域咨询缺乏明确描述。
19	网络安全研究	研究网络空间安全涉及的学科理论基础和方法论，研究网络安全新兴技术及应用、产业发展趋势，以及网络安全法律法规、政策、标准等。	缺乏对 AI 安全前沿研究（如大模型安全、对抗性机器学习）、量子计算安全研究、元宇宙安全研究等新兴和交叉领域研究的明确强调。
20	网络安全培训和评价	开展网络安全培训方案和相关课程的设计、开发和持续改进，实施授课等培训活动，开展评价活动，例如：理论知识考试、技能操作考核、业绩评审、竞赛选拔等。	缺乏对实战化培训与评价，涵盖 AI 安全人才培训，以及利用 AI 工具提升培训效率的明确要求。

3）知识体系的不足

国内网络安全人才能力框架在知识体系方面的不足主要体现在：一是新兴技术知识覆盖不足。知识体系（K01-K10）在 AI 安全（如对抗性机器学习原理、大模型安全）、隐私计算相关密码技术（如同态加密、后量子密码）、云原生安全原理、DevSecOps 流程等新时期关键知识点上，缺乏足够的深度和明确的知识单元。二是实战化知识体现不足。缺乏对实战化攻防理论、安全体系韧性理论、威胁狩猎方法论等与实际对抗紧密相关的知识的明确定义。

序号	知识领域	知识代码	知识单元	知识描述	不足之处（新时期视角）
1	网络安全基础	K01-001	网络安全概念及发展历程	信息安全概念、信息安全属性、信息安全视角、信息安全保障框架模型；网络安全发展历程、发展现状和发展趋势等；国内外网络安全产业发展情况等	缺乏对“新质生产力”和“实战化”背景下，网络安全发展新范式（如主动防御、零信任、人工智能）的体现，未能充分反映当前网络安全前沿理念。
2		K01-002	网络安全管理基本知识	风险管理、供应链安全管理、运营管理、应急管理、业务连续性、管理体系、认证认可、漏洞管理等基本知识	未明确融入 DevSecOps 基本理念、数据治理基础、AI 安全治理基础等新时期管理的实践。
3		K01-003	网络安全技术基本知识	网络体系、通信技术、计算机组成原理、操作系统、密码学基础、PKI/CA 体系、身份鉴别、访问控制等基本知识	缺乏对云原生（容器、微服务、K8s）基础、大数据平台安全基础、AI 基础模型和算法原理等新兴技术原理的覆盖。
4		K01-004	国内外网络安全法律法	国内外网络安全法律法规政策战略和监管机制等	对中国特有的《数据安全法》《个人信息保护法》以及 AI、工业互联

			规和政策		网等新兴领域的最新政策法规，缺乏明确强调。
5		K01-005	国内外网络安全标准	国内、国外、国际网络安全标准	缺乏对 AI 安全标准、数据安全国家标准（如数据分类分级）等新时期重要标准的具体提及。
6		K01-006	网络安全最佳实践	解决方案或者经验等	缺乏对 DevSecOps 实践、零信任实践、AI 安全实践等新时期前沿最佳实践的明确提及。
7	网络安全管理知识	K02-001	供应链安全管理	国内外供应链安全发展现状，供应链安全管理方法、技术及工具等	缺乏对供应链软件物料清单（SBOM）管理、供应链攻击防御策略等新兴风险和实践的深入。
8		K02-002	应急管理方法和技术	业务连续性，事件管理，应急预案编制、维护和演练等操作系统、中间件、数据库等常用应急处置方法	缺乏对自动化应急响应（SOAR）、实战化应急演练、AI 驱动的事件分析等现代化应急管理手段的体现。
9		K02-003	网络安全风险管理	风险评估、风险处置方法、技术和实施	缺乏对风险量化评估、业务风险转化、AI 风险评估等新时期复杂风险管理能力的覆盖。
10		K02-004	网络安全审计方法和技术	通用审计准则和方法；网络安全审计准则、方法、审计技术、信息化项目管理等	缺乏对自动化审计、云环境审计、AI 系统审计等新兴审计实践的描述。
11		K02-005	网络安全认证认可	认证相关基本概念、认可相关基本概念审核知识等	缺乏对数据安全认证、AI 安全认证体系等新时期特定领域认证的明确提及。
12	数据安全知识	K03-001	数据安全管理和技术	数据安全基本概念、数据安全技术，数据安全治理与保障等	缺乏对数据分类分级实践、数据全生命周期安全管理（采集、存储、使用、传输、共享、销毁）、数据要素安全流通等中国国情下特有且重要的实践的深入。
13		K03-002	个人信息保护管理和技术	个人信息保护政策，个人信息保护技术工具等	缺乏对个人信息跨境传输合规、个人信息匿名化/去标识化技术，以及隐私计算技术（如联邦学习、差分隐私、同态加密）在个人信息保护中应用的深入。
14	网络安全建模技术知识	K04-001	系统建模理论和常用方法	数学基础、模型概念、建模原理、系统建模方法等	缺乏对云原生系统建模、工业互联网系统建模等新时期复杂系统建模知识的覆盖。
15		K04-002	威胁建模理论和常用方法	威胁建模的作用、常用的威胁建模方法等	缺乏对 AI 威胁建模（如针对对抗性攻击、数据投毒的建模）等新兴威胁建模的知识。
16		K04-003	安全架构模	网络安全架构、系统安全架构	缺乏对云原生安全架构、零信任架

			型及设计方法	模型及常用设计方法等	构、数据安全架构、AI 系统安全架构等新时期主流架构的知识覆盖。
17	网络安全开发、测试及攻防技术知识	K05-001	安全开发	软件安全设计、代码实现安全、资源使用安全、配置管理安全、软件工程等	缺乏对 DevSecOps 流程与工具链、安全左移理念、API 安全开发等新时期开发实践的深入。
18		K05-002	系统安全工程	系统安全工程理论及实施等	缺乏对云环境安全工程、工业控制系统安全工程等新环境下的系统安全工程知识。
19		K05-003	网络安全威胁和漏洞管理	威胁和漏洞概念，漏洞的发现、利用和提交等技术、方法和流程	缺乏对漏洞生命周期管理、威胁情报驱动的漏洞分析、AI 模型漏洞管理等新时期实践的深入。
20		K05-004	安全测试、评估方法	常用测试和评估方法，如黑盒测试、灰盒测试、白盒测试及压力测试等	缺乏对自动化应用安全测试（SAST/DAST/IAST）、容器安全扫描、AI 系统安全测试（鲁棒性、偏见性、公平性测试）等新兴测试方法的知识。
21		K05-005	渗透测试方法和技术	Web 安全、中间件、数据库等常见安全漏洞及利用方法，安全渗透测试知识，常用渗透测试工具等	缺乏对高级渗透测试技术（绕过、免杀）、移动应用渗透测试、IoT/OT 渗透测试等新场景下的渗透测试方法。
22		K05-006	网络攻防技术	网络攻击原理、常见攻击方法、攻击技术和攻击后果，以及防御措施等	缺乏对高级持续性威胁（APT）攻击原理、勒索病毒攻击技术、供应链攻击原理、红蓝对抗策略与技术等新时期复杂攻防技术的知识。
23	网络产品原理与应用知识	K06-001	备份/灾备方法与技术	系统和数据的备份/恢复、灾备方法与技术等	缺乏对云备份/灾备、分布式系统灾备、数据湖灾备等新兴环境下的灾备方法。
24		K06-002	网络设备功能及原理	交换机、路由器等网络设备工作原理、配置及网络架构设计相关知识	缺乏对 SDN/NFV 技术、云网络安全功能（VPC、安全组）等新兴网络技术的知识。
25		K06-003	网络安全产品功能及原理	网络安全产品原理及应用（防火墙、入侵检测、网闸、VPN 等）	缺乏对云安全产品（CWPP、CSPM、CASB）、XDR（扩展检测与响应）、SOAR（安全编排自动化与响应）等新兴安全产品的知识。
26		K06-004	操作系统安全原理及使用	Windows 和 Linux/Unix 等主流操作系统、虚拟机和容器等常用安全技术、安全配置和安全加固	缺乏对容器安全、K8s 安全、Serverless 安全等云原生环境下的操作系统安全知识。
27		K06-005	中间件安全原理及使用	中间件功能原理（通信支持、应用支持、公共服务等）、安全配置及安全加固等	缺乏对 API 网关安全、消息队列安全等新兴中间件安全知识的覆盖。

28		K06-006	数据库安全技术及使用	数据库安全防护技术及方法、安全配置和加固，包括数据库的加密、用户管理、备份还原、数据脱敏、审计等	缺乏对大数据平台安全（Hadoop、Spark）、NoSQL 数据库安全等新兴数据库安全知识的覆盖。
29	网络安全监测分析技术知识	K07-001	网络安全监测方法和技术	流量监控、事件监控、容量监控等	缺乏对威胁狩猎、基于 AI 的异常行为检测、日志聚合分析（ELKStack 等）等主动性、智能化监测手段的知识。
30		K07-002	网络安全分析方法和技术	网络流量分析、恶意代码、日志分析等	缺乏对自动化分析、威胁情报驱动的分析、机器学习在安全分析中应用等更高级分析方法的知识。
31	调查取证技术知识	K08-001	调查取证方法和技术	电子数据取证概念、取证模型、电子数据取证管理、电子数据证据的勘验和司法鉴定流程、电子数据取证相关技术等	缺乏对云环境取证、容器取证、AI 系统取证等新兴环境下的取证方法。
32	密码技术与应用知识	K09-001	密码技术、密码产品及服务功能及原理	密码算法、协议、密钥管理等相关技术，工具、产品、服务及解决方案等	缺乏对后量子密码（PQC）、同态加密、零知识证明等隐私计算相关密码技术的前沿知识。
33	专项领域知识	K10-001	新技术新应用安全	云计算、大数据、物联网、人工智能、区块链、5G 等	描述过于通用，缺乏对 AI 安全（大模型安全、对抗性机器学习）、量子计算安全、元宇宙安全、车联网安全等具体新兴技术安全挑战的深度。
34		K10-002	特定行业网络安全知识	电信、能源、金融、交通等行业特定的网络安全知识	对金融科技（FinTech）、工业互联网安全（OT/ICS 安全）、医疗健康信息安全等新兴行业细分领域的安全知识覆盖不足。
35		K10-003	缺失	缺失	缺乏对实战化攻防理论、安全体系韧性理论、网络攻防演练方法论、威胁狩猎理论与实践等实战领域知识的明确定义。
36		K10-004	所开发课程涉及的专业知识	所开发课程的相关理论、技术及工具使用方法等	应涵盖新时期知识。

4）技能体系的不足

国内网络安全人才能力框架在技能体系方面的不足主要体现在：一是缺少新兴技术技能。技能体系（S01-S02）中，缺乏对 AI 模型和系统安全漏洞分析与修复、生成对抗性样本、AI 伦理合规性审查、实

施隐私计算技术、容器安全配置与管理等 AI、数据、云原生领域核心实践技能的明确定义。二是实战化技能强调不足。对 0day 漏洞挖掘与利用、高级渗透测试与红队工具开发、组织和实施威胁狩猎活动、APT 攻击溯源与归因等高强度攻防技能的体现不足。三是自动化与 DevSecOps 技能欠缺。对 CI/CD 流水线安全自动化、自动化安全测试工具集成与调优等 DevSecOps 实践所需技能描述不足。

技能类别	代码	技能描述	不足（新时期视角）
通用技能	S01-001	能与组织内部和/或外部沟通与协调	缺乏对 AI 时代下人机协作、与 AI 工具有效沟通的隐性要求。
	S01-002	能理解组织业务，识别网络安全目标	缺乏针对 AI、大数据、云原生等新兴业务模式及其安全目标的深入理解能力要求。
	S01-003	能够建立和/或执行网络安全相关制度、策略或机制	缺乏对 DevSecOps、自动化安全流程编排等新型安全机制建立和执行能力的体现。
	S01-004	能够理解和应用与组织网络安全目标相关的法律法规、政策和标准	缺乏对《数据安全法》《个人信息保护法》，以及伦理人工智能规范等新时期重要法律法规的深度应用能力。
专业技能			
网络安全管理	S02-01-001	能够制定和实施网络安全规划	缺乏对人工智能安全规划、数据要素安全规划等战略性、可视规划能力的体现。
	S02-01-002	能协调/提供网络安全保障资源	对资源协调在云环境、混合 IT/OT 环境下的复杂性体现不足。
	S02-01-003	能组织执行风险管理，预判安全风险趋势	缺乏对 AI 风险评估、数据风险要素评估，以及利用 AI 进行风险趋势预测的能力。
	S02-01-004	能组织建立和运行应急体系	缺乏对自动化事故响应（SOAR）、实战化事故演练组织能力的要求。
	S02-01-005	能组织建立、运行和评估网络安全防护体系	对云储安全防护、人工智能系统安全防护等新兴防护体系的建立和评估能力的不足凸显。
	S02-01-006	能够对网络数据安全、个人信息保护和密码管理等进行规划和管理	缺乏对 AI 系统数据安全与治理、数据要素流通安全规划的深入研究。
数据安全	S02-02-001	能够识别不同数据阶段、不同业务应用场景所面临的安全风险	缺乏对要素数据化背景下的数据流转、数据交易等新型场景安全风险的识别能力。
	S02-02-002	能够运用数据安全工具、方法和技术保护数据安全	对数据分类分级工具、隐私计算工具（如联邦学习、差分隐私、同态加密）的深度应用和实践能力描述不足。
	S02-02-003	能够对数据安全建议开展风险评估，并提出整改	对数据要素匮乏流通安全风险评估的专门要求。
个人信息保护	S02-03-001	能够识别个人信息在不同阶段面临的安全风险	缺乏对个人信息匿名化/去标识化技术在实践中的应用能力。

	S02-03-002	能够运用个人信息保护工具、方法和技术保护个人信息	个人信息保护中应用的实践能力缺乏针对隐私的计算工具（如联邦学习、差分隐私）。
	S02-03-003	能够对个人信息保护工作进行符合性审查，并提出整改建议	缺乏对 AI 模型中个人信息隐私保护的审查能力。
密码管理	S02-04-001	能识别密码需求并配制密码应用方案	缺乏针对隐私计算相关密码技术（类似加密、安全多方计算）应用方案编制能力。
	S02-04-002	能引发密码保护产品，方法和技术实施密码保护	缺乏对隐私计算相关密码技术在实际保护中的实施能力。
	S02-04-003	能够对信息系统密码应用安全性进行评估并提出整改建议	缺乏对后量子密码应用安全性的评估能力。
网络安全需求分析	S02-05-001	能够识别网络安全保护对象的风险，并分析其面临的安全	缺乏对人工智能系统、云原生、工业互联网等新型保护对象的安全风险识别与分析能力。
网络安全架构设计	S02-06-001	能理解网络安全需求	（此为通用理解，特定补充，但其应用应涵盖新时期需求。）
	S02-06-002	能设计网络安全架构	缺乏对云原生安全架构、零信任架构、数据安全架构、AI 系统安全架构等新时期主流架构的设计实践能力。
	S02-06-003	能完成网络安全及信息化设备选型	对云安全产品、XDR、SOAR 等新型安全产品的选型能力体现不足。
网络安全开发	S02-07-001	能用特定语言、常见安全框架与组件和软件安全开发方法进行安全编码	缺乏对 DevSecOps 实践、安全左移、云原生应用安全开发（容器、微服务）的实践能力。
	S02-07-002	能管理代码安全漏洞	（用于通用管理能力，无需特定补充，但其管理可挖掘新时期漏洞类型。）
	S02-07-003	能力设计和执行安全测试计划、方法和示例	缺乏对自动化应用安全测试（SAST/DAST/IAST）、容器安全扫描、AI 系统安全测试（鲁棒性、偏见性、公平性测试）的实践能力。
供应链安全	S02-08-001	能识别供应链安全风险	缺乏对供应链软件清单（SBOM）分析、开源组件风险识别等新兴实践的深入。
	S02-08-002	能实施供应链安全保护	（此为通用实施能力，消耗了特定补充，但其应用应揭露新时期的风险。）
	S02-08-003	能够对供应链安全实施风险评估	（为此为通用评估能力，补充了特定的补充，但其评估应揭露新时期的风险。）
网络安全集成	S02-09-001	能够完成网络安全及信息化产品部署、配置、调试及设置	缺乏对云安全产品、XDR、SOAR 等新型安全产品部署、配置和调试的能力。
	S02-09-002	能够使用测试工具和测试方法实施安全集成测试	（此为通用测试能力，消耗特定补充，但其应用应涵盖新时期产品。）

	S02-09-003	能诊断和解决系统集成过程中的异常问题	（此处为通用问题解决能力，消耗特定补充，但其应用应涵盖新时期产品。）
网络安全运输维护	S02-10-001	能够维护网络及网络设备的安全运行	（此处为通用运维能力，消耗特定补充，但其运维对象应涵盖新时期网络设备和协议。）
	S02-10-002	能维护操作系统、服务器、存储设备及终端设备等的安全运行	缺乏对容器、K8s 等云环境运维能力的体现。
	S02-10-003	能够完成应用系统、中间件的管理、维护和安全防护工作	（其中为通用运维能力，消耗了特定的补充，但其应用系统应涵盖新时期的应用架构。）
	S02-10-004	能够完成数据库系统管理、维护和安全防护等	缺乏对大数据平台安全管理、维护和防护的能力。
网络安全监测与分析	S02-11-001	能收集、整理、管理威胁信息	缺乏对威胁情报的生产与消费等主动性威胁信息管理能力。
	S02-11-002	能够识别并评估可能危及组织和/或合作伙伴利益的网络威胁和事件	缺乏对高级持续性威胁（APT）识别与评估的能力。
	S02-11-003	能够使用各类方法和工具进行网络安全监控分析	缺乏对威胁狩猎、人工智能驱动的异常行为检测与分析等主动性、标记化监测分析能力。
网络安全事故	S02-12-001	能够对网络威胁和安全事件进行跟踪响应和执行	（其中为通用响应能力，消耗特定补充，但其响应对象应产生新时期威胁。）
	S02-12-002	能够编制网络安全事件应急预案	（此为通用编制能力，消耗特定补充，但其预案应涵盖新时期威胁。）
	S02-12-003	能够完成网络安全事件发现、研判和信息报送	（此处为通用发现研判能力，消耗特定补充，但其对象应涵盖新时期事件。）
	S02-12-004	能够利用常见的安全技术手段，对网络安全事件进行追踪、追踪追踪、追根溯源	缺乏对 AI 驱动的自动化响应（SOAR）的实践能力。
	S02-12-005	能开展事故预案开展事故演练	缺乏对实战化攻防演练的组织与执行能力。
网络安全测试	S02-13-001	能够完成脆弱性测试和渗透性测试	缺乏对高级渗透测试（绕过、免杀）、移动应用渗透测试、IoT/OT 渗透测试等新场景的渗透测试能力。
	S02-13-002	能对被测系统提出修复防护建议	（这为通用建议能力建议，消耗特定的补充，但其应涵盖新时期的威胁。）
网络安全评估	S02-14-001	能识别资产、威胁、脆弱性和现有安全控制措施	（其中为通用识别能力，采购特定补充，但其对象应为新时期资产和威胁。）
	S02-14-002	能够使用各种评估相关工具和方法分析并评估安全风险	缺乏对 AI 系统风险评估、云原生环境风险评估等新兴场景下的风险评估能力。
	S02-14-003	能根据风险分析结果，提出风险支付建议，并编制评估报告	（由此为通用建议能力建议，补充特定补充，但其应揭示新时期风险。）
网络安全审	S02-15-	能够评估和管理网络安全审计风险	（此处为通用评估能力，补充特定补充，

计	001		但其评估对象应涵盖新时期审计风险。）
	S02-15-002	能力管理、组织和实施审计	（此处为通用管理能力，可补充特定补充，但其审计对象应涵盖新时期系统。）
	S02-15-003	能够形成审计结论、提出审计建议、编制网络安全审计报告、并跟踪审计	（此项为通用审计能力，消除特定补充，但其审计对象应覆盖新时期系统。）
网络安全认证	S02-16-001	能够对受审核方的信息进行收集和分析	（此处为通用分析能力，支出特定补充，但其对象应为新时期认证。）
	S02-16-002	能按照审核准则编制审核计划	（用于通用计划能力，支出特定补充，但其对象应用于新时期认证。）
	S02-16-003	能依据审核计划开展审核活动，发现不符合项并编制审核报告	（用于通用审核能力，支出特定补充，但其对象应为新时期认证。）
电子数据取证	S02-17-001	能够使用普遍取证方法和工具进行调查取证	缺乏对云环境取证、容器取证、AI 系统取证等新兴环境下的取证能力。
	S02-17-002	能够完成电子数据恢复	（用于通用恢复能力，消耗特定补充，但其对象应为新时期数据源。）
	S02-17-003	能够完成电子证据数据的提取、固定和保护	（其中为通用保护能力，消耗特定补充，但其对象应为新时期数据源。）
	S02-17-004	能够完成电子证据数据的勘察、分析和归档	（此处为通用分析归档能力，消耗特定补充，但其对象应为新时期数据源。）
网络安全咨询	S02-18-001	能帮助用户识别和确定网络安全需求	（此处为通用识别能力，可补充特定内容，但其对象应满足新时期需求。）
	S02-18-002	能够帮助用户进行网络安全方面的规划和设计	（此项为通用规划设计能力，支出特定补充，但其对象应满足新时期需求。）
	S02-18-003	能够帮助用户建立网络安全管理体系、技能体系和事故体系	（用于通用建立能力，支出特定补充，但其对象应为新时期体系。）
网络安全科研	S02-19-001	能力掌握第一研究领域发展现状和趋势	（此项为通用掌握能力，借以特定补充，但其对象适用于新时期研究领域。）
	S02-19-002	能够运用相关知识，开展网络安全研究和创新，例如研究新技术及应用、法律法规、政策文件、标准等	对人工智能安全、量子计算安全、元宇宙安全等新兴技术研究和创新能力的匮乏。
	S02-19-003	能开展网络安全学术交流	（此处为通用交流能力，消耗特定补充，但其交流内容应涵盖新时期研究。）
网络安全培训与评价	S02-20-001	能识别和分析网络安全职业培训需求	（此处为通用识别能力，可补充特定内容，但其对象应满足新时期需求。）
	S02-20-002	能根据培训需求设计培训课程，实施网络安全培训，改进所培训的内容	缺乏对实战化培训、AI 安全人才培训设计与实施的强调。
	S02-20-003	能够对被培训人员掌握知识和技能的程度进行评价	缺乏对实战能力、人工智能安全技能评价的方法。

5）工作角色的不足

国内网络安全人才能力框架在角色方面的不足主要体现在：一是新兴复合型角色缺失。工作角色分类缺乏 AI 安全架构师、威胁狩猎专家、数据隐私架构师、DevSecOps 工程师等新时期高度复合型或战略型角色的明确定义。二是角色任务未完全匹配新需求。现有角色关联的工作任务未能完全体现新时期背景下职责的深化和扩展。三是角色定义过于宽泛。任务涵盖范围过于宽泛，导致与其他专业化角色重叠，不利于人才的精准培养和岗位设置。

序号	工作角色	工作任务	不足（新时期视角）
1	网络安全管理人员	网络安全需求分析网络安全规划和管理	未明确 AI 安全治理、数据要素安全规划等战略性任务。缺乏对高层决策者（如 CSO）角色的专门细化，难以体现安全治理与业务战略的深度融合。
2	数据安全保护人员	网络安全需求分析网络数据安全保护	缺乏对数据要素化背景下数据流通安全、隐私计算技术应用等新任务的覆盖。未区分数据安全管理与数据隐私保护的特定任务。
3	个人信息保护人员	网络安全需求分析个人信息保护	缺乏对个人信息跨境传输合规、AI 模型中个人信息隐私保护等新挑战的任务覆盖。
4	密码应用人员	网络安全需求分析密码技术应用	缺乏对隐私计算相关密码技术（如同态加密）等前沿密码应用任务的覆盖。
5	网络安全咨询人员	网络安全咨询	缺乏对 AI 安全、数据要素安全、工业互联网安全等新兴领域咨询任务的覆盖。
6	网络安全架构设计人员	网络安全需求分析网络安全架构设计	缺乏对云原生安全架构、零信任架构、AI 系统安全架构等新时期主流架构的设计任务。
7	网络安全开发集成人员	网络安全需求分析网络安全开发供应链安全管理网络安全集成实施	缺乏对 DevSecOps 实践、云原生应用安全开发、AI 应用开发安全，以及自动化集成等任务的覆盖。
8	网络安全运维人员	网络安全运维	缺乏对云原生环境（容器、K8s）运维、大数据平台运维、工业控制系统（ICS）/运营技术（OT）运维安全等新任务的覆盖。
9	网络安全监测分析人员	网络安全监测和分析	缺乏对威胁狩猎、AI 驱动的智能监测分析等主动性、智能化监测分析任务的覆盖。
10	网络安全应急管理人员	网络安全应急管理	缺乏对实战化攻防演练组织与执行、AI 驱动的自动化应急响应、APT 攻击溯源与归因等高强度实践任务的覆盖。
11	网络安全审计人员	网络安全审计	缺乏对 AI 系统审计、云环境审计等新兴审计任务的覆盖。
12	电子数据取证人员	电子数据取证	缺乏对云环境取证、容器取证、AI 系统取证等新兴环境取证任务的覆盖。
13	网络安全测评人员	网络安全测试网络安全评估	缺乏对自动化应用安全测试、容器安全扫描、AI 系统安全测试（鲁棒性、偏见性、公平性测试）等新任务的覆盖。

14	网络安全防护人员	网络安全集成实施网络安全运维护网络安全测试	该角色范围过于宽泛，与“网络安全集成实施”“网络安全运维”“网络安全测试”等已有角色存在任务重叠。未体现新兴防护理念（如零信任）。
15	网络安全认证人员	网络安全认证	缺乏对数据安全认证、AI 安全认证等新兴认证任务的覆盖。
16	网络安全科学研究人员	网络安全科学研究	缺乏对 AI 安全前沿研究（如大模型安全、对抗性机器学习）、量子计算安全研究、元宇宙安全研究等新兴和交叉领域研究任务的覆盖。
17	网络安全培训人员	网络安全培训和评价	缺乏对实战化培训与评价、AI 安全人才培训设计与实施等新任务的覆盖。
18	其他	（无）	（无）

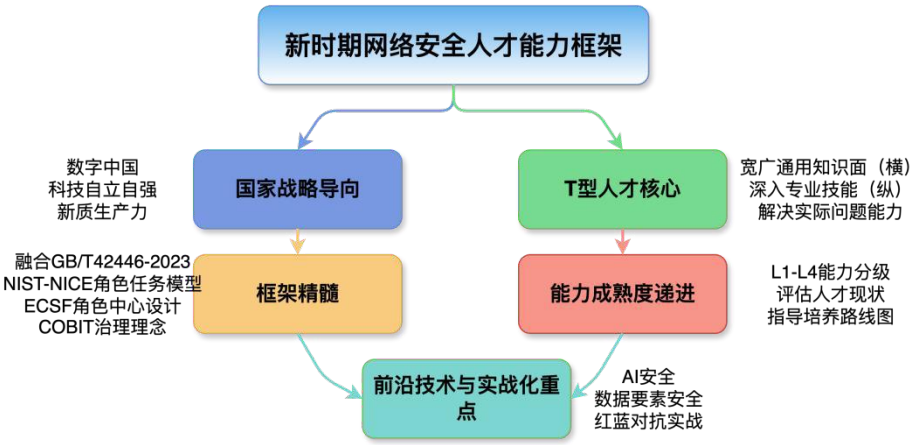
第四章 新时期的网络安全人才能力框架

通过深刻剖析现有网络安全人才能力框架在应对人工智能时代、实战化攻防和数据合规等新时期挑战时的不足，企业亟须更关注实战、更融合新兴技术、更符合中国国情且更加操作性的新框架，呈现新时期网络安全人才的全面画像，以及定义和评估人才的工具，来指导网络安全人才的培养、评估和管理。

4.1 新时期网络安全人才能力框架的核心理念

安全牛针对现有网络安全人才能力框架的挑战，提出“新时期网络安全人才能力框架”的解决方案，为企业提供清晰的能力框架，指引企业人才的使用、培养、评价和管理。

新时期中国网络安全人才能力框架是以国标 GB/T42446-2023）为基础，深度融入中国特有的国家战略、政策法规、技术热点和产业发展需求，并结合国外主流人才框架（NISTNICE、ECSF、e-CF）的研究结果，设计构建一个科学、前置、可落地的人才能力框架。



新时期中国网络安全人才能力框架

- **国家战略导向：**新时期中国网络安全人才能力框架设计紧密结合“数字中国”“科技自立自强”“新质生产力”等国家战略，确保人才培养方向与国家发展高度一致。网络安全人才不仅要培养懂技术，更要培养国家网络安全意识。

- **以“T 型人才”为核心：**强调培养具备宽广通用知识面（“一横”）和在至少一个或多个领域有深入专业技能（“一纵”）的复合型人才，解决传统人才培养中“悟多不精”或“精但不通”的痛点，确保人才获得宏观视野，进而解决实际问题的能力。

- **框架精髓：**本框架继承了 GB/T42446-2023 的系统分类，结合 NISTNICE 的角色－任务－知识－技能－能力（KSA）模型、ECSF 以角色为中心的设计思想，并引入 COBIT 在治理上的理念，在与国家标准的权威融合的同时，结合国际最佳实践的便捷性和拓扑度，打破了框架的架构。

- **能力成熟度递进：**框架构建了分阶段的能力成熟度模型（L1-L4），不仅是评估人才现状的标尺，更是指导企业循序渐进和评估人才培养的路线图。解决国家标准缺乏能力分级的痛点，让企业“知道怎么”培养才能达到更高水平。

- **AI、数据安全、实战化重点：**框架突出对 AI 安全、数据要素安全、红蓝对抗等前沿与实战化需求的覆盖，确保人才能够真正应对新时期复杂多变、高强度的网络安全威胁，而不仅仅停留在理论和合规层面。

4.2 新时期网络安全人才能力框架的基本要素

新时期中国网络安全人才能力框架的基本要素包括网络安全工作的工作类别、工作角色和关键任务，这几大要素从宏观到具体，层层递进，呈现一个新时期网络安全人才的全能力画像，为探讨人才的实践路径奠定了坚实的基础。

新时期中国网络安全人才能力框架的基本要素

4.2.1 拓展新时期的工作类别

网络安全工作的工作类别是框架中的最高体系，直接承载了企业安全目标或国家网络安全战略，为后续的工作角色设定了宏观的范围和边界，是所有具体工作的起点。**网络安全工作的工作类别的设计**可以帮助企业从全局角度把握所需要的网络安全人才职能的全貌，解决企业不知道网络安全领域到底有哪

些方面的困惑，是构建人才梯队和战略设定的基础。

新时期中国网络安全人才能力框在 GB/T42446-20235 个大工作类别基础上，进行了强化和拓展，强化了已有工作类别的工作任务，并新增拓展了数据安全与隐私保护类、AI 安全与治理类、实战攻防与威胁狩猎类等 3 个核心类别，更全面地覆盖新时期网络安全人才的复杂性和专业化需求，以适应更加复杂和专业化的安全需求，特别是将数据安全、AI 安全和实战攻防作为独立的类别，体现了新时期的战略重点。这 8 个大工作类别共同构成了新时期网络安全人才的能力广度：

工作类别	新时期工作任务
网络安全管理	网络安全需求分析，网络安全规划和管理，网络数据安全保护，个人信息保护，密码技术应用，网络安全咨询 （拓展）制定 AI 伦理与治理政策，安全治理体系评估与优化
网络安全建设	网络安全需求分析，网络安全架构设计，网络安全开发，供应链安全管理，网络安全集成实施，网络数据安全保护，个人信息应用，密码技术应用 （拓展）云原生安全架构设计与实现，AI 系统安全架构设计
网络安全运营	网络安全运维，网络安全监测和分析，网络安全应急管理，网络数据安全保护，个人信息保护，密码技术应用 （拓展）AI 驱动的安全运营，威胁狩猎实践
网络安全审计和评估	网络安全审计，网络安全测试，网络安全评估，网络安全认证，电子数据取证 （拓展）AI 系统安全审计与评估，实战化攻防演练评估
网络安全科研教育	网络安全研究，网络安全培训和评价 （拓展）AI 安全前沿技术研究，量子计算安全研究，元宇宙安全研究
数据安全与隐私保护类（拓展）	（拓展）网络数据安全保护，个人信息保护 数据要素安全流通保障，隐私计算技术应用与管理
AI 安全与治理类（拓展）	（拓展）AI 系统安全架构设计，AI 模型安全评估与加固，AI 应用安全开发与测试，AI 伦理与合规治理，AI 数据安全与隐私保护
实战攻防与威胁狩猎类（拓展）	网络安全测试，网络安全应急管理 （拓展）组织和实施威胁狩猎活动，开展高强度红蓝对抗演练，进行 APT 攻击溯源与归因，0day 漏洞挖掘与利用

4.2.2 新时期新增和深化的重点角色

网络安全工作的工作角色从属于的工作类别，定义了其日常职责，是执行网络安全工作任务的行为和责任的集合。工作角色帮助解决企业需要什么岗位的人，使人才需求从宏观类别具体到可操作的岗位。对于从业者而言，工作角色提供了清晰的职业定位和发展需要方向，是其职业生涯规划的起点。工作角色也承接了“T 型人才”中“一纵”的方向初步判断。融合型“新时期中国网络安全人才能力框架”在 GB/T42446-2023 的 18 个角色基础上，丰富了角色的工作任务，制定更贴近新时期角色的实际工作任务内容，为人才培养和能力评估提供具体指引，以应对新时期挑战。

序号	工作角色	新时期工作任务
1	网络安全管理人员	网络安全需求分析，网络安全规划和管理， （新增）网络数据安全保护，个人信息保护，密码技术应用，网络安全咨询，制定 AI 伦理与治理政策，安全治理体系评估与优化
2	数据安全保护人员	网络安全需求分析，网络数据安全保护 （深化）个人信息保护，密码技术应用，数据要素安全流通保障，实施隐私计算技术
3	个人信息保护人员	网络安全需求分析，个人信息保护 （深化）个人信息跨境传输合规性保障、AI 模型中个人信息隐私保护
4	密码应用人员	网络安全需求分析，密码技术应用 （深化）隐私计算相关密码技术应用
5	网络安全咨询人员	网络安全咨询 （深化）AI 安全、数据要素安全、工业互联网安全等新兴领域咨询
6	网络安全架构设计人员	网络安全需求分析，网络安全架构设计 （深化）云原生、零信任、AI 系统安全架构设计
7	网络安全开发集成人员	网络安全需求分析，网络安全开发，供应链安全管理，网络安全集成实施 （深化）云原生应用开发安全、AI 应用开发安全，自动化安全集成
8	网络安全运维人员	网络安全运维 （深化）云原生环境运维安全、大数据平台运维安全、工业控制系统/运营技术（OT）运维安全
9	网络安全监测分析人员	网络安全监测和分析 （深化）组织和实施威胁狩猎活动、利用 AI 进行智能监测分析
10	网络安全应急管理人员	网络安全应急管理 （深化）开展高强度红蓝对抗演练、进行 APT 攻击溯源与归因、利用 AI 进行自动化应急响应
11	网络安全审计人员	网络安全审计（深化）AI 系统审计、云环境审计
12	电子数据取证人员	电子数据取证（深化）云环境取证、容器取证、AI 系统取证
13	网络安全测评人员	网络安全测试、网络安全评估 （深化）自动化应用安全测试、容器安全扫描、AI 系统安全测试，AI 系统风险评估、云原生环境风险评估
14	网络安全防护人员	可拆分或融入其他更具体的角色中，或重新定义为更聚焦的角色（如 DevSecOps 工程师、云原生安全架构师）
15	网络安全认证人员	网络安全认证 （深化）数据安全认证、AI 安全认证
16	网络安全科学研究人员	网络安全科学研究 （深化）AI 安全前沿研究、量子计算安全研究、元宇宙安全研究
17	网络安全培训人员	网络安全培训和评价 （深化）实战化培训与评价、AI 安全人才培训设计与实施
18	其他	（无）

