2020

安全服务人才发展路线图

NSFOCUS

目录

一、 概述

随着安全服务业务模式的体系化发展，多元化培养安全人才迫在眉睫。无论是企业还是安全服务提供商都需要明确的人才培养体系。基于安全工作场景的岗位设计和明确的岗位发展路线可以帮助员工快速成长，人才的多元化和体系化会促进安全服务业务的创新进程。

本文将从安全岗位方向、岗位级别和岗位的核心业务技术等方面综合设计人才发展路线路。

二、 应用场景

本文档主要用于员工职业规划和认证体系设计。

1. 职业规划

安全服务各部门进行员工个人职业规划时，可以参考岗位名称、岗位方向和岗位核心技能。在发展方向和岗位级别两个维度综合绘制成长路线图，并以核心技能熟练度作为关键里程碑。

2. 培训认证

不同的岗位应采取针对性的使用策略，例如：一线综合团队在使用本说明时需注意关注“一专多能”的设计理念。基础岗位的核心任务是员工都需要能够独立交付，业务交付技能达到一定熟练度后，可以在专业方向上继续深造。

三、 安全服务岗位

1. 岗位方向划分

安全服务专业岗位划分为六个方向，包括：安全评估、安全开发、安全运维、安全应急、安全测试及安全咨询。

- **安全评估**：专注于风险评估领域，针对不同 IT 环境及业务场景可以采用先进的，有效地的评估模型准确地发现安全风险。
- **安全开发**：专注于应用软件安全开发全生命管控领域，针对软件开发的每个阶段开展有效的安全管控活动，从源头上解决安全风险。
- **安全运维**：专注于安全事件闭环管理领域，在事件的感知、保护、检测、响应和恢复环节持续地开展安全防护工作，动态对抗安全风险。

- **安全应急**：专注于突发的安全事件应急处置领域，在安全事件分析，取证，追踪及恢复方面快速响应，帮助企业快速止损。
- **安全测试**：专注于安全攻防对抗和攻防技术研究领域，在安全测试技术、对抗技术和漏洞深度研究方面不断探索，促进企业安全建设水平。
- **安全咨询**：专注于企业安全风险管理、安全治理和安全控制体系研究领域，在安全规划、安全体系建设和风险管理等方面不断探索，帮助企业真正把安全建设做好。

2. 岗位级别划分

在每个岗位方向上设置三个岗位级别，包括：基础岗位（Associate），专业岗位（Practitioner）和专家岗位（Expert）。

说明：某些专业岗位有细分领域，例如安全评估专家会细分为工控安全评估专家、云平台安全评估专家、CII 安全评估专家及物联网安全评估专家等。只要在细分领域上通过考核，即可获得专业岗位级别。

(1) 岗位认证原则

岗位认证分为横向（岗位方向）和纵向（岗位级别）两类。

- 基础岗位可以向任何专业岗位方向认证，通过专业岗位认证即可；
- 专业岗位跨岗位方向晋升专家岗位需要先取得专家岗位方向的专业岗位认证；
- 横向认证岗位数量不限。

(2) 岗位描述与核心任务

岗位描述字段对岗位的职责进行概要说明，核心任务是岗位日常的关键工作任务。

岗位名称	岗位描述	关键技能
安全测试工程师	模拟攻击者视角对企业各类系统进安全测试，全面发现存在的安全漏洞。	渗透测试（web、APP、无线、IOT 等）
高级安全测试工程师（按模式细分）	完成复杂场景、新技术领域、高竞争环境下安全测试工作。	1、精英测试 2、攻防竞赛
安全攻防专家	专注于安全攻防实战，有组织的开展高端攻防活动，评价企业安全防护水平。并通过团队赋能，提升团队整体安全攻防实力。	1、红蓝对抗 2、对手仿真

