ICS 35.030
CCS L80

T/CAICI

中 国 通 信 企 业 协 会 团 体 标 准

T/CAICI 98—2024

网络与数据安全运营岗位职业能力规范

Professional competence specification for network and data security operations positions

2024-12-03 发布　　2024-12-25 实施

中国通信企业协会　发布

目　　次

前　言

本文件按照 GB/T 1.1—2020《标准化工作导则　第 1 部分：标准化文件的结构和起草规则》的规定起草。

本文件由中国通信企业协会标准化管理委员会提出并归口。

本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件主要起草单位：杭州安恒信息技术股份有限公司、中移建设有限公司浙江分公司、联通（广东）产业互联网有限公司、杭州职业技术学院、浙江建设职业技术学院、华南师范大学、韩山师范学院、云南轻纺职业学院、上海东海职业技术学院、南京工业大学浦江学院、广西职业技术学院、广东财贸职业学院。

本文件主要起草人：苗春雨、卢小波、杜廷龙、陈星、韩超、胡曦、林兵、苏轶、陈云志、宣乐飞、邵梁、陈晓伟、李瑞维、林怀恭、钟平、李铸、白旭乾、张居阳、徐焱鑫、陈盛、孟勤、罗云芳、黎斌、项尚清、孟威。

网络与数据安全运营岗位职业能力规范

1 范围

本文件规定了网络与数据安全运营岗位及能力要求。

本文件适用于第三方评估机构以及企业对网络与数据安全运营岗位能力的评估、指导和培训等。用人单位的相关人员聘用、培训与考核可参照使用。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 25069—2022 信息安全技术 术语

GB/T 37988—2019 信息安全技术 数据安全能力成熟度模型

3 术语和定义

GB/T 25069—2022 和 GB/T 37988—2019 界定的术语和定义适用于本文件。

3.1

数据 data

是指任何以电子或者其他方式对信息的记录。

3.2

数据安全 data security

通过采取必要措施，确保数据处于有效保护和合法利用的状态，以及具备保障持续安全状态的能力

[来源：GB/T 35274—2023，3.2]

3.3

数据处理 data handling

数据操作的系统执行,以实现特定目的的数据收集、存储、使用、加工、传输、提供、公开、销毁等活动。

[来源：GB/T 35274—2023，3.17]

3.4

个人信息　personal information

以电子或者其他方式记录的能够单独或者与其他信息结合识别特定自然人身份或者反映特定自然人活动情况的各种信息。

[来源：GB/T 35273—2020，3.1]

3.5

风险评估　risk assessment

风险识别、风险分析和风险评价的整个过程。

[来源：GB/T 20984—2022，3.1.2]

3.6

应急响应　emergency response

组织为了应对突发/重大信息安全事件的发生所做的准备，以及在事件发生后所采取的措施。

[来源：GB/T 24363—2009，3.4]

3.7

安全策略　security policy

用于治理某一组织及其系统内管理、保护并分发影响安全及有关元素的资产（包括敏感信息）的一组规则、指导和实践。

[来源：GB/T 25069—2022，3.3]

3.8

风险管理　risk management

指导和控制组织相关风险的协调活动。

[来源：GB/T 25069—2022，3.168]

4　缩略语

下列缩略语适用于本文件。

ICMP	因特网控制报文协议	Internet Control Message Protocol
IP	网际互连协议	Internet Protocol
SOAR	安全编排自动化响应	Security Orchestration, Automation and Response
SOC	安全运营中心	security operations center
SSL	安全套接层	Secure Socket Layer
TCP	传输控制协议	Transmission Control Protocol
TLS	传输层安全性协议	Transport Layer Security
UDP	用户数据报协议	User Datagram Protocol