4.2.3 新时期新增和深化的关键任务

网络安全工作的关键任务是为了实现组织相关目标，由网络安全人员执行的一个或一组具体工作活动和内容，是连接工作角色与所需知识、技能的桥梁，是人才能力评估的最小颗粒度。关键任务主要是解决职责岗位是干什么的问题，指导企业设计具体的岗位说明（任务简介），并据此评估候选人或现有员工的实际操作能力。对于员工来说，任务清单是其日常工作的指引，也是其能力提升的具体目标。每个工作角色都由一系列关键任务支撑，是工作角色的具体化表现。融合型“新时期中国网络安全人才能力框架”在 GB/T42446-2023 的 20 项任务基础上，深化了已有的 20 个任务，并新增了识别 AI 模型脆弱性、大模型应用风险管理、威胁狩猎、实战攻防、高级威胁防御、漏洞挖掘、数据要素安全、数据流通技术等 8 个任务，制定更贴近新时期的实际工作内容，为人才培养和能力评估提供具体指引，以应对新时期挑战。

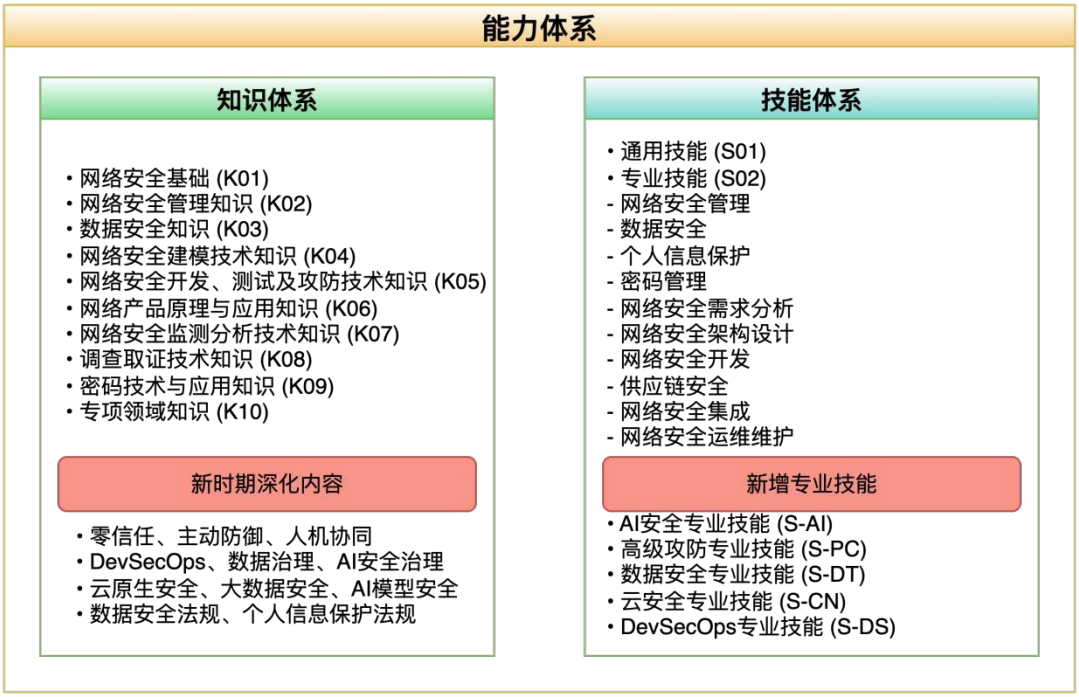
序号	工作任务	新时期视角工作任务描述
1	网络安全规划和管理	指导、制定、监督和执行网络安全战略规划、策略制度和体制机制。综合协调相关人员，采取各类网络安全控制措施，降低并缓解系统安全风险； （深化）AI 安全治理、数据要素安全规划，确保人才发展与国家数字经济战略高度对齐。
2	网络数据安全保护	针对网络数据收集、存储、使用、加工、传输、提供、公开等环节，采取措施保障网络数据安全； （深化）数据要素化背景下的数据流通安全保障，以及 AI 训练数据和推理数据的安全保护，确保数据全生命周期安全合规。
3	个人信息保护	针对个人信息收集、存储、使用、加工、传输、提供、公开、删除等环节，采取措施保障个人信息安全； （深化）个人信息跨境传输合规性保障，以及 AI 模型中个人信息的隐私保护与匿名化处理。
4	密码技术应用	运用密码技术，进行信息系统安全密码保障的架构设计、系统集成、检测评估、运维管理、密码咨询等； （深化）隐私计算相关密码技术（如同态加密、安全多方计算）的原理、应用与管理。
5	网络安全需求分析	依据法律法规、政策标准及业务流程要求，开展符合性需求分析、业务所依赖的信息通信技术（ICT）持续运行需求分析、数据安全需求分析等，定期或在遇到重大网络安全事件时对组织网络安全需求进行复审； （深化）AI 系统和云原生环境的安全需求分析，以及数据要素流动对安全需求的洞察。
6	网络安全架构设计	依据网络安全需求分析、ICT 基础设施现状，组织环境和业务特点等，从物理环境、通信网络、计算环境、区域边界等方面进行网络安全架构设计，形成网络安全架构实施方案； （深化）云原生安全架构、零信任架构、数据安全架构、AI 系统安全架构，确保架构的前瞻性和韧性。

7	网络安全开发	实现软件、硬件安全架构及功能开发，并对其进行测试、更新和维护；融入 DevSecOps 流程，实现安全左移， （深化）云原生应用、AI 应用的开发安全，确保从源头构建安全。
8	供应链安全管理	运用供应链安全管理的方法、工具和技术，控制供应链安全风险，管理供应商及网络安全和信息化相关产品和服务的采购； （深化）软件物料清单分析与管理，以及对开源组件的安全评估与风险控制。
9	网络安全集成实施	网络安全项目管理，信息系统安全集成过程中软硬件设备与系统的安装、调试、测试、配置、故障处理和工程实施，以及配合验收交付； （深化）与 SOC、态势、威胁情报、XDR、SOAR、云平台、数据平台、AI 平台集成。
10	网络安全运维	利用网络安全技术/工具，根据网络安全相关标准和制度流程，操作、运行、维护和管理信息系统； （深化）容器、K8s 等云原生环境的运维，以及工业控制系统（ICS）/运营技术（OT）的维护安全。
11	网络安全监测和分析	利用相关技术、工具和情报信息等对目标系统进行安全监测、分析和预警，并提出应对威胁的措施和改进建议； （深化）威胁狩猎、AI 驱动的智能监测分析，实现从被动告警到主动发现。
12	网络安全应急管理	组织编制网络安全事件应急预案，实施网络安全应急演练，在应对突发/重大网络安全事件时，采取必要的应急处置措施将信息系统和业务恢复到正常状态，并进行事件溯源和调查取证； （深化）实战化攻防演练的组织与执行，以及 AI 驱动的自动化应急响应，提升快速止损能力。
13	网络安全审计	依据审计依据，在规定的审计范围内，监督和评价网络安全控制措施的设计有效性和执行有效性，确定被审计对象满足审计依据的程度，并提出网络安全工作改进的意见和建议； （深化）AI 系统审计、云环境审计，以及针对数据流动的合规审计。
14	网络安全测试	对目标系统的脆弱性和防御机制有效性进行验证，发现安全问题并提出改进建议；根据测试依据，识别并测试系统和产品的安全性； （深化）自动化应用安全测试（SAST/DAST/IAST）、容器安全扫描、AI 系统安全测试（鲁棒性、偏见性、公平性测试）。
15	网络安全评估	评估信息系统、业务及相关网络数据等的符合性和面临的网络安全风险，对风险进行识别、分析、评价，提出改进建议； （深化）AI 系统风险评估、云原生环境风险评估，以及供应链安全风险评估。
16	网络安全认证	对网络安全管理体系、服务、产品等开展认证与审核； （深化）数据安全认证、AI 安全认证体系。
17	电子数据取证	对电子数据进行提取、固定、恢复、分析等工作； （深化）云环境取证、容器取证、AI 系统取证，以及针对高级持续性威胁（APT）的深度取证。
18	网络安全咨询	根据组织的安全目标，提供安全规划、设计、实施、运维、管理等方面的政策法规和技术咨询服务； （深化）AI 安全、数据要素安全、工业互联网安全等新兴领域咨询。

19	网络安全研究	研究网络空间安全涉及的学科理论基础和方法论，研究网络安全新兴技术及应用、产业发展趋势，以及网络安全法律法规、政策、标准等； （深化）AI 安全前沿研究（如大模型安全、对抗性机器学习）、量子计算安全研究、元宇宙安全研究。
20	网络安全培训和评价	开展网络安全培训方案和相关课程的设计、开发和持续改进，实施授课等培训活动，开展评价活动，例如：理论知识考试、技能操作考核、业绩评审、竞赛选拔等；融入实战化培训与评价， （深化）AI 安全人才培训，并利用 AI 工具提升培训效率。
KT-AI01	AI 模型安全评估与加固（新增）	（新增）识别 AI 模型脆弱性，采取防御对抗性攻击、数据投毒措施，保障 AI 模型完整性与鲁棒性，确保 AI 系统可信赖运行。
KT-AI02	大模型应用安全开发与测试	（新增）针对大模型（LLM）应用的特有风险（如提示词注入、数据泄露、不当内容生成），进行安全编码、测试和防护，保障 AI 应用业务安全。
KT-PC01	组织和实施威胁狩猎活动（新增）	（新增）运用高阶分析技术和主动探索方法，在海量日志、流量和端点数据中主动搜索隐藏的、未被传统安全工具检测到的高级持续性威胁（APT）和异常活动，实现先敌发现。
KT-PC02	开展高强度红蓝对抗演练（新增）	（新增）模拟真实攻击场景，测试组织防御体系的有效性，提升团队实战能力，并促进攻防经验转化，实现以攻促防。
KT-PC03	进行 APT 攻击溯源（新增）	（新增）针对高级持续性威胁（APT）攻击，进行深度分析、追踪溯源，识别攻击者身份、目的和攻击链，为精准打击提供情报支持。
KT-PC04	漏洞挖掘与利用（新增）	（新增）发现并利用未公开的安全漏洞，用于渗透测试、红蓝对抗或提交漏洞奖励平台，提升安全研究深度和前瞻性防御能力。
KT-DT01	数据要素安全流通流程设计与保障（新增）	（新增）确保数据作为生产要素在收集、存储、加工、传输、交易、提供、公开等流通环节的合规性、隐私性和安全性，支撑数字经济发展。
KT-DT02	实施隐私计算技术（新增）	（新增）运用联邦学习、同态加密、安全多方计算等技术，在保护数据隐私的前提下，实现数据价值的协同利用和数据“可用不可见”，促进数据合规共享。

4.3 新时期网络安全人才能力框架的能力体系

工作角色从属于的工作类别，由一系列关键任务支撑，完成这些关键任务需要的能力体系包括知识、技能和能力水平，这是安全人才核心能力和熟练程度的关键要素。



人才能力框架的能力体系

4.3.1 新时期深化的知识体系

网络安全知识是网络安全人员通过经验或教育获取的事实、信息、真理、原理或领悟，是技能的基础，是理解安全威胁、技术原理和合规要求的前提。解决了知其然不知其然的问题，为人才的分析、判断和创新提供理论支撑。没有足够的知识储备，技能的运用将是盲目而缺乏深度的，是完成关键任务的关键，是技能才能发挥对应作用的内在支撑。

融合型“新时期中国网络安全人才能力框架”在 GB/T42446-2023 的 10 个知识领域基础上，参考并融合国标知识领域与新时期拓展，深化框架的新兴技术内容，确保人才的知识储备能够覆盖前沿技术。

序号	知识领域	知识代码	知识单元	新时期视角知识描述
1	网络安全基础	K01-001	网络安全概念及发展历程	信息安全概念、信息安全属性、信息安全视角、信息安全保障框架模型；网络安全发展历程、发展现状和发展趋势等；国内外网络安全产业发展情况等。（深化）网络空间安全新范式（如主动防御、零信任、人机协同）。
2		K01-002	网络安全管理基本知识	风险管理、供应链安全管理、运营管理、应急管理、业务连续性、管理体系、认证认可、漏洞管理等基本知识；（深化）DevSecOps 基本理念、数据治理基础、AI 安全治理基础。
3		K01-003	网络安全技术基本	网络体系、通信技术、计算机组成原理、操作系统、密码学基础、PKI/CA 体系、身份鉴别、访问控制等基本知识；（深

			知识	化）云原生（容器、微服务、K8s）基础、大数据平台安全基础、AI 基础模型和算法原理。
4		K01-004	国内外网络安全法律法规和政策	国内外网络安全法律法规政策战略和监管机制等； （深化）《数据安全法》《个人信息保护法》《关键信息基础设施安全保护条例》，以及 AI、工业互联网、生成式 AI 等领域最新政策法规。
5		K01-005	国内外网络安全标准	国内、国外、国际网络安全标准； （深化）AI 安全标准、数据安全国家标准（如数据分类分级）。
6		K01-006	网络安全最佳实践	解决方案或者经验等； （深化）DevSecOps 实践、零信任实践、AI 安全实践等。
7	网络安全管理知识	K02-001	供应链安全管理	国内外供应链安全发展现状，供应链安全管理方法、技术及工具等； （深化）供应链软件物料清单（SBOM）管理、供应链攻击防御策略。
8		K02-002	应急管理方法和技术	业务连续性、事件管理、应急预案编制、维护和演练等；操作系统、中间件、数据库等常用应急处置方法； （深化）自动化应急响应（SOAR）、实战化应急演练、AI 驱动的事件分析。
9		K02-003	网络安全风险管理	风险评估、风险处置等方法、技术和实施； （深化）风险量化评估、业务风险转化、AI 风险评估方法。
10		K02-004	网络安全审计方法和技术	通用审计准则和方法；网络安全审计准则、方法、审计技术、信息化项目管理等； （深化）自动化审计、云环境审计、AI 系统审计方法。
11		K02-005	网络安全认证认可	认证相关基本概念、认可相关基本概念；审核知识等； （深化）数据安全认证、AI 安全认证体系。
12	数据安全知识	K03-001	数据安全管理和技术	数据安全基本概念、数据安全技术，数据安全治理与保障等； （深化）数据分类分级实践、数据全生命周期安全管理（采集、存储、使用、传输、共享、销毁）、数据要素安全流通。
13		K03-002	个人信息保护管理和技术	个人信息保护政策，个人信息保护技术工具等； （深化）个人信息跨境传输合规、个人信息匿名化/去标识化技术、隐私计算技术（如联邦学习、差分隐私、同态加密）在数据保护中的应用。
14	网络安全建模技术知识	K04-001	系统建模理论和常用方法	数学基础、模型概念、建模原理、系统建模方法等； （深化）云原生系统建模、工业互联网系统建模。
15		K04-002	威胁建模理论和常用方法	威胁建模的作用、常用的威胁建模方法等； （深化）AI 威胁建模（如针对对抗性攻击、数据投毒的建模）。
16		K04-003	安全架构模型及设	网络安全架构、系统安全架构模型及常用设计方法等； （深化）云原生安全架构、零信任架构、数据安全架构、AI

			计方法	系统安全架构。
17	网络安全开发、测试及攻防技术知识	K05-001	安全开发	软件安全设计、代码实现安全、资源使用安全、配置管理安全、软件工程等； （深化）DevSecOps 流程与工具链、安全左移理念、API 安全开发。
18		K05-002	系统安全工程	系统安全工程理论及实施等； （深化）云环境安全工程、工业控制系统安全工程。
19		K05-003	网络安全威胁和漏洞管理	威胁和漏洞概念，漏洞的发现、利用和提交等技术、方法和流程； （深化）漏洞生命周期管理、威胁情报驱动的漏洞分析、AI 模型漏洞管理。
20		K05-004	安全测试、评估方法	常用测试和评估方法，如黑盒测试、灰盒测试、白盒测试及压力测试等； （深化）自动化应用安全测试（SAST/DAST/IAST）、容器安全扫描、AI 系统安全测试（鲁棒性、偏见性、公平性测试）。
21		K05-005	渗透测试方法和技术	Web 安全、中间件、数据库等常见安全漏洞及利用方法，安全渗透测试知识，常用渗透测试工具等； （深化）高级渗透测试技术、AI 大模型的渗透测试、移动应用渗透测试、IoT/OT 渗透测试。
22		K05-006	网络攻防技术	网络攻击原理、常见攻击方法、攻击技术和攻击后果，以及防御措施等； （深化）高级持续性威胁（APT）攻击原理、勒索病毒攻击技术、供应链攻击原理、红蓝对抗策略与技术。
23	网络产品原理与应用知识	K06-001	备份/灾备方法与技术	系统和数据的备份/恢复、灾备方法与技术等； （深化）云备份/灾备、分布式系统灾备、数据湖灾备。
24		K06-002	网络设备功能及原理	交换机、路由器等网络设备工作原理、配置及网络架构设计相关知识； （深化）SDN/NFV 技术、云网络安全功能（VPC、安全组）。
25		K06-003	网络安全产品功能及原理	网络安全产品原理及应用（防火墙、入侵检测、网闸、VPN 等）； （深化）云安全产品（CWPP、CSPM、CASB）、XDR（扩展检测与响应）、SOAR（安全编排自动化与响应）等。
26		K06-004	操作系统安全原理及使用	Windows 和 Linux/Unix 等主流操作系统、虚拟机和容器等常用安全技术、 （深化）安全配置和安全加固；容器安全、K8s 安全、Serverless 安全。
27		K06-005	中间件安全原理及使用	中间件功能原理（通信支持、应用支持、公共服务等）、安全配置及安全加固等； （深化）API 网关安全、消息队列安全。
28		K06-006	数据库安	数据库安全防护技术及方法、安全配置和加固，包括数据库

			全技术及使用	的加密、用户管理、备份还原、数据脱敏、审计等； （深化）大数据平台安全（Hadoop、Spark）、NoSQL 数据库安全。
29	网络安全监测分析技术知识	K07-001	网络安全监测方法和技术	流量监控、事件监控、容量监控等； （深化）威胁狩猎技术、基于 AI 的异常行为检测、日志聚合分析（ELKStack 等）。
30		K07-002	网络安全分析方法和技术	网络流量分析、恶意代码、日志分析等； （深化）自动化分析、威胁情报驱动的分析、机器学习在安全分析中的应用。
31	调查取证技术知识	K08-001	调查取证方法和技术	电子数据取证概念、取证模型、电子数据取证管理、电子数据证据的勘验和司法鉴定流程、电子数据取证相关技术等； （深化）云环境取证、容器取证、AI 系统取证。
32	密码技术与应用知识	K09-001	密码技术、密码产品及服务功能及原理	密码算法、协议、密钥管理等相关技术，工具、产品、服务及解决方案等； （深化）后量子密码（PQC）、同态加密、零知识证明等隐私计算相关密码技术。
33	专项领域知识	K10-001	新技术新应用安全	云计算、大数据、物联网、人工智能、区块链、5G 等； （深化）AI 安全（大模型安全、对抗性机器学习、可信 AI）、量子计算安全、元宇宙安全、车联网安全。
34		K10-002	特定行业网络安全知识	电信、能源、金融、交通等行业特定的网络安全知识； （深化）金融科技安全、工业互联网安全（OT/ICS 安全）、医疗健康信息安全。
35		K10-003	相关知识	（深化）实战领域相关知识：强调实战化攻防理论、安全体系韧性理论、网络攻防演练方法论、威胁狩猎理论与实践。
36		K10-004	所开发课程涉及的专业知识	所开发课程的相关理论、技术及工具使用方法等。

4.3.2 新时期深化的技能体系

网络安全技能是网络安全从业人员通过教育、培训、经验或其他方式完成任务的一种能力。完成关键任务，必须掌握相应的技能，技能是知识的实践转化和外部表现，能够从理论审视实际场景，解决具体问题的操作能力，也是人才是否具备实战能力的关键，解决了“纸上谈兵”的问题。

融合型“新时期中国网络安全人才能力框架”在 GB/T42446-2023 的 4 个通用技能和 20 个专业技能体系的基础上，参考并融合国标知识领域与新时期拓展，深化了通用技能和专业技能，并新增了 AI 安全专业技能、高级攻防专业技能、数据安全专业技能、云安全专业技能、DevSecOps5 个专业技能，重点突出了实战、创新和人工智能相关技能，确保人才具备新时期需要的解决实际问题的能力。

技能类别	代码	新时期视角技能描述
通用技能	S01-001	能与组织内部和/或外部沟通与协调； （深化）AI 时代下的人机协调沟通。
	S01-002	能够理解组织业务，识别网络安全目标； （深化）新兴数字业务（如 AI、大数据、云原生）的安全目标。
	S01-003	能够建立和/或执行网络安全相关制度、策略或机制； （深化）DevSecOps 实践和自动化安全流程编排机制。
	S01-004	能够理解和应用与组织网络安全目标相关的法律法规、政策和标准； （深化）《数据安全法》《个人信息保护法》、人工智能伦理规范和新兴安全标准。
专业技能		
网络安全管理	S02-01-001	能够制定和实施网络安全规划； （深化）AI 安全规划和数据要素安全规划。
	S02-01-002	能够协调/提供网络安全保障资源； （深化）复杂云环境和 IT/OT 融合环境下的资源协调。
	S02-01-003	能组织执行风险管理，预判安全风险趋势； （深化）AI 风险评估、数据要素风险评估，并能利用 AI 进行风险趋势预测。
	S02-01-004	能组织建立和运行事故体系； （深化）自动化事故响应（SOAR）和实战化事故演练的组织。
	S02-01-005	能够组织建立、运行和评估网络安全防护体系； （深化）云原生安全防护和人工智能系统安全防护体系。
	S02-01-006	能够对网络数据安全、个人信息保护和密码管理等进行规划和管理； （深化）AI 系统数据安全与治理规划和数据流通安全规划。
数据安全	S02-02-001	能够识别在数据不同环节、不同业务应用场景下面临的安全风险； （深化）数据要素化背景下数据流转和数据交易场景的安全风险。
	S02-02-002	能够运用数据安全工具、保护数据安全的方法和技术； （深化）应用数据分类分级工具、隐私计算工具（如联邦学习、增量隐私）。
	S02-02-003	能够对数据安全开展风险评估，并提出整改建议； （新增）数据流通安全风险评估。
个人信息保护	S02-03-001	能够识别个人信息在不同阶段面临的安全风险； （深化）个人信息匿名化/去标识化技术实践。
	S02-03-002	能够运用个人信息保护工具、保护个人信息的方法和技术； （深化）应用个人信息化/去标识化、隐私计算工具。
	S02-03-003	能够对个人信息保护工作进行符合性审查，并提出整改建议； （深化）AI 模型中个人信息隐私保护的审查。
密码管理	S02-04-001	能识别密码需求并配制密码应用方案； （深化）隐私计算相关密码技术的应用方案配制（类似形态加密）。
	S02-04-002	能够运用密码保护产品、方法和技术实施密码保护；应用隐私计算相关密码技术。
	S02-04-003	能够对信息系统密码应用安全性进行评估并提出整改建议； （深化）后量子密码应用安全性的评估。

网络安全需求分析	S02-05-001	能够识别网络安全保护对象，并分析其面临的安全风险； （深化）人工智能系统、云突破、工业互联网等新型保护对象的风险分析。
网络安全架构设计	S02-06-001	能够理解网络安全需求。
	S02-06-002	能设计网络安全架构； （深化）云原生安全架构、零信任架构、数据安全架构、AI 系统安全架构。
	S02-06-003	能完成网络安全及信息化设备选型； （深化）云安全产品、XDR、SOAR 等新型安全产品。
网络安全开发	S02-07-001	能用特定语言、常见安全框架与组件和软件安全开发方法进行安全编码； （深化）DevSecOps、安全左移、云实践应用安全开发。
	S02-07-002	能够管理代码安全漏洞。
	S02-07-003	能设计和执行安全测试计划、方法和案例； （深化）自动化应用安全测试（SAST/DAST/IAST）、集装箱安全扫描、AI 系统安全测试（鲁棒性、偏见性、公平性测试）。
供应链安全	S02-08-001	能识别供应链安全风险；供应链软件清单（SBOM）分析、开源组件风险识别。
	S02-08-002	能实施供应链安全保护。
	S02-08-003	能够对供应链安全实施风险评估。
网络安全集成	S02-09-001	能够完成网络安全及信息化产品部署、配置、调试及设置； （深化）云安全产品、XDR、SOAR 平台集成。
	S02-09-002	能够使用测试工具和测试方法实施安全集成测试。
	S02-09-003	能够诊断和解决系统集成过程中的异常问题。
网络安全运输维护	S02-10-001	能够维护网络及网络设备的安全运行。
	S02-10-002	能维护操作系统、服务器、存储设备及终端设备等的安全运行； （深化）容器、K8s 等云原生环境的维护。
	S02-10-003	能够完成应用系统、中间件的管理、维护和安全防护工作。
	S02-10-004	能够完成数据库系统管理、维护和安全防护等； （新增）核心大数据平台安全管理。
网络安全监测与分析	S02-11-001	能收集、整理、管理威胁信息； （深化）威胁情报的生产与消费。
	S02-11-002	能识别并评估可能危及组织和/或合作伙伴利益的网络威胁和事件； （深化）高级持续性威胁（APT）识别与评估。
	S02-11-003	能够利用各类方法和工具进行网络安全监控分析； （新增）重点威胁狩猎、AI 驱动的异常行为检测与分析。
网络安全事故	S02-12-001	能够对网络威胁和安全事件进行跟踪响应和执行。
	S02-12-002	能够编制网络安全事件应急预案。
	S02-12-003	能够完成网络安全事件发现、研判和信息报送。

	S02-12-004	能够利用常见的安全技术手段，对网络安全事件进行威胁抑制、开源排查、追踪溯源； （深化）AI 驱动的自动化应急响应（SOAR）。
	S02-12-005	能依据应急预案开展事故演练； （深化）护网行动等实战化攻防演练的组织与执行。
网络安全测试	S02-13-001	能够完成脆弱性测试和渗透性测试；深入高级渗透测试（绕过、免杀）、移动应用渗透测试、IoT/OT 渗透测试。
	S02-13-002	能对被测系统提出修复防护建议。
网络安全评估	S02-14-001	能够识别资产、威胁、脆弱性和现有的安全控制措施。
	S02-14-002	使用各类能力评估相关工具和方法分析并评估安全风险； （深化）AI 系统风险评估、云原生环境风险评估。
	S02-14-003	能根据风险分析结果，提出风险支付建议，并编制评估报告。
网络安全审计	S02-15-001	能够评估和管理网络安全审计风险。
	S02-15-002	能力管理、组织和实施审计。
	S02-15-003	能够形成审计结论、提出审计建议、编制网络安全审计报告，并跟踪审计。
网络安全认证	S02-16-001	能够对受审核方的信息进行收集和分析。
	S02-16-002	能按照审核准则编制审核计划。
	S02-16-003	能依据审核计划开展审核活动，发现不符合项并编制审核报告。
电子数据取证	S02-17-001	能够使用各类取证方法和工具进行调查取证； （深化）云环境取证、容器取证、AI 系统取证。
	S02-17-002	能够完成电子数据恢复。
	S02-17-003	能够完成电子证据数据的提取、固定和保护。
	S02-17-004	能够完成电子证据数据的勘验、分析和归档。
网络安全咨询	S02-18-001	能够帮助用户识别和确定网络安全需求。
	S02-18-002	能够帮助用户进行网络安全方面的规划和设计。
	S02-18-003	能够帮助用户建立网络安全管理体系、技术体系和应急体系。
网络安全科研	S02-19-001	能掌握第一学期研究领域的发展现状和趋势。
	S02-19-002	能够运用相关知识，开展网络安全研究和创新，例如新技术及应用、法律法规、政策文件、标准等； （深化）人工智能安全、量子计算安全等新兴技术研究和创新。
	S02-19-003	能开展网络安全学术交流。
网络安全培训与评价	S02-20-001	能识别和分析网络安全职业培训需求。
	S02-20-002	能根据培训需求设计培训课程，实施网络安全培训，改进所培训的内容； （深化）实战化培训、AI 安全人才培训设计与实施。

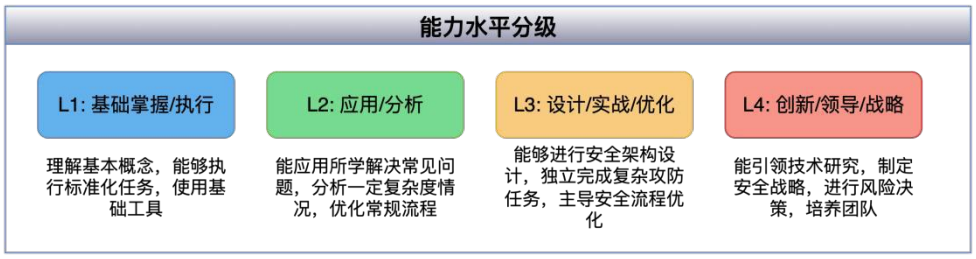
	S02-20-003	能够对被培训人员掌握知识和技能的程度进行评价； （深化）实战能力、人工智能安全技能评价。
AI 安全专业技能（新增）	S-AI01	（新增）能够对 AI 模型和系统进行安全漏洞分析与修复，包括对抗性攻击、数据投毒、模型窃取等）。
	S-AI02	（新增）能够对抗生成性样本并设计相应的防御策略（对抗性机器学习攻防）。
	S-AI03	（新增）能够对 AI 系统进行安全测试与评估（如鲁棒性测试、提示词注入测试、公平性/偏见性测试）。
	S-AI04	（新增）能够进行 AI 伦理合规性审查与风险评估（识别 AI 应用中的伦理和社会风险）。
高级攻防专业技能（新增）	S-PC01	（新增）能够进行 0day 漏洞挖掘与利用（识别并利用未公开漏洞）。
	S-PC02	（新增）能够与红队工具开发进行高级渗透测试（设计并实施复杂渗透场景，开发免杀工具）。
	S-PC03	（新增）能组织和威胁实施狩猎活动（主动在海量数据中发现隐藏威胁）。
	S-PC04	（新增）能够进行 APT 攻击溯源与终点，分析攻击链，识别攻击者身份和目的。
数据安全专业技能（新增）	S-DT01	（新增）能够实施隐私计算技术（例如联邦学习、同态加密、安全多方计算的部署与管理）。
	S-DT02	（新增）能够进行数据流安全审计与分析（追踪不同系统中的数据、初始的流转安全）。
	S-DT03	（新增）能应用数据脱敏/加密工具并进行策略优化（针对复杂业务场景的数据安全防护）。
云安全专业技能（新增）	S-CN01	（新增）能够进行容器安全配置与管理（Docker、Kubernetes 安全队列）。
	S-CN02	（新增）能编写并优化 K8s 安全策略（如 NetworkPolicy、Pod 安全策略）。
	S-CN03	（新增）能集成与优化云安全服务（CSPM、CWPP、CASB 等云安全产品）。
DevSecOps 专业技能（新增）	S-DS01	（新增）能设计并实施 CI/CD 安全自动化（将安全测试、扫描工具集成到 DevOps 流程）。
	S-DS02	（新增）能够实现安全编码规范并进行自动化审查（在代码开发阶段发现并修复安全问题）。
	S-DS03	（新增）能够进行自动化安全测试工具集成与调优（SAST、DAST、IAST 工具的有效运用）。

4.3.3 引入能力水平与量化说明

网络安全能力水平是从业人员知识掌握的深度和技能运用的熟练程度，以及在复杂情况下综合运用知识和技能解决问题的能力。完成一项关键任务，所需知识和技能的掌握都应达到一定的能力水平，是所有知识和技能的衡量标准。

为弥补 GB/T42446-2023 的不足，融合型“新时期中国网络安全人才能力框架”引入分级能力要求，

将人才能力划分为四个递进的层次，为人才评估和培养提供量化标准，使企业能够准确判断人才当前能力的分级阶段，精准规划其向更高层次发展。



网络安全能力水平

L1-L4 的能力水平分级：

L1：基础掌握/执行：理解基本概念，能够执行标准化任务，使用基础工具。

L2：应用/分析：能应用所学常见问题，分析大量复杂度解决情况，优化核心流程。

L3：设计/实战/优化：能够进行安全架构设计，独立完成复杂攻防任务，主导安全流程优化，具备实战经验。

L4：创新/领导/战略：能引领技术研究，制定安全战略，进行风险决策，培养团队，推动行业发展。

4.3.4 新时期任务与相关知识、技能的对应并新增水平分级

融合型“新时期中国网络安全人才能力框架”在 GB/T42446-2023 的 20 个工作任务对应相关知识和技能的基础上，参考并融合国标知识领域与新时期拓展，对新增的 8 个工作任务进行了对应，并深化了已有 20 个工作任务的对应，同时增加了完成任务所需要的知识和技能的能力水平。

序号	工作任务	对应相关知识	对应相关技能	新时期视角技能描述	能力水平
1	网络安全规划与管理	K01-001K01-002,K01-003,K01-004K01-005,K01-006、K02-001、K02-002、K02-003、K02-004、K02-005	S01-001、S01-002、S01-003、S01-004.S02-01-001、S02-01-002、S02-01-003、S02-01-004、S02-01-005、S02-01-006	对应相关知识：K01-001（网络安全概念及发展历程）[L3]K01-004（网络安全法律法规和政策）[L3]K02-003（网络安全风险管理，包含 AI 风险评估方法）[L3]K02-005（网络安全认证认可，包含 AI 安全认证体系）[L2]；对应相关技能：S01-001（沟通与协调）[L3]S02-01-003（组织执行风险管理，能利用 AI 预判安全风险趋势）[L3]S02-01-006（能对网络数据安全、个人信息保护和密码管理等进行规划	L3

				和管理，主题 AI 系统数据安全与治理规划）[L2]	
2	网络数据安全保护	K01-001、K01-002、K01-003、K01-004、K01-005、K01-006K03-001	S01-001、S01-002、S01-003、S01-004、S02-02-001S02-02-002、S02-02-003	对应相关知识：K03-001（数据安全管理和技术，包含数据要素安全流通）[L3]K03-002（个人信息保护管理和技术，包含隐私计算技术）[L2]K-DT01（隐私计算技术原理与应用）[L3]；对应相关技能：S02-02-002（能运用数据安全工具、方法和技术保护数据安全，深度应用隐私计算工具）[L3]S-DT01（能实施隐私计算技术）[L3]S-DT02（能进行数据流安全审计与分析）[L2]	L3
3	个人信息保护	K01-001K01-002,K01-003,K01-004、K01-005,K01-006K03-002	S01-001、S01-002、S01-003S01-004、S02-03-001、S02-03-002、S02-03-003	对应相关知识：K03-002（个人信息保护管理和技术，包含个人信息跨境结算传输合规、匿名化/去标识计算化技术、隐私计算化技术）[L3]；对应相关技能：S02-03-002（能运用个人信息保护工具、方法和技术保护个人信息，深度应用隐私工具）[L3]S02-03-003（能对个人信息保护工作进行符合性审查，区域 AI 模型中个人信息隐私保护审查）[L2]	L3
4	密码技术应用	K01-001、K01-002K01-003K01-004、K01-005、K01-006K09-001	S01-001、S01-002,S01-003.S01-004、S02-04-001、S02-04-002、502-04-003	对应相关知识：K09-001（密码技术、密码产品及服务功能及原理，包含后量子密码、同态加密等隐私相关计算密码技术）[L3]；对应相关技能：S02-04-002（能引发密码保护产品，方法和技术实施密码保护，深度应用计算隐私相关密码技术）[L3]S02-04-003（能对信息系统密码应用安全性进行评估并提出修改建议，得出后量子密码应用评估）[L2]	L3
5	网络安全需求分析	K01-001、K01-002、K01-003、K01-004、K01-005、K01-006K04-001、K06-003K10-0	S01-001、S01-002、S01-003、S01-004、S02-05-001	对应相关知识：K01-002（网络安全管理基本知识）[L2]K04-001（系统建模理论和常用方法，包含云重建系统建模）[L2]K10-001（新应用安全，包含 AI 安全）[L2]包括技能：S01-002（能理解业务，识别网络安全目标组织）[L3]S02-05-001（能够识别网络安全保护对象，并分析其面临的安全风险，	L3