安全攻防研究员	专注于安全测试技术的研究，并针对新型漏洞和高级攻击手法进行深入研究，形成企业可以复用的攻防成果。	1、漏洞研究 2、APT 研究
安全合规工程师	将安全标准转化为企业安全建设参考。并综合分析安全评估数据，评价企业安全遵从性。并基于最佳实践和参考标准导出安全整改建议。	1、差距分析 2、标准解读 3、等级保护协助
安全合规顾问 （按合规细分）	为企业制定合规计划并评价企业安全策略有效性。快速响应新的合规要求，并快速给出安全合规建议，辅助企业迎检监管机构检查工作。	1、安全认证协助（等级保护咨询、UPDSS 协助认证、ISO27001 协助认证、GDPR 合规咨询） 2、安全迎检
安全体系架构师 （按体系细分）	为企业构建适当的，有效的安全体系，并可持续改进企业安全体系的成熟度。管控体系涉及领域较多，不同领域可设立专门岗位。	管控体系设计（包括不限于应急体系、安全开发管理体系、安全域、数据安全体系）
安全规划师	制定和维护网络安全计划，战略和政策，以支持并符合组织网络安全举措和法规遵从。	安全规划
安全治理专家	组织高层管理者开展信息安全治理活动。包括对安全管理活动的评价、指导、监视。以及和利益相关者的沟通。	安全治理
安全开发工程师	从代码层面分析新的或现有的计算机应用程序，软件或专用实用程序的安全性并提供可操作的建议和代码层面的参考。	1、源代码审计 2、编码规范编制 3、安全组件开发
安全开发管控专家 （按阶段细分）	在整个系统开发生命周期中设计，开发，测试和评估信息系统安全。	1、安全开发全管控 2、安全架构分析
安全架构师	确保在企业架构的所有方面（包括参考模型，细分市场和解决方案架构以及支持这些任务和业务流程的最终系统）充分解决保护组织的使命和业务流程所需的利益相关方安全需求。	1、安全架构管理 2、架构安全评审
安全运维工程师	使用从各种网络防御工具（例如，IDS 警报，防火墙，网络流量日志）收集的数据来分析其	1、安全监控 2、安全加固 3、安全告警处置

	环境中发生的事件，以减轻威胁。并利用常见安全工具发现系统漏洞及配置缺陷。	4、安全情报处置 5、安全日志分析 6、漏洞扫描 7、配置检查
基础设施安全专家（按架构细分）	从基础设施的测试，实施，部署，维护和管理各环节分析和设计基础架构硬件和软件安全规范和架构。	1、 安全配置规范设计 2、 网络架构分析 3、 安全域设计 4、 漏洞闭环管理
安全保障专家	在企业重要时期制定安全保障方案并组织团队开展安全保障工作。	1、 保障组织设计 2、 统筹管理设计 3、 防御能力评估 4、 安全策略优化 5、 监控能力构建
攻击研判分析专家	负责企业处理安全事件的分析及研判工作，覆盖安全事件全生命周期管理（从评估和识别、检测和分析、响应和恢复各环节的事件管理）	1、攻击分析研判 2、入侵关联分析 3、攻击路径分析 4、攻击团队画像 5、突发事件规则自定义
安全运维架构师	针对企业的安全需求进行统筹管理。围绕企业各类安全能力开展运维工作，确保安全能力达到可运营状态。实现运维过程的统筹管理。	安全运维体系设计
安全风险评估专家（按领域细分）	对信息技术系统采用的管理，运营和技术安全控制措施进行独立综合评估，以确定控制的整体有效性。	1、风险评估 2、新领域安全风险评估（CII、工业控制系统等）
安全风险管理专家	设计企业信息安全风险管理体系，配合企业风险管理工作，确保信息系统运行在可接受的风险水平之下。	信息安全风险管理咨询
数据安全工程师	根据需要收集和分析定性和定量数据，并创建评估分析报告，综合评价企业安全遵从性报告。	1、数据需求分析 2、数据安全评估
数据安全顾问	设计并优化数据模型，理解数据安全需求及控制措施、结合业务场景分析数据安全风险	1、 数据模型设计 2、 数据安全体系设计