5 职业概况

5.1 职业名称

安全运营工程师、数据安全管理员

5.2 职业编码

2-02-10-07 信息安全工程技术人员

2-02-38-12 数据安全工程技术人员

5.3 职业定义

从事网络安全、数据安全需求分析挖掘、技术方案设计、项目实施、运营管理等工作的工程技术人员。

5.4 职业技能等级

安全运营工程师：本职业共设 3 个等级，分别为初级、中级、高级。

数据安全管理员：本职业共设 3 个等级，分别为初级、中级、高级。

5.5 职业环境条件

室内、室外。

5.6 职业能力特征

具有较强的学习能力、计算能力、表达能力及分析、推理和判断能力。

5.7 普通受教育程度

大学专科毕业及以上（或同等学力）。

5.8 培训学时要求

初级不少于 40 标准学时；中级不少于 40 标准学时；高级不少于 40 标准学时。以上学时含线上及线下学时。

5.9 职业技能鉴定要求

5.9.1 申报条件

安全运营工程师

具备以下条件之一者可申报初级：

a） 具备相关专科学历，从事本职业或相关职业技术工作满 1 年；

b） 具备相关本科及以上学历（含在读未取得证书的的应届毕业生）；

c） 取得高级技工学校、技师学院毕业证书后，累计从事本职业或相关职业工作 1 年（含）以上。

具备以下条件之一者可申报中级：

a） 具备大学专科学历，从事本职业或相关职业技术工作满 2 年；

b） 具备大学本科及以上学历，从事本职业或相关职业技术工作满 1 年；

c） 具备大学本科第二学历或硕士学历（含在读未取得证书的应届毕业生）；

d） 取得高级技工学校、技师学院毕业证书后，累计从事本职业或相关职业工作 2 年（含）以上。

具备以下条件之一者可申报高级：

a） 取得高级技工学校、技师学院毕业证书后，已从事本职业技术工作满 3 年或取得中级安全运营认证后，继续从事本职业技术工作满 1 年；

b） 具备大学本科学历或学士学位，或大学专科学历，已从事本职业技术工作满 3 年或取得中级安全运营认证后，继续从事本职业技术工作满 1 年；

c） 具备硕士学位或第二学士学位，已从事本职业技术工作满 1 年；

d） 具备相关专业博士学位，已从事本职业技术工作满 1 年，或取得中级安全运营认证后，继续从事本职业技术工作满 1 年。

数据安全管理员

具备以下条件之一者可申报初级：

a） 具备大学本科及以上学历（含在读的应届毕业生）；

b） 具备大学专科学历，从事本职业或相关职业技术工作满 1 年；

c） 取得高级技工学校、技师学院毕业证书后，累计从事本职业或相关职业工作 2 年（含）以上。

具备以下条件之一者可申报中级：

a） 具备大学本科及以上学历（含在读的应届毕业生）；

b） 具备大学专科学历，从事本职业或相关职业技术工作满 2 年；

c） 取得高级技工学校、技师学院毕业证书后，累计从事本职业或相关职业工作 3 年（含）以上。

具备以下条件之一者可申报高级：

a） 取得高级技工学校、技师学院毕业证书后，已从事本职业技术工作满 4 年或取得中级数据安全管理员认证后，继续从事本职业技术工作满 2 年；

b） 具备大学本科学历或学士学位，或大学专科学历，已从事本职业技术工作满 3 年或取得中级数据安全管理员认证后，继续从事本职业技术工作满 1 年；

c） 具备硕士学位或第二学士学位，已从事本职业技术工作满 2 年或取得中级数据安全管理员认证后，继续从事本职业技术工作满 1 年；

d） 具备相关专业博士学位，已从事本职业技术工作满 1 年，或取得中级数据安全管理员认证后，继续从事本职业技术工作满 1 年。

5.9.2 鉴定方式

鉴定方式分为理论知识考试、技能考核。理论知识考试以笔试、机考等方式为主，主要考核从业人员从事本职业（专业）应掌握的基本要求和相关知识要求；技能考核主要采用现场操作、模拟操作等方式进行，主要考核从业人员从事本职业（专业）应具备的技能水平。

初、中、高级理论知识考试、技能考核均实行百分制，理论知识考核成绩和技能考核成绩皆达 80 分（含）以上者视为合格。

5.9.3 监考人员、考评人员与考生配比

理论知识考试中的监考人员与考生配比不低于 1∶15，且每个考场不少于 2 名监考人员。技能考核监考人员与考生配比不低于 1∶10，且每个考场不少于 2 名监考人员。