		01,K10-002		涵盖 AI 系统、云突破风险识别）[L3]	
6	网络安全架构设计	K01-001、K01-002、K01-003、K01-004、K01-005、K01-006、K04-002、K04-003、K05-003、K05-006、K10-001、K10-002	S01-001,S01-002、S01-003、S01-004、S02-06-001,502-06-002S02-06-003	对应相关知识：K04-003（安全架构模型及设计方法，包含 AI 系统、云原生、零信任、数据安全架构）[L3]K01-003（网络安全技术基本知识）[L2]；对应相关技能：S02-06-002（能设计网络安全架构，曲面 AI 系统、云架构等安全架构设计）[L3]S02-06-001（能理解网络安全需求）[L3]	L3
7	网络安全开发	K01-001、K01-002、K01-003、K01-004、K01-005、K01-006、K04-002K05-001、K05-002、K05-003、K05-004K10-001K10-002	S01-001,S01-002、S01-003.S01-004,S02-07-001S02-07-002、S02-07-003	对应相关知识：K05-001（安全开发，包含 DevSecOps 流程）[L3]K10-001（新型应用安全，包含 AI 应用安全开发）[L2]；对应相关技能：S02-07-001（能用特定语言进行安全编码，涵盖 DevSecOps 实践）[L3]S-DS01（能设计并实施 CI/CD 简化安全自动化）[L2]S-DS02（能落地安全编码规范并进行自动化审查）[L3]	L3
8	供应链安全管理	K01-001、K01-002、K01-003、K01-004、K01-005、K01-006K02-001、K10-001、K10-002	S01-001,S01-002,S01-003S01-004,S02-08-001,S02-08-002S02-08-003	对应相关知识：K02-001（供应链安全管理，包含 SBOM 管理）[L3]；对应相关技能：S02-08-001（能识别供应链安全风险，覆盖 SBOM 分析）[L3]S02-08-002（能实施供应链安全保护，涵盖开源组件风险识别）[L2]	L3
9	网络安全集成实施	K01-001、K01-002、K01-003、K01-004、K01-005、K01-006、K05-002、K05-003K05-004、K10-001、	S01-001S01-002、S01-003、S01-004、S02-09-001,502-09-002、S02-09-003	对应相关知识：K06-003（网络安全产品功能及原理，包含 XDR、SOAR 原理）[L2]；对应相关技能：S02-09-001（能完成网络安全及信息化产品、配置、调试及设置，涵盖 XDR、SOAR 集成）[L3]	L3

		K10-002			
10	网络安全运输维护	K01-001、K01-002K01-003、K01-004、K01-005、K01-006K05-003、K05-006K06-001、K06-002.K06-003、K06-004、K06-005K06-006K07-001K07-002,K10-001 K10-002	S01-001、S01-002、S01-003、S01-004、S02-10-001、SO2-10-002、502-10-003、S02-10-004	对应相关知识：K06-004（操作系统安全原理及使用，包含容器、K8s 安全）[L2]K06-006（数据库安全技术及使用，包含大数据平台安全）[L2]；对应相关技能：S02-10-002（能维护操作系统、服务器、仓储设备及终端设备等的安全运行，天线容器、K8s 运维）[L3]S02-10-004（能完成数据库系统管理、维护和安全防护等，涵盖大数据平台运维）[L2]	L3
11	网络安全监测与分析	K01-001K01-002、K01-003、K01-004、K01-005、K01-006、K02-002、K05-003K05-005、K05-006K06-002,K06-003、K07-001、K07-002、K10-001、K10-002	S01-001,S01-002,S01-003.S01-004,S02-11-001、S02-11-002S02-11-003	对应相关知识：K07-001（网络安全监测方法和技术，包含威胁狩猎）[L3]K07-002（网络安全分析方法和技术，包含安全分析中应用的机器学习）[L2]相关技能：S02-11-003（能使用各类方法和工具进行网络安全监控驱动分析、威胁狩猎、人工智能监测）[L3]S-PC03（能组织和实施威胁狩猎活动）[L3]	L3
12	网络安全事故管理	K01-001、K01-002、K01-003、K01-004、K01-005、K01-006、K02-002、K05-003、K05-005、K05-006、K06-001、K07-001、	S01-001、S01-002、S01-003S01-004、S02-12-001、S02-12-002、S02-12-003.S02-12-004S02-12-005	对应相关知识：K02-002（管理应急方法和技术，包含自动化应急响应）[L3]K05-006（网络攻防技术，包含红蓝对抗策略）[L3]K08-001（调查取证方法和技术,包含 APT 攻击取证）[L2]；对应相关技能：S02-12-004（能利用常见安全技术手段进行应对，包含 AI 自动化应急响应）[L3]S02-12-005（能进行 APT 攻击溯源与漏洞）[L3]	L3

		K07-002、K08-001、K10-001、K10-002			
13	网络安全审计	K01-001K01-002、K01-003、K01-004、K01-005、K01-006K02-004K10-001,K10-002	S01-001、S01-002、S01-003、S01-004、S02-15-001S02-15-002、S02-15-003	对应相关知识：K02-004（网络安全审计方法和技术，包含自动化审计）[L2]K10-001（新技术新安全，包含人工智能系统审计）[L2]相关技能：S02-15-002（能管理、组织和实施审计，覆盖自动化审计）[L3]S02-15-003（能做出审计结论，构建 AI 系统审计）[L2]应答自动化任务能力水平应用：L3	L3
14	网络安全测试	K01-001、K01-002、K01-003、K01-004K01-005、K01-006、K02-003、K05-003、K05-004、K05-005、K07-002、K10-001K10-002	S01-001、S01-002、S01-003、S01-004、S02-13-001,S02-13-002	对应相关知识：K05-004（安全测试、评估方法，包含 AI 系统安全测试）[L3]K05-005（渗透测试方法和技术，包含高级渗透测试）[L3]；对应相关技能：S02-13-001（能完成脆弱性测试和渗透性测试，平面 AI 系统安全测试，高级渗透测试）[L3]	L3
15	网络安全评估	K01-001,K01-002,K01-003,K01-004、K01-005.K01-006、K02-003,K05-003,K05-005,K07-002,K10-001,K10-002	S01-001、S01-002、S01-003、S01-004、S02-14-001S02-14-002、S02-14-003	对应相关知识：K02-003（网络安全风险管理，包含 AI 风险评估）[L3]K10-001（全新安全，包含云重建环境安全）[L2]K02-001（供应链安全管理）[L2]相关技能：S02-14-002（能使用各类评估相关工具和方法分析并评估安全风险，覆盖 AI 系统、云应用风险评估）[L3]	L3
16	网络安全认证	K01-001,K01-002,K01-003,K01-004K01-005,K01-006,K02-003、K02-005、K10-001K10-002	S01-001S01-002、S01-003、S01-004、S02-16-001,S02-16-002,S02-16-003	对应相关知识：K02-005（网络安全认证认可，数据安全认证、AI 安全认证体系）[L2]相关技能：S02-16-003（能依据审核计划开展审核活动，发现不符合项并编制审核报告，概览数据安全认证、AI 安全认证）[L3]	L3

17	电子数据取证	K01-001、K01-002、K01-003、K01-004、K01-005K01-006K08-001K10-001、K10-002	S01-001501-002、S01-003、S01-004、S02-17-001、S02-17-002、S02-17-003、S02-17-004	对应相关知识：K08-001（调查取证方法和技术，包含云环境取证、AI 系统取证）[L3]K05-006（网络攻防技术，包含 APT 攻击原理）[L2]；对应相关技能：S02-17-001（能使用各类取证方法和工具进行调查取证，框架云环境取证、AI 系统取证）[L3]S-PC04（能进行 APT 攻击源与前沿）[L3]	L3
18	网络安全咨询	K01-001、K01-002、K01-003、K01-004K01-005、K01-006K10-001、K10-002	S01-001、S01-002、S01-003、S01-004S02-18-001S02-18-002、S02-18-003	对应相关知识：K10-001（新技术新应用安全，包含人工智能安全）[L3]K03-001（数据安全管理和技术，包含数据需求安全）[L2]K10-002（特定行业网络安全知识，包含工业互联网安全）[L2]相关技能：S02-18-001（能帮助用户识别和确定网络安全需求，掌握新兴领域需求识别）[L3]包括任务能力水平：L3	L3
19	网络安全研究	K01-001、K01-002、K01-003、K01-004、K01-005K01-006K10-001,K10-002,K10-003	S01-001、S01-002、S01-003、S01-004、S02-19-001S02-19-002、S02-19-003	对应相关知识：K10-001（新技术新应用安全，包含 AI 安全前沿研究）[L4]K09-001（密码技术与知识，包含后量子密码）[L3]相关技能：S02-19-002（能运用相关知识，开展网络安全研究和创新，论坛新兴技术研究）[L4]S-AI01（能对 AI 模型和系统应对安全漏洞分析与修复）[L3]任务能力水平：L4	L4
20	网络安全培训与评价	K01-001、K01-002K01-003、K01-004、K01-005、K01-006,K10-001、K10-002、K10-004	S01-001S01-002,S01-003、S01-004、S02-20-001S02-20-002、S02-20-003	对应相关知识：K10-003（实战领域相关知识，包含实战攻防理论）[L2]K10-001（新应用安全，包含 AI 安全）[L2]；对应相关技能：S02-20-002（能根据培训需求培训课程，实施网络安全培训，内容实战化、AI 安全培训设计）[L3]S02-20-003（能对被培训人员掌握知识和技能的程度进行评价，主题实战能力、AI 安全技能评价）[L3]	L3
21	AI 模型安全评估与分析（新增）	KT-AI01	S-AI01、S-AI03	S-AI01（能对 AI 模型和系统进行安全漏洞分析与修复）[L3]S-AI03（能对 AI 系统进行安全测试与评估）[L3]	L3
22	大模型应	KT-AI02	S-AI03、S02-07-001	S-AI03（能对 AI 系统进行安全测试与	L3

	用安全开发与测试（新增）			评估）[L3]S02-07-001（能用特定语言进行安全编码）[L3]	
23	组织和实施威胁狩猎活动（新增）	KT-PC01	S-PC03、S-PC06、S02-11-003	S-PC03（能组织和实施威胁狩猎活动）[L3]S-PC06（能进行威胁情报分析与应用）[L3]S02-11-003（能使用各类方法和工具进行网络安全监控分析）[L3]	L3
24	开展高强度红蓝对抗演练（新增）	KT-PC02	S-PC02、S02-12-005	S-PC02（能进行高级渗透测试与红队工具开发）[L4]S02-12-005（能进行抽样调查预案开展演练）[L3]	L4
25	进行 APT 攻击溯源与终点（新增）	KT-PC03	S-PC04、S02-17-001	S-PC04（能进行 APT 攻击溯源与精准）[L4]S02-17-001（能使用主流取证方法和工具进行调查取证）[L3]	L4
26	0day 漏洞挖掘与利用（新增）	KT-PC04	S-PC01、S02-13-001	S-PC01（能进行 0day 漏洞挖掘与利用）[L4]S02-13-001（能完成渗透测试）[L3]	L4
27	数据保障安全流通流程设计与（新增）	KT-DT01	S-DT02、S02-02-002	S-DT02（能进行数据流安全审计与分析）[L3]S02-02-002（能运用数据安全工具保护数据安全）[L3]	L3
28	实施隐私计算技术（新增）	KT-DT02	S-DT01、S02-04-002	S-DT01（能实施隐私计算技术）[L3]S02-04-002（能实施密码保护产品实施密码保护）[L2]	L3

第五章 新时期的网络安全人才治理

企业需要构建系统、高效的网络安全人才治理和管理体系，以赋能企业安全能力，其中人才治理指导管理的方向，管理体系是实施的关键，量化评估是改进持续的基石。本报告将引入 COBIT 治理框架，通过深入探讨企业在新时期落地网络安全人才培养的具体方法论和实践路径，探讨人才治理的核心理念、人才梯队和发展策略，并通过成熟度提供可落地、可操作的指导，帮助企业建立保障网络安全人才培养和能力建设持续有效提升的治理机制，并提供量化评估方法。

5.1 新时期网络安全人才治理与管理体系

网络安全人才治理应保障网络安全人才治理目标与企业战略对齐，并且是一个系统性、长期性工程。本报告基于 COBIT 框架，构建结构性、可规范性、与业务目标高度一致的网络安全人才治理与管理体系，并与 IT 治理一起纳入企业整体治理，确保网络安全人才能够转化为实际的业务价值。

网络安全人才治理与管理体系

5.1.1 新时期网络安全人才治理的核心原则

安全牛基于 COBIT 理论，提出网络安全人才治理应保障网络安全人才治理目标与企业战略对齐。网络安全人才治理原则包括：

- 满足业务需求：确保网络安全人才发展计划直接响应高层管理者（CSO/CDO）、业务部门、合规部门乃至最终用户的需求。人才培养应以支持业务发展、降低核心风险为导向。

- 能力覆盖：网络安全人才能力应覆盖企业内部所有与网络安全相关或受其影响的职能和流程，包括 IT、研发、业务部门等。

- 治理与管理分离：明确网络安全人才治理（制定战略、设定目标、监督绩效）与管理（执行日常人才培养、录用、考核）的职责边界，避免权责不清。

- 动态治理体系：网络安全人才治理体系必须适应网络安全威胁和技术（特别是数据安全、主动防御、实战攻防、人工智能等）的快速演进，需要持续评估、调整和优化。

- 架构定制：网络安全人才治理体系应根据企业规模、行业特点和战略目标进行定制化，而不是一刀切。

5.1.2 新时期网络安全人才治理体系

安全牛基于 COBIT 理论，将网络安全人才治理体系分为治理域和管理域两个域，不同域的活动包括不同的责任主体和核心职责：

1）网络安全人才的治理

网络安全人才治理的责任主体应为董事会、高层管理（CIO、CSO、CDO）、网络安全战略委员会等。

核心职责包括：

- 确定人才治理框架：制定网络安全人才战略、政策和核心职责分配（如明确维护 CSO/CDO 在人才发展中的领导作用）。

- 预定人才价值实现：监督人才发展项目是否交付预期（如降低安全事件数量、提升合规性），并根据“网络安全人才与能力影响量化指标体系”评估 ROI。

- 确保人才风险优化：评估因人才问题、技能不足或 AI 技术风险带来的人才风险，并批准相应的风险缓解策略。

- 确保人才资源优化：优化网络安全人力资源配置，确保人才与关键安全需求能力匹配。

运作方式：通过定期战略会议、审查季度/年度报告、批准重大投资和政策。

2）网络安全人才的管理

网络安全人才的管理责任主体应为 CSO、安全部门负责人、HR 部门安全人才负责人、各业务部门安全负责人。

核心职责包括：

- 人才战略规划与组织

  - 管理网络安全人才战略：将高层治理目标转化为具体的人才发展战略，明确“T 型人才”在各工作类别中的应用。

  - 设计网络安全与组织结构：定义具体的工作角色（如 AI 安全工程师、威胁狩猎专家），建立语音的报表关系和职业发展路径。

  - 规划网络安全人才发展项目：制定基础 L1-L4 各阶段的培训计划、实战演练方案。

- 人才招聘与队伍建设

  - 获取网络安全人才：执行招聘策略（内培外引），高效选拔并引导新员工团队。

  - 发展网络安全能力：实施分层定制化培训、导师制、轮岗制，开展人工智能安全和实战化培训。

  - 实施人才保留计划：落地职业通道、绩效激励、员工关怀等。

- 人才交付与支持

  - 有效利用网络安全人才：将具备所需技能的人才部署到关键安全职能和项目中（如 AI 安全项目、应急响应团队）。

  - 提供人才支持与资源：为安全人员提供必要的工具、平台（如安全靶场）和持续学习资源。

- 人才监控与评估

  - 监控网络安全人才能力：实施“网络安全人才与影响量化指标体系”，持续追踪人才能力提升和项目贡献。

  - 评估人才发展项目：定期评估培训、实战演练等项目的有效性，识别改进空间。

  - 评估人才成熟度：利用“企业网络安全应用人才管理成熟度模型”定期评估组织整体和各团队的人才能力成熟度。

5.2 新时期网络安全人才管理成熟度模型

基于 CMMI（能力成熟度模型集成）框架的核心思想，安全牛设计了递进等级的人才管理成熟度框架，从过程管理的角度，系统性地描述企业网络安全人才管理能力的演进，实现网络安全人才管理过程的可度量、可优化，为企业提供评估自身人才管理现状的标尺，从无序到卓越的系统化改进提供一条可实施的路径。

人才管理成熟度框架

1）核心设计理念：

- 过程导向：该管理成熟度框架重点关注人才管理的过程，强调人才的选拔、培养、评估和激励等活动，都应被视为可重复、可度量、可优化的过程。

- 分级演进：该成熟度框架将管理能力分为 5 个等级，每个等级代表一个可达到的成熟状态。企业可以清晰地看到从一个等级提升到下一个等级所需的具体条件和行动，实现了循序渐进地改进。

- 价值驱动：成熟度框架的每个等级的提升，意味着人才管理过程更加可控、可预测、可量化，最终转化为更强的企业安全能力和更高的商业价值。

2）框架维度要素描述：

成熟度框架核心聚焦于人才能力与发展管理，涵盖了企业在人才方面的所有核心活动。包括五大管理维度：

- 人才规划与需求设计维度：包括人才岗位需求分析、能力需求定义、人才梯队规划。

- 人才能力建设与培养维度：包括人才培训体系设计、实战化训练、导师制、轮岗机制。
- 人才绩效评估与激励维度：包括人才考核体系建立、能力水平评估、绩效与薪酬挂钩、非物质激励。
- 人才职业发展与保留维度：包括人才职业路径设计、人才流失分析、内部转岗机制。
- 人才治理与文化维度：包括高层参与、人才战略与业务对齐。

3）成熟度框架各阶段特征描述

基于人才管理成熟度框架，各阶段人才能力与发展管理特点如下：

L1 初始级

初始级阶段，企业的人才管理过程是反应式的，安全人才的招聘、培养和管理更多依赖个人经验和临时决策。

各维度特征：

人才规划与需求：缺乏系统性的岗位需求分析，没有清晰的人才需求和能力地图，人才招聘依赖模糊的经验。

能力建设与培养：培训通常是临时性的，缺乏系统化的课程设计。没有明确的实战化训练，员工能力提升主要靠个人摸索。

绩效评估与激励：绩效评估标准不统一，缺乏与能力水平挂钩的考核体系，激励机制随机性强。

职业发展与保留：没有正式的职业发展路径，员工流失率高，缺乏有效的人才保留策略。

治理与文化：高层对安全人才的战略价值认知不足，人才管理与企业战略脱节。安全文化薄弱。

L2 已管理级

已管理级阶段，人才管理过程有规划，但执行缺乏标准化。企业开始意识到人才管理问题，并采取一些初步的管理措施，但尚未形成统一的、可复制的流程。

各维度特征：

人才规划与需求：团队开始根据具体项目进行人才需求分析，形成非正式的人才需求，但全企业没有统一标准。

能力建设与培养：制定了基础的培训计划，但课程体系不完善。开始尝试一些实战训练（如参加外

部攻防演练），但缺乏系统性的复盘和改进。

绩效评估与激励：建立了初步的绩效考核流程，但考核标准仍带有主观性。开始提供一些物质激励，但与能力提升的关联不强。

职业发展与保留：部分团队开始探索为员工提供职业发展方向，但缺乏正式的晋升通道。

治理与文化：安全负责人开始向高层汇报人才问题，但人才战略尚未上升到企业战略层面。

L3 已定义级

已定义级阶段，人才管理过程被清晰地定义、文档化和标准化，并在整个企业范围内统一执行。这是企业告别混乱、实现体系化建设的关键阶段。

各维度特征：

人才规划与需求：建立了统一的人才能力需求体系，所有岗位的知识、技能、能力水平（L1-L4）被清晰定义和文档化。

能力建设与培养：拥有系统化、分层级、定制化的培训体系，课程与能力需求紧密挂钩。建立了常态化的实战靶场和攻防演练复盘机制。导师制和轮岗制被正式纳入人才发展流程。

绩效评估与激励：建立了基于能力水平（L1-L4）的考核体系，评估标准客观且透明。绩效与晋升、薪酬调整、专项奖励等激励措施实现制度化。

职业发展与保留：设计了多维度的职业发展通道（技术专家、管理、项目管理），并有清晰的晋升标准。人才流失分析成为常态。

治理与文化：安全人才战略已成为企业整体战略的一部分，并有专门委员会进行定期审议。安全文化开始内化为企业基因。

L4 量化管理级

在此阶段，已定义的人才管理过程被量化并得到控制。企业能够通过数据和指标，实时监控人才发展情况，并进行数据驱动的决策。

各维度特征：

人才规划与需求：人才需求不仅被定义，还与业务绩效、安全风险指标进行量化关联。

能力建设与培养：培训效果通过量化指标进行精确评估（如 MTTR 改进率、攻防演练排名、漏洞修复率等），并根据数据反馈动态调整课程内容。

绩效评估与激励：考核体系与“网络安全人才与能力影响量化指标体系”高度联动，实现了个人贡献与整体安全效能的量化关联。人才评估不再依赖主观判断，而是基于客观数据。

职业发展与保留：能够通过数据分析预测人才流失风险，并提前进行干预。

治理与文化：高层决策基于量化数据进行，人才投入的 ROI 清晰可见，人才管理成为企业重要的业务指标。

L5 优化级

在此阶段，企业的人才管理不仅可量化，而且能够专注于持续改进和创新。人才管理成为企业核心竞争力的源泉，并能引领行业发展。

各维度特征：

人才规划与需求：能够通过前瞻性研究和数据分析，预判未来 3～5 年的新兴人才需求，并提前进行规划。

能力建设与培养：建立了自我学习、自我进化的培训体系。能够利用 AI 工具进行个性化学习路径推荐、智能评估，实现培训效率的最优化。

绩效评估与激励：激励机制具备高度的创新性和适应性，能够吸引和留住顶尖的“战略型”人才。

职业发展与保留：人才发展路径能够根据行业趋势和个人潜力进行动态调整，并能为行业输出标准和最佳实践。

治理与文化：安全文化已成为企业的核心基因，人才管理体系能够自主学习和进化，成为行业人才发展的“黄埔军校”。

5.3 新时期网络安全人才发展策略

构建适应新时期挑战的网络安全人才梯队，需要从战略层面进行规划，并落实到招聘、培养、发展和激励的各个层面，并构建清晰的职业发展路径，这是激励网络安全人才持续学习、提升，并最终实现个人价值的关键。

人才发展路径

1）单点领域人才

单点领域人才主要集中于特定的技术领域，知识面相对狭窄，缺乏对安全全局的理解，往往依赖标准化操作手册。解决特定的、重复性的安全问题。

典型岗位：安全运维员、漏洞扫描员、安全设备配置员。

发展路径建议：

夯实“一横”基础：主动学习网络安全基础知识（如 TCP/IP、操作系统原理）、国内法律法规（《网络安全法》等保障基本要求）、安全管理流程、行业通用安全标准，通过内部培训和 CISP、CompTIASecurity+等基础认证来拓宽知识面。

专注深耕“一竖”：聚焦一个核心技术领域（如 Web 安全、网络安全），深入学习其原理和技术细节，积极参与实战项目和基础安全竞赛，争取在该领域达到 L3 的专业深度。

2）高级 T 型人才

专业领域已经达到高级水平，能够独立解决复杂问题，引领技术方向。同时，具备宽广的通用安全

知识面，理解安全治理、合规要求、业务流程，并具备良好的沟通协作能力。能够从管理的角度看待技术问题。

典型岗位：高级渗透测试专家、资深安全架构师、高级数据安全工程师、威胁狩猎专家、资深安全开发工程师。

发展路径建议：

- 持续深耕“一竖”：参与高难度安全项目，挑战复杂技术难题，研究漏洞 0day，掌握自动化工具开发能力。

- 全面拓宽“一横”：深入学习风险管理、安全忧虑、安全文化建设等管理知识；主动了解企业业务流程和 IT 架构；参与跨部门协作，提升项目管理和沟通协调能力。

- 与实践结合：将“一横”的广度与“一纵”的深度结合，尝试将技术方案用业务语言表达，将技术发现转化为业务风险洞察。

3）多维π型复合人才

核心安全领域（如实战攻防）达到专家水平，并具备较宽的通用安全知识面。能够独立承担复杂任务，但跨领域间的深度融合和战略影响力提升空间。多维 T 型人才不仅在原有的 T 型“一竖”上持续精进，还能发展出甚至个第三深度技能（如从“实战攻防”专家发展为同时具备“AI 安全”和“数据隐私计算”深度的“π型复合人才”或“梳子型人才”）。同时，具备卓越的领导力、战略思维和跨部门协调能力，能够从业务方面思考安全，推动安全从业务创新成为业务创新的一部分。

典型岗位：企业安全架构师、AI 安全科学家、安全研发总监。

发展路径建议：

- 发展第二条/第三条“一竖”：以第一条“一竖”为基础，选择相邻或互补的新兴领域（如 AI 安全专家发展数据安全能力），进行深度学习和实践。积极参与跨领域项目，如 AI 安全产品的设计与开发、隐私方案计算的落地。

- 提升领导力与战略思维：参与高层安全决策，承担团队管理职责，主导大型复杂安全项目。通过外部高端管理培训，提升对行业趋势的判断力、战略规划和资源整合能力。

- 构建个人品牌与行业影响力：参与行业标准制定、在行业会议上分享经验、发表高水平研究成果、积极贡献开源社区，成为行业内的意见领袖。

- 强化人文素养与职业道德：尤其针对高管层和关键基础设施单位，提升职业操守、风险意识和人文素养，确保在复杂利益冲突中做出正确判断。

4）多维π型网络安全领导人才

对于 L4 层的安全领导者人才，尤其是 CSO/安全总监等 L4 创新/治理层人才，除了上述发展路径，还应具备超越技术范围的多维π型领导力，不仅技术过硬，更具备驾驭组织、驱动战略商业领导力，驱动安全战略与业务目标的深度融合，将技术风险转化为可管理的商业战略，并有效影响组织决策。

典型岗位：首席安全官（CSO）、首席数据官（CDO）。

发展路径建议：

- 风险语言的“翻译”能力。技术专家与董事会、业务部门常常存在认知鸿沟，因此安全部门领导者应掌握“风险翻译”能力，将复杂的技术漏洞、攻击事件，转化为董事会和业务部门能理解的商业风险，例如，财务损失、品牌声誉受损的概率、法律责任罚款。具体应能够充分了解安全风险，将安全预算申请与具体业务目标（如市场扩张、云服务上架）的风险控制直接关联。

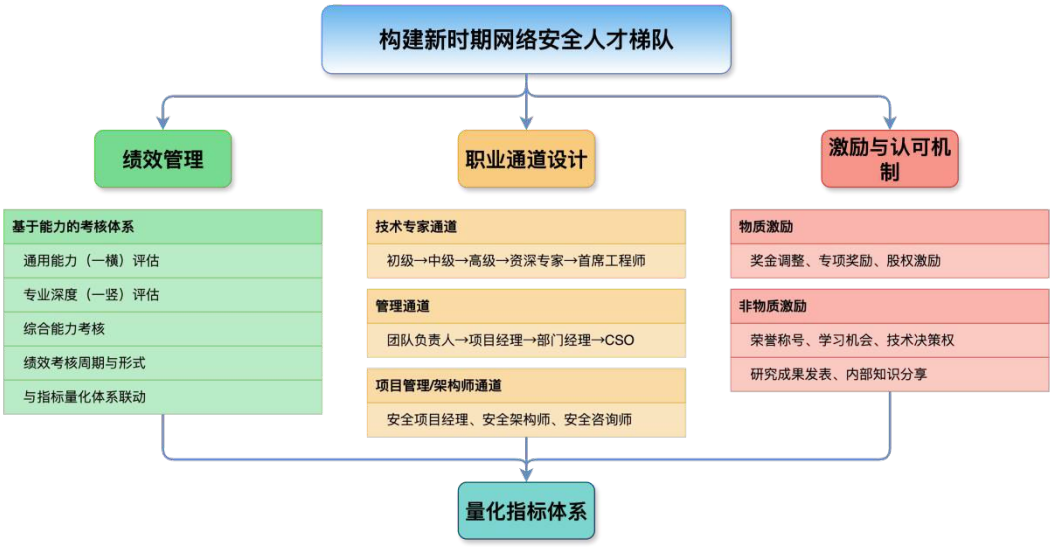
- 跨部门影响力与安全左移推动力。安全部门通常没有对业务、研发部门的直接管辖权，因此安全部门应具备横向影响力，将安全视作“业务加速器”而非“审批阻碍者”，并通过建立信任和提供价值赋能，推动业务部门、研发部门主动落实安全要求，实现“安全左移”。具体应主导 DevSecOps 转型或跨部门数据安全委员会的成立和高效运作，用流程机制确保安全内嵌到业务起点。

- 预算申请与资源整合能力。安全预算往往被视为“成本”，难以争取资源，因此安全部门领导者需掌握“战略预算”能力，能够制定有说服力的安全战略预算，不再仅基于合规要求，而是基于风险资产价值、业务增长预期以及投资回报率（ROI）进行论证。具体应能够清晰定义安全投资的“防御价值”和“创新价值”，并成功整合跨部门资源（如与研发部门共享技术栈、与法务部门协同合规流程）。

- 危机沟通与管理能力。重大安全事件对组织信任和品牌声誉构成致命威胁，因此安全部门领导者应具备在重大安全事件发生时的快速决策能力和专业沟通能力，对内稳定军心、对外管理公众和媒体预期，并负责与监管机构的沟通。具体应领导制定并定期演练“安全危机沟通剧本”，确保在压力下能够保持清晰、透明和有责任感的姿态，将负面影响降至最低。

5.4 构建新时期网络安全人才梯队

企业应建立科学的职业发展体系和绩效管理机制，通过多维度职业通道、多元化激励机制和量化指标体系，打造 T 型、π型复合型安全人才梯队，解决人才招引留用难的问题。



构建新时期网络安全人才梯队

1）绩效管理

- 建立基于能力的考核体系：考核体系应直接与“融合框架”中定义的知识、技能和能力水平（L1-L4）挂钩，实现考核的精准化和标准化，解决“不知道怎么评估”的难题。

  ■ 考核指标：通用能力（“一横”）应评估员工对法律法规、通用安全管理流程、跨部门协作的掌握程度。可通过笔试、案例分析、跨部门协作项目中的表现进行评估。专业深度（“一竖”）应评估特定技术领域的专业技能和实战能力。可通过实操考试（如模拟攻防渗透、AI 模型安全测试）、项目成果评审（如 AI 模型安全评估报告、安全架构设计方案）、代码审查、内部技术分享质量、外部专业认证获取情况等形式进行考核。

  ■ 综合能力考核：考核解决复杂问题、创新思维、团队协作、领导力、风险判断等软技能，重点针对中高级人才。

  ■ 绩效考核周期与形式：采用定期（季度/年度）考核与动态（项目结束/任务完成）考核相结合的方式。绩效考核应结合日常表现、项目贡献、360 度反馈、实战演练成绩，以及所获得的专业认证和员工发表的技术成果。

  ■ 与指标量化体系联动：将员工个人绩效与本报告后续章节的“网络安全人才与能力影响量化指标体系”中的部分指标（如 MTTD/MTTR 改进、漏洞修复率、AI 模型缺陷表现、攻防演练排名等）挂钩，实现贡献个人与整体安全诚信的量化关联，提高核查的核查性和说服力，预防“陷入困境比不响”的痛点。

- 设计多维度的职业通道：

■ 技术专家通道：为专注技术深度、热衷钻研的员工提供清晰的晋升路径，如：初级工程师→中级工程师→高级工程师→资深专家→首席工程师/安全科学家等技术职级，鼓励员工在“一竖”上不断精进，甚至发展多条“一竖”成为“π型”复合型人才。

■ 管理通道：为具备领导潜力的员工提供晋升路径，如：团队负责人→项目经理→部门经理/总监→CSO 等管理职级，该通道注重领导力组织、协调、战略规划和资源管理能力的培养。

■ 项目管理/架构师通道：为具备项目承担、方案设计、跨职能协调能力的员工提供专门通道，如安全项目经理、安全架构师、安全咨询师等。

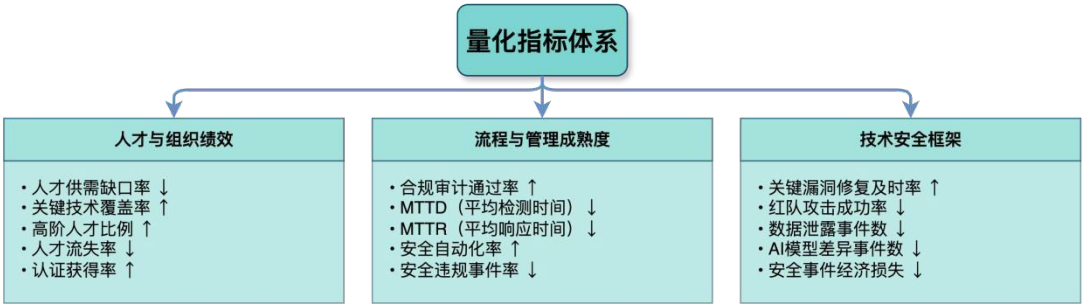
● 激励与认可机制：

■ 物质激励：除了常规奖金调整和奖金外，可设立专项奖励，如安全漏洞挖掘奖金、优秀攻防演练团队奖金、重点项目突破奖金，甚至对核心人才实施股权激励或选项计划，与绩效考核结果紧密结合。

■ 非物质激励：争夺荣誉（如“安全之星”“攻防先锋”“技术创新奖”）、提供高价值学习机会（顶尖行业峰会、高端培训）、赋予更大的技术决策权和创新空间、支持公开发表研究成果、组织内部知识分享和交流活动。这些措施激励措施有助于提升人才的成就感和归属感，有效解决“人才招引留用难”的问题。