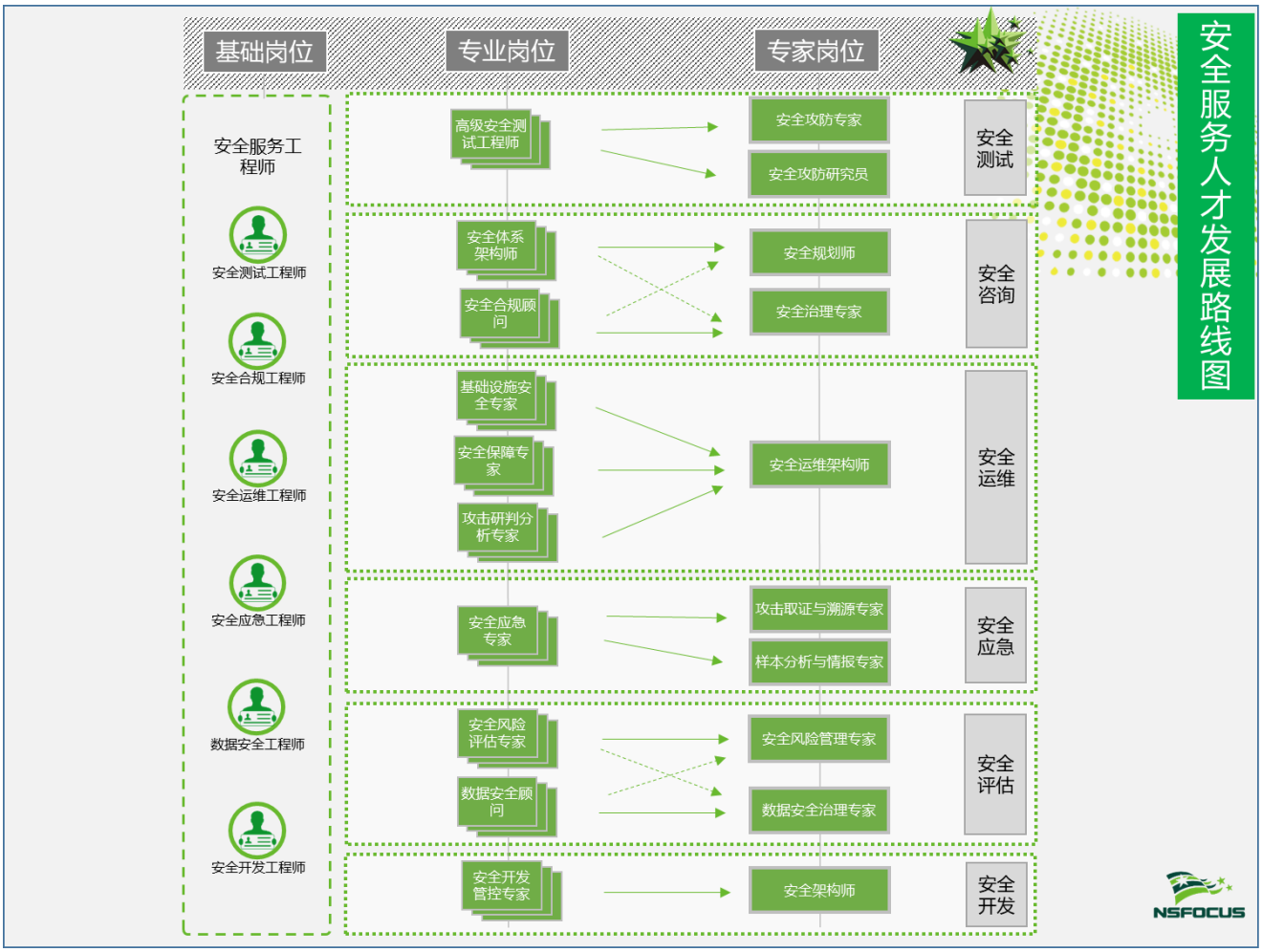
	及自身的法律风险，并基于最佳实践和参考标准导出指导建议。	
数据安全治理专家	组织高层管理者开展数据安全治理活动。包括对数据安全管理活动的评价、指导、监视。以及和利益相关这的沟通。	数据安全治理
安全应急工程师	协助完成网络安全事件的调查及处置并完成应急响应报告编制工作。	应急响应
安全应急专家 （按技能细分）	针对突发网络安全事件开展调查，分析并给出安全处置建议。组织企业应急演练并牵头完成威胁狩猎工作。	1、应急演练 2、应急响应 3、威胁狩猎
攻击取证与溯源专家	针对安全事件开展安全取证工作并给予数据进行攻击溯源。	1、攻击取证 2、攻击溯源
样本分析与情报专家	对攻击样本进行逆向分析并应用到威胁情报消费场景。	1、样本分析 2、威胁情报管理

四、 岗位发展路线图

安全服务人才发展路线图以安全服务岗位为基础，岗位从基础岗位走向专家岗位。

- 基础岗位强调“一专多能”，不进行方向划分。可以根据业务比重，设立专门的工程师岗位；
- 专业岗位进行了抽象概括，可直接设立综合性岗位，也可以从架构、领域、体系及技能等维度进行细分；
- 专家岗位有岗位方向归属，但是对其他方向的专业工位技能有熟练度的要求。