5.9.4 鉴定时间

理论知识考试时间不少于 90min；操作技能考核时间不少于 150min。

5.9.5 鉴定场所设备

理论知识考试：在标准教室或标准联网多媒体计算机教室进行。

技能操作考核：在模拟环境中进行，考试结束后能完成环境的还原。

5.9.6 鉴定机构要求

鉴定机构需具备中国通信企业协会评定的安全培训资质。

6 基本要求

6.1 职业道德基础知识

1）遵纪守法，爱岗敬业。

2）勤奋进取，忠于职守。

3）认真负责，团结协作。

4）爱护设备，安全操作。

5）诚实守信，讲求信誉。

6）勇于创新，精益求精。

6.2 基础理论知识

1）网络安全知识。

2）密码技术知识。

3）数据分类分级知识。

4）数据治理知识。

5）数据处理活动安全管理知识。

6）数据安全风险管理知识。

7）数据计算与数据存储知识。

8）数据运营与技术指导知识。

9）数据安全开发知识。

10）软件设计与开发知识。

11）应急响应管理知识。

12）数据安全知识。

13）网络产品原理与应用知识。

14）网络安全监测分析技术知识。

15）密码应用知识。

6.3 相关法律、法规、标准知识

1）《中华人民共和国劳动法》相关知识。

2）《中华人民共和国民法典》相关知识。

3）《中华人民共和国网络安全法》相关知识。

4）《中华人民共和国数据安全法》相关知识。

5）《中华人民共和国个人信息保护法》相关知识。

6）《中华人民共和国密码法》相关知识。

7）《中华人民共和国保守国家秘密法》 相关知识。

8）《中华人民共和国刑法》相关知识。

9）《关键信息基础设施安全保护条例》相关知识。

10）《数据出境安全评估办法》相关知识。

11）其他数据安全相关法律法规、管理规定、标准相关知识。

7 工作要求

本标准初级、中级、高级的技能要求和相关知识要求依次递进，高级别涵盖基础级别的要求。

安全运营工程师职业技能及职级一览见表 1。

表 1 安全运营工程师职业技能及职级

职业技能	工作内容		
	初级	中级	高级
风险识别	1. 能够了解 Web 漏洞的成因、危害与测试方法； 2. 能够了解网络漏洞的成因、危害与测试方法； 3. 能够掌握扫描器的原理与实践过程； 4. 能够掌握常见漏洞的原理与验证实践	1. 能够了解风险识别的基本概念和方法； 2. 能够了解风险识别的内容、流程、工具和技术； 3. 能够了解资产运营及管理的基本内容和方法； 4. 能够了解脆弱性管理的关键技术和方法，包括漏洞扫描、渗透测试、弱口令检测、配置核查等的概念、规范、步骤和工具等方面	—
安全防御	1. 能够掌握防火墙设备的功能、原理和实践； 2. 能够掌握 Web 应用防火墙设备的功能、原理和使用实践； 3. 能够掌握堡垒机设备的功能、原理和使用实践；	1. 能够了解网络安全纵深防御体系的基本概念、目的、要素和实践； 2. 能够了解安全加固的基本内容和技巧，能够了解安全加固服务、安全加固前的准备、安全加固的操作、如何规避安全加固的风险和了解常见的操作系统、中间件和数据库的漏洞加固和问题处理等方面内容；	1. 能够掌握理解入侵和攻击模拟的原理和方法，掌握入侵和攻击模拟的工具和技能；

表 1　安全运营工程师职业技能及职级（续）

职业技能	工作内容		
	初级	中级	高级
安全防御	4. 能够掌握审计类设备的功能、原理和使用实践	3. 能够了解威胁情报运营的基本概念和方法； 4. 能够了解威胁情报的定义、类型（分级分类）、管理流程； 5. 能够了解欺骗防御的基本原理和技术，了解采用主动防御方法进行威胁搜寻和检测、使用主动防御概念来遏制攻击者等； 6. 能够了解红队评估的基本概念和方法，了解红队评估的使用的相关模型、攻击手段、信息收集等	2. 能够掌握安全运营防御模型的理论和实践，根据安全策略、风险评估和业务需求，设计、实施、管理和评估安全运营防御模型
安全检测	1. 能够掌握全流量审计预警的原理与实践； 2. 能够掌握 EDR 终端防护功能、原理和使用实践； 3. 能够掌握态势感知系统功能、原理和使用实践； 4. 能够掌握网络监控和分析的基本技术和方法，包括网络协议的概述、分层模型、网络访问/链路层、TCP/IP、HTTP、SSL&TLS、Wireshark、ICMP、UDP、常见攻击类型及特征	1. 能够掌握威胁检测与分析的基本概念、方法和流程； 2. 能够掌握威胁检测与分析的核心技能和工具	1. 能够了解入侵分析原理和实践，能够识别攻击者的行为模式和目标，并进行取证和响应； 2. 能够掌握构建和分析时间线，能够使用工具和技巧来收集、处理、关联和可视化时态数据，以及使用关键的分析方法来解读和利用时间线
事件响应	1. 能够了解安全事件响应的定义、网络安全应急响应管理与相关法规、网络安全应急响应模型与流程、网络安全事件分级和分类、网络安全典型事件； 2. 能够了解如何通过系统信息、用户信息、启动项、任务计划、进程、服务、文件系统等方面排查黑客的攻击痕迹； 3. 能够了解 Linux 应急响应排查的整个过程	1. 能够了解事件分级分类的标准、如何进行应急响应； 2. 能够了解 windows 终端检测与排查，通过系统信息、用户信息、启动项、任务计划、进程、服务、文件系统等方面排查黑客的攻击痕迹； 3. 能够了解 Linux 终端检测与排查，掌握 Linux 应急响应排查的整个过程； 4. 能够掌握预防和处置钓鱼邮件的基本技术和方法； 5. 能够掌握通过系统信息、用户信息、启动项、任务计划、进程、服务、文件系统等方面排查远控木马的攻击痕迹； 6. 能够了解勒索病毒网络安全应急响应的基本技术和方法； 7. 能够掌握通过常见数据库类型、常见数据库日志等方面排查和应对数据库攻击的威胁； 8. 能够掌握通过溯源反制技术排查和应对黑客的攻击行为	1. 能够掌握应急响应的标准规范、技术，能够掌握应急响应的理论和实践； 2. 能够掌握恶意样本分析方法，能够对 Windows 及 Linux 平台下的恶意样本进行深入分析，揭示其功能、行为和攻击技术