2）量化指标

量化指标体系是衡量人才投入的关键，应将抽象的能力提升转化为可计量的绩效，为高层决策和持续改进提供数据支撑。指标体系可以从三个维度全面评估人才和能力的价值：



量化指标体系

● 人才与组织绩效：保障人才队伍规模、结构、能力水平和稳定性的安全。

● 流程与管理成熟度：评估安全管理流程的效率、标准化和自动化水平。

- 技术安全框架：反思企业实际的安全防护效果和风险水平。

核心量化指标：人才价值与安全实现（示例）

维度	核心指标	计算方法/意义	趋势判断	关联人才能力
人才与组织能力	人才供需缺口率	（待招聘安全岗位数/目标安全岗位总数）×100%。反映人才数量缺口。	↓（降低）	人力资源规划、人才吸引力
	关键技术覆盖率	（具备某关键技能数量/需求该技能岗位数量）×100%。关键技能如 AI 安全、高级渗透。	↑（提高）	与发展、T 型人才培养
	高阶人才比例	（L3/L4 级别安全人才数/安全人才总数）×100%。反映人才梯队深度。	↑（提高）	职业发展路径、复合型人才培养
	人才流失率	（安全人才离职人数/安全人才平均人数）×100%。反映人才保留能力。	↓（降低）	薪酬福利、职业发展、企业文化
	认证获得率	（持有相关安全认证人数/安全人才总数）×100%。特别是高阶/新兴领域认证。	↑（提高）	学习积极性、培训效果
	关键技术覆盖率	（具备 AI 安全/OT 安全/隐私计算等关键技能人数 / 需求该技能岗位总数）×100%。	↑（提高）	发展、π型人才培养
流程与管理成熟度	合规审计通过率	（合规审计通过次数/总审计次数）×100%。如保审、数据合规审查等。	↑（提高）	治理管理、合规专员能力
	MTTD（平均检测时间）	从安全事件发生到被检测到的平均时间。	↓（降低）	安全运营、威胁狩猎、AI 驱动检测
	MTTR（平均响应时间）	从安全事件检测到完全解决的平均时间。	↓（降低）	应急响应、事件支出、自动化编排
	安全自动化率	（自动化执行的安全任务数/总安全任务数）×100%。	↑（提高）	DevSecOps、安全开发、AI 赋能运营
	安全违规策略率	（违规事件数/检查总数）×100%。反映制度执行力。	↓（降低）	安全治理、管理能力
技术安全前沿	关键漏洞修复及时率	(SLA 内修复的关键漏洞数/总关键漏洞数）×100%。	↑（提高）	漏洞管理、安全运维、修复效率
	红队攻击成功率	红队模拟攻击成功突破防御的比例。	↓（降低）	实战攻防、防御体系素质
	数据泄露事件数	每年/每季度确认的数据泄露事件总数。	↓（降低）	数据安全、隐私保护、AI 数据安全
	AI 模型差异事件数	确认 AI 模型被篡改、投毒或对抗性攻击成功次数。	↓（降低）	AI 安全、模型防御能力
	安全事件经济损失	因安全事件造成的直接和间接的经济损失。	↓（降低）	风险管理、事件影响控制

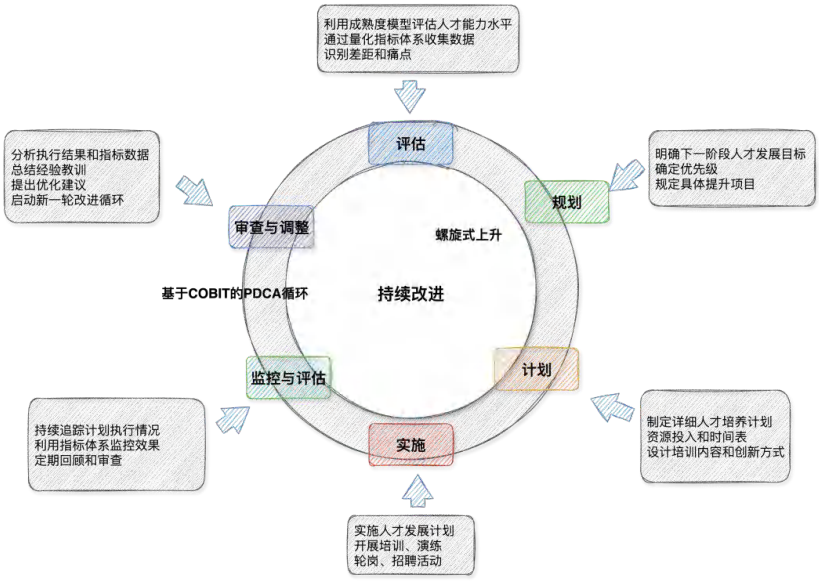
	AI 模型安全事件数	确认发生的 AI 模型安全事件总数（包含对抗攻击、数据投毒、提示词注入等）	↓（降低）	AI 安全、模型防御能力
	红队实战攻击成功率	（红队模拟攻击成功突破核心系统边界或获取指定权限的次数 / 总演练次数）×100%。	↓（降低）	实战攻防、防御体系素质

关键量化指标采集方法论与行业基准参考：

核心指标	数据采集方法论（落地实践）	行业阈值参考（指导性建议）
MTTD（平均检测时间）	工具依赖： 依赖 SIEM/SOC 平台或威胁狩猎工具自动记录**“原始事件发生时间”至“安全事件告警生成时间”**的时间戳。前提是告警规则需覆盖关键资产和业务逻辑。	关键业务： 目标应 ＜15 分钟。一般业务： 目标应 ＜60 分钟。
MTTR（平均响应时间）	工具依赖： 依赖 SOAR 平台或工单系统 自动记录**“安全事件工单开启时间”至“事件彻底解决/关闭时间”**的时间戳。前提是 SOAR 剧本（Playbook）需覆盖主要应急流程。	金融/关键基础设施：目标应 ＜60 分钟。一般企业： 目标应 ＜4 小时。
红队实战攻击成功率	标准化演练规则：必须在安全靶场或高度仿真的环境中进行，以**“突破核心业务系统边界”、“获取最高管理权限”或“泄露指定高价值数据”**为成功标准。成功率应由第三方或独立紫队专家进行公正评估。	成熟企业： 目标应 ＜10%。高安全要求行业（如电力、金融）： 目标应 ＜5%。
安全自动化率	数据采集： 统计每月由 SOAR/DevSecOps 流水线自动处理和处置（无需人工干预）的安全任务总数，与总任务数进行比较。	L3 已定义级目标： ＞30%。L4 量化管理级目标： ＞60%（主要为重复性运营任务）。

5.5 新时期网络安全人才治理的持续改进机制

构建网络安全人才治理的持续改进机制，是实现网络安全人才能力的螺旋式上升的关键。



■ 人才评估：定期利用“企业网络安全应用人才管理成熟度模型”评估当前人才能力水平和发展阶段，并通过“网络安全人才与能力影响量化指标体系”收集数据，识别差距和痛点。

■ 人才规划：制定详细的人才培养、引进、发展计划，包括资源投入、时间表、责任人员，并设计具体的培训内容和创新方式。

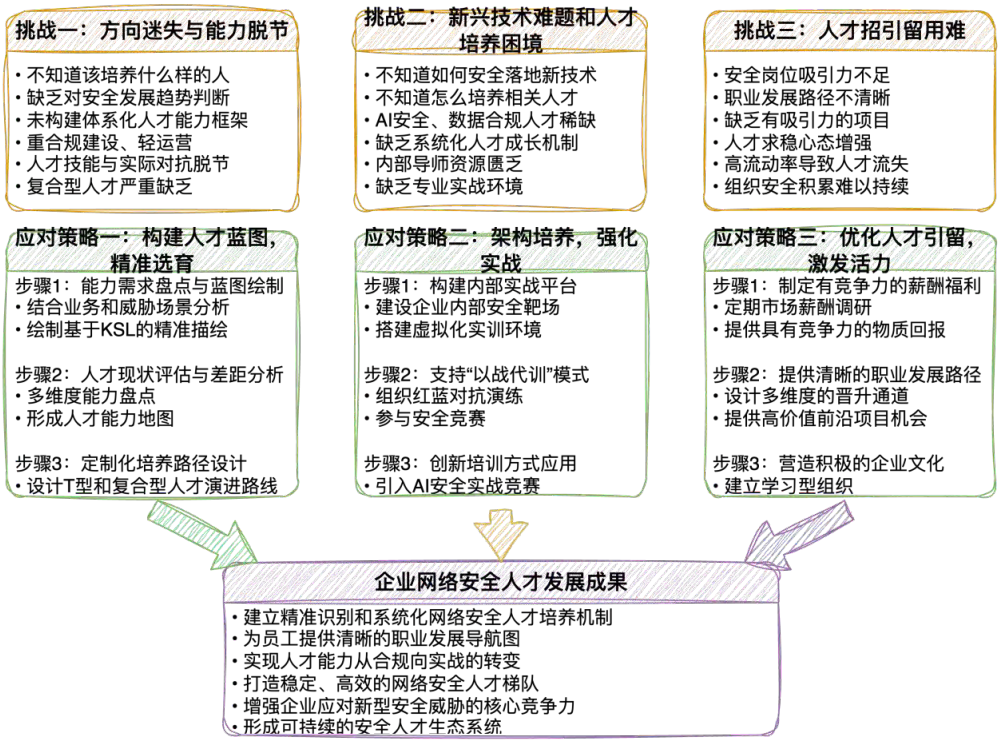
■ 人才建设：实施人才发展计划，开展各项培训、演练、轮岗、招聘活动。

■ 人才评估：持续追踪计划执行情况，利用指标体系监控效果，并定期进行回顾和审查。

■ 评价调整：分析执行结果和指标数据，总结经验教训，识别成功因素和失败原因，提出优化建议直至治理层，启动新一轮的改进循环。

5.6 企业网络安全人才发展常见挑战与应对策略

企业在“新时期”背景下，常常在网络安全人才发展上面临着双重困境：一方面，“不知道该培养什么样的人”和“不知道怎么培养”的困惑普遍存在，导致企业在人才选拔和培养上缺乏方向；另外，人才招引难、留用难的问题存在十分突出，导致企业难以在国内搭建帐篷的人才梯队，主要问题是企业未能建立起一套精准识别和系统网络安全人才培养机制，而员工也缺乏清晰的职业发展“导航图”。核心解决方案是企业需构建精准识别和系统化网络安全人才培养机制，为员工提供清晰的职业发展导航图。



企业网络安全人才发展常见挑战与应对策略

挑战一：方向迷失与能力脱节

企业普遍“不知道该培养什么样的人”，缺乏对未来安全发展趋势的准确判断，未能构建体系化的人才能力框架。这导致招聘模糊，培养目标不清楚。加之长期“重合规建设、轻运营”，安全投入未能转化为实战能力，使在人工智能威胁、APT 攻击、护网演练等实战背景下，具备实战经验、跨领域知识的复合型人才，特别是能够应对人工智能、云原生等新兴技术的专家严重缺乏。人才技能与实际对抗脱节、安全防线形同虚设。

安全牛建议构建人才蓝图，精准选育

运用本报告提出的融合型“新时期中国网络安全人才能力框架”和人才能力蓝图体系，构建企业独有的人才能力地图。

步骤 1：能力需求盘点与蓝图绘画：

参照框架中的“工作类别”“工作角色”和“关键任务”，结合企业自身业务和威胁场景，进行深入的战场分析和能力需求调研。

为每个网络安全岗位（包括 AI 安全工程师、威胁狩猎专家等新兴角色）绘制出基于知识（K）、技能（S）和能力水平（L1-L4）的精准描绘，明确“所需人才”的具体相当于。例如，一个“AI 安全测试

工程师”在“AI 模型鲁棒性测试”任务上需要达到 L3 级别，对应的知识是“对抗性机器学习原理”，技能是“生成对抗样本并运用模型评估工具”。

步骤 2：人才现状评估与差距分析：

利用蓝图体系对现有员工进行能力盘点，通过多维度评估（如：笔试、实操考试、项目成果评审、360 度反馈、实战演练表现）。形成企业内部的“人才能力地图”，清晰识别个人和团队在各能力点上的优势与短板，量化与理想蓝图之间的差距。

步骤 3：定制化培养路径设计：

参照差距分析结果，为个人和设计 T 型人才和复合型人才的演进路线。参照《企业网络安全应用人才管理成熟度模型》和《人才演进路线图》，明确每个阶段的知识、技能、能力水平目标。制定人才发展计划（IDP），包括培训课程、项目任务、轮岗机会等。

挑战二：新兴技术难题和人才培养困境

虽然企业普遍认识到 AI、大数据、数据安全合规等技术的重要性并积极应用，但随之而来的是“不知道如何安全落地、如何自身保障安全，以及如何培养相关人才”的困惑。AI 系统本身的脆弱性（如对抗性攻击、数据投毒）和数据合规的复杂性，对人才提出了法律、技术、管理三位一体的复合要求，但市场上此类人才极度稀缺，现有团队能力匮乏。

企业普遍面临“不知道怎么培养”。大多数企业缺乏系统化的人才成长，机制人才培养路径不明晰，内部导师资源匮乏，缺乏专业实战环境（如安全靶场）和定制化培训内容。这导致安全职业发展框架，人员能力提升缓慢，企业难以形成可持续、有竞争力的人才梯队。

安全牛建议架构培养，强化实战

建立系统化、实战化的培训与发展体系，将安全能力从“合规”转化为“实战”。

步骤 1：构建内部实战平台：

投入资源建设企业内部安全靶场、攻防实验室，或与第三方专业机构合作搭建虚拟化实训环境。提供安全可控、高度仿真的实战演练平台，弥补传统培训缺乏实操性的不足。

步骤 2：支持“以战代训”模式：

常态化组织内部红蓝对抗演练、威胁狩猎行动，将攻防任务 xxx 日常工作。鼓励员工参与国家级/行业级安全竞赛。让安全人员在真实的对抗场景中学习、成长和解决问题，加速经验积累和能力提升。

步骤 3：创新方式培训应用：

引入 AI 安全实战竞赛、校企联合培养项目（如共建 AI 安全实验室）、资深专家导师制作、定期技术沙龙和内部知识分享会。提升培训的高效、高效和实用性，满足新兴技术领域的人才培养需求。

步骤 4：明确能力与激励挂钩：

将实战演练表现、贡献、新技能获取和能力水平（L1-L4）的提升，作为绩效考核和职业回顾的重点项目。激励员工积极参与学习和实践，确保人才培养能够转化为可量化的业务价值。

挑战三：人才招引留用难

企业部分安全岗位吸引力不足、职业发展路径不清晰、缺乏应对项目，以及经济形势波动下人才求稳心态等因素，又导致“人才留不住”，高流动率使企业“人才失血”的困境，持续存在组织的安全积累。

安全牛建议优化人才引留，激发活力

打造威胁人才生态和职业发展环境，吸引和留住高素质网络安全人才。

步骤 1：制定有竞争力的薪酬福利体系：

定期进行市场薪酬调研，结合人才形象和水平，提供具有市场竞争力的物质回报。确保企业在人才争夺战中具备基础的竞争力。

步骤 2：提供清晰的职业发展路径和常见项目：

将本报告的“人才演进路线图”在企业内部装备化，设计多维度的突出通道（技术专家、管理、项目管理），并提供参与 AI 安全、红蓝对抗、数据安全治理等高价值、有前沿项目的机会。让员工看到明确的成长空间和高价值的工作机会，激发内生动力，减少流失。

步骤 3：营造积极的企业文化：

建立学习型组织，鼓励创新、分享、试错，形成开放、引领、互助的企业文化。定期组织团队建设活动，提升团队凝聚力。提升员工归属感和工作满意度，打造员工愿意留下的“软环境”。

步骤 4：加强外部合作，拓展人才来源：

积极与高校建立长期合作关系，开展订单式培养、实习基地建设。参与行业竞赛、安全社区，提前锁定和吸引潜力人才。拓宽人才引进渠道，构建稳定、激励的人才引进。

第六章 新时期网络安全人才设计实践

企业应针对新时期的业务特点，结合“新时期中国网络安全人才框架”分析网络安全人才需求，通过人才治理和人才路径管理，推进高效选才育才管理，培养高级的 T 型人才和多面复合型人才，同时为员工指明明确清晰的成长方向，实现个人与企业的双赢。

6.1 新时期网络安全人才需求设计

基于新时期网络安全人才能力框架可以设计人才能力需求，以应用于：

- 招聘与面试：企业根据上述体系设计人才能力画像，并作为招聘简介，在面试中围绕关键任务展开提问，并设计对应的技能实操测试，根据结果表现评估其能力水平。
- 人才盘点与能力评估：定期对照蓝图体系（如年度绩效评估），对现有员工进行能力盘点，识别个人在知识、技能和能力水平上与短板的优势，形成个人能力地图。
- 人才培养需求分析：根据员工能力评估结果，精准定位培训需求。例如，若某员工的“AI 模型可信赖性”知识水平为 L1，而其岗位要求 L3，则方便安排相应的进阶培训。
- 外包与供应商管理：运用此评估外部安全服务体系的人才能力和服务质量，确保合作方的专业性。

安全牛结合“新时期中国网络安全人才框架”，为企业展示新时期典型网络安全人才需求示例，企业应通过对自身业务进行分析，设计符合自身业务的“T 型人才”能力需求，为适应新时期网络安全人才的培养和发展提供清晰、可操作的指引。

新时期通用典型人才需求示例如下：

1）首席安全官（CSO）

维度	描述
工作类别	网络安全治理与管理类（C01）：专注于企业网络安全与数据安全的战略规划、风险治理与文化建设。
工作角色	首席安全官（CSO）：负责企业网络安全的战略规划、资源整合、风险治理与文化建设，将安全与企业业务发展深度融合。
关键任务	1.网络安全规划和管理：指导、制定、监督和执行网络安全战略规划。 2.制定网络安全政策：提供安全规划、设计、管理等方面的政策法规 3.制定人工智能伦理与治理政策：负责人工智能应用的安全合规与伦理治理，确保人工智

	能技术健康发展。 4.网络安全监督和评价：组织和监督对网络安全的监督和评价。
所需知识（K）&水平（L）	K01-004（网络安全法律法规和政策）[L3] K02-003（网络安全风险管理，包含人工智能风险评估方法）[L3] K02-005（网络安全知识、AI 安全知识体系）[L2] K03-001（数据安全管理和技术，包含数据要素安全流通）[L3] K10-003（实战领域相关知识，安全体系理论）[L3]
所需技能（S）和水平（L）	S01-001（能与组织内部和/或外部沟通与协调）[L3] S01-002（能理解组织业务，识别网络安全目标）[L3] S02-01-001（能制定和实施网络安全规划，区域 AI 安全规划）[L3] S02-01-003（能执行组织风险管理，能利用 AI 预判安全风险趋势）[L3] S02-01-004（能组织建立和运行应急体系）[L3]
整体任务能力水平	L4（创新/领导/战略）：能够从整体进行安全战略规划，平衡企业安全与业务发展，对企业安全和业务发展产生积极影响。

说明：

“一竖”：CSO 的专业深度体现在其对安全治理、风险管理和安全战略规划的精深造诣上。其核心“一竖”并非单一技术，而是对网络安全、数据安全、AI 安全等多个领域的战略风险有深刻洞察和量化评估的能力。他们需要具备将宏观战略转化为可落地实施的策略，并能够基于实战结果和量化指标进行持续优化的专业能力。

“一横”：CSO 的通用广度是其能力的核心体现。应具备强大的业务理解、跨部门沟通协调能力，能够将复杂的技术风险转化为业务语言，向董事会汇报。同时，并需要对国内外的法律法规、AI 伦理标准、行业趋势有全面掌握。这种广度使其能够整合企业内外部资源，推动安全文化建设，并确保安全战略与企业整体发展战略高度一致。

2）DevSecOps 工程师

维度	描述
工作类别	网络安全架构与建设类（C02）：重点在于将安全左移到软件开发生命周期，实现持续安全保障。
工作角色	DevSecOps 工程师：负责将安全能力左移到软件开发全生命周期，实现安全编码、自动化安全测试与集成，保障应用系统从开发到部署的持续安全。
关键任务	1.网络安全开发：负责进行安全编码，并帮助开发团队修复漏洞。 2.KT-DS01－设计并实施 CI/CD 模拟安全自动化：将安全测试、扫描工具集成到 DevOps 流程中。 3.KT-DS02－落地安全编码规范：制定安全编码规范，并通过自动化工具进行审查。 4.KT-DS03－自动化安全测试工具集成与调优：负责 SAST、DAST、IAST 工具的集成、

	部署与规则调优。
所需知识（K）&水平（L）	K05-001（安全开发，包含 DevSecOps 流程与理念）[L3] K05-004（安全测试、评估方法，包含 SAST/DAST/IAST）[L3] K06-004（网络安全原理使用及包含容器、K8s 安全）[L2] K10-001（新技术新应用安全，包含云架构安全）[L2]
所需技能（S）和水平（L）	S02-07-001（能用特定语言进行安全编码，涵盖 DevSecOps 实践）[L3] S-DS01（能设计并实施 CI/CD 模拟安全自动化）[L3] S-DS02（能落地安全编码规范并进行自动化审查）[L3] S-DS03（能进行自动化测试安全工具集成与调优）[L3]
整体任务能力水平	L3（设计/实战/优化）：能够将安全实践内嵌到开发流程，实现持续安全保障。

说明：

“一竖”：DevSecOps 工程师的核心“一竖”是将安全实践融入流水线的自动化能力。这包括自动化安全编码审查、自动化安全测试工具（SAST/DAST/IAST）的集成与调优，以及容器和云原生环境的安全配置与管理。

“一横”：DevSecOps 工程师的通用广度体现在其对软件开发、系统运维护网络安全的全面理解。他们不仅是安全专家，更是能够与开发和运维团队无缝协作的桥梁。他们需要理解业务需求，掌握编程和运维脚本能力，将安全左移的理念在实践中落地。

3）威胁狩猎专家

维度	描述
工作类别	实战攻防与威胁狩猎类（C08）：重点在于主动发现、识别并追踪潜在的、结合传统安全工具检测到的高级威胁。
工作角色	威胁狩猎专家：运用高阶分析技术和主动探索方法，在海量日志、流量和端点数据中主动搜索隐藏的、结合传统安全工具检测到的高级持续性威胁（APT）和异常活动。
关键任务	1.KT-PC01－组织和实施威胁狩猎活动：基于威胁情报和攻击者行为模式（如 ATT&CK 框架），制定威胁狩猎假设和策略。 2.网络安全监测和分析：利用各类工具和方法进行网络安全监控分析，特别是威胁狩猎。 3.KT-PC03－进行 APT 攻击溯源与预警：针对发现的威胁进行深度溯源，识别攻击者身份、目的和攻击链。 4.电子数据取证：利用取证方法和工具，对狩猎发现的威胁进行调查取证。
所需知识（K）&水平（L）	K-PC01（威胁狩猎方法论与实战）[L3] K-PC02(ATT&CK 框架深度理解与应用）[L3] K07-001（网络安全监测方法和技术，包含威胁狩猎）[L3] K08-001（调查取证方法和技术，包含 APT 攻击取证）[L3]
所需技能（S）和水平（L）	S-PC03（能组织和实施威胁狩猎活动）[L3] S-PC04（能进行 APT 攻击溯源与威胁）[L3]

	S02-11-003（能使用人群方法和工具进行网络安全监控分析，头部威胁狩猎）[L3] S02-17-001（能使用人群取证方法和工具进行调查取证，云环境取证、AI 系统取证）[L3]
整体任务能力水平	L3（设计/实战/优化）：能够独立制定和执行威胁狩猎计划，发现并深度溯源隐藏的高级威胁。

说明：

“一竖”：威胁狩猎专家的核心“一竖”是威胁狩猎方法论与实践和 APT 攻击溯源与归因。其深度体现在能够基于威胁情报和攻击者行为模式（如 ATT&CK 框架）制定狩猎假设，并运用大数据分析技术在海量数据中主动发现隐藏的威胁。

“一横”：威胁狩猎专家的通用广度体现在其对网络安全监测分析、应急响应、数字取证和威胁情报管理的全面理解。需要将狩猎结果转化为防御规则和威胁情报，并与防御运营、事件响应团队进行高效协作。

4）IT/OT 融合安全专家：

维度	描述
工作类别	网络安全架构与建设类（C02）/网络安全运营与保障类（C03）
工作角色	IT/OT 融合安全专家：具备 IT 安全和工业控制系统（ICS）/运营技术（OT）双重知识背景，负责设计、实施和运维 IT/OT 融合环境下的安全防护体系。
关键任务	1.网络安全需求分析：识别工控系统、工业网络、生产流程等面临的安全风险。 2.网络安全架构设计：设计 IT/OT 融合环境下的安全架构，包括安全域划分、隔离与边界防护。 3.网络安全运维：维护工控系统、工业网络设备等的安全运行。 4.网络安全测试：能够完成针对工业控制系统的脆弱性测试和渗透测试。 5.网络安全评估：评估工业控制系统与平台的安全风险。
所需知识（K）&水平（L）	K01-003（网络安全技术基本知识）[L3] K04-001（系统建模理论和常用方法，包含工业互联网系统建模）[L3] K10-002（特定行业网络安全知识，包含工业互联网安全，OT/ICS 安全）[L3] K06-004（网络安全原理及使用，包含工控系统网络）[L3]
所需技能（S）和水平（L）	S02-05-001（能识别网络安全保护对象，并分析其面临的安全风险，头部 OT 风险）[L3] S02-06-002（能设计网络安全架构，特别是 IT/OT 融合架构）[L3] S02-10-002（能维护网络安全运行，特别是 OT 系统）[L3] S02-13-001（能完成风险性测试和渗透性测试，特别是 IoT/OT 渗透测试）[L3] S02-14-002（能使用评估相关工具和方法分析并评价安全，特别是 OT 风险）[L3]
整体任务能力水平	L3（设计/实战/优化）：能够独立设计和实施 IT/OT 融合安全防护体系，并进行工控风险系统评估和实战对抗。

说明：

“一竖”：IT/OT 融合安全专家的核心“一竖”是工业控制系统（ICS）/运营技术（OT）安全。其深度体现在对工业协议、工控系统脆弱性，以及 IT/OT 融合环境下特有的攻击面和防御技术的精深掌握。

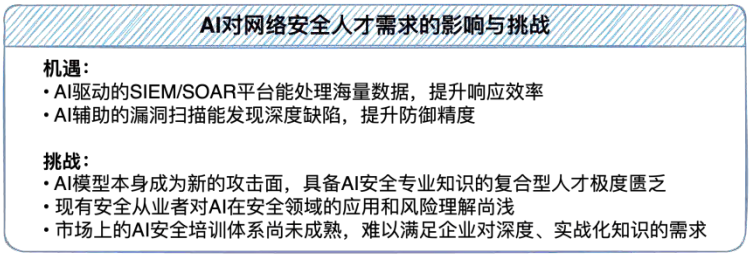
“一横”：IT/OT 融合安全专家的通用广度体现在其对传统 IT 安全架构、网络安全运维，以及工业生产流程的全面理解。他们能够跨越 IT 和 OT 两大领域，将 IT 安全理念和技术应用于工业场景，并与生产运维人员进行有效沟通，共同保障业务连续性。

6.2 AI 时代的网络安全人才设计

AI 技术的飞速发展，正在以突破性的速度构建网络攻防格局。既带来了提升防御效率的巨大机遇，也催生了全新的攻击面和风险。传统安全人才培养模式已无法满足 AI 时代的需求，企业必须加速人才转型。

6.2.1AI 对网络安全人才需求的影响与挑战

AI 技术重塑网络安全格局，企业必须加速人才转型，培养兼具 AI 技术与安全专业知识的复合型人才，实现从传统安全向 AI 安全的人力资源进阶。



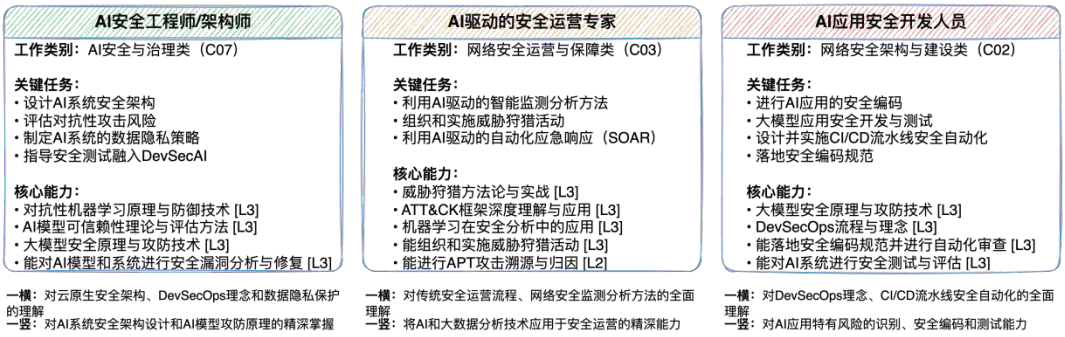
AI 对网络安全人才需求的影响与挑战

AI 技术正被广泛评估威胁检测、漏洞挖掘、安全运营自动化和事件响应中。例如，AI 驱动的 SIEM/SOAR 平台能够处理海量，提升响应效率；AI 辅助的漏洞扫描能够发现深度的缺陷。这极大地提升了安全团队的工作效率和防御精度，同时也对安全人员提出了掌握大数据分析、机器学习训练模型和部署的新要求。

同时，AI 模型本身已成为新的攻击面。当前具备 AI 安全专业知识和能力的复合型人才极度匮乏。大多数现有安全从业者对 AI 在安全领域的应用和风险理解尚浅，而市场上的 AI 安全培训体系尚未成熟，内容可能满足企业对深度、实战化知识的需求。这种人才供给的滞后性，使企业在拥抱 AI 的同时，面临着巨大的安全风险。

6.2.2AI 时代网络安全人才关键能力与技能

为有效应对人工智能带来的机遇与挑战，人工智能时代的网络安全人才须具备以下关键能力与技能：



AI 时代网络安全人才关键角色与能力

1）AI 安全工程师/架构师：

维度	描述
工作类别	AI 安全与治理类（C07）：专门应对 AI 系统自身（模型、数据、算法）的安全风险和治理需求。
工作角色	AI 安全架构师：负责 AI 系统、AI 模型和 AI 应用的全生命周期安全架构设计、评估与优化，确保其符合安全合规要求并具备较高的韧性。
关键任务	1.KT-AI01－设计 AI 系统安全架构:设计符合业务需求和合规标准的 AI 系统安全架构，包括数据输入、模型训练、模型推理、结果输出各阶段的安全控制。 2.KT-AI02－评估对抗性攻击风险：评估 AI 模型对抗性攻击、数据投毒、模型盗窃等风险，并设计相应的防御机制。 3.KT-AI03－制定 AI 系统的数据隐私策略：制定 AI 系统的数据隐私保护策略，包括联邦学习、差分隐私等隐私计算技术的应用。 4.KT-AI04－指导安全测试封装 DevSecAI：指导 AI 开发团队将 AI 安全测试封装 DevSecAI 流程，确保安全左移。
所需知识（K）&水平（L）	K04-003（安全架构模型及设计方法，包含 AI 系统安全架构）[L3] K-AI01（对抗性机器学习原理与防御技术）[L3] K-AI02(AI 模型可信赖性理论与评估方法）[L3] K-AI03（大模型安全原理与攻防技术）[L3] K03-002（个人信息保护管理和技术，隐私技术计算）[L2] K-AI04（第一人工智能安全法律法规与伦理标准）[L2]
所需技能（S）和水平（L）	S02-06-002（能设计网络安全架构，涵盖 AI 系统安全架构）[L3] S-AI01（能对 AI 模型和系统进行安全漏洞分析与修复）[L3] S-AI03（能对 AI 系统进行安全测试与评估）[L3] S-AI04（能对 AI 伦理合规性审查与风险评估）[L2] S-DS01（能设计并实施 CI/CD 模拟安全自动化）[L2]
整体任务能力水平	L3（设计/实战/优化）：能够独立设计和实施复杂的 AI 系统安全架构，并进行风险评估。

说明：

“一竖”：AI 安全架构师的专业深度在于对 AI 系统安全架构设计和 AI 模型攻防原理的精深掌握。他们能够识别 AI 模型在训练、推理过程中的脆弱性，设计并实施对抗性攻击的防御机制。这是其核心技术壁垒。

“一横”：AI 安全架构师的通用广度体现在其对云原生安全架构、DevSecOps 理念和数据隐私保护的理解。他们需要将 AI 安全融入企业的整体技术架构中，并与开发团队、安全团队、数据团队协同工作，确保 AI 系统的安全左移和全生命周期安全。

2）AI 驱动的安全运营专家：

维度	描述
工作类别	网络安全运营与保障类（C03）：专门利用 AI 技术提升安全运营效率、实现自动化响应。
工作角色	AI 驱动的安全运营专家：负责将 AI、大数据技术应用于安全监控、威胁检测和事件响应，通过自动化编排提升运营效率，并进行威胁狩猎。
关键任务	1.网络安全监测和分析：利用 AI 驱动的智能监测分析方法，对目标系统进行安全监测、分析和预警。 2.KT-PC01－组织和实施威胁狩猎活动：基于威胁情报和攻击者行为模式，运用高阶分析技术，主动搜索隐藏威胁。 3.网络安全应急管理：利用 AI 驱动的自动化应急响应（SOAR），对网络威胁和安全事件进行跟踪响应和处置。
所需知识（K）&水平（L）	K07-001（网络安全监测方法和技术，包含威胁狩猎技术）[L3] K07-002（网络安全分析方法和技术，包含机器学习在安全分析中的应用）[L3] K-PC01（威胁狩猎方法论与实战）[L3] K-PC02(ATT&CK 框架深度理解与应用）[L3] K02-002（应急管理方法和技术，包含自动化应急响应 SOAR）[L3]
所需技能（S）&水平（L）	S02-11-003（能使用各类方法和工具进行网络安全监控分析，涵盖 AI 驱动检测）[L3] S-PC03（能组织和实施威胁狩猎活动）[L3] S-PC04（能进行 APT 攻击溯源与归因）[L2] S02-12-004（能利用常见安全技术手段，涵盖 AI 驱动的自动化应急响应 SOAR）[L3]
整体任务能力水平	L3（设计/实战/优化）：能够独立制定并执行 AI 驱动的安全运营和威胁狩猎策略，并能进行自动化应急响应编排。

说明：

“一竖”：AI 驱动的安全运营专家的核心“一竖”是将 AI 和大数据分析技术应用于安全运营的精深能力。这包括利用 AI 进行智能监测分析、自动化应急响应编排（SOAR），以及将威胁情报转化为可执行的威胁狩猎策略。其深度体现在不仅会操作工具，更能基于机器学习原理和高阶分析技术，主动在海

量数据中发现隐藏的威胁，并进行深度溯源和归因。

“一横”：AI 驱动的安全运营专家的通用广度体现在其对传统安全运营流程、网络安全监测分析方法，以及应急管理体系的全面理解。他们需要熟悉各类安全工具（如 SIEM/SOAR/XDR 平台），了解传统威胁情报的生命周期，并具备良好的沟通协调能力，能将 AI 分析结果转化为可执行的防御策略，并与红队、开发团队等进行协同。这种广度使其能够将 AI 工具无缝集成到整体安全体系中，避免形成“技术孤岛”。

3）AI 应用安全开发人员：

维度	描述
工作类别	网络安全架构与建设类（C02）：专注于将安全左移到 AI 应用开发生命周期，实现持续安全保障。
工作角色	AI 应用安全开发人员：负责将 AI 安全能力左移到 AI 应用开发全生命周期，实现安全编码、自动化安全测试与集成，保障应用系统从开发到部署的持续安全。
关键任务	1.网络安全开发：负责进行安全编码，特别是 AI 应用的安全编码，并协助开发团队修复漏洞。 2.KT-AI02-大模型应用安全开发与测试：针对大模型（LLM）应用的特有风险（如提示词注入、数据泄露），进行安全编码、测试和防护。 3.KT-DS01－设计并实施 CI/CD 流水线安全自动化：将 AI 应用的安全测试、扫描工具集成到 CI/CD 流程中。 4.KT-DS02－落地安全编码规范：制定并推行 AI 应用的安全编码规范，并通过自动化工具进行审查。
所需知识（K）&水平（L）	K05-001（安全开发，包含 DevSecOps 流程与理念）[L3] K10-001（新技术新应用安全，包含 AI 应用安全开发）[L2] K-AI03（大模型安全原理与攻防技术）[L3] K05-004（安全测试、评估方法，包含自动化应用安全测试 SAST/DAST）[L3]
所需技能（S）&水平（L）	S02-07-001（能用特定语言进行安全编码，涵盖 DevSecOps 实践）[L3] S-DS01（能设计并实施 CI/CD 流水线安全自动化）[L2] S-DS02（能落地安全编码规范并进行自动化审查）[L3] S-AI03（能对 AI 系统进行安全测试与评估，特别是大模型应用）[L3]
整体任务能力水平	L3（设计/实战/优化）：能够将安全实践内嵌到 AI 应用开发流程，实现持续安全保障。

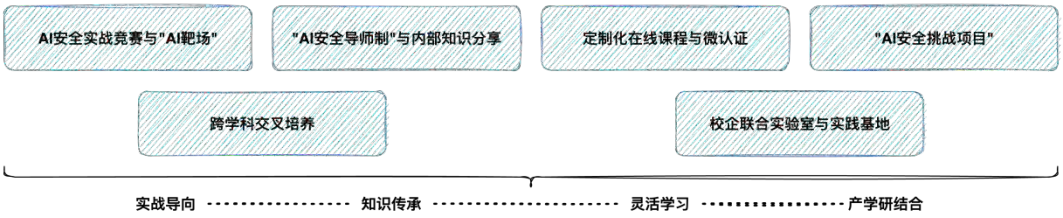
说明：

“一竖”：AI 应用安全开发人员的核心“一竖”是对 AI 应用特有风险的识别、安全编码和测试能力。他们不仅要掌握传统的安全编码规范，更要精通针对大语言模型（LLM）等 AI 应用的特有安全测试方法（如提示词注入、数据泄露测试），并能设计和实施相应的防护机制。这是其在新时期最具价值的专业深度。

“一横”：AI 应用安全开发人员的通用广度体现在其对 DevSecOps 理念、CI/CD 流水线安全自动化以及云原生应用开发安全的全面理解和实践能力。他们需要作为安全专家嵌入到开发团队中，将安全左移的理念在实践中落地，确保安全从 AI 应用的源头被构建，而不是在后期进行修补。他们需要同时具备开发、运维和安全的综合技能，成为弥合安全与工程团队之间鸿沟的桥梁。

6.2.3 打造 AI 时代的网络安全人才培训方式

为快速培养人工智能安全人才，传统的理论教学模式已明显不足。企业必须采用创新、实战导向的培训方式，加速人才能力提升。



打造 AI 时代的网络安全人才培训方式

- AI 安全实战竞赛与“AI 靶场”：组织或参与 AI 安全实战竞赛，如对抗样本攻防赛、大模型提示词注入挑战赛、AI 模型漏洞挖掘赛。建设企业内部“AI 靶场”，模拟 AI 模型攻击与防御场景，让安全在对抗中提升实战人员能力和建设速度。

- “AI 安全导师制”与内部知识分享：邀请行业内极少数具备 AI 安全背景的专家导师，对内部员工进行仿一指导，加速知识和经验的传承。定期组织 AI 安全技术沙龙、案例分享会，促进内部知识传播和共同学习。

- 定制化在线课程与微认证：针对 AI 特定安全模块（如对抗性攻击防御、可信 AI、大模型安全）开发或采购定制化的在线课程和微认证，提供灵活、碎片化的学习路径，方便员工随时随地提升技能。

- 跨学科交叉培养：打破传统专业壁垒，鼓励多学科背景的人才进入人工智能安全领域。提供交叉学科课程，培养具备业务、安全、IT 技术等复合背景的人工智能安全人才。

- 校企联合实验室与实践基地：企业与高校、科研机构共建 AI 安全联合实验室和实训基地，聚焦 AI 安全前沿问题（如大模型安全、对抗性机器学习），提供真实的 AI 攻防环境和数据集。学生和从业者可在实际项目中学习，弥合理论与实践的鸿沟。

注：AI 时代下的人才培养方式不断创新，详情请见安全牛另一份报告《网络安全人才培训指南》。

6.2.4 网络安全角色的‘AI 训练师’转型实践

AI 时代的网络安全人才，必须实现从简单的“AI 操作员”向更具战略性的“AI 训练师”的转型。对于安全领域的专业人士而言，“AI 训练师”的价值体现在能够将自身的实战经验、专业知识和合规要求转化为 AI 模型可学习的“隐性知识”，从而驱动安全防御体系的智能化和自动化。因为安全的效果高度依赖于专家知识的沉淀与转化。安全人员不能仅仅满足于使用 AI 安全产品（AI 操作员），更要成为能够引导、优化和塑造这些 AI 能力的“训练师”。以下将阐述典型网络安全角色向“AI 训练师”的转型路径与实践任务。

以下是几个典型网络安全岗位向“AI 训练师”转型的具体实践：

1）安全分析师 → AI 安全模型训练师角色转型：

核心目标： 将人类专家的威胁分析经验，转化为 AI 模型的“实战直觉”，提升检测的精准度和覆盖面。

实践任务：

- 高质量样本标注： 不只是简单地投喂数据，而是为 AI 模型提供经过专家研判和标注的高质量攻击样本，例如，标注出新型钓鱼邮件中复杂的社工技巧、恶意流量中隐藏的 C2 通信特征。
- 误报/漏报归因与纠正： 当 AI 模型产生误报或漏报时，深入分析其决策逻辑，找出原因，并提供明确的反馈（Feedback Loop）来纠正模型。例如，“这个告警是误报，因为该流量模式属于正常的业务 API 调用”，通过这种方式教会模型区分正常与异常。
- 对抗性样本训练： 主动生成或引入能绕过当前 AI 模型的“对抗性样本”，并将其加入训练集，从而提升模型的鲁棒性，使其能防御更高级的规避攻击。

2）数据安全官 → AI 隐私合规训练师角色转型：

核心目标： 将复杂的法律法规和合规要求，内化为 AI 模型自身的“行为准则”，实现合规的自动化。

实践任务：

- 合规性与安全性标注： 为 AI 大模型提供海量的安全与合规标注数据。例如，标注哪些内容属于个人隐私信息（PII）、哪些属于商业秘密、哪些内容可能涉及歧视或违法，从而训练模型具备内容审查和风险识别能力。
- 安全指令微调（Instruction Tuning）： 设计并微调 AI 模型的指令，使其能够准确理解并执行与

数据安全相关的任务。例如，训练模型在被要求生成一份包含客户信息的报告时，能自动进行数据脱敏或直接拒绝不合规的请求。

- 红队测试与风险场景注入： 模拟恶意用户，通过“提示词注入”等方式测试 AI 模型的数据泄露风险，并将发现的风险场景转化为训练数据，提升模型的防御能力。

3）应急响应专家 → AI 自动化响应编排师角色转型：

核心目标： 将应急响应（IR）的最佳实践和决策逻辑，转化为 AI 驱动的 SOAR 平台可执行的、智能化的响应剧本（Playbook）。

实践任务：

- 响应剧本设计与“训练”：基于 ATT&CK 等框架，设计针对不同攻击场景（如勒索软件、Webshell）的自动化响应流程，并将其“教授”给 SOAR 平台。这不仅仅是拖拽流程，更是对 AI 决策逻辑的优化。
- 决策阈值调优： 设定和优化 AI 在自动化响应中的决策阈值。例如，当 AI 判断某主机的威胁等级达到多少分时，应自动执行“网络隔离”，当达到更高分时，应执行“主机快照并关机”。这种调优需要丰富的实战经验。
- 演练与复盘优化： 通过攻防演练，检验 AI 自动化响应剧本的有效性，并根据演练结果进行复盘，持续优化 AI 的响应策略，使其更快速、更精准。

6.3 主动防御与攻防实战的网络安全人才设计

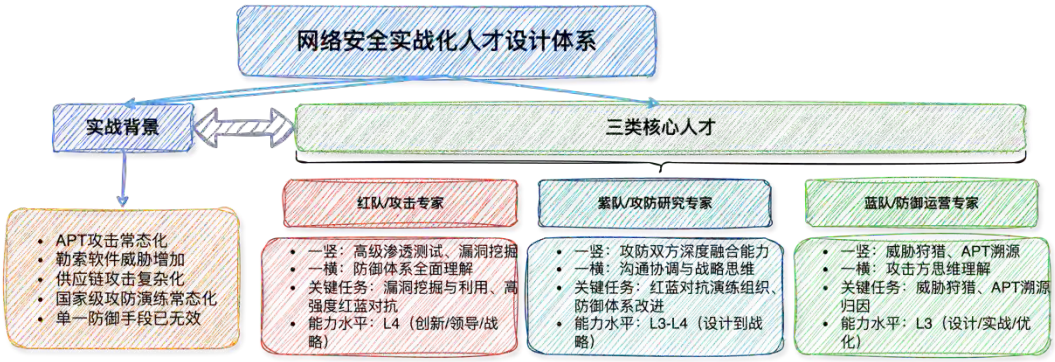
网络安全已进入“实战对抗时代”，高级持续性威胁（APT）、勒索软件等高级威胁极度化，且攻击手段不断演进。这要求人才必须从过去关注合规清单出发，转向培养攻防兼备的综合实战能力，构建真正的“铜墙铁墙”。

6.3.1 网络安全实战化背景与人才需求变化

勒索软件、供应链攻击、APT 攻击等已成为企业面临的头号威胁。这些攻击目标明确、策略持续时间长、破坏性强的特点，单一的防御手段已无法应对。同时，国家层面加强网络安全实战化、常态化、常态化的攻防能力，并通过“护网行动”等高强度演练进行考核。企业必须以人才为导向，提升瞄准真实攻击的能力。

6.3.2 实战型网络安全人才关键能力与技能

网络安全已进入实战对抗时代，组织面临的挑战包括如 APT 攻击常态化、勒索软件威胁增加、供应链攻击复杂化等，组织急需培养攻防兼备的 T 型人才，包括专注于高级渗透测试和漏洞挖掘的红队/攻击专家、专注于威胁狩猎和 APT 溯源的蓝队/防御运营专家、融合攻防双方能力，促进防御体系改进的紫队/攻防研究专家。



网络安全实战化人才设计体系

1）红队/攻击专家：

维度	描述
工作类别	实战攻防与威胁狩猎类（C08）：专注于模拟攻击者，发现和利用系统漏洞，以提升防御方的安全能力。
工作角色	红队/攻击专家：具备高级渗透测试、漏洞利用和攻击链构造能力，能模拟真实攻击者行为，发现防御体系的薄弱环节。
关键任务	1.KT-PC04—漏洞挖掘与利用：发现并利用未公开的安全漏洞（0day 漏洞），用于渗透测试或红蓝对抗。 2.网络安全测试：能够完成脆弱性测试和渗透性测试，特别是高级渗透测试（绕过、免杀）。 3.KT-PC02-开展高强度红蓝对抗演练：作为攻击方，模拟真实攻击场景，测试防御体系的有效性。 4.网络安全开发：具备独立开发攻击工具和自动化脚本的能力。
所需知识（K）&水平（L）	K05-005（渗透测试方法和技术，包含高级渗透测试技术）[L3] K05-006（网络攻防技术，包含红蓝对抗策略与技术）[L3] K-PC04(0day 漏洞挖掘技术）[L4] K01-003（网络安全技术基本知识）[L3]
所需技能（S）&水平（L）	S-PC01（能进行 0day 漏洞挖掘与利用）[L4] S-PC02（能进行高级渗透测试与红队工具开发）[L4] S02-13-001（能完成脆弱性测试和渗透性测试，涵盖高级渗透测试）[L3] S02-07-001（能用特定语言进行安全编码）[L3]
整体任务能力水平	L4（创新/领导/战略）：能够发现并利用 0day 漏洞，主导高强度红蓝对抗演练，并能

	开发创新性攻击工具。

说明：

“一竖”：红队/攻击专家的核心“一竖”是对高级渗透测试、漏洞挖掘和攻击链构造的精深掌握。这包括能够发现并利用未公开的安全漏洞（0day 漏洞），设计和实施复杂的渗透场景，开发免杀工具以绕过防御系统。其深度体现在能够像真正的威胁行为者一样思考和行动，不断突破防御方的防线，从而发现潜在的安全风险和防御盲区。

“一横”：红队专家的通用广度体现在其对防御体系和通用安全知识的全面理解。为了成功绕过防御，他们必须理解蓝队如何进行安全运营、部署了哪些安全工具、如何进行告警分析和应急响应。这种广度使其能够针对性地制定攻击策略，并能在攻击结束后，从防御方视角复盘，提供更具建设性的防御改进建议。

2）蓝队/防御运营专家：

维度	描述
工作类别	网络安全运营与保障类（C03）/实战攻防与威胁狩猎类（C08）：专注于发现、防御和响应高级威胁，确保组织安全韧性。
工作角色	蓝队/防御运营专家：负责日常安全运营，但更侧重于威胁狩猎、事件深度分析与溯源，能将攻防经验转化为防御体系改进。
关键任务	1.KT-PC01－组织和实施威胁狩猎活动：基于威胁情报和攻击者行为模式，主动搜索隐藏威胁。 2.网络安全监测和分析：利用各类工具进行网络安全监控分析，特别是威胁狩猎。 3.KT-PC03－进行 APT 攻击溯源与归因：对发现的威胁进行深度溯源，识别攻击者身份、目的和攻击链。 4.网络安全应急管理：组织和参与针对高强度威胁的应急响应。
所需知识（K）&水平（L）	K-PC01（威胁狩猎方法论与实战）[L3] K-PC02(ATT&CK 框架深度理解与应用）[L3] K07-001（网络安全监测方法和技术，包含威胁狩猎）[L3] K08-001（调查取证方法和技术，包含 APT 攻击取证）[L3] K05-006（网络攻防技术）[L3]
所需技能（S）&水平（L）	S-PC03（能组织和实施威胁狩猎活动）[L3] S-PC04（能进行 APT 攻击溯源与归因）[L3] S-PC06（能进行威胁情报分析与应用）[L3] S02-11-003（能使用各类方法和工具进行网络安全监控分析，涵盖威胁狩猎）[L3] S02-12-004（能利用常见安全技术手段进行威胁抑制、入侵排查、追踪溯源）[L3]
整体任务能力水平	L3（设计/实战/优化）：能够独立制定并执行威胁狩猎计划，发现并深度溯源隐藏的高级威胁。

说明：

“一竖”：蓝队/防御运营专家的核心“一竖”是对威胁狩猎、APT 攻击溯源和事件深度分析的精深能力。这包括能够基于威胁情报主动搜索网络中隐藏的威胁，运用大数据分析技术在海量数据中追踪攻击者的战术、技术和过程（TTPs），并进行深度取证和归因。

“一横”：蓝队专家的通用广度体现在其对攻击方思维和通用安全防御体系的全面理解。为了有效地进行防御，他们必须了解攻击者是如何进行渗透、利用何种漏洞，这使他们能更好地识别异常行为并预测潜在的攻击。此外，他们还需要熟悉应急管理流程、风险评估方法，并能与各部门进行高效沟通，将狩猎结果转化为防御体系的改进措施。

3）紫队/攻防研究专家：

维度	描述
工作类别	实战攻防与威胁狩猎类（C08）：专注于将攻防经验转化为防御体系的改进。
工作角色	紫队/攻防协同专家：具备攻防双方视角，负责促进红队和蓝队之间的协作，将实战发现转化为防御体系的改进和安全策略的优化。
关键任务	1.KT-PC02-开展高强度红蓝对抗演练：作为裁判或协调方，统筹组织和规划红蓝对抗演练，确保演练目标达成。 2.KT-PC05一将实战发现转化为防御体系改进：在演练后，负责复盘总结，分析攻防双方的战术、技术和过程（TTPs），并将结果转化为防御方可执行的优化措施。 3.网络安全应急管理：在应急演练中，促进红队攻击与蓝队防御之间的有效协同。 4.网络安全评估：对攻防演练发现的风险进行量化评估，并提供风险处置建议。
所需知识（K）&水平（L）	K05-006（网络攻防技术，包含红蓝对抗策略与技术）[L4] K-PC02(ATT&CK 框架深度理解与应用）[L3] K10-003（实战领域相关知识，强调攻防演练方法论）[L3] K02-003（网络安全风险管理，包含风险量化评估）[L3]
所需技能（S）&水平（L）	S-PC02（能进行高级渗透测试与红队工具开发）[L3] S-PC03（能组织和实施威胁狩猎活动）[L3] S-PC05（能将实战发现转化为防御体系改进）[L3] S01-001（能与组织内部和/或外部沟通与协调）[L4] S02-01-004（能组织建立和运行应急体系）[L3]
整体任务能力水平	L3（设计/实战/优化）-L4（创新/领导/战略）：能够主导高强度攻防演练的组织，并有效推动安全体系的持续改进。其能力介于 L3 和 L4 之间，取决于其领导力和战略影响力。

说明：

“一竖”：紫队专家的核心“一竖”是攻防双方的深度融合能力。这是一种独特的复合型能力，要求他们既要掌握红队的高级渗透技术，又要理解蓝队的防御运营策略。其深度体现在能够作为“桥梁”，

将红队的攻击发现和蓝队的防御难点进行系统性转化和整合，形成一套完整的防御优化方案。

“一横”：紫队专家的通用广度体现在其卓越的沟通协调能力、项目管理能力和战略思维。他们需要统筹组织和规划红蓝对抗演练，确保演练目标的达成，并在演练后进行深度复盘。他们能够从业务风险的角度量化攻防结果，向高层提供决策支持，并推动安全体系的持续改进。这种广度使其能够将攻防对抗的成果，有效地转化为企业安全能力的螺旋式上升。

6.3.3 锻造攻防兼备的精兵人才的培养方式

为培养实战型人才，必须打破传统的“纸上谈兵”模式，建立以实战为核心的培养体系。

- 国家级/行业级攻防演练的深度参与复盘：积极组织和参与“护网行动”“强网杯”等国家级/行业级攻防演练。更重要的是，演练后必须进行深度复盘（Post-Mortem），分析攻防双方的战术、技术和过程（TTPs），将演练中暴露的防御点转化为人才的重点板，并指导防御体系的改进。

- 企业内部常态化攻防演练与安全靶场建设：投入资源建设企业内部安全靶场（网络靶场），环境模拟真实业务系统和网络环境。定期组织内部红蓝演练对抗训练，让安全人员在安全可控中进行实战对抗，提升发现、防御和响应能力。靶场可根据业务特点定制，如工业控制系统靶场、金融交易系统靶场。

- “以战代训”与轮岗机制：将人才培养 xxx 日常工作。安排安全人员在真实项目中承担攻防任务，如进行内部渗透测试、漏洞挖掘、响应值班。无论安全团队内部轮岗，让防御人员体验攻击视角，攻击了解防御难点，培养攻防人员兼备的 T 型人才。

- 威胁狩猎团队建设与实训：组建专业的威胁狩猎团队，提供大数据分析、机器学习、威胁情报分析等技能培训。通过实际的威胁狩猎项目，团队主动发现和响应潜在威胁的能力，而不是等待同样的培养。

- 网络安全竞赛与 CTF 的深度挖掘：鼓励员工和学生积极参与网络安全（CTF-夺旗），将其作为提升实战能力的重要手段。企业可定期组织内部 CTF 比赛，并根据比赛结果评估人才的实战能力，作为提升和奖励的竞赛能力。

- 安全研究与漏洞挖掘项目：设立内部安全研究项目，鼓励员工进行前沿安全技术研究、0day 漏洞挖掘。提供必要的资源和启发，支持将研究成果转化为员工防御能力或行业贡献。

- 外部专家引入与联合培养：邀请顶尖的红队、威胁狩猎专家进行内部授课专家和实战指导。与专业安全厂商合作，定制化开发实战培训课程和演练方案。

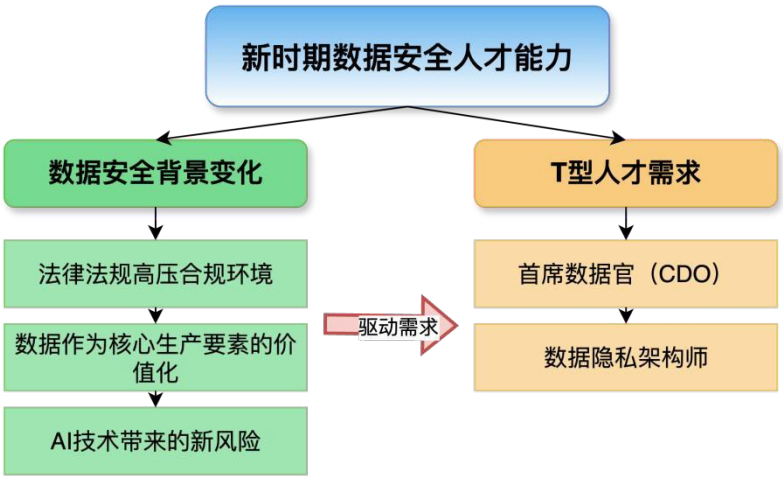
注：AI 时代下的人才培养方式不断创新，详情请见安全牛另一份报告《网络安全人才培训指南》。

6.4 数据安全的网络安全人才设计

在“新时期”背景下，企业对数据安全人才的需求不再局限于传统的运维和合规。因为国家法律法规（如《数据安全法》和《个人信息保护法》）对数据保护提出了更高、更严格的要求。同时，数据被提升为核心“生产要素”，企业迫切需要在保障安全的前提下实现数据的价值化和流通。

6.4.1 数据安全背景与人才需求变化

数据安全的需求变化催生了对传统数据安全人才的转型需求。传统的数据库管理员或安全运维人员，已无法同时应对法律合规、数据价值化、AI 技术和底层技术实现等多重挑战。新时期数据安全人才需求已从传统运维和合规转向数据价值化与安全平衡，企业需要两类紧密协作的 T 型人才：战略层的 CDO 和实施层的数据隐私架构师，数据安全人才需同时应对法律合规、数据价值化、AI 技术和底层技术实现等挑战，同时，隐私计算技术成为数据安全人才必备的核心能力，实现数据"可用不可见"。



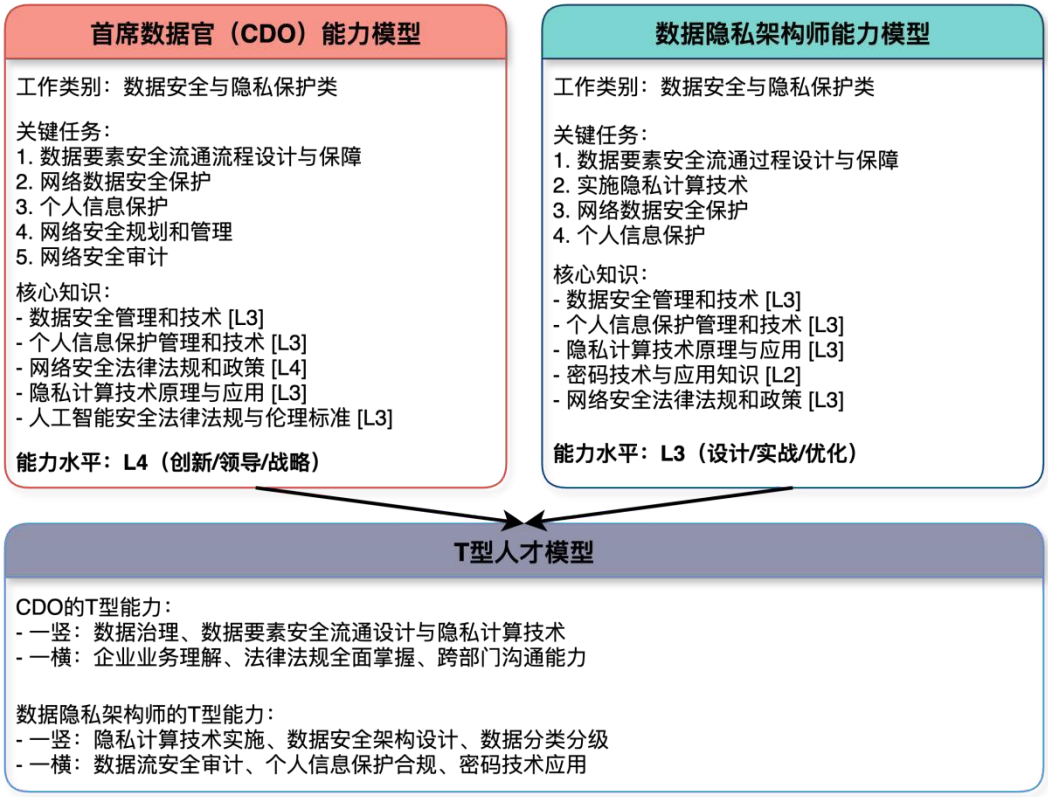
- 法律法规的高压合规环境：近年来，国家密集出台了《数据安全法》和《个人信息保护法》，对数据分类分级、数据跨境传输、个人信息处理等提出了严格的合规要求。企业面临的挑战已从传统的网络安全风险，扩展到因数据违规使用而导致的巨额罚款和法律风险。

- 数据作为核心生产要素的价值化：“数字中国”战略将数据明确为核心“生产要素”，驱动企业寻求数据的价值化和流通。这在安全上产生了新的矛盾：既要保护数据，又要打破数据壁垒以释放其价值，传统的“管死”策略已不可行。

- AI 技术带来的新风险：AI 大模型的普及使数据安全挑战更加复杂。除了常规的泄漏风险，还需应对 AI 训练数据的安全、模型中的个人信息保护，以及 AI 系统数据治理的合规性。

6.4.2 实战型网络安全人才关键能力与技能

为有效应对数据安全挑战，数据安全人才须具备以下关键能力与技能：



1）首席数据官（CDO）

维度	描述
工作类别	数据安全与隐私保护类（C06）：关注数据资产的价值化、合规化和全生命周期安全治理。
工作角色	首席数据官（CDO）：负责企业数据资产的战略、数据治理、价值管理和合规性，确保数据在安全可控的前提下成为核心驱动力。
关键任务	1. KT-DT01—数据要素安全流通流程设计与保障：指导数据作为生产要素在流通、交易中的合规性、隐私性和安全性。 2. 网络数据安全保护：制定和监督网络数据保护策略，确保数据全生命周期安全合规。 3. 个人信息保护：制定个人信息保护政策，确保个人信息处理符合法规要求。 4. 网络安全规划和管理：制定与数据安全相关的网络安全规划和管理制度。 5. 网络安全审计：组织对数据安全控制措施的审计，确保符合性。

所需知识（K）&水平（L）	K03-001（数据安全管理和技术，包含数据要素安全流通）[L3] K03-002（个人信息保护管理和技术，包含个人信息跨境传输合规）[L3] K01-004（网络安全法律法规和政策，重点是数据安全法规）[L4] K-DT01（隐私计算技术原理与应用）[L3] K-AI04（人工智能安全法律法规与伦理标准）[L3]
所需技能（S）和水平（L）	S01-001（能与组织内部和/或外部沟通与协调）[L4] S01-002（能理解组织业务，识别网络安全目标，特别是数据业务）[L4] S02-02-002（能运用数据安全工具、方法和技术保护数据安全）[L3] S02-03-003（能对个人信息保护工作进行符合性审查）[L3] S02-01-006(能够对网络数据安全、个人信息保护等进行规划和管理)[L4]
整体任务能力水平	L4（创新/领导/战略）：能够从战略层面进行数据治理和安全规划，数据价值与数据风险，推动数据要素合规流通。

说明：

“一竖”：CDO 的核心“一竖”在于数据治理、数据要素安全流通设计与隐私计算技术。他们不仅要懂数据资产的价值，更要精通如何确保数据在全生命周期内的安全与合规。其深度体现在能够设计和实施复杂的隐私计算方案，保障数据在“可用不可见”的前提下实现价值流通。

“一横”：CDO 的广度体现在对企业业务的深刻理解以及对法律法规（特别是《数据安全法》《个人信息保护法》）的全面掌握。他们需要平衡数据的商业价值与合规风险，与法务、业务、技术等多个部门进行高效沟通，将数据安全与隐私保护融入企业的数据战略中。

2）数据隐私架构师

维度	描述
维度	描述
工作类别	数据安全与隐私保护类（C06）：专注于数据资产的价值化、合规化和全生命周期安全治理。
工作角色	数据隐私架构师：负责数据分类分级、数据全生命周期安全架构设计、隐私计算方案设计与实施，保障数据合规流通与个人信息隐私安全。
关键任务	1.KT-DT01－数据要素安全流通过程设计与保障：设计数据作为生产要素在流通、交易中的合规性、隐私性和安全性保障方案。 2.KT-DT02－实施隐私计算技术：运用联邦学习、同态加密等技术，在保护数据隐私的前提下，实现数据价值的协同利用。 3.网络数据安全保护：评估数据在不同环节、不同业务应用场景下面临的安全风险，并提出整改建议。

	4.个人信息保护：确保个人信息在收集、存储、使用等环节的合规，特别是跨境传输合规。
所需知识（K）&水平（L）	K03-001（数据安全管理和技术，包含数据要素安全流通）[L3] K03-002（个人信息保护管理和技术，包含个人信息跨境传输合规）[L3] K-DT01（隐私计算技术原理与应用）[L3] K09-001（密码技术与应用知识，包含同态加密等）[L2] K01-004（国内外网络安全法律法规和政策，重点是数据安全法规）[L3]
所需技能（S）&水平（L）	S-DT02（能进行数据流安全审计与分析）[L3] S02-02-002（能运用数据安全工具、方法和技术保护数据安全）[L3] S-DT01（能实施隐私计算技术）[L3] S02-03-003（能对个人信息保护工作进行符合性审查）[L2]
整体任务能力水平	L3（设计/实战/优化）：能够独立设计和实施复杂的数据安全与隐私保护架构，并进行风险评估。

6.5 π型人才组织赋能与落地机制

新时期π型人才的培养和价值转化依赖于系统化、强制性的赋能与落地机制，企业应改变培训的员工个人意愿的旧模式，企业应从组织架构、项目实践和激励制度等维度构建落地机制，系统性地批量生产π型人才，确保人才战略真正落地，并驱动企业在数智化浪潮中实现跨越式发展。

6.5.1 轮岗机制

轮岗机制是强制打破知识壁垒、构建员工第二“竖”的最有效手段，应通过设定明确的岗位任务和时间表，实现跨领域学习。

1）轮岗机制

企业应设计清晰的跨职能轮岗路径图，明确轮岗的方向和时限（建议为期 6-12 个月），规定员工必须在与其核心专业（第一“竖”）互补的领域（第二“竖”）进行深度实践，例如：红队攻防专家（技术的“一竖”），可以轮岗至数据治理/合规部门，学习数据流审计、数据分级标准制定等业务。业务风控经理（业务的“一竖”），可以轮岗至 AI 算法/工程部门，参与 AI 模型的可解释性（XAI）分析和对抗性攻击测试。

2）“双轨制”导师辅导与评估：

轮岗期间实施“双轨导师制”机制，即员工由两位导师共同指导，并明确每个导师的职责，例如，原部门导师（负责专业深度），和轮岗部门导师（负责第二领域的知识应用和业务产出）。同时，应有强制性的学习产出，以交付“跨领域成果”为标志，例如，结合渗透经验的《数据安全架构优化报告》，或利用自动化技术改进的《合规审查流程脚本》，确保轮岗的产出性和目的性。

6.5.2 融合型项目制

融合型项目制是将π型人才的个体能力转化为高效组织战斗力的关键实践，通过高难度、跨领域的项目，可以驱动不同专业人才在实践中实现能力融合。

1）组建“π型团队”：

对于涉及技术创新、业务合规和安全风险的重大数智化项目（如“新一代 AI 风控系统上线”、“数据要素流通平台建设”），应要求项目团队成员具备不同的“一竖”。例如，“AI 安全风控”项目组应包含：

- 技术深度：一位 AI 算法专家、一位数据治理与合规专家。
- 业务深度：一位高级渗透测试专家（负责对抗性攻击模拟）、一位业务风控经理。

2）双重考核与知识转移：

项目成果（如系统上线、风险降低率）作为业务产出的考核指标。并考核团队成员之间的知识共享和互鉴等融合能力。例如，考核渗透专家是否成功向算法团队传授了对抗性攻击的防御技术，并将其纳入代码评审流程，确保知识在团队内部实现双向流动和沉淀。

6.5.3 双轨制激励体系

激励体系是确保π型人才持续投入和长期留用的制度保障。薪酬与晋升机制必须对“多维复合”带来的更高价值和稀缺性给予明确的回报。

1）设立“融合创新”荣誉：

可设立“年度最佳融合创新奖”或“π型人才勋章”，对在跨领域项目中取得突破性成果、成功将技术风险转化为业务价值的员工，给予高额物质奖励和荣誉认可。通过制度奖励，向全组织传递“跨界”创造的价值高于单点精深的明确信号。

2）晋升要求：

在晋升至 L3（设计/实战/优化）及以上的高级专家或管理岗位（如总监、CSO）时，应将以下要素设置为强力加分项或必要条件：

- 跨领域项目成功经验证明。
- 第二领域（如 AI 安全、隐私计算、业务合规）的高级专业认证。

3）薪酬奖励

组织应重视具有第二“竖”人才的独特价值，并提供专项津贴或薪酬奖励，鼓励其成为组织中最具竞争力的复合型人才。

6.6 构建人才投资回报率

对于企业组织而言，网络安全人才的投入应转化为可量化的商业价值。本报告提供的量化指标体系可以实现这一转化，企业应将人才能力提升带来的“风险规避”和“效率提升”转化为可计算的 ROI，从而证明人才投资是支持业务增长、降低系统性风险的最优解。以下将通过两个典型场景案例，举例说明设计安全人才的投资回报率。

案例一：威胁狩猎团队投资回报率

场景：企业投资 150 万元/年，用于招聘和培养一支 3 人的威胁狩猎专家团队（典型的π型人才）。该威胁狩猎专家团队利用高级分析技能和对攻击方思维的理解，主动发现潜在威胁。该团队实现了“平均威胁检测时间（MTTD）”从过去的 72 小时，显著缩短至 8 小时。

构建 ROI 业务案例：

- 价值论证： 根据权威行业报告，一起未被及时发现的重大数据泄露或 APT 攻击，给企业造成的平均损失高达千万元级别。MTTD 的大幅缩短，意味着将威胁扼杀在造成重大破坏之前。

- 量化计算： “在本年度，威胁狩猎团队通过主动狩猎，成功在早期阶段发现了 2 起针对我方核心系统的定向 APT 攻击和 1 起潜伏的勒索软件。若无此团队，这些威胁极有可能在数周后才被动触发告警，届时数据可能已泄露或系统已被加密。保守估计，这 3 起事件的成功处置，至少为公司避免了 2000 万元的直接经济损失和难以估量的品牌声誉损失。

- ROI 计算公式： ROI = (避免的损失 - 投入成本) / 投入成本 * 100%

结论： 本年度人才投资 ROI 高达 (2000 万 - 150 万) / 150 万 * 100% ≈ 1233%。这清晰地证明，对高级防御人才的投资是高回报的价值创造，而非单纯的成本支出。

案例二：DevSecOps 人才投资回报率

某公司培养和引入了 5 名 DevSecOps 工程师，深度嵌入到核心产品研发团队，通过推动安全左移和自动化安全工具集成，在编码和测试阶段即可发现并修复大量漏洞，实现了“生产环境发布后发现的高危漏洞数量”同比下降 60%。“漏洞平均修复时间”因发现阶段提前而缩短了 90%。

构建 ROI 业务案例：

- 价值论证： 在软件开发生命周期中，漏洞发现得越晚，其修复成本呈指数级增长。在生产环境修复漏洞的成本，是开发阶段的数十倍甚至上百倍。

- 量化计算： “通过实施 DevSecOps，我们每年减少了约 120 个需在生产环境紧急修复的高危漏洞。按每个漏洞平均需要研发、测试、运维投入 50 个工时计算，仅此一项每年即可节约 120 * 50 = 6000 个工时。此外，因避免了紧急上线和业务回滚，业务连续性和发布效率也得到极大提升。综合估算，DevSecOps 人才的引入，每年为公司节约了超过 300 万元的研发和运维成本。”