表 1　安全运营工程师职业技能及职级（续）

职业技能	工作内容		
	初级	中级	高级
运营管理	—	1. 能够掌握通过安全运营制度及流程规范和优化安全运营的工作； 2. 能够掌握通过安全运营指标衡量和评估安全运营的效果和效率； 3. 能够掌握通过持续改进、分析和自动化（SOAR）提升安全运营的效果和效率。	1. 能够掌握在安全运营中设计及应用指标、实现自动化和持续改进的方法和技术，达成安全运营的优化和转型目标
SOC 设计与规划	—	—	1. 能够了解构建安全运营中心所需的关键要素，包括 SOC 的架构、人员、流程、技术、工具、服务和指标； 2. 能够掌握 SOC 的设计原则和方法，能够根据不同的场景和需求，设计出适合组织的 SOC 解决方案

数据安全管理员职业技能及职级一览见表 2。

表 2　数据安全管理员职业技能及职级

职业技能	工作内容		
	初级	中级	高级
数据安全管理	1. 能掌握利用工具进行数据资产识别的技能； 2. 能掌握编制数据资产清单的技能； 3. 能了解数据分类规则，掌握数据分类技能； 4. 能了解数据分级规则，掌握数据分级技能	1. 能了解数据安全治理方法，能够掌握数据安全防护方案编制技能； 2. 能了解相关国家标准和行业标准，能够掌握数据分类分级规则制定技能； 3. 能了解数据资产清单格式，掌握数据资产清单制定技能； 4. 能进行数据资产安全保护和安全运维	1. 能了解组织数据安全治理策略，掌握数据安全治理方案制定技能； 2. 能了解具体业务安全需求，掌握构建数据安全防护体系的技能； 3. 能根据数据安全治理方案，编制数据安全管理制度； 4. 熟悉相关国家和行业标准等，掌握制定/更新数据安全保护仿真策略的方法
数据安全建设与运维	1. 能根据数据安全建设方案，掌握数据安全产品部署技能； 2. 能够掌握数据安全产品规则配置与更新方法；	1. 能了解数据建设/整改方案要求，掌握数据安全建设/整改实施技能； 2. 能掌握各种数据安全保护工具与系统的高级操作技能；	1. 能够领导和组织数据安全建设与运维工作； 2. 能够了解数据安全合规和风险管控要求，掌握数据安全建设方案制定技能；