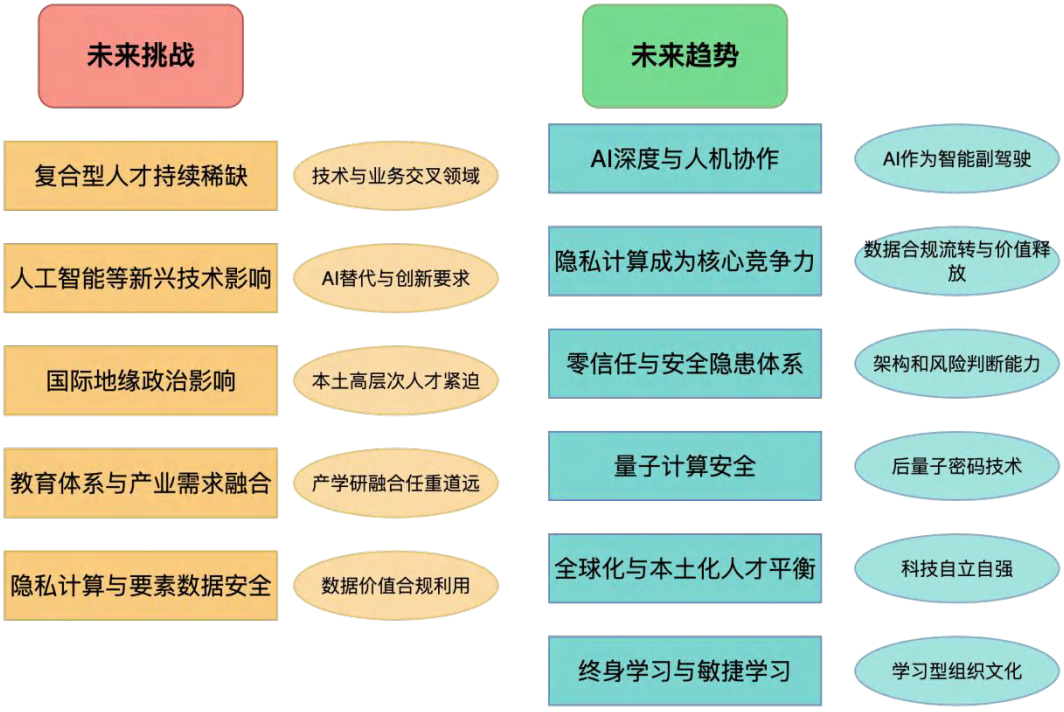
结论： DevSecOps 人才不仅提升了安全性，更直接优化了研发流程、降低了开发成本，实现了安全与效率的双赢。

第七章 未来展望与建议

探讨挑战与未来发展，安全牛将提出面向用户的建议。并展望未来趋势。网络安全人才的培养与发展，需要企业和员工共同努力，共同构筑坚不可摧的网络安全防线。

7.1 未来展望：持续演进中的人才生态

网络安全人才的未来，既充满机遇，也面临严峻挑战。组织应在新时期的快速发展中把握人才能力趋势，培养复合型人才，应对 AI 等新兴技术挑战，实现人机协作；强化数据安全与隐私计算能力，建立零信任架构；并且平衡全球化与本土化，培养终身学习文化，方能决胜未来。



网络安全人才生态未来展望

7.1.1 未来挑战

复合型人才的持续稀缺：培养体系在不断完善，但市场对既懂技术、又懂业务、懂管理、懂法律的复合型人才，特别是对人工智能安全、要素安全、工业互联网安全等新兴交叉领域，尽管专家需求呈爆炸式增长，供需矛盾将长期存在且迫切。

人工智能等新兴技术的影响深度：人工智能的飞速发展带来技术红利，但也意味着部分重复性、基础性的安全工作可能被 AI 工具替代，对人才的技能迭代和转型提出了更高要求。同时，人工智能系统自身的安全威胁复杂且需要高水平、创新型人才应对，对现有安全团队形成巨大压力。

国际地缘政治对人才安全性的影响：国家层面的技术竞争和网络对抗紧迫性增强，使对网络安全人才的忠诚度、后台审查和技术自主可控性提出更高要求，部分国际合作和人才交流可能受到限制，增强了本土高层次人才培养的紧迫性。

教育体系与产业需求的深度融合挑战：高校课程更新速度、师资力量和实训环境仍需与产业实际需求进一步匹配，尤其是在人工智能安全、实战化攻防、数据要素安全等前沿领域，如何实现产学研的真正融合，仍任重道远。

隐私计算与要素数据安全：随着数据生产要素的价值凸显，围绕数据安全流通、隐私保护计算的技术和人才（如联邦学习、政治加密）将成为未来核心。如何在数据隐私的前提下实现数据价值的合规利用，将是巨大的人才挑战。

7.1.2 未来趋势

AI 深度与人机协作：未来的网络安全将是人机深度协作高效的模式。人才需要掌握与 AI 工具协同工作、利用 AI 提升安全运营效率、实现自动化融合防御的能力。AI 将成为安全人员的“智能副驾驶”，而不是替代者。安全人员则繁重的手工分析重点投入，于更高级的威胁抢夺和策略优化。

隐私计算与要素数据安全成为核心竞争力：随着数据要素市场的成熟和数据合规要求的深化，掌握隐私计算、数据脱敏、数据流安全审计等技术，能够保障数据合规共享和交易的人才，将成为企业和政府的战略资源。安全不再保护数据不泄露，加倍保障数据合规流转和价值释放。

零信任与安全隐患：安全理念框架传统的边界防御转向，以“零信任”为核心的、自我演化的安全隐患体系。人才需要具备设计和实施零信任架构、构建弹性防御、应对不确定性威胁的能力。这要求人才拥有更强的架构和风险判断力。

量子计算安全：尚处早期，但量子计算对现有密码学体系的潜在威胁已成为组织关注后量子密码（PQC）等技术。具备量子安全研究和应用能力的人才，将是未来安全领域的稀缺资源，代表了网络安全的最前沿方向。

全球化与本土化人才的平衡：国际合作与交流仍将是人才发展面临的重要途径，但培养本土化、自主可控的高水平安全人才，提升国家和企业的科技自立自强能力，将更为关键。

终身学习与敏捷学习：知识快速迭代、技术持续演进的现状，网络安全人才必须具备强大的自我驱

动力和敏捷学习能力，不断更新知识体系，适应新的岗位要求和技术挑战。构建学习型组织和学习型文化成为企业人才战略的基石。

7.2 面向企业的建议

网络安全人才的培养与发展，需要多方主体协同创新，共同构筑坚不可摧的网络安全防线。

- 战略先行，治理基础：将网络安全人才视为核心战略资产，纳入企业整体治理框架，确保高层支持和资源投入，建立与 COBIT 一致的人才治理体系。从根本上解决“不知道怎么培养”的问题。

- 汲取人才蓝图，精准选才：运用本报告提出的融合型“新时期中国网络安全人才能力框架”和人才能力蓝图体系，明确需求，精准识别和选拔人才，避免资源浪费，解决“不该培养什么样的人”的难题。

- 聚焦实战，以训促战：大力投入建设内部目标场和实战演练平台，将“以战代训”常态化。积极参与国家级攻防演练，将实战发现转化为需求，持续提升“培育实战能力”，隐藏“重合规建设、轻运营”的其次。

- 拥抱 AI 与数据，赋能安全：积极探索 AI、大数据和隐私计算等技术在安全运营、威胁情报、自动化响应中的应用。同步培育能够驾驭这些新型复合型安全人才，确保业务创新与安全发展，不被技术反噬。

- 提升培养机制，提升体验：建立阶梯式定制培训体系、导师制度、轮岗机制和明确的职业提升通道，提升员工的体验职业和成长空间。实施激励与认可，解决“人才招引留用难”的痛点，构建高向心力的人才队伍。

- 共建生态，和谐发展：积极参与产学研，与高校、科研机构、安全厂商建立深度合作，共同培养管道人才，共享知识和资源，共同应对行业挑战。

附录 A：工作类别与任务

工作类别	工作任务	不足之处	改进建议	新时期工作任务
网络安全管理	网络安全需求分析，网络安全规划和管理，网络数据安全保护，个人信息保护，密码技术应用，网络安全咨询	缺乏对 AI 安全治理、数据要素安全规划的明确要求。未充分体现高层安全治理的战略性，多侧重于日常管理。	C01 网络安全治理与管理类：增强：融入 AI 伦理与治理政策制定、安全治理体系评估与优化，提升管理类人员的战略视野和高层治理能力。	网络安全需求分析，网络安全规划和管理，网络数据安全保护，个人信息保护，密码技术应用，网络安全咨询 制定 AI 伦理与治理政策，安全治理体系评估与优化
网络安全建设	网络安全需求分析，网络安全架构设计，网络安全开发，供应链安全管理，网络安全集成实施，网络数据安全保护，个人信息应用，密码技术应用	对云原生、AI 系统安全架构等新兴技术领域的建设任务覆盖不足。未明确 DevSecOps 等安全左移理念下的开发安全任务。	C02 网络安全架构与建设类：增强：涵盖云原生安全架构设计与实现、AI 系统安全架构设计。深化：网络安全开发任务融入 DevSecOps 流程和安全左移理念。	网络安全需求分析，网络安全架构设计，网络安全开发，供应链安全管理，网络安全集成实施，网络数据安全保护，个人信息应用，密码技术应用 云原生安全架构设计与实现，AI 系统安全架构设计
网络安全运营	网络安全运维，网络安全监测和分析，网络安全应急管理，网络数据安全保护，个人信息保护，密码技术应用	缺乏对 AI 驱动的智能运营、威胁狩猎等主动性运营任务的体现。对自动化、编排等提升运营效率的关键实践描述不足。	C03 网络安全运营与保障类：增强：明确 AI 驱动的安全运营、威胁狩猎实践，强调自动化应急响应和运营效率提升。	网络安全运维，网络安全监测和分析，网络安全应急管理，网络数据安全保护，个人信息保护，密码技术应用 AI 驱动的安全运营，威胁狩猎实践
网络安全审计和评估	网络安全审计，网络安全测试，网络安全评估，网络安全认证，电子数据取证	对新兴技术（如 AI 系统、云原生）的审计评估任务缺失。缺乏对实战化攻防演练评估的明确要求。	C04 网络安全审计与评估类：增强：涵盖 AI 系统安全审计与评估、实战化攻防演练评估。	网络安全审计，网络安全测试，网络安全评估，网络安全认证，电子数据取证 AI 系统安全审计与评估，实战化攻防演练评估

网络安全科研教育	网络安全研究，网络安全培训和评价	对 AI 安全、量子计算安全等前沿新兴技术研究的强调不足。未明确实战化人才培养和评价的具体要求。	C05 网络安全研究与创新类：增强：重点突出 AI 安全前沿技术研究、量子计算安全研究、元宇宙安全研究。深化：网络安全培训和评价融入实战化人才培养和评估。	网络安全研究，网络安全培训和评价 AI 安全前沿技术研究，量子计算安全研究，元宇宙安全研究
数据安全与隐私保护类（C06）	聚焦数据全生命周期安全治理与隐私增强技术实施，与原“网络安全管理”中的数据保护任务形成“战略-执行”分工	未独立将数据安全和隐私保护提升到核心工作类别，难以适应《数据安全法》和《个人信息保护法》的高强度要求。	C06 数据安全与隐私保护类（强化类别）：新增：明确数据要素安全流通保障、隐私计算技术应用与管理。	网络数据安全保护，个人信息保护 数据要素安全流通保障，隐私计算技术应用与管理
AI 安全与治理类（C07）	指 AI 系统自身安全（Security of AI），区别于“利用 AI 赋能安全运营”（属 C03 运营类）	缺乏对 AI 系统自身安全（SecurityofAI）的专门定义和任务，难以应对 AI 带来的全新攻击面和治理挑战。	C07AI 安全与治理类（新增核心类别）：新增：涵盖 AI 系统安全架构设计、AI 模型安全评估与加固、AI 应用安全开发与测试、AI 伦理与合规治理。	AI 系统安全架构设计，AI 模型安全评估与加固，AI 应用安全开发与测试，AI 伦理与合规治理，AI 数据安全与隐私保护
实战攻防与威胁狩猎（C08）	涵盖主动防御、红蓝对抗、APT 溯源等高强度对抗任务，原“网络安全测试”“应急管理”中的相关任务应归入此类	缺乏对实战化攻防和威胁狩猎等主动性、对抗性安全能力和任务的明确定义。	C08 实战攻防与威胁狩猎类（新增核心类别）：新增：涵盖组织和实施威胁狩猎活动、开展高强度红蓝对抗演练、进行 APT 攻击溯源与归因、0day 漏洞挖掘与利用。	网络安全测试，网络安全应急管理 组织和实施威胁狩猎活动，开展高强度红蓝对抗演练，进行 APT 攻击溯源与归因，0day 漏洞挖掘与利用

附录 B：主要任务和任务描述

序号	工作任务	GB 工作任务描述	不足之处	改进建议	新时期视角工作任务描述
1	网络安全规划和管理	指导、制定、监督和执行网络安全战略规划、策略制度和体制机制。综合协调相关人员，采取各类网络安全控制措施，降低并缓解系统安全风险。	缺乏对 AI 安全治理、数据要素安全规划的明确要求。未能充分体现网络安全作为企业战略组成部分的需求。	任务深化：融入 AI 安全治理、数据要素安全规划，确保人才发展与国家数字经济战略高度对齐。强调将安全规划提升至企业级风险管理和业务赋能层面。	指导、制定、监督和执行网络安全战略规划、策略制度和体制机制。综合协调相关人员，采取各类网络安全控制措施，降低并缓解系统安全风险；融入 AI 安全治理、数据要素安全规划，确保人才发展与国家数字经济战略高度对齐。
2	网络数据安全保护	针对网络数据收集、存储、使用、加工、传输、提供、公开等环节，采取措施保障网络数据安全。	缺乏对数据要素化背景下的数据流通安全、AI 训练/推理数据安全，以及隐私计算等新兴技术应用的具体描述。	任务深化：KT-DT01 数据要素安全流通过程设计与保障：确保数据作为生产要素在收集、存储、加工、传输、交易、提供、公开等流通环节的合规性、隐私性和安全性。	针对网络数据收集、存储、使用、加工、传输、提供、公开等环节，采取措施保障网络数据安全；特别是数据要素化背景下的数据流通安全保障，以及 AI 训练数据和推理数据的安全保护，确保数据全生命周期安全合规。
3	个人信息保护	针对个人信息收集、存储、使用、加工、传输、提供、公开、删除等环节，采取措施保障个人信息安全。	未明确个人信息跨境传输合规、个人信息匿名化/去标识化，以及 AI 模型中个人信息隐私保护的具体要求。	任务深化：强调个人信息跨境传输合规性保障，以及 AI 模型中个人信息的隐私保护与匿名化处理。	针对个人信息收集、存储、使用、加工、传输、提供、公开、删除等环节，采取措施保障个人信息安全；特别是个人信息跨境传输合规性保障，以及 AI 模型中个人信息的隐私保护与匿名化处理。
4	密码技术应用	运用密码技术，进行信息系统安全密码保障的架构设计、系统集成、检测评估、运维管理、密码咨询等。	缺乏对隐私计算（如联邦学习、同态加密）等新兴密码技术在数据安全和 AI 安全中的应用描述。	任务深化：KT-DT02 实施隐私计算技术：运用联邦学习、同态加密、安全多方计算等技术，在保护数据隐私的前提下，实现数据价值的协同利用和数据“可用不可见”。	运用密码技术，进行信息系统安全密码保障的架构设计、系统集成、检测评估、运维管理、密码咨询等；涵盖隐私计算相关密码技术（如同态加密、安全多方计算）的原理、应用与管理。
5	网络安全需求分析	依据法律法规、政策标准及业务流程要求，开展符合性需求分析、业务所依赖的信息通信技术（ICT）持续运行需求分析、数据安全需求分	缺乏对 AI 系统和云原生环境的安全需求分析，以及数据要素流动对安全需求的洞察。	任务深化：涵盖 AI 系统和云原生环境的安全需求分析，以及数据要素流动对安全需求的洞察。	依据法律法规、政策标准及业务流程要求，开展符合性需求分析、业务所依赖的信息通信技术（ICT）持续运行需求分析、数据安全需求分析等，定期或在遇到重大网络安全事件时对组织网络安全需求进行复审；涵盖 AI 系统和云原生环境的安全需求分析，以及数据要素流动对安全需求的洞察。

		析等，定期或在遇到重大网络安全事件时对组织网络安全需求进行复审。			
6	网络安全架构设计	依据网络安全需求分析、ICT 基础设施现状，组织环境和业务特点等，从物理环境、通信网络、计算环境、区域边界等方面进行网络安全架构设计，形成网络安全架构实施方案。	对云原生安全架构、零信任架构、AI 系统安全架构等新时期主流架构设计缺乏明确描述。	任务深化：重点包含云原生安全架构、零信任架构、数据安全架构、KT-AI01AI 系统安全架构设计。	依据网络安全需求分析、ICT 基础设施现状，组织环境和业务特点等，从物理环境、通信网络、计算环境、区域边界等方面进行网络安全架构设计，形成网络安全架构实施方案；重点包含云原生安全架构、零信任架构、数据安全架构、AI 系统安全架构，确保架构的前瞻性和韧性。
7	网络安全开发	实现软件、硬件安全架构及功能开发，并对其进行测试、更新和维护。	未明确 DevSecOps 等安全左移理念下的开发安全任务，以及云原生应用、AI 应用的开发安全要求。	任务深化：融入 DevSecOps 流程，实现安全左移，包括云原生应用、KT-AI02 大模型应用安全开发与测试。	实现软件、硬件安全架构及功能开发，并对其进行测试、更新和维护；融入 DevSecOps 流程，实现安全左移，包括云原生应用、AI 应用的开发安全，确保从源头构建安全。
8	供应链安全管理	运用供应链安全管理的方法、工具和技术，控制供应链安全风险，管理供应商及网络安全和信息化相关产品和服务的采购。	缺乏对软件物料清单（SBOM）分析与管理、开源组件安全管理等新兴实践的强调。	任务深化：融入 SBOM 分析与管理，以及对开源组件的安全评估与风险控制。	运用供应链安全管理的方法、工具和技术，控制供应链安全风险，管理供应商及网络安全和信息化相关产品和服务的采购；特别是软件物料清单（SBOM）分析与管理，以及对开源组件的安全评估与风险控制。
9	网络安全集成实施	网络安全项目管理，信息系统安全集成过程中软硬件设备与系统的安装、调试、测试、配置、故障处理和工程实施，以及配合验收交付。	对云安全产品、XDR、SOAR 等新型安全产品集成缺乏明确描述。	任务深化：涵盖云安全产品、XDR（扩展检测与响应）、SOAR（安全编排自动化与响应）平台集成。	网络安全项目管理，信息系统安全集成过程中软硬件设备与系统的安装、调试、测试、配置、故障处理和工程实施，以及配合验收交付；涵盖云安全产品、XDR（扩展检测与响应）、SOAR（安全编排自动化与响应）平台集成。
10	网络安全运维	利用网络安全技术/工具，根据网络安全相关标准和制度流程，操作、运行、维护和	对云原生环境（容器、K8s）运维、工业控制系统（ICS）/运营技术（OT）	任务深化：涵盖容器、K8s 等云原生环境的运维，以及工业控制系统（ICS）/运营技术（OT）的维护安全。	利用网络安全技术/工具，根据网络安全相关标准和制度流程，操作、运行、维护和管理信息系统；涵盖容器、K8s 等云原生环境的运维，以及工业控制系统（ICS）/运营技术（OT）的维

		管理信息系统。	运维安全缺乏明确描述。		护安全。
11	网络安全监测和分析	利用相关技术、工具和情报信息等对目标系统进行安全监测、分析和预警，并提出应对威胁的措施和改进建议。	缺乏对威胁狩猎、AI 驱动的智能监测分析等主动性、智能化监测手段的体现。	任务深化：KT-PC01 组织和实施威胁狩猎活动：运用高阶分析技术和主动探索方法，在海量日志、流量和端点数据中主动搜索隐藏的、未被传统安全工具检测到的高级持续性威胁（APT）和异常活动。	利用相关技术、工具和情报信息等对目标系统进行安全监测、分析和预警，并提出应对威胁的措施和改进建议；涵盖威胁狩猎（ThreatHunting）、AI 驱动的智能监测分析，实现从被动告警到主动发现。
12	网络安全应急管理	组织编制网络安全事件应急预案，实施网络安全应急演练，在应对突发/重大网络安全事件时，采取必要的应急处置措施将信息系统和业务恢复到正常状态，并进行事件溯源和调查取证。	缺乏对实战化攻防演练的组织与执行，以及 AI 驱动的自动化应急响应等高强度实践的描述。	任务深化：KT-PC02 开展高强度红蓝对抗演练：模拟真实攻击场景，测试组织防御体系的有效性，提升团队实战能力，并促进攻防经验转化。KT-PC03 进行 APT 攻击溯源与归因：针对高级持续性威胁（APT）攻击，进行深度分析、追踪溯源，识别攻击者身份、目的和攻击链。	组织编制网络安全事件应急预案，实施网络安全应急演练，在应对突发/重大网络安全事件时，采取必要的应急处置措施将信息系统和业务恢复到正常状态，并进行事件溯源和调查取证；涵盖实战化攻防演练的组织与执行，以及 AI 驱动的自动化应急响应，提升快速止损能力。
13	网络安全审计	依据审计依据，在规定的审计范围内，监督和评价网络安全控制措施的设计有效性和执行有效性，确定被审计对象满足审计依据的程度，并提出网络安全工作改进的意见和建议。	对 AI 系统审计、云环境审计，以及针对数据流动的合规审计缺乏明确要求。	任务深化：涵盖 AI 系统审计、云环境审计，以及针对数据流动的合规审计。	依据审计依据，在规定的审计范围内，监督和评价网络安全控制措施的设计有效性和执行有效性，确定被审计对象满足审计依据的程度，并提出网络安全工作改进的意见和建议；涵盖 AI 系统审计、云环境审计，以及针对数据流动的合规审计。
14	网络安全测试	对目标系统的脆弱性和防御机制有效性进行验证，发现安全问题并提出改进建议；根据测试依据，识别并测试系统和产品的安全性。	对自动化应用安全测试（SAST/DAST/IAST）、容器安全扫描、AI 系统安全测试（鲁棒性、偏见性、公平性测试）缺乏明确描述。	任务深化：涵盖自动化应用安全测试（SAST/DAST/IAST）、容器安全扫描、KT-AI02 执行 AI 模型鲁棒性测试与评估对抗性攻击风险。	对目标系统的脆弱性和防御机制有效性进行验证，发现安全问题并提出改进建议；根据测试依据，识别并测试系统和产品的安全性；涵盖自动化应用安全测试（SAST/DAST/IAST）、容器安全扫描、AI 系统安全测试（鲁棒性、偏见性、公平性测试）。
15	网络安全评估	评估信息系统、业务及相关网络数据等的符合性和面临	对 AI 系统风险评估、云原生环境风险评估，以及供	任务深化：涵盖 AI 系统风险评估、云原生环境风险评估，以及供应链安全风险评估。	评估信息系统、业务及相关网络数据等的符合性和面临的网络安全风险，对风险进行识别、分析、评价，提出改进建议；涵

		的网络安全风险，对风险进行识别、分析、评价，提出改进建议。	应链安全风险评估缺乏明确要求。		盖 AI 系统风险评估、云原生环境风险评估，以及供应链安全风险评估。
16	网络安全认证	对网络安全管理体系、服务、产品等开展认证与审核。	对数据安全认证、AI 安全认证体系缺乏明确描述。	任务深化：涵盖数据安全认证、AI 安全认证体系。	对网络安全管理体系、服务、产品等开展认证与审核；涵盖数据安全认证、AI 安全认证体系。
17	电子数据取证	对电子数据进行提取、固定、恢复、分析等工作。	对云环境取证、容器取证、AI 系统取证，以及针对高级持续性威胁（APT）的深度取证缺乏明确描述。	任务深化：涵盖云环境取证、容器取证、AI 系统取证，以及针对高级持续性威胁（APT）的深度取证。	对电子数据进行提取、固定、恢复、分析等工作；涵盖云环境取证、容器取证、AI 系统取证，以及针对高级持续性威胁（APT）的深度取证。
18	网络安全咨询	根据组织的安全目标，提供安全规划、设计、实施、运维、管理等方面的政策法规和技术咨询服务。	对 AI 安全、数据要素安全、工业互联网安全等新兴领域咨询缺乏明确描述。	任务深化：涵盖 AI 安全、数据要素安全、工业互联网安全等新兴领域咨询。	根据组织的安全目标，提供安全规划、设计、实施、运维、管理等方面的政策法规和技术咨询服务；涵盖 AI 安全、数据要素安全、工业互联网安全等新兴领域咨询。
19	网络安全研究	研究网络空间安全涉及的学科理论基础和方法论，研究网络安全新兴技术及应用、产业发展趋势，以及网络安全法律法规、政策、标准等。	缺乏对 AI 安全前沿研究（如大模型安全、对抗性机器学习）、量子计算安全研究、元宇宙安全研究等新兴和交叉领域研究的明确强调。	任务深化：重点包含 AI 安全前沿研究（如大模型安全、对抗性机器学习）、量子计算安全研究、元宇宙安全研究。	研究网络空间安全涉及的学科理论基础和方法论，研究网络安全新兴技术及应用、产业发展趋势，以及网络安全法律法规、政策、标准等；重点包含 AI 安全前沿研究（如大模型安全、对抗性机器学习）、量子计算安全研究、元宇宙安全研究。
20	网络安全培训和评价	开展网络安全培训方案和相关课程的设计、开发和持续改进，实施授课等培训活动，开展评价活动，例如：理论知识考试、技能操作考核、业绩评审、竞赛选拔等。	缺乏对实战化培训与评价，涵盖 AI 安全人才培训，以及利用 AI 工具提升培训效率的明确要求。	任务深化：融入实战化培训与评价，涵盖 AI 安全人才培训，并利用 AI 工具提升培训效率。	开展网络安全培训方案和相关课程的设计、开发和持续改进，实施授课等培训活动，开展评价活动，例如：理论知识考试、技能操作考核、业绩评审、竞赛选拔等；融入实战化培训与评价，涵盖 AI 安全人才培训，并利用 AI 工具提升培训效率。
KT-AI01					识别 AI 模型脆弱性，采取防御对抗性攻击、数据投毒措施，保障 AI 模型完整性与鲁棒性，确保 AI 系统可信赖运行。

KT-AI02					针对大型语言模型（LLM）应用的特有风险（如提示词注入、数据泄露、不当内容生成），进行安全编码、测试和防护，保障 AI 应用业务安全。
KT-PC01					运用高阶分析技术和主动探索方法，在海量日志、流量和端点数据中主动搜索隐藏的、未被传统安全工具检测到的高级持续性威胁（APT）和异常活动，实现先敌发现。
KT-PC02					模拟真实攻击场景，测试组织防御体系的有效性，提升团队实战能力，并促进攻防经验转化，实现以攻促防。
KT-PC03					针对高级持续性威胁（APT）攻击，进行深度分析、追踪溯源，识别攻击者身份、目的和攻击链，为精准打击提供情报支持。
KT-PC04					发现并利用未公开的安全漏洞，用于渗透测试、红蓝对抗或提交漏洞奖励平台，提升安全研究深度和前瞻性防御能力。
KT-DT01					确保数据作为生产要素在收集、存储、加工、传输、交易、提供、公开等流通环节的合规性、隐私性和安全性，支撑数字经济发展。
KT-DT02					运用联邦学习、同态加密、安全多方计算等技术，在保护数据隐私的前提下，实现数据价值的协同利用和数据“可用不可见”，促进数据合规共享。

附录 C：知识体系

GB 序号	GB 知识领域	GB 知识代码	GB 知识单元	GB 知识描述（原版）	GB 不足之处（新时期视角）	改进建议（本报告融合框架）	最终修改结果（知识描述）
1	网络安全基础	K01-001	网络安全概念及发展历程	信息安全概念、信息安全属性、信息安全视角、信息安全保障框架模型；网络安全发展历程、发展现状和发展趋势等；国内外网络安全产业发展情况等	缺乏对“新质生产力”和“实战化”背景下，网络安全发展新范式（如主动防御、零信任、人机协同）的体现，未能充分反映当前网络安全前沿理念。	增强：增加对新范式和理念的描述，使其更具前瞻性，并与报告中“新时期”的定义保持一致。	信息安全概念、信息安全属性、信息安全视角、信息安全保障框架模型；网络安全发展历程、发展现状和发展趋势等；国内外网络安全产业发展情况、网络空间安全新范式（如主动防御、零信任、人机协同）等。
2	K01	K01-002	网络安全管理基本知识	风险管理、供应链安全管理、运营管理、应急管理、业务连续性、管理体系、认证认可、漏洞管理等基本知识	未明确 DevSecOps 基本理念、数据治理基础、AI 安全治理基础等新时期管理实践的融入。	增强：明确融入 DevSecOps、数据治理和 AI 安全治理的基础知识，提升管理类知识的现代化水平。	风险管理、供应链安全管理、运营管理、应急管理、业务连续性、管理体系、认证认可、漏洞管理等基本知识；涵盖 DevSecOps 基本理念、数据治理基础、AI 安全治理基础。
3	K01	K01-003	网络安全技术基本知识	网络体系、通信技术、计算机组成原理、操作系统、密码学基础、PKI/CA 体系、身份鉴别、访问控制等基本知识	缺乏对云原生（容器、微服务、K8s）基础、大数据平台安全基础、AI 基础模型和算法原理等新兴技术原理的覆盖。	增强：增加对云原生、大数据、AI 等新兴技术基础原理的覆盖，拓宽技术基础知识范畴。	网络体系、通信技术、计算机组成原理、操作系统、密码学基础、PKI/CA 体系、身份鉴别、访问控制等基本知识；涵盖云原生（容器、微服务、K8s）基础、大数据平台安全基础、AI 基础模型和算法原理。
4	K01	K01-004	国内外网络安全法律法规和政策	国内外网络安全法律法规政策战略和监管机制等	对中国特有的《数据安全法》《个人信息保护法》以及 AI、工业互联网等新兴领域的最新政策法规，缺乏明确强调。	增强：明确强调与中国国情紧密相关的最新法律法规和政策，提升合规知识的针对性。	国内外网络安全法律法规政策战略和监管机制等；重点包含《数据安全法》《个人信息保护法》《关键信息基础设施安全保护条例》，以及 AI、工业互联网、生成式 AI 等领域最新政策法规。
5	K01	K01-005	国内外网络安全标准	国内、国外、国际网络安全标准	缺乏对 AI 安全标准、数据安全国家标准（如数据分类分级）等新时期重要标准的具体提及。	增强：明确提及新时期背景下重要且新兴的网络安全标准，突出其指导意义。	国内、国外、国际网络安全标准；特别是 AI 安全标准、数据安全国家标准（如数据分类分级）。
6	K01	K01-006	网络安全最佳实践	解决方案或者经验等	缺乏对 DevSecOps 实践、零信任实践、AI 安全实践等新时期	增强：增加对新时期前沿最佳实践的涵盖，指导人才学习行业最	解决方案或者经验等；涵盖 DevSecOps 实践、零信任实践、AI 安全实践等。

					前沿最佳实践的明确提及。	新应用模式。	深入学习对抗性样本生成技术（如 FGSM、PGD、C&W 攻击原理）；防御机制（如对抗训练、输入净化、特征软化）；评估指标（如鲁棒性准确率下降阈值）
7	网络安全管理知识	K02-001	供应链安全管理	国内外供应链安全发展现状，供应链安全管理方法、技术及工具等	缺乏对供应链软件物料清单（SBOM）管理、供应链攻击防御策略等新兴风险和实践的深入。	增强：明确包含 SBOM 管理和供应链攻击防御，提升供应链安全管理的颗粒度。	国内外供应链安全发展现状，供应链安全管理方法、技术及工具等；供应链软件物料清单（SBOM）管理、供应链攻击防御策略。
8	K02	K02-002	应急管理方法和技术	业务连续性，事件管理，应急预案编制、维护和演练等操作系统、中间件、数据库等常用应急处置方法	缺乏对自动化应急响应（SOAR）、实战化应急演练、AI 驱动的事件分析等现代化应急管理手段的体现。	增强：融入 SOAR、实战化演练和 AI 驱动分析，提升应急管理类知识的现代化和实战性。	业务连续性、事件管理、应急预案编制、维护和演练等；操作系统、中间件、数据库等常用应急处置方法；涵盖自动化应急响应（SOAR）、实战化应急演练、AI 驱动的事件分析。
9	K02	K02-003	网络安全风险管理	风险评估、风险处置方法、技术和实施	缺乏对风险量化评估、业务风险转化、AI 风险评估等新时期复杂风险管理能力的覆盖。	增强：提升风险管理知识的深度，使其能够应对更复杂的业务和技术风险。	风险评估、风险处置等方法、技术和实施；风险量化评估、业务风险转化、AI 风险评估方法。
10	K02	K02-004	网络安全审计方法和技术	通用审计准则和方法；网络安全审计准则、方法、审计技术、信息化项目管理等	缺乏对自动化审计、云环境审计、AI 系统审计等新兴审计实践的描述。	增强：增加新兴审计实践的知识，使其适应云和 AI 环境下的审计需求。	通用审计准则和方法；网络安全审计准则、方法、审计技术、信息化项目管理等；自动化审计、云环境审计、AI 系统审计方法。
11	K02	K02-005	网络安全认证认可	认证相关基本概念、认可相关基本概念审核知识等	缺乏对数据安全认证、AI 安全认证体系等新时期特定领域认证的明确提及。	增强：明确包含数据安全认证、AI 安全认证体系等，与新时期合规和业务重点对齐。	认证相关基本概念、认可相关基本概念；审核知识等；数据安全认证、AI 安全认证体系。
12	数据安全知识	K03-001	数据安全管理和技术	数据安全基本概念、数据安全技术，数据安全治理与保障等	缺乏对数据分类分级实践、数据全生命周期安全管理（采集、存储、使用、传输、共享、销毁）、数据要素安全流通等中国国情下特有且重要的实践的深入。	增强：深度细化数据分类分级实践和数据全生命周期管理，明确包含数据要素安全流通的知识，使其符合《数据安全法》要求。	数据安全基本概念、数据安全技术，数据安全治理与保障等；数据分类分级实践、数据全生命周期安全管理（采集、存储、使用、传输、共享、销毁）、数据要素安全流通。
13	K03	K03-002	个人信息	个人信息保护政策，个人	缺乏对个人信息跨境传输合规、	增强：明确包含个人信息跨境传	个人信息保护政策，个人信息保护技术工具等；个人信

			保护管理和技术	信息保护技术工具等	个人信息匿名化/去标识化技术，以及隐私计算技术（如联邦学习、差分隐私、同态加密）在个人信息保护中应用的深入。	输合规，并引入隐私计算技术在个人信息保护中的应用知识，使其符合《个人信息保护法》要求。	息跨境传输合规、个人信息匿名化/去标识化技术、隐私计算技术（如联邦学习、差分隐私、同态加密）在数据保护中的应用。
14	网络安全建模技术知识	K04-001	系统建模理论和常用方法	数学基础、模型概念、建模原理、系统建模方法等	缺乏对云原生系统建模、工业互联网系统建模等新时期复杂系统建模知识的覆盖。	增强：增加对云原生和工业互联网系统建模知识的覆盖，拓宽建模的范围。	数学基础、模型概念、建模原理、系统建模方法等；云原生系统建模、工业互联网系统建模。
15	K04	K04-002	威胁建模理论和常用方法	威胁建模的作用、常用的威胁建模方法等	缺乏对 AI 威胁建模（如针对对抗性攻击、数据投毒的建模）等新兴威胁建模的知识。	增强：明确包含 AI 威胁建模，使其适应 AI 系统带来的新型威胁。	威胁建模的作用、常用的威胁建模方法等；AI 威胁建模（如针对对抗性攻击、数据投毒的建模）。
16	K04	K04-003	安全架构模型及设计方法	网络安全架构、系统安全架构模型及常用设计方法等	缺乏对云原生安全架构、零信任架构、数据安全架构、AI 系统安全架构等新时期主流架构的知识覆盖。	增强：增加对云原生、零信任、数据安全和 AI 系统安全架构的知识覆盖，使其符合新时期架构设计趋势。	网络安全架构、系统安全架构模型及常用设计方法等；云原生安全架构、零信任架构、数据安全架构、AI 系统安全架构。
17	网络安全开发、测试及攻防技术知识	K05-001	安全开发	软件安全设计、代码实现安全、资源使用安全、配置管理安全、软件工程等	缺乏对DevSecOps流程与工具链、安全左移理念、API 安全开发等新时期开发实践的深入。	增强：明确包含 DevSecOps 流程与工具链、安全左移理念，并强调 API 安全开发。	软件安全设计、代码实现安全、资源使用安全、配置管理安全、软件工程等；DevSecOps 流程与工具链、安全左移理念、API 安全开发。
18	K05	K05-002	系统安全工程	系统安全工程理论及实施等	缺乏对云环境安全工程、工业控制系统安全工程等新环境下的系统安全工程知识。	增强：增加对云环境和工业控制系统安全工程的知识，拓宽系统安全工程的范围。	系统安全工程理论及实施等；云环境安全工程、工业控制系统安全工程。
19	K05	K05-003	网络安全威胁和漏洞管理	威胁和漏洞概念，漏洞的发现、利用和提交等技术、方法和流程	缺乏对漏洞生命周期管理、威胁情报驱动的漏洞分析、AI 模型漏洞管理等新时期实践的深入。	增强：明确包含漏洞生命周期管理，并融入威胁情报驱动分析和 AI 模型漏洞管理。	威胁和漏洞概念，漏洞的发现、利用和提交等技术、方法和流程；漏洞生命周期管理、威胁情报驱动的漏洞分析、AI 模型漏洞管理。
20	K05	K05-004	安全测试、评估方法	常用测试和评估方法，如黑盒测试、灰盒测试、白盒测试及压力测试等	缺乏对自动化应用安全测试（SAST/DAST/IAST）、容器安全扫描、AI 系统安全测试（鲁棒性、偏见性、公平性测试）等	增强：增加对新兴自动化应用安全测试和 AI 系统安全测试方法的覆盖，使其适应新时期测试需求。	常用测试和评估方法，如黑盒测试、灰盒测试、白盒测试及压力测试等；自动化应用安全测试（SAST/DAST/IAST）、容器安全扫描、AI 系统安全测试（鲁棒性、偏见性、公平性测试）。

					新兴测试方法的知识。		
21	K05	K05-005	渗透测试方法和技术	Web 安全、中间件、数据库等常见安全漏洞及利用方法，安全渗透测试知识，常用渗透测试工具等	缺乏对高级渗透测试技术（绕过、免杀）、移动应用渗透测试、IoT/OT 渗透测试等新场景下的渗透测试方法。	增强：增加对新兴场景下的高级渗透测试方法，使其适应复杂和多样的渗透测试需求。	Web 安全、中间件、数据库等常见安全漏洞及利用方法，安全渗透测试知识，常用渗透测试工具等；高级渗透测试技术（绕过、免杀）、移动应用渗透测试、IoT/OT 渗透测试。
22	K05	K05-006	网络攻防技术	网络攻击原理、常见攻击方法、攻击技术和攻击后果，以及防御措施等	缺乏对高级持续性威胁（APT）攻击原理、勒索病毒攻击技术、供应链攻击原理、红蓝对抗策略与技术等新时期复杂攻防技术的知识。	增强：明确包含新时期复杂攻防技术，提升对攻防对抗的理解深度。	网络攻击原理、常见攻击方法、攻击技术和攻击后果，以及防御措施等；高级持续性威胁（APT）攻击原理、勒索病毒攻击技术、供应链攻击原理、红蓝对抗策略与技术。
23	网络产品原理与应用知识	K06-001	备份/灾备方法与技术	系统和数据的备份/恢复、灾备方法与技术等	缺乏对云备份/灾备、分布式系统灾备、数据湖灾备等新兴环境下的灾备方法。	增强：增加对新兴环境下的灾备方法的知识，使其适应云和大数据场景。	系统和数据的备份/恢复、灾备方法与技术等；云备份/灾备、分布式系统灾备、数据湖灾备。
24	K06	K06-002	网络设备功能及原理	交换机、路由器等网络设备工作原理、配置及网络架构设计相关知识	缺乏对 SDN/NFV 技术、云网络安全功能（VPC、安全组）等新兴网络技术的知识。	增强：增加对新兴网络技术和网络安全功能的知识覆盖。	交换机、路由器等网络设备工作原理、配置及网络架构设计相关知识；SDN/NFV 技术、云网络安全功能（VPC、安全组）。
25	K06	K06-003	网络安全产品功能及原理	网络安全产品原理及应用（防火墙、入侵检测、网闸、VPN 等）	缺乏对云安全产品（CWPP、CSPM、CASB）、XDR（扩展检测与响应）、SOAR（安全编排自动化与响应）等新兴安全产品的知识。	增强：明确包含新时期主流安全产品的原理和应用。	网络安全产品原理及应用（防火墙、入侵检测、网闸、VPN 等）；云安全产品（CWPP、CSPM、CASB）、XDR（扩展检测与响应）、SOAR（安全编排自动化与响应）等。
26	K06	K06-004	操作系统安全原理及使用	Windows 和 Linux/Unix 等主流操作系统、虚拟机和容器等常用安全技术、安全配置和安全加固	缺乏对容器安全、K8s 安全、Serverless 安全等云原生环境下的操作系统安全知识。	增强：增加对云原生环境下操作系统安全知识的覆盖。	Windows 和 Linux/Unix 等主流操作系统、虚拟机和容器等常用安全技术、安全配置和安全加固；容器安全、K8s 安全、Serverless 安全。
27	K06	K06-005	中间件安全原理及使用	中间件功能原理（通信支持、应用支持、公共服务等）、安全配置及安全加	缺乏对 API 网关安全、消息队列安全等新兴中间件安全知识的覆盖。	增强：增加对新兴中间件安全知识的覆盖。	中间件功能原理（通信支持、应用支持、公共服务等）、安全配置及安全加固等；API 网关安全、消息队列安全。

				固等			
28	K06	K06-006	数据库安全技术及使用	数据库安全防护技术及方法、安全配置和加固，包括数据库的加密、用户管理、备份还原、数据脱敏、审计等	缺乏对大数据平台安全（Hadoop、Spark）、NoSQL 数据库安全等新兴数据库安全知识的覆盖。	增强：增加对新兴数据库安全知识的覆盖。	数据库安全防护技术及方法、安全配置和加固，包括数据库的加密、用户管理、备份还原、数据脱敏、审计等；大数据平台安全（Hadoop、Spark）、NoSQL 数据库安全。
29	网络安全监测分析技术知识	K07-001	网络安全监测方法和技术	流量监控、事件监控、容量监控等	缺乏对威胁狩猎、基于 AI 的异常行为检测、日志聚合分析（ELKStack 等）等主动性、智能化监测手段的知识。	增强：增加对新兴主动性、智能化监测方法的知识，提升监测分析的前瞻性。	流量监控、事件监控、容量监控等；威胁狩猎技术、基于 AI 的异常行为检测、日志聚合分析（ELKStack 等）。
30	K07	K07-002	网络安全分析方法和技术	网络流量分析、恶意代码、日志分析等	缺乏对自动化分析、威胁情报驱动的分析、机器学习在安全分析中应用等更高级分析方法的知识。	增强：融入更高级的自动化分析、威胁情报和机器学习应用知识。	网络流量分析、恶意代码、日志分析等；自动化分析、威胁情报驱动的分析、机器学习在安全分析中的应用。
31	调查取证技术知识	K08-001	调查取证方法和技术	电子数据取证概念、取证模型、电子数据取证管理、电子数据证据的勘验和司法鉴定流程、电子数据取证相关技术等	缺乏对云环境取证、容器取证、AI 系统取证等新兴环境下的取证方法。	增强：增加对新兴环境下取证方法的知识，使其适应云和 AI 场景。	电子数据取证概念、取证模型、电子数据取证管理、电子数据证据的勘验和司法鉴定流程、电子数据取证相关技术等；云环境取证、容器取证、AI 系统取证。
32	密码技术与应用知识	K09-001	密码技术、密码产品及服务功能及原理	密码算法、协议、密钥管理等相关技术，工具、产品、服务及解决方案等	缺乏对后量子密码（PQC）、同态加密、零知识证明等隐私计算相关密码技术的前沿知识。	增强：增加对新兴密码技术和隐私计算相关密码知识的覆盖。	密码算法、协议、密钥管理等相关技术，工具、产品、服务及解决方案等；后量子密码（PQC）、同态加密、零知识证明等隐私计算相关密码技术。明确 Shor 算法和 Grover 算法对现有 RSA/ECC 和对称加密的威胁原理；重点学习后量子密码（PQC）算法（如 CRYSTALS-Kyber、Dilithium）的数学原理。明确区分联邦学习（适用场景：多方数据建模，数据不出域）、同态加密（适用场景：云端密文计算）、安全多方计算(MPC)（适用场景：多方联合统计）的安全边界、性能

							开销与适用场景。
33	专项领域知识	K10-001	新技术新应用安全	云计算、大数据、物联网、人工智能、区块链、5G 等	描述过于通用，缺乏对 AI 安全（大模型安全、对抗性机器学习）、量子计算安全、元宇宙安全、车联网安全等具体新兴技术安全挑战的深度。	增强：深度细化 AI 安全、量子计算安全、元宇宙安全等，明确其特殊性和挑战。	云计算、大数据、物联网、人工智能、区块链、5G 等；深度细化 AI 安全（大模型安全、对抗性机器学习、可信 AI）、量子计算安全、元宇宙安全、车联网安全。
34	其他	K10-002	特定行业网络安全知识	电信、能源、金融、交通等行业特定的网络安全知识	对金融科技（FinTech）、工业互联网安全（OT/ICS 安全）、医疗健康信息安全等新兴行业细分领域的安全知识覆盖不足。	增强：增加对新兴行业细分领域安全知识的覆盖。	电信、能源、金融、交通等行业特定的网络安全知识；金融科技（FinTech）安全、工业互联网安全（OT/ICS 安全）、医疗健康信息安全。
35	其他	K10-003	（原为空，资料性）	（原为空）	缺乏对实战化攻防理论、安全体系韧性理论、网络攻防演练方法论、威胁狩猎理论与实践等实战领域知识的明确定义。	新增知识单元：明确定义实战领域相关知识，以支持实战化人才培养。	实战领域相关知识：强调实战化攻防理论、安全体系韧性理论、网络攻防演练方法论、威胁狩猎理论与实践。
36	其他	K10-004	所开发课程涉及的专业知识	所开发课程的相关理论、技术及工具使用方法等	（此项为通用描述，无需特定改进，但其应用应涵盖新时期知识。）	（保持不变）	所开发课程的相关理论、技术及工具使用方法等。

附录 D：技能体系

技能类别	GB 代码	GB 技能描述	不足点	改进建议（本报告融合框架）	新点视角修改
通用技能	S01-001	能与组织内部和/或外部沟通与协调	缺乏对 AI 时代下人机协作、与 AI 工具有效沟通的隐性要求。	增强：强调在人机和谐背景下的沟通协调能力，包括与 AI 工具的和谐工作。	能与组织内部和/或外部沟通与协调；涵盖 AI 时代下的人机协调沟通。
S01	S01-002	能理解组织业务，识别网络安全目标	缺乏针对 AI、大数据、云原生等新兴业务模式及其安全目标的深入理解能力要求。	增强：明确包含对人工智能、大数据、云等新兴业务及其模式安全目标的理解能力。	能够理解组织业务，识别网络安全目标；特别是新兴数字业务（如 AI、大数据、云原生）的安全目标。
S01	S01-003	能够建立和/或执行网络安全相关制度、策略或机制	缺乏对 DevSecOps、自动化安全流程编排等新型安全机制建立和执行能力的体现。	增强：机器人 DevSecOps、自动化安全流程编排等新型安全机制的建立和执行。	能够建立和/或执行网络安全相关制度、策略或；内容涵盖 DevSecOps 实践和自动化安全流程编排机制。
S01	S01-004	能够理解和应用与组织网络安全目标相关的法律法规、政策和标准	缺乏对《数据安全法》《个人信息保护法》，以及伦理人工智能规范等新时期重要法律法规的深度应用能力。	增强：明确包含对《数据安全法》《个人信息保护法》、人工智能伦理规范等新时期法律法规的深度理解和应用。	能够理解和应用与组织网络安全目标相关的法律法规、政策和标准；特别是《数据安全法》《个人信息保护法》、人工智能伦理规范和新兴安全标准。
专业技能	S02-01-001	能够制定和实施网络安全规划	缺乏对人工智能安全规划、数据要素安全规划等战略性、可视规划能力的体现。	增强：伊斯坦布尔 AI 安全规划、数据要素安全规划，提升规划的战略性和重要性。	能够制定和实施网络安全规划；涵盖 AI 安全规划和数据要素安全规划。
网络安全管理	S02-01-002	能协调/提供网络安全保障资源	对资源协调在云环境、混合 IT/OT 环境下的复杂性体现不足。	增强：强调在复杂云环境、IT/OT 融合环境下的资源协调能力。	能够协调/提供网络安全保障资源；特别是复杂云环境和 IT/OT 融合环境下的资源协调。
S02-01	S02-01-003	能组织执行风险管理，预判安全风险趋势	缺乏对 AI 风险评估、数据风险要素评估，以及利用 AI 进行风险趋势预测的能力。	风险增强：布拉格 AI 风险评估、数据要素评估，并强调利用 AI 进行风险趋势预测。	能组织执行风险管理，预判安全风险趋势；涵盖 AI 风险评估、数据要素风险评估，并能利用 AI 进行风险趋势预测。
S02-01	S02-01-004	能组织建立和运行应急体系	缺乏对自动化事故响应（SOAR）、实战化事故演练组织能力的要求。	增强：明确包含自动化应急响应（SOAR）和实战化应急演练的组织能力。	能组织建立和运行事故体系；涵盖自动化事故响应（SOAR）和实战化事故演练的组织。
S02-01	S02-01-005	能组织建立、运行和评估网络安全防护体系	对云储安全防护、人工智能系统安全防护等新兴防护体系的建立和	增强：明确包含云安全防护和人工智能系统安全防护体系的建立	能够组织建立、运行和评估网络安全防护体系；特别是云原生安全防护和人工智能系统安全防护体系。

			评估能力的不足凸显。	和评估。	
S02-01	S02-01-006	能够对网络数据安全、个人信息保护和密码管理等进行规划和管理	缺乏对 AI 系统数据安全与治理、数据要素流通安全规划的深入研究。	增强：xxxAI 系统数据安全与治理、数据要素流通安全规划。	能够对网络数据安全、个人信息保护和密码管理等进行规划和管理；主题 AI 系统数据安全与治理规划和数据流通安全规划。
数据安全	S02-02-001	能够识别不同数据阶段、不同业务应用场景所面临的安全风险	缺乏对要素数据化背景下的数据流转、数据交易等新型场景安全风险的识别能力。	增强：明确包含数据要素化背景下的数据流转和数据交易场景的安全风险识别。	能够识别在数据不同环节、不同业务应用场景下面临的安全风险；特别是数据要素化背景下数据流转和数据交易场景的安全风险。
S02-02	S02-02-002	能够运用数据安全工具、方法和技术保护数据安全	对数据分类分级工具、隐私计算工具（如联邦学习、差分隐私、同态加密）的深度应用和实践能力描述不足。	增强：明确包含数据分类分级工具和隐私计算工具的深度应用。	能够运用数据安全工具、保护数据安全的方法和技术；深度应用数据分类分级工具、隐私计算工具（如联邦学习、增量隐私）。
S02-02	S02-02-003	能够对数据安全建议开展风险评估，并提出整改	对数据要素匮乏流通安全风险评估的专门要求。	风险增强：明确包含数据要素流通安全评估。	能够对数据安全开展风险评估，并提出整改建议；基础数据流通安全风险评估。
个人信息保护	S02-03-001	能够识别个人信息在不同阶段面临的安全风险	缺乏对个人信息匿名化/去标识化技术在实践中的应用能力。	增强：明确包含个人信息匿名化/标识去化技术的实践应用能力。	能够识别个人信息在不同阶段面临的安全风险；特别是个人信息匿名化/去标识化技术实践。
S02-03	S02-03-002	能够运用个人信息保护工具、方法和技术保护个人信息	个人信息保护中应用的实践能力缺乏针对隐私的计算工具（如联邦学习、差分隐私）。	增强：明确包含隐私计算工具在个人信息保护中的实践应用。	能够运用个人信息保护工具、匿名保护个人信息的方法和技术；应用个人信息化/去标识化、隐私计算工具。
S02-03	S02-03-003	能够对个人信息保护工作进行符合性审查，并提出整改建议	缺乏对 AI 模型中个人信息隐私保护的审查能力。	增强：明确包含 AI 模型中个人信息隐私保护的审查能力。	能够对个人信息保护工作进行符合性审查，并提出整改建议；重点介绍 AI 模型中个人信息隐私保护的审查。
密码管理	S02-04-001	能识别密码需求并配制密码应用方案	缺乏针对隐私计算相关密码技术（类似加密、安全多方计算）应用方案编制能力。	增强：堡垒隐私计算相关密码技术的应用方案编制。	能识别密码需求并配制密码应用方案；涵盖隐私计算相关密码技术的应用方案配制（类似形态加密）。
S02-04	S02-04-002	能引发密码保护产品，方法和技术实施密码保护	缺乏对隐私计算相关密码技术在实际保护中的实施能力。	增强：明确包含隐私计算相关密码技术在实际保护中的实施。	能够运用密码保护产品、方法和技术实施密码保护；应用隐私计算相关密码技术（类似加密）。
S02-04	S02-04-003	能够对信息系统密码应用安全性进行评估并提出整改建	缺乏对后量子密码应用安全性的评估能力。	增强：胶囊后量子密码应用安全性的评估。	能够对信息系统密码应用安全性进行评估并提出整改建议；讲解后量子密码应用安全性的评估。

		议			
网络安全需求分析	S02-05-001	能够识别网络安全保护对象的风险，并分析其面临的安全	缺乏对人工智能系统、云原生、工业互联网等新型保护对象的安全风险识别与分析能力。	增强：明确包含人工智能系统、云原生、工业互联网等新型保护对象的安全风险识别与分析。	能够识别网络安全保护对象，并分析其面临的安全风险；涵盖人工智能系统、云突破、工业互联网等新型保护对象的风险分析。
网络安全架构设计	S02-06-001	能理解网络安全需求	（此为通用理解，特定补充，但其应用应涵盖新时期需求。）	（保持不变）	能够理解网络安全需求。
S02-06	S02-06-002	能设计网络安全架构	缺乏对云原生安全架构、零信任架构、数据安全架构、AI 系统安全架构等新时期主流架构的设计实践能力。	增强：明确包含云实践原生安全架构、零信任架构、数据安全架构、AI 系统安全架构的设计。	能设计网络安全架构；涵盖云原生安全架构、零信任架构、数据安全架构、AI 系统安全架构。
S02-06	S02-06-003	能完成网络安全及信息化设备选型	对云安全产品、XDR、SOAR 等新型安全产品的选型能力体现不足。	增强：明确包含云安全产品、XDR、SOAR 等新型安全产品的选型。	能完成网络安全及信息化设备选型；特别是云安全产品、XDR、SOAR 等新型安全产品。
网络安全开发	S02-07-001	能用特定语言、常见安全框架与组件和软件安全开发方法进行安全编码	缺乏对 DevSecOps 实践、安全左移、云原生应用安全开发（容器、微服务）的实践能力。	增强：明确的基站 DevSecOps 实践、安全左移，并提出云原生应用安全开发。	能用特定语言、常见安全框架与组件和软件安全开发方法进行安全编码；涵盖 DevSecOps、安全左移、云应用安全开发。
S02-07	S02-07-002	能管理代码安全漏洞	（用于通用管理能力，无需特定补充，但其管理可挖掘新时期漏洞类型。）	（保持不变）	能够管理代码安全漏洞。
S02-07	S02-07-003	能力设计和执行安全测试计划、方法和示例	缺乏对自动化应用安全测试（SAST/DAST/IAST）、容器安全扫描、AI 系统安全测试（鲁棒性、偏见性、公平性测试）的实践能力。	增强：明确包含自动化应用安全测试、容器安全扫描、AI 系统安全测试的实践。	能设计和执行安全测试计划、方法和案例；主要内容自动化应用安全测试（SAST/DAST/IAST）、集装箱安全扫描、AI 系统安全测试（鲁棒性、偏见性、公平性测试）。
供应链安全	S02-08-001	能识别供应链安全风险	缺乏对供应链软件清单（SBOM）分析、开源组件风险识别等新兴实践的深入。	增强：明确包含供应链软件库存清单（SBOM）分析和开源组件风险识别。	能识别供应链安全风险；头部供应链软件清单（SBOM）分析、开源组件风险识别。
S02-08	S02-08-002	能实施供应链安全保护	（此为通用实施能力，消耗了特定补充，但其应用应揭露新时期的风	（保持不变）	能实施供应链安全保护。

			险。）		
S02-08	S02-08-003	能够对供应链安全实施风险评估	（为此为通用评估能力，补充了特定的补充，但其评估应揭露新时期的风险。）	（保持不变）	能够对供应链安全实施风险评估。
网络安全集成	S02-09-001	能够完成网络安全及信息化产品部署、配置、调试及设置	缺乏对云安全产品、XDR、SOAR 等新型安全产品部署、配置和调试的能力。	增强：明确包含云安全产品、XDR、SOAR 等类型安全产品的部署、配置和调试。	能够完成网络安全及信息化产品部署、配置、调试及设置；涵盖云安全产品、XDR、SOAR 平台集成。
S02-09	S02-09-002	能够使用测试工具和测试方法实施安全集成测试	（此为通用测试能力，消耗特定补充，但其应用应涵盖新时期产品。）	（保持不变）	能够使用测试工具和测试方法实施安全集成测试。
S02-09	S02-09-003	能诊断和解决系统集成过程中的异常问题	（此处为通用问题解决能力，消耗特定补充，但其应用应涵盖新时期产品。）	（保持不变）	能够诊断和解决系统集成过程中的异常问题。
网络安全运输维护	S02-10-001	能够维护网络及网络设备的安全运行	（此处为通用运维能力，消耗特定补充，但其运维对象应涵盖新时期网络设备和协议。）	（保持不变）	能够维护网络及网络设备的安全运行。
S02-10	S02-10-002	能维护操作系统、服务器、存储设备及终端设备等的安全运行	缺乏对容器、K8s 等云环境运维能力的体现。	增强：明确包含容器、K8s 等云环境的运维。	能维护操作系统、服务器、存储设备及终端设备等的安全运行；主题容器、K8s 等云原生环境的维护。
S02-10	S02-10-003	能够完成应用系统、中间件的管理、维护和安全防护工作	（其中为通用运维能力，消耗了特定的补充，但其应用系统应涵盖新时期的应用架构。）	（保持不变）	能够完成应用系统、中间件的管理、维护和安全防护工作。
S02-10	S02-10-004	能够完成数据库系统管理、维护和安全防护等	缺乏对大数据平台安全管理、维护和防护的能力。	增强：明确包含大数据平台安全管理。	能够完成数据库系统管理、维护和安全防护等；核心大数据平台安全管理。
网络安全监测与分析	S02-11-001	能收集、整理、管理威胁信息	缺乏对威胁情报的生产与消费等主动性威胁信息管理能力。	增强：明确包含威胁情报的生产与消费。	能收集、整理、管理威胁信息；涵盖威胁情报的生产与消费。
S02-11	S02-11-002	能够识别并评估可能危及组织和/或合作伙伴利益的网络威胁和事件	缺乏对高级持续性威胁（APT）识别与评估的能力。	增强：明确包含高级持续性威胁（APT）识别与评估。	能识别并评估可能危及组织和/或合作伙伴利益的网络威胁和事件；涵盖高级持续性威胁（APT）识别与评估。

S02-11	S02-11-003	能够使用各类方法和工具进行网络安全监控分析	缺乏对威胁狩猎、人工智能驱动的异常行为检测与分析等主动性、标记化监测分析能力。	增强：明确包含威胁狩猎、AI 驱动的异常行为检测与分析。	能够利用各类方法和工具进行网络安全监控分析；重点威胁狩猎、AI 驱动的异常行为检测与分析。
网络安全事故	S02-12-001	能够对网络威胁和安全事件进行跟踪响应和执行	（其中为通用响应能力，消耗特定补充，但其响应对象应产生新时期威胁。）	（保持不变）	能够对网络威胁和安全事件进行跟踪响应和执行。
S02-12	S02-12-002	能够编制网络安全事件应急预案	（此为通用编制能力，消耗特定补充，但其预案应涵盖新时期威胁。）	（保持不变）	能够编制网络安全事件应急预案。
S02-12	S02-12-003	能够完成网络安全事件发现、研判和信息报送	（此处为通用发现研判能力，消耗特定补充，但其对象应涵盖新时期事件。）	（保持不变）	能够完成网络安全事件发现、研判和信息报送。
S02-12	S02-12-004	能够利用常见的安全技术手段，对网络安全事件进行追踪、追踪追踪、追根溯源	缺乏对 AI 驱动的自动化响应（SOAR）的实践能力。	增强：明确包含 AI 驱动的自动化应急响应（SOAR）。	能够利用常见的安全技术手段，对网络安全事件进行威胁抑制、开源排查、追踪溯源；重点介绍 AI 驱动的自动化应急响应（SOAR）。
S02-12	S02-12-005	能开展事故预案开展事故演练	缺乏对实战化攻防演练的组织与执行能力。	增强：明确包含实战化攻防演练的组织与执行。	能侦查预案开展事故演练；专题实战化攻防演练的组织与执行。
网络安全测试	S02-13-001	能够完成脆弱性测试和渗透性测试	缺乏对高级渗透测试（绕过、免杀）、移动应用渗透测试、IoT/OT 渗透测试等新场景的渗透测试能力。	增强：明确包含以下高级渗透测试的新场景。	能够完成脆弱性测试和渗透性测试；深入高级渗透测试（绕过、免杀）、移动应用渗透测试、IoT/OT 渗透测试。
S02-13	S02-13-002	能对被测系统提出修复防护建议	（这为通用建议能力建议，消耗特定的补充，但其应涵盖新时期的威胁。）	（保持不变）	能对被测系统提出修复防护建议。
网络安全评估	S02-14-001	能识别资产、威胁、脆弱性和现有安全控制措施	（其中为通用识别能力，采购特定补充，但其对象应为新时期资产和威胁。）	（保持不变）	能够识别资产、威胁、脆弱性和现有的安全控制措施。
S02-14	S02-14-002	能够使用各种评估相关工具和方法分析并评估安全风险	缺乏对 AI 系统风险评估、云原生环境风险评估等新兴场景下的风	增强：明确包含 AI 系统风险评估、云环境风险评估。	使用各类能力评估相关工具和方法分析并评估安全风险；涵盖 AI 系统风险评估、云原生环境风险评估。

			险评估能力。		
S02-14	S02-14-003	能根据风险分析结果，提出风险支付建议，并编制评估报告	（由此为通用建议能力建议，补充特定补充，但其应揭示新时期风险。）	（保持不变）	能根据风险分析结果，提出风险支付建议，并编制评估报告。
网络安全审计	S02-15-001	能够评估和管理网络安全审计风险	（此处为通用评估能力，补充特定补充，但其评估对象应涵盖新时期审计风险。）	（保持不变）	能够评估和管理网络安全审计风险。
S02-15	S02-15-002	能力管理、组织和实施审计	（此处为通用管理能力，可补充特定补充，但其审计对象应涵盖新时期系统。）	（保持不变）	能力管理、组织和实施审计。
S02-15	S02-15-003	能够形成审计结论、提出审计建议、编制网络安全审计报告、并跟踪审计	（此项为通用审计能力，消除特定补充，但其审计对象应覆盖新时期系统。）	（保持不变）	能够形成审计结论、提出审计建议、编制网络安全审计报告，并跟踪审计。
网络安全认证	S02-16-001	能够对受审核方的信息进行收集和分析	（此处为通用分析能力，支出特定补充，但其对象应为新时期认证。）	（保持不变）	能够对受审核方的信息进行收集和分析。
S02-16	S02-16-002	能按照审核准则编制审核计划	（用于通用计划能力，支出特定补充，但其对象应用于新时期认证。）	（保持不变）	能按照审核准则编制审核计划。
S02-16	S02-16-003	能依据审核计划开展审核活动，发现不符合项并编制审核报告	（用于通用审核能力，支出特定补充，但其对象应为新时期认证。）	（保持不变）	能依据审核计划开展审核活动，发现不符合项并编制审核报告。
电子数据取证	S02-17-001	能够使用普遍取证方法和工具进行调查取证	缺乏对云环境取证、容器取证、AI 系统取证等新兴环境下的取证能力。	增强：明确包含新环境下的取证能力。	能够使用各类取证方法和工具进行调查取证；主要内容包括云环境取证、容器取证、AI 系统取证。
S02-17	S02-17-002	能够完成电子数据恢复	（用于通用恢复能力，消耗特定补充，但其对象应为新时期数据源。）	（保持不变）	能够完成电子数据恢复。
S02-17	S02-17-003	能够完成电子证据数据的提取、固定和保护	（其中为通用保护能力，消耗特定补充，但其对象应为新时期数据源。）	（保持不变）	能够完成电子证据数据的提取、固定和保护。

S02-17	S02-17-004	能够完成电子证据数据的勘察、分析和归档	（此处为通用分析归档能力，消耗特定补充，但其对象应为新时期数据源。）	（保持不变）	能够完成电子证据数据的勘验、分析和归档。
网络安全咨询	S02-18-001	能帮助用户识别和确定网络安全需求	（此处为通用识别能力，可补充特定内容，但其对象应满足新时期需求。）	（保持不变）	能够帮助用户识别和确定网络安全需求。
S02-18	S02-18-002	能够帮助用户进行网络安全方面的规划和设计	（此项为通用规划设计能力，支出特定补充，但其对象应满足新时期需求。）	（保持不变）	能够帮助用户进行网络安全方面的规划和设计。
S02-18	S02-18-003	能够帮助用户建立网络安全管理体系、技能体系和事故体系	（用于通用建立能力，支出特定补充，但其对象应为新时期体系。）	（保持不变）	能够帮助用户建立网络安全管理体系、技能体系和应急体系。
网络安全科研	S02-19-001	能力掌握第一研究领域发展现状和趋势	（此项为通用掌握能力，借以特定补充，但其对象适用于新时期研究领域。）	（保持不变）	能掌握第一学期研究领域的发展现状和趋势。
S02-19	S02-19-002	能够运用相关知识，开展网络安全研究和创新，例如研究新技术及应用、法律法规、政策文件、标准等	对人工智能安全、量子计算安全、元宇宙安全等新兴技术研究和创新能力的匮乏。	增强：明确包含人工智能安全、量子计算安全、元宇宙安全等新兴技术的研究和创新。	能够运用相关知识，开展网络安全研究和创新，例如新技术及应用、法律法规、政策文件、标准等；涵盖人工智能安全、量子计算安全、元宇宙安全等新兴技术研究和创新。掌握混合加密方案设计与实施，具备在现有 TLS/VPN/IPSec 架构中集成 PQC 算法的试点应用技能。
S02-19	S02-19-003	能开展网络安全学术交流	（此处为通用交流能力，消耗特定补充，但其交流内容应涵盖新时期研究。）	（保持不变）	能开展网络安全学术交流。
网络安全培训与评价	S02-20-001	能识别和分析网络安全职业培训需求	（此处为通用识别能力，可补充特定内容，但其对象应满足新时期需求。）	（保持不变）	能识别和分析网络安全职业培训需求。
S02-20	S02-20-002	能根据培训需求设计培训课程，实施网络安全培训，改	缺乏对实战化培训、AI 安全人才培训设计与实施的强调。	强化：明确包含实战化培训、AI 安全人才培训的设计与实施。	能根据培训需求设计培训课程，实施网络安全培训，改进所培训的内容；涵盖实战化培训、AI 安全人才培训设

		进所培训的内容			计与实施。
S02-20	S02-20-003	能够对被培训人员掌握知识和技能的程度进行评价	缺乏对实战能力、人工智能安全技能评价的方法。	增强：明确包含实战能力、AI 安全技能评价。	能够对被培训人员掌握知识和技能的程度进行评价；主题实战能力、人工智能安全技能评价。
新增 AI 安全专业技能	S-AI01	能够对 AI 模型和系统进行安全漏洞分析与修复（包括对抗性攻击、数据投毒、模型窃取等）。	GB 国标未覆盖 AI 系统自身安全漏洞分析与修复的专门技能。	新增：补充 AI 系统安全实践技能空白，以便能够应对 AI 特有攻击。	能够对 AI 模型和系统进行安全漏洞分析与修复（包括对抗性攻击、数据投毒、模型窃取等）。
	S-AI02	能够对抗生成性样本并设计相应的防御策略（对抗性机器学习攻防）。	GB 国标未覆盖对抗性攻击的生成和防御实践技能。	新增：修复 AI 对抗性攻防的技能空白，提升 AI 模型鲁棒性。	能够对抗生成性样本并设计相应的防御策略（对抗性机器学习攻防）。
	S-AI03	能够对 AI 系统进行安全测试与评估（如鲁棒性测试、提示词注入测试、公平性/偏见性测试）。	国标未覆盖 AI 系统特有的安全测试与评估技能。	新增：弥补 AI 系统安全测试的技能空白，保证 AI 系统在应用前的安全性。	能够对 AI 系统进行安全测试与评估（如鲁棒性测试、提示词注入测试、公平性/偏见性测试）。掌握使用工具，进行模型鲁棒性测试、模型偷窃模拟和防御效果验证。
	S-AI04	能够进行 AI 伦理合规性审查与风险评估（识别 AI 应用中的伦理和社会风险）。	国标未覆盖人工智能伦理合规性审查与风险评估技能。	新增：弥补人工智能治理领域的技术空白，适应人工智能法律法规和伦理要求。	能够进行 AI 伦理合规性审查与风险评估（识别 AI 应用中的伦理和社会风险）。
新增高级攻防专业技能	S-PC01	能够进行 0day 漏洞挖掘与利用（识别并利用未公开漏洞）。	GB 国标渗透测试技术未深入到 0day 挖掘和利用。	新增：提升渗透测试技能深度，从而能够发现和利用未知漏洞的能力。	能够进行 0day 漏洞挖掘与利用（识别并利用未公开漏洞）。
	S-PC02	能够与红队工具开发进行高级渗透测试（设计并实施复杂渗透场景，开发免杀工具）。	GB 国标渗透测试技能未涉及高级渗透和红队工具开发。	新增：提升渗透测试技能的实战化和对抗性，产生适应红队行动需求。	能够与红队工具开发进行高级渗透测试（设计并实施复杂渗透场景，开发免杀工具）。
	S-PC03	能组织和威胁实施狩猎活动（主动在海量数据中发现隐藏威胁）。	GB 国标缺乏威胁狩猎的专用技能。	新增：弥补主动防御技能空白，提升威胁发现的先发能力。	能组织和威胁实施狩猎活动（主动在海量数据中发现隐藏威胁）。
	S-PC04	能够进行 APT 攻击溯源与终	GB 国标应急响应技能未深入研究	新增：提升应急响应技能的深度	能够进行 APT 攻击溯源与终点（深度分析攻击链，识别