表 2　数据安全管理员职业技能及职级（续）

职业技能	工作内容		
	初级	中级	高级
数据安全建设与运维	3. 能掌握典型数据安全保护工具与系统的基本操作技能； 4. 能够掌握日常数据安全运维工作基本技能	3. 能够掌握组织和开展日常数据安全运维和检查技能； 4. 能根据重要时期保障数据安全保护方案组织与实施相关保障活动	3. 能够根据检查或测评结果，制定数据安全整改方案； 4. 能掌握重要时期保障等特殊时期数据安全保护方案编制技能
数据安全开发与测试	1. 能了解数据生命周期各阶段安全风险； 2. 能掌握数据安全产品代码编写技能； 3. 能了解数据安全产品的软硬件集成方法； 4. 能掌握数据安全集成项目进行联调联测技能	1. 能了解数据安全需求分析方法与途径； 2. 能够结合数据安全产品方案和数据安全要求，掌握数据安全产品测试方案编制方法； 3. 能掌握数据安全产品的合规和有效性测试验证技能； 4. 能掌握数据安全产品测试环境构建技能	1. 能够依据数据安全合规要求，设计数据安全产品开发方案； 2. 能掌握数据安全产品改进与优化方法； 3. 能根据相关合规要求和数据安全要求，对数据安全产品进行测试； 4. 能根据相关数据安全互联互通要求，掌握数据安全产品集成方案设计技能
数据安全评估	1. 能了解数据资产风险要素识别方法； 2. 能掌握数据处理活动风险识别技能； 3. 能根据组织数据安全风险评估方案，进行数据安全风险计算； 4. 能根据组织数据安全管理制度，进行数据安全合规性评估	1. 能掌握数据安全渗透测试组织与实施方法； 2. 能掌握重要数据数据安全评估技能； 3. 能根据数据安全风险评估方案，制定数据安全评估计划； 4. 能掌握数据安全风险评估报告编写技能	1. 能根据数据安全管理制度，制定数据安全风险管理策略； 2. 能根据数据安全风险评估策略，制定数据安全风险评估方案； 3. 能掌握数据安全审计技能； 4. 能根据相关法律法规标准要求，制定数据出境安全评估方案
数据安全监测与应急	1. 能掌握安全监测系统/平台告警处理方法； 2. 能掌握数据异常行为判断与检测技能； 3. 能根据应急响应预案，对数据安全相关产品进行应急操作； 4. 能根据灾难恢复预案，进行系统恢复	1. 能掌握数据异常行为分析技能； 2. 能够对数据安全事件进行取证； 3. 能根据组织数据安全管理制度，制定灾难备份与恢复方案； 4. 能根据组织灾难恢复预案，进行业务恢复	1. 能根据数据安全管理制度，制定及优化数据安全监测方案； 2. 能制定应急演练方案并组织演练活动； 3. 能掌握数据安全应急响应预案制定技能； 4. 能够对数据安全事件进行追踪溯源

8　权重表

划分初级、中级、高级 3 个职业技能评价等级。职业技能及职级要求，评价机制分为理论和技能实

操两部分。具体评价维度及权重见表 3 和表 4。

表 3　安全运营工程师理论知识权重

项目		技能等级		
		初级	中级	高级
基础知识	职业道德	10	10	10
	基础理论	20	20	20
专业知识	风险识别	20	10	—
	安全防御	20	20	20
	安全检测	20	15	20
	事件响应	10	15	10
	运营管理	—	10	10
	SOC 设计与规划	—	—	10
合计		100	100	100

表 4　安全运营工程师技能要求权重

项目		技能等级		
		初级	中级	高级
技能要求	风险识别	30	15	—
	安全防御	25	25	20
	安全检测	25	20	30
	事件响应	20	20	20
	运营管理	—	20	20
	SOC 设计与规划	—	—	10
合计		100	100	100

数据安全管理员理论知识权重见表 5。

表 5　数据安全管理员理论知识权重

项目		技能等级		
		初级	中级	高级
基础知识	职业道德	5	5	5
	基础知识	20	10	5
专业知识	数据安全管理	5	10	15
	数据安全建设与运维	25	20	17

表 5　数据安全管理员理论知识权重（续）

项目		技能等级		
		初级	中级	高级
专业知识	数据安全开发与测试	20	20	15
	数据安全评估	10	15	20
	数据安全监测与应急	15	20	23
合计		100	100	100

数据安全管理员技能要求权重见表 6。

表 6　数据安全管理员技能要求权重

项目		技能等级		
		初级	中级	高级
技能要求	数据安全管理	15	20	25
	数据安全建设与运维	25	23	20
	数据安全开发与测试	25	20	15
	数据安全评估	15	17	20
	数据安全监测与应急	20	20	20
合计		100	100	100

参 考 文 献

[1] GB/T 42446—2023 信息安全技术 网络安全从业人员能力基本要求

[2] GB/T 43697—2024 数据安全技术 数据分类分级规则

[3] GZB—2023 数据安全工程技术人员国家职业标准

[4] 《中华人民共和国网络安全法》

[5] 《中华人民共和国数据安全法》

[6] 《中华人民共和国个人信息保护法》

[7] 信息安全技术 数据安全风险评估方法（征求意见稿）（2023 版）

[8] 网络安全技术 网络安全运维实施指南（征求意见稿）（2024 版）

中国通信企业协会团体标准

网络与数据安全运营岗位职业能力规范

T/CAICI 98—2024

*

人民邮电出版社出版发行

北京市丰台区成寿寺路 11 号邮电出版大厦

邮政编码：100164

北京华邦印刷有限公司印刷

*

开本：880×1230　1/16　　2024 年 12 月第 1 版

印张：1.25　　2024 年 12 月北京第 1 次印刷

字数：36 千字

15115・4282

定价：40.00 元

本书如有印装质量问题，请与本社联系 电话：(010)53915956