		点（深度分析攻击链，识别攻击者身份和目的）。	APT 攻击的深度溯源和终点。	和实战性，使其能够响应高级威胁。	攻击者身份和目的）。
新增数据安全专业技能	S-DT01	能够实施隐私计算技术（例如联邦学习、同态加密、安全多方计算的部署与管理）。	国标未覆盖隐私计算技术的实施技能。	新增：补充数据隐私保护技术实践空白，适应数据合规共享需求。	能够实施隐私计算技术（例如联邦学习、同态加密、安全多方计算的部署与管理）。掌握使用 PySyft、FATE 等框架，设计和部署跨机构的联邦学习或安全多方计算方案，并进行性能和安全评估。
	S-DT02	能够进行数据流安全审计与分析（追踪不同系统中的数据、初始的流转安全）。	国标缺乏数据流安全审计的专项技能。	新增：弥补数据全生命周期安全管理中的审计技能空白。	能够进行数据流安全审计与分析（追踪不同系统中的数据、初始的流转安全）。
	S-DT03	能深度应用数据脱敏/加密工具并进行策略优化（针对复杂业务场景的数据安全防护）。	国标数据脱敏/加密技能应用深度不足。	增强：提升数据安全工具应用的深度和策略优化能力。	能深度应用数据脱敏/加密工具并进行策略优化（针对复杂业务场景的数据安全防护）。
新增云重建安全专业技能	S-CN01	能够进行容器安全配置与管理（Docker、Kubernetes 安全队列）。	国标未覆盖容器安全配置和管理技能。	新增：修复云环境修复实践技能空白，适应云环境修复防护需求。	能够进行容器安全配置与管理（Docker、Kubernetes 安全队列）。
	S-CN02	能编写并优化 K8s 安全策略（如 NetworkPolicy、Pod 安全策略）。	GB 国标未覆盖 K8s 安全编写的策略技能。	新增：矫正云矫正安全策略编排技能空白。	能编写并优化 K8s 安全策略（如 NetworkPolicy、Pod 安全策略）。
	S-CN03	能集成与优化云安全服务（CSPM、CWPP、CASB 等云安全产品）。	GB 国标未覆盖云安全服务集成与优化技能。	新增内容：补足云安全产品集成和优化技能空白。	能集成与优化云安全服务（CSPM、CWPP、CASB 等云安全产品）。
新增 DevSecOps 专业技能	S-DS01	能设计并实施 CI/CD 安全自动化（将安全测试、扫描工具集成到 DevOps 流程）。	GB 国标未覆盖 DevSecOps 流程自动化技能。	新增内容：弥补开发安全左移的自动化实践技能空白。	能设计并实施 CI/CD 安全自动化（将安全测试、扫描工具集成到 DevOps 流程）。
	S-DS02	能够实现安全编码规范并进行自动化审查（在代码开发阶段发现并修复安全问题）。	GB 国标安全编码规范落地技能未加强自动化审查。	新增内容：提升安全编码规范落地和自动化审查的能力。	能够实现安全编码规范并进行自动化审查（在代码开发阶段发现并修复安全问题）。

	S-DS03	能够进行自动化安全测试工具集成与调优（SAST、DAST、IAST 工具的有效运用）。	GB 国标自动化安全测试工具集成和调优技能描述不足。	增强：提升自动化安全测试工具的实践应用和优化能力。	能够进行自动化安全测试工具集成与调优（SAST、DAST、IAST 工具的有效运用）。

附录 E：工作任务和知识技能对应

GB 序号	工作任务	对应相关知识	对应相关技能	不足点（新点视角）	改进建议	改进结果（知识、技能、水平）
1	网络安全规划与管理	K01-001K01-002,K01-003,K01-004K01-005,K01-006、K02-001、K02-002、K02-003、K02-004、K02-005	S01-001、S01-002、S01-003、S01-003.S02-01-001、S02-01-002、S02-01-003、S02-01-004、S02-01-005、S02-01-006	缺乏人工智能安全治理、数据要素安全规划等知识技能映射。缺乏明确的能力水平要求。	增强知识：增加 K02-003（风险量化评估、AI 风险评估方法）、K02-005（AI 安全认证体系）技能增强：增加 S02-01-003（利用 AI 进行风险趋势预测）、S02-01-006（架构 AI 系统数据安全与治理规划）水平引入：明确 L1-L4 要求	对应相关知识：K01-001（网络安全概念及发展历程）[L3]K01-004（网络安全法律法规和政策）[L3]K02-003（网络安全风险管理，包含 AI 风险评估方法）[L3]K02-005（网络安全认证认可，包含 AI 安全认证体系）[L2]对应相关技能：S01-001（沟通与协调）[L3]S02-01-003（组织执行风险管理，能利用 AI 预判安全风险趋势）[L3]S02-01-006（能对网络数据安全、个人信息保护和密码管理等进行规划和管理，主题 AI 系统数据安全与治理规划）[L2]整体任务能力水平：L3
2	网络数据安全保护	K01-001、K01-002、K01-003、K01-004、K01-005、K01-006K03-001	S01-001、S01-002、S01-003、S01-004、S02-02-001S02-02-002、S02-02-003	缺乏对要素数据化背景下的数据流通安全、人工智能训练/推理数据安全、隐私计算等新兴技术应用的具体知识技能映射，以及能力水平要求。	知识增强：增加 K03-001（数据要素安全流通）、K03-002（隐私计算技术）、K-DT01（隐私计算技术原理与应用）技能增强：增加 S02-02-002（深度应用隐私计算工具）、S-DT01（能实施计算隐私技术）、S-DT02（能进行数据流安全审计）水平引入：明确 L1-L4 要求	对应相关知识：K03-001（数据安全管理和技术，包含数据要素安全流通）[L3]K03-002（个人信息保护管理和技术，包含隐私计算技术）[L2]K-DT01（隐私计算技术原理与应用）[L3]对应相关技能：S02-02-002（能运用数据安全工具、方法和技术保护数据安全，深度应用隐私计算工具）[L3]S-DT01（能实施隐私计算技术）[L3]S-DT02（能进行数据流安全审计与分析）[L2]整体任务能力水平：L3
3	个人信息保护	K01-001K01-002,K01-003,K01-004、K01-005,K01-006K03-002	S01-001、S01-002、S01-003S01-004、S02-03-001、S02-03-002、S02-03-003	缺乏对个人信息跨境传输合规、AI 模型中个人信息隐私保护、匿名化/去标识化技术应用的具体知识技能映射，以及能力水平要求。	知识增强：增加 K03-002（个人信息跨境传输合规、匿名化/去标识化、隐私计算技术）技能增强：增加 S02-03-002（深度应用隐私计算工具）、S02-03-003（界面 AI 模型中个人隐私信息保护审查）水平引入：明确 L1-L4 要求	对应相关知识：K03-002（个人信息保护管理和技术，包含个人信息跨境结算传输合规、匿名化/去标识计算化技术、隐私计算化技术）[L3]对应相关技能：S02-03-002（能运用个人信息保护工具、方法和技术保护个人信息，深度应用隐私工具）[L3]S02-03-003（能对个人信息保护工作进行符合性审查，区域 AI 模型中个人信息隐私保护审查）[L2]整体任务能力水平：L3
4	密码技术应	K01-001、	S01-001、	缺乏对隐私计算相关密	增强知识：增加 K09-001（后量子密码、同态	对应相关知识：K09-001（密码技术、密码产品及

	用	K01-002K01-003K01-004、K01-005、K01-006K09-001	S01-002,S01-003.S01-004、S02-04-001、S02-04-002、502-04-003	码技术（类似于加密、安全多方计算）、后量子密码等前沿密码技术在应用中的知识技能映射，以及能力水平要求。	加密等隐私计算相关密码技术）技能增强：增加 S02-04-002（深度应用隐私计算相关密码技术）、S02-04-003（底层后量子密码应用评估）水平引入：明确 L1-L4 要求	服务功能及原理，包含后量子密码、同态加密等隐私相关计算密码技术）[L3]对应相关技能：S02-04-002（能引发密码保护产品，方法和技术实施密码保护，深度应用计算隐私相关密码技术）[L3]S02-04-003（能对信息系统密码应用安全性进行评估并提出整改建议，得出后量子密码应用评估）[L2]整体任务能力水平：L3
5	网络安全需求分析	K01-001、K01-002、K01-003、K01-004、K01-005、K01-006K04-001、K06-003K10-001,K10-002	S01-001、S01-002、S01-003、S01-004、S02-05-001	对缺乏人工智能系统、云原生环境、要素数据流动等新时期安全需求分析知识技能映射，以及能力水平要求。	增强知识：增加 K04-001（云原生系统建模）、K10-001（AI 安全）技能增强：增加 S02-05-001（底层 AI 系统、云原生风险识别）水平引入：明确 L1-L4 要求	对应相关知识：K01-002（网络安全管理基本知识）[L2]K04-001（系统建模理论和常用方法，包含云重建系统建模）[L2]K10-001（新应用安全，包含 AI 安全）[L2]对应技能：S01-002（能理解业务，识别网络安全目标组织）[L3]S02-05-001（能够识别网络安全保护对象，并分析其面临的安全风险，涵盖 AI 系统、云突破风险识别）[L3]整体任务能力水平：L3
6	网络安全架构设计	K01-001、K01-002、K01-003、K01-004、K01-005、K01-006、K04-002、K04-003、K05-003、K05-006、K10-001、K10-002	S01-001,S01-002、S01-003、S01-004、S02-06-001,502-06-002S02-06-003	缺乏对云原生安全架构、零信任架构、数据安全架构、AI 系统安全架构等新时期架构设计知识技能映射，以及能力水平要求。	增强知识：增加 K04-003（AI 系统安全架构）、K04-003（云安全架构、零信任架构、数据安全架构）技术增强：增加 S02-06-002（涵盖 AI 系统安全架构设计等）水平引入：明确 L1-L4 要求	对应相关知识：K04-003（安全架构模型及设计方法，包含 AI 系统、云原生、零信任、数据安全架构）[L3]K01-003（网络安全技术基本知识）[L2]对应相关技能：S02-06-002（能设计网络安全架构，曲面 AI 系统、云架构等安全架构设计）[L3]S02-06-001（能理解网络安全需求）[L3]整体任务能力水平：L3
7	网络安全开发	K01-001、K01-002、K01-003、K01-004、K01-005.K01-006K04-002K05-001、K05-002、K05-003、K05-004K10-001K10-002	S01-001,S01-002、S01-003.S01-004,S02-07-001S02-07-002、S02-07-003	缺乏对 DevSecOps 实践、安全左移、云原生应用、AI 应用开发安全知识技能映射，以及能力水平要求。	知识增强：增加 K05-001（DevSecOps 流程）、K10-001（AI 应用安全开发）技能增强：增加 S02-07-001（DevSecOps 实践）、S-DS01（能设计并实施 CI/CD 规范安全自动化）、S-DS02（能落地安全编码规范）水平引入：明确 L1-L4 要求	对应相关知识：K05-001（安全开发，包含 DevSecOps 流程）[L3]K10-001（新型应用安全，包含 AI 应用安全开发）[L2]对应相关技能：S02-07-001（能用特定语言进行安全编码，涵盖 DevSecOps 实践）[L3]S-DS01（能设计并实施 CI/CD 简化安全自动化）[L2]S-DS02（能落地安全编码规范并进行自动化审查）[L3]整体任务能力水

						平：L3
8	供应链安全管理	K01-001、K01-002、K01-003、K01-004、K01-005、K01-006K02-001、K10-001、K10-002	S01-001,S01-002,S01-003S01-004,S02-08-001,S02-08-002S02-08-003	缺乏对软件清单（SBOM）管理、开源组件安全管理等新时期实践的知识技能映射，以及能力水平要求。	增强知识：增加 K02-001（SBOM 管理）技能增强：增加 S02-08-001（封面 SBOM 分析）、S02-08-002（封面开源组件风险识别）水平引入：明确 L1-L4 要求	对应相关知识：K02-001（供应链安全管理，包含 SBOM 管理）[L3]对应相关技能：S02-08-001（能识别供应链安全风险，覆盖 SBOM 分析）[L3]S02-08-002（能实施供应链安全保护，涵盖开源组件风险识别）[L2]整体任务能力水平：L3
9	网络安全集成实施	K01-001、K01-002、K01-003、K01-004、K01-005、K01-006、K05-002、K05-003K05-004、K10-001、K10-002	S01-001S01-002、S01-003、S01-004、S02-09-001,502-09-002、S02-09-003	缺乏对云安全产品、XDR、SOAR 等新型安全产品集成知识技能映射，以及能力要求。	增强知识：增加 K06-003（XDR、SOAR 原理）技能增强：增加 S02-09-001（涵盖 XDR、SOAR 集成）水平引入：明确的 L1-L4 要求	对应相关知识：K06-003（网络安全产品功能及原理，包含 XDR、SOAR 原理）[L2]对应相关技能：S02-09-001（能完成网络安全及信息化产品、配置、调试及设置，涵盖 XDR、SOAR 集成）[L3]整体任务能力水平：L3
10	网络安全运输维护	K01-001、K01-002K01-003、K01-004、K01-005、K01-006K05-003、K05-006K06-001、K06-002.K06-003、K06-004、K06-005K06-006K07-001K07-002,K10-001K10-002	S01-001、S01-002、S01-003、S01-004、S02-10-001、SO2-10-002、502-10-003、S02-10-004	缺乏对云原生环境（容器、K8s）运维、大数据平台运维、工业控制系统（ICS）/运营技术（OT）运维安全知识技能映射，以及能力水平要求。	增强知识：增加 K06-004（容器、K8s 安全）、K06-006（大数据平台安全）技能增强：增加 S02-10-002（载体、K8s 运维）、S02-10-004（载体大数据平台运维）水平引入：明确 L1-L4 要求	对应相关知识：K06-004（操作系统安全原理及使用，包含容器、K8s 安全）[L2]K06-006（数据库安全技术及使用，包含大数据平台安全）[L2]对应相关技能：S02-10-002（能维护操作系统、服务器、仓储设备及终端设备等的安全运行，天线容器、K8s 运维）[L3]S02-10-004（能完成数据库系统管理、维护和安全防护等，涵盖大数据平台运维）[L2]整体任务能力水平：L3
11	网络安全监测与分析	K01-001K01-002、K01-003、K01-004、K01-005、K01-006、K02-002、K05-003K05-005、K05-006K06-002,K06-003、K07-001、	S01-001,S01-002,S01-003.S01-004,S02-11-001、S02-11-002S02-11-003	缺乏对威胁狩猎、人工智能驱动的智能监测分析知识技能映射，以及能力水平要求。	知识增强：增加 K07-001（威胁狩猎）、K07-002（机器学习在安全分析中应用）技能增强：增加 S02-11-003（威胁狩猎、人工智能驱动监测）、S-PC03（能和实施威胁狩猎活动）水平引入：明确 L1-L4 要求	对应相关知识：K07-001（网络安全监测方法和技术，包含威胁狩猎）[L3]K07-002（网络安全分析方法和技术，包含安全分析中应用的机器学习）[L2]相关技能：S02-11-003（能使用各类方法和工具进行网络安全监控驱动分析、威胁狩猎、人工智能监测）[L3]S-PC03（能组织和实施威胁狩猎活动）[L3]整体任务能力水平：L3

		K07-002、K10-001、K10-002				
12	网络安全事故管理	K01-001、K01-002、K01-003、K01-004、K01-005、K01-006、K02-002、K05-003、K05-005、K05-006、K06-001、K07-001、K07-002、K08-001、K10-001、K10-002	S01-001、S01-002、S01-003S01-004、S02-12-001、S02-12-002、S02-12-003.S02-12-004 S02-12-005	缺乏对实战化攻防演练组织与执行、AI 驱动的自动化应急响应、APT 攻击溯源与后果等高强度实践知识技能映射，以及能力水平要求。	技能增强：增加 K02-002（自动化应急响应）、K05-006（红蓝对抗策略）、K08-001（APT 攻击取证）技能增强：增加 S02-12-004（AI 自动化应急响应）、S02-12-005（实战化练）、S-PC04（能进行 APT 攻击溯源与救援）水平引入：明确 L1-L4 要求	对应相关知识：K02-002（管理应急方法和技术，包含自动化应急响应）[L3]K05-006（网络攻防技术，包含红蓝对抗策略）[L3]K08-001（调查取证方法和技术，包含 APT 攻击取证）[L2]对应相关技能：S02-12-004（能利用常见安全技术手段进行应对，包含 AI 自动化应急响应）[L3]S02-12-005（能进行APT攻击溯源与漏洞)[L3]整体任务能力水平：L3
十三	网络安全审计	K01-001K01-002、K01-003、K01-004、K01-005、K01-006K02-004K10-001,K10-002	S01-001、S01-002、S01-003、S01-004、S02-15-001S02-15-002、S02-15-003	缺乏对人工智能系统审计、云审计、自动化审计以及新时期审计知识技能映射、能力水平要求。	知识增强：增加 K02-004（自动化审计）、K10-001（AI 系统审计）技能增强：增加 S02-15-002（覆盖自动化审计）、S02-15-003（覆盖 AI 系统审计）水平引入：明确 L1-L4 要求	对应相关知识：K02-004（网络安全审计方法和技术，包含自动化审计）[L2]K10-001（新技术新安全，包含人工智能系统审计）[L2]相关技能：S02-15-002（能管理、组织和实施审计，覆盖自动化审计）[L3]S02-15-003（能做出审计结论，构建 AI 系统审计）[L2]应答自动化任务能力水平应用：L3
14	网络安全测试	K01-001、K01-002、K01-003、K01-004K01-005、K01-006、K02-003、K05-003、K05-004、K05-005、K07-002、K10-001K10-002	S01-001、S01-002、S01-003、S01-004、S02-13-001,S02-13-002	缺乏对自动化应用安全测试（SAST/DAST/IAST）、容器安全扫描、AI 系统安全测试（鲁棒性、偏见性、公平性测试）等新时期测试方法知识技能映射，以及能力水平要求。	增强知识：增加 K05-004（AI 系统安全测试）、K05-005（高级渗透测试）技能增强：增加 S02-13-001（内容 AI 系统安全测试）、S-PC02（能进行高级渗透测试）水平引入：明确 L1-L4 要求	对应相关知识：K05-004（安全测试、评估方法，包含 AI 系统安全测试）[L3]K05-005（渗透测试方法和技术，包含高级渗透测试）[L3]对应相关技能：S02-13-001（能完成脆弱性测试和渗透性测试，平面 AI 系统安全测试，高级渗透测试）[L3]整体任务能力水平：L3
15	网络安全评估	K01-001,K01-002,K01-003,K01-004、K01-004.K01-006、K02-003,K05-003,K	S01-001、S01-002、S01-003、S01-004、S02-14-001S02-14-002、S02-14-003	缺乏对 AI 系统风险评估、云原生环境风险评估、供应链安全风险评估等新时期的知识技能映	知识增强：增加 K02-003（AI 风险评估）、K10-001（云原生环境安全）、K02-001（供应链安全）技能增强：增加 S02-14-002（框架 AI 系统、云内部风险评估）水平引入：明确	对应相关知识：K02-003（网络安全风险管理，包含 AI 风险评估）[L3]K10-001（全新安全，包含云重建环境安全）[L2]K02-001（供应链安全管理）[L2]相关技能：S02-14-002（能使用各类评估相关

		05-005,K07-002,K10-001,K10-002		射评估，以及能力水平要求。	L1-L4 要求	工具和方法分析并评估安全风险，覆盖 AI 系统、云应用风险评估）[L3]整体任务能力水平：L3
16	网络安全认证	K01-001,K01-002,K01-003,K01-004K01-005,K01-006,K02-003、K02-005、K10-001K10-002	S01-001S01-002、S01-003、S01-004、S02-16-001,S02-16-002,S02-16-003	缺乏对数据安全认证、AI 安全认证体系等新时期认证知识技能映射，以及能力水平要求。	增强知识：增加 K02-005（数据安全认证、AI 安全认证体系）技能增强：增加 S02-16-003（底层数据安全认证、AI 安全认证）引入水平：明确 L1-L4 要求	对应相关知识：K02-005（网络安全认证认可，数据安全认证、AI 安全认证体系）[L2]相关技能：S02-16-003（能依据审核计划开展审核活动，发现不符合项并编制审核报告，概览数据安全认证、AI 安全认证）[L3]整体任务能力水平：L3
17	电子数据取证	K01-001、K01-002、K01-003、K01-004、K01-005K01-006K08-001K10-001、K10-002	S01-001501-002、S01-003、S01-004、S02-17-001、S02-17-002、S02-17-003、S02-17-004	缺乏对云环境取证、容器取证、AI 系统取证、APT 攻击深度取证等新时期取证知识技能映射，以及能力水平要求。	增强知识：增加 K08-001（云环境取证、AI 系统取证）、K05-006（APT 攻击原理证）技能增强：增加 S02-17-001（面向云环境取证、AI 系统取证）、S-PC04（能进行 APT 攻击溯源与可信度）水平引入：明确的 L1-L4 要求	对应相关知识：K08-001（调查取证方法和技术，包含云环境取证、AI 系统取证）[L3]K05-006（网络攻防技术，包含 APT 攻击原理）[L2]对应相关技能：S02-17-001（能使用各类取证方法和工具进行调查取证，框架云环境取证、AI 系统取证）[L3]S-PC04（能进行 APT 攻击源与前沿）[L3]整体任务能力水平：L3
18	网络安全咨询	K01-001、K01-002、K01-003、K01-004K01-005、K01-006K10-001、K10-002	S01-001、S01-002、S01-003、S01-004S02-18-001S02-18-002、S02-18-003	缺乏对人工智能安全、数据要素安全、工业互联网安全等新兴领域咨询知识技能映射，以及能力水平要求。	增强知识：增加 K10-001（人工智能安全）、K03-001（数据要素安全）、K10-002（工业互联网安全）技能增强：增加 S02-18-001（新兴领域需求识别）水平引入：明确 L1-L4 要求	对应相关知识：K10-001（新技术新应用安全，包含人工智能安全）[L3]K03-001（数据安全管理和技术，包含数据需求安全）[L2]K10-002（特定行业网络安全知识，包含工业互联网安全）[L2]相关技能：S02-18-001（能帮助用户识别和确定网络安全需求，掌握新兴领域需求识别）[L3]对应任务能力水平：L3
19	网络安全研究	K01-001、K01-002、K01-003、K01-004、K01-005K01-006K10-001,K10-002,K10-003	S01-001、S01-002、S01-003、S01-004、S02-19-001S02-19-002、S02-19-003	缺乏对 AI 安全前沿研究（如大模型安全、对抗性机器学习）、量子计算安全研究、元宇宙安全研究等新兴和交叉领域研究知识技能映射，以及能力水平要求。	知识增强：增加 K10-001（AI 安全前沿研究）、K09-001（后量子密码）技能增强：增加 S02-19-002（面罩新兴技术研究）、S-AI01（能对 AI 模型和系统进行安全漏洞分析与修复）水平引入：明确 L1-L4 要求	对应相关知识：K10-001（新技术新应用安全，包含 AI 安全前沿研究）[L4]K09-001（密码技术与知识，包含后量子密码）[L3]相关技能：S02-19-002（能运用相关知识，开展网络安全研究和创新，论坛新兴技术研究）[L4]S-AI01（能对 AI 模型和系统应对安全漏洞分析与修复）[L3]任务能力水平：L4
20	网络安全培	K01-001、	S01-001S01-002,S01-00	缺乏对实战化培训与评	增强知识：增加 K10-003（实战攻防理论）技	对应相关知识：K10-003（实战领域相关知识，包

	训与评价	K01-002K01-003、K01-004、K01-005、K01-006,K10-001、K10-002、K10-004	3、S01-004、S02-20-001S02-20-002、S02-20-003	价、AI 安全人才培训设计与实施、AI 工具提升培训效率的知识技能映射以及能力水平要求。	能增强：增加 S02-20-002（底层实战化、AI 安全培训设计）、S02-20-003（底层实战能力、AI 安全技能评价）水平引入：明确 L1-L4 要求	含实战攻防理论）[L2]K10-001（新应用安全，包含 AI 安全）[L2]对应相关技能：S02-20-002（能根据培训需求培训课程，实施网络安全培训，内容实战化、AI 安全培训设计）[L3]S02-20-003（能对被培训人员掌握知识和技能的程度进行评价，主题实战能力、AI 安全技能评价）[L3]整体任务能力水平：L3
	新增任务	KT-AI01	AI 模型安全评估与分析	K-AI01（对抗性机器学习原理与防御）[L3]K-AI02(AI 模型可信赖性理论）[L3]K-AI03（大型模型安全原理与攻防技术）[L2]	S-AI01（能对 AI 模型和系统进行安全漏洞分析与修复）[L3]S-AI03（能对 AI 系统进行安全测试与评估）[L3]	整体任务能力水平：L3
	新增任务	KT-AI02	大模型应用安全开发与测试	K-AI03（大模型安全原理与攻防技术）[L3]K05-001（安全开发）[L2]	S-AI03（能对 AI 系统进行安全测试与评估）[L3]S02-07-001（能用特定语言进行安全编码）[L3]	整体任务能力水平：L3
	新增任务	KT-PC01	组织和实施威胁狩猎活动	K-PC01（威胁狩猎方法论）[L3]K-PC02(ATT&CK 框架深度理解）[L3]K07-001（网络安全监测方法）[L2]	S-PC03（能组织和实施威胁狩猎活动）[L3]S-PC06（能进行威胁情报分析与应用）[L3]S02-11-003（能使用各类方法和工具进行网络安全监控分析）[L3]	整体任务能力水平：L3
	新增任务	KT-PC02	开展高强度红蓝对抗演练	K-PC02(ATT&CK 框架深度理解）[L3]K05-006（网络攻防技术）[L3]K10-003（实战领域相关知识）[L2]	S-PC02（能进行高级渗透测试与红队工具开发）[L4]S02-12-005（能进行抽样调查预案开展演练）[L3]	整体任务能力水平：L4
	新增任务	KT-PC03	进行 APT 攻击溯源与终点	K-PC02(ATT&CK 框架深	S-PC04（能进行 APT 攻击溯源与精准）	整体任务能力水平：L4

				度理解)[L3]K05-006(网络攻防技术) [L3]K08-001（调查取证方法和技术）[L3]	[L4]S02-17-001（能使用主流取证方法和工具进行调查取证）[L3]	
	新增任务	KT-PC04	0day 漏洞挖掘与利用	K-PC04(0day 漏洞挖掘技术）[L4]K05-005（渗透测试方法和技术）[L3]	S-PC01（能进行 0day 漏洞挖掘与利用） [L4]S02-13-001（能完成渗透测试）[L3]	整体任务能力水平：L4
	新增任务	KT-DT01	数据保障安全流通流程设计与	K03-001（数据安全管理和技术)[L3]K03-002(个人信息保护管理和技术）[L2]	S-DT02（能进行数据流安全审计与分析） [L3]S02-02-002（能运用数据安全工具保护数据安全）[L3]	整体任务能力水平：L3
	新增任务	KT-DT02	实施隐私计算技术	K-DT01（隐私计算技术原理与应用） [L3]K09-001（密码技术与应用知识）[L2]	S-DT01（能实施隐私计算技术） [L3]S02-04-002（能实施密码保护产品实施密码保护）[L2]	整体任务能力水平：L3

附录 F：角色和工作任务对应

序号	角色	工作任务	不足	改进建议	修改结果
1	网络安全管理人员	网络安全需求分析网络安全规划和管理	未明确 AI 安全治理、数据要素安全规划等战略性任务。缺乏对高层决策者（如 CSO）角色的专门细化，难以体现安全治理与业务战略的深度融合。	角色增强：细化为“安全治理专家”“首席安全官（CSO）/首席数据官（CDO）”等。任务增强：增加制定 AI 伦理与治理政策、安全治理体系评估与优化等战略性任务。	工作任务：网络安全需求分析，网络安全规划和管理，网络数据安全保护，个人信息保护，密码技术应用，网络安全咨询，制定 AI 伦理与治理政策，安全治理体系评估与优化
2	数据安全保护人员	网络安全需求分析网络数据安全保护	缺乏对数据要素化背景下数据流通安全、隐私计算技术应用等新任务的覆盖。未区分数据安全管理与数据隐私保护的特定任务。	角色增强：细化为“数据隐私架构师”“数据治理专家”。任务增强：增加数据要素安全流通保障、实施隐私计算技术等任务。	工作任务：网络安全需求分析，网络数据安全保护，个人信息保护，密码技术应用，数据要素安全流通保障，实施隐私计算技术
3	个人信息保护人员	网络安全需求分析个人信息保护	缺乏对个人信息跨境传输合规、AI 模型中个人信息隐私保护等新挑战的任务覆盖。	任务增强：明确个人信息保护任务中涵盖个人信息跨境传输合规性保障、AI 模型中个人信息隐私保护。	工作任务：网络安全需求分析，个人信息保护（涵盖个人信息跨境传输合规性保障、AI 模型中个人信息隐私保护）
4	密码应用人员	网络安全需求分析密码技术应用	缺乏对隐私计算相关密码技术（如同态加密）等前沿密码应用任务的覆盖。	任务增强：明确密码技术应用任务中包含隐私计算相关密码技术应用。	工作任务：网络安全需求分析，密码技术应用（涵盖隐私计算相关密码技术应用）
5	网络安全咨询人员	网络安全咨询	缺乏对 AI 安全、数据要素安全、工业互联网安全等新兴领域咨询任务的覆盖。	任务增强：明确网络安全咨询任务中涵盖 AI 安全咨询、数据要素安全咨询、工业互联网安全咨询。	工作任务：网络安全咨询（涵盖 AI 安全、数据要素安全、工业互联网安全等新兴领域咨询）
6	网络安全架构设计人员	网络安全需求分析网络安全架构设计	缺乏对云原生安全架构、零信任架构、AI 系统安全架构等新时期主流架构的设计任务。	任务增强：明确网络安全架构设计任务中涵盖云原生安全架构设计、零信任架构设计、AI 系统安全架构设计。	工作任务：网络安全需求分析，网络安全架构设计（涵盖云原生、零信任、AI 系统安全架构设计）
7	网络安全开发集成人员	网络安全需求分析网络安全开发供应链安全管理网络安全集成实施	缺乏对 DevSecOps 实践、云原生应用安全开发、AI 应用开发安全，以及自动化集成等任务的覆盖。	角色增强：细化为“DevSecOps 工程师”。任务增强：明确网络安全开发任务中涵盖云原生应用开发安全、AI 应用开发安全、CI/CD 流水线安全自动化。	工作任务：网络安全需求分析，网络安全开发（涵盖云原生应用开发安全、AI 应用开发安全），供应链安全管理，网络安全集成实施（涵盖自动化安全集成）
8	网络安全运维人员	网络安全运维	缺乏对云原生环境（容器、K8s）运维、大数据平台运维、工业控制系统（ICS）/运营技术（OT）运维安全等新任务的覆盖。	任务增强：明确网络安全运维任务中涵盖云原生环境运维安全、大数据平台运维安全、工业控制系统/运营技术（OT）运维安全。	工作任务：网络安全运维（涵盖云原生环境运维安全、大数据平台运维安全、工业控制系统/运营技术、OT 运维安全）
9	网络安全监测分	网络安全监测和分析	缺乏对威胁狩猎、AI 驱动的智能监测分析	角色增强：细化为“威胁狩猎专家”“AI 驱动安全分析	工作任务：网络安全监测和分析（涵盖组织和实施

	析人员		等主动性、智能化监测分析任务的覆盖。	师”。任务增强：明确网络安全监测和分析任务中涵盖组织和实施威胁狩猎活动、利用 AI 进行智能监测分析。	威胁狩猎活动、利用 AI 进行智能监测分析）
10	网络安全应急管理人员	网络安全应急管理	缺乏对实战化攻防演练组织与执行、AI 驱动的自动化应急响应、APT 攻击溯源与归因等高强度实践任务的覆盖。	角色增强：细化为“高级事件响应专家”“攻防协同专家（紫队）”。任务增强：明确网络安全应急管理任务中涵盖开展高强度红蓝对抗演练、进行 APT 攻击溯源与归因、利用 AI 进行自动化应急响应。	工作任务：网络安全应急管理（涵盖开展高强度红蓝对抗演练、进行 APT 攻击溯源与归因、利用 AI 进行自动化应急响应）
11	网络安全审计人员	网络安全审计	缺乏对 AI 系统审计、云环境审计等新兴审计任务的覆盖。	任务增强：明确网络安全审计任务中涵盖 AI 系统审计、云环境审计。	工作任务：网络安全审计（涵盖 AI 系统审计、云环境审计）
12	电子数据取证人员	电子数据取证	缺乏对云环境取证、容器取证、AI 系统取证等新兴环境取证任务的覆盖。	任务增强：明确电子数据取证任务中涵盖云环境取证、容器取证、AI 系统取证。	工作任务：电子数据取证（涵盖云环境取证、容器取证、AI 系统取证）
13	网络安全测评人员	网络安全测试网络安全评估	缺乏对自动化应用安全测试、容器安全扫描、AI 系统安全测试（鲁棒性、偏见性、公平性测试）等新任务的覆盖。	任务增强：明确网络安全测试任务中涵盖自动化应用安全测试、容器安全扫描、AI 系统安全测试。明确网络安全评估任务中涵盖 AI 系统风险评估、云原生环境风险评估。	工作任务：网络安全测试（涵盖自动化应用安全测试、容器安全扫描、AI 系统安全测试），网络安全评估（涵盖 AI 系统风险评估、云原生环境风险评估）
14	网络安全防护人员	网络安全集成实施网络安全运维网络安全测试	该角色范围过于宽泛，与“网络安全集成实施”“网络安全运维”“网络安全测试”等已有角色存在任务重叠。未体现新兴防护理念（如零信任）。	建议：拆分或融入其他更具体的角色中，或重新定义为“安全体系实施者”等更聚焦的角色。任务增强：若保留，则需涵盖零信任体系实施、新兴安全产品部署与优化。	建议：该角色在新框架下可被更专业化的角色（如 DevSecOps 工程师、云原生安全架构师）替代或任务融入其他角色。
15	网络安全认证人员	网络安全认证	缺乏对数据安全认证、AI 安全认证等新兴认证任务的覆盖。	任务增强：明确网络安全认证任务中涵盖数据安全认证、AI 安全认证。	工作任务：网络安全认证（涵盖数据安全认证、AI 安全认证）
16	网络安全科学研究人员	网络安全科学研究	缺乏对 AI 安全前沿研究（如大模型安全、对抗性机器学习）、量子计算安全研究、元宇宙安全研究等新兴和交叉领域研究任务的覆盖。	角色增强：细化为“AI 安全科学家”“量子安全研究员”。任务增强：明确网络安全科学研究任务中涵盖 AI 安全前沿研究、量子计算安全研究、元宇宙安全研究。	工作任务：网络安全科学研究（涵盖 AI 安全前沿研究、量子计算安全研究、元宇宙安全研究）
17	网络安全培训人员	网络安全培训和评价	缺乏对实战化培训与评价、AI 安全人才培训设计与实施等新任务的覆盖。	任务增强：明确网络安全培训和评价任务中涵盖实战化培训与评价、AI 安全人才培训设计与实施。	工作任务：网络安全培训和评价（涵盖实战化培训与评价、AI 安全人才培训设计与实施）
18	其他	（无）	（占位符，无具体任务定义）	建议：移除此占位符，新时期所有网络安全相关工作应有明确的角色或归入现有角色范畴。	建议：移除该行，具体工作任务应归入明确的工作角色。

参考文献：

【1】 网络安全法。[2017]

【2】 数据安全法。[2021]

【3】 个人信息保护法。[2021]

【3】 GB/T 42446-2023《网络安全人员能力要求》[2023]

【3】 网络安全产业人才发展报告。信通院、工业和信息化部教育与考试中心、中国网络空间新兴技术安全创新论坛等。[2024]

【3】 European e-Competences Framework 3.0.[2013]

【3】 European cybersecurity skills framework.[2022]

【3】 NICE-NIST 信息安全人才框架。[2017]