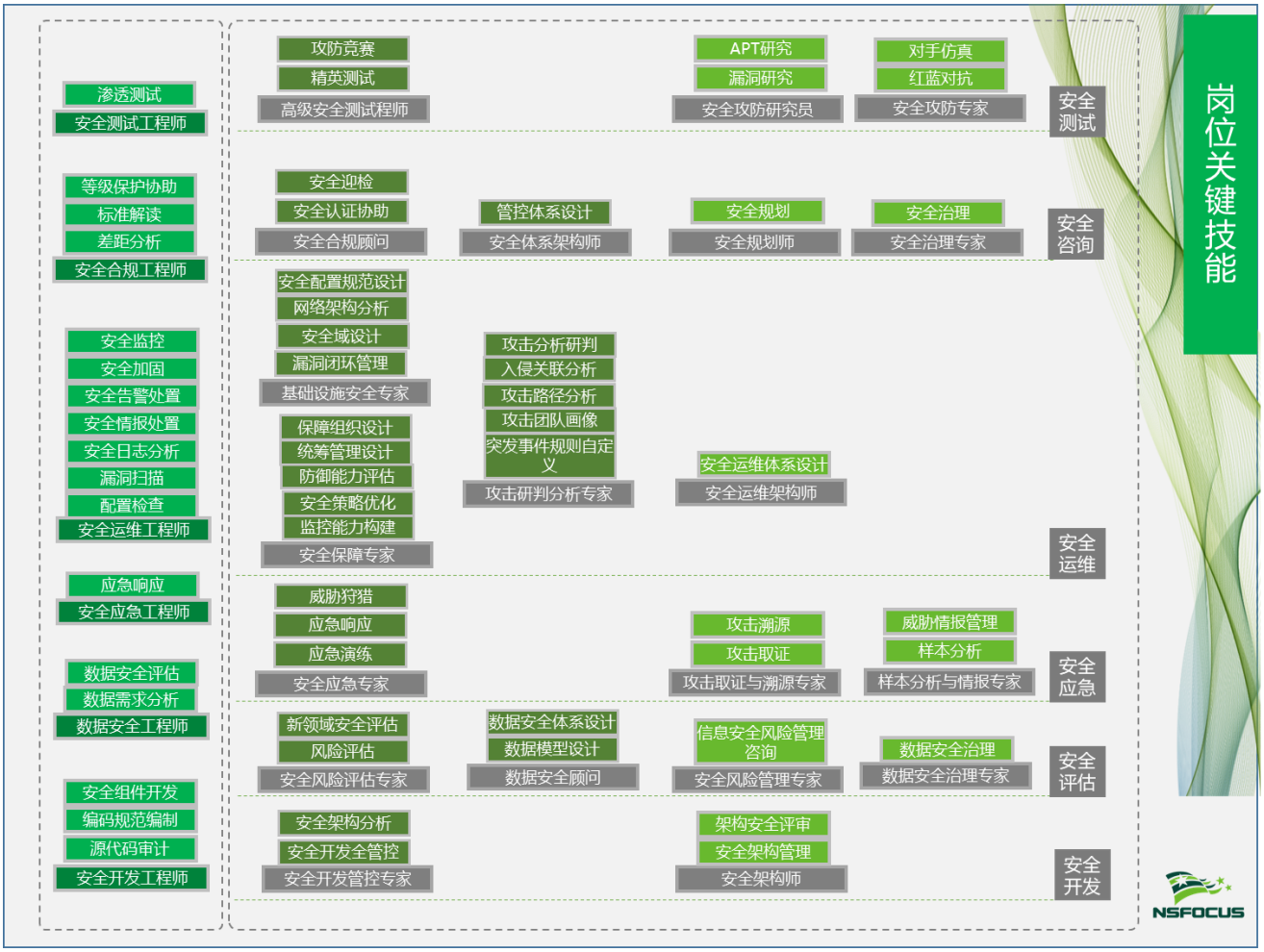
人才发展路线图如下：



附录A　　核心任务解释

名称	解释说明
安全组件	在软件开发过程中，按照一定规范可以直接引用的具有安全功能的代码片段或程序包。
精英测试	传统渗透测试的改进模式，根据测试目标的特点构建测试框架并精选框架上每个环节最适合的测试人员。已测试结果最优为目标。
对手仿真	高度模仿 APT 攻击模式，在一定时间周期内采用高级持续化手法持续评估企业安全防护能力。
安全开发管控	在应用软件开发每个阶段开展适合的安全管控活动，安全管控活动兼具效率和效果以符合开发进度期望。

附录B　核心任务全景图


渗透测试
安全测试工程师
等级保护协助
标准解读
差距分析
安全合规工程师
安全监控
安全加固
安全告警处置
安全情报处置
安全日志分析
漏洞扫描
配置检查
安全运维工程师
应急响应
安全应急工程师
数据安全评估
数据需求分析
数据安全工程师
安全组件开发
编码规范编制
源代码审计
安全开发工程师
攻防竞赛
精英测试
高级安全测试程师
APT研究
漏洞研究
安全攻防研究员
对手仿真
红蓝对抗
安全攻防专家
安全测试
安全迎检
安全认证协助
安全合规顾问
管控体系设计
安全体系架构师
安全规划
安全规划师
安全治理
安全治理专家
安全咨询
安全配置规范设计
网络架构分析
安全域设计
漏洞闭环管理
基础设施安全专家
攻击分析研判
入侵关联分析
攻击路径分析
攻击团队画像
突发事件规则自定义
攻击研判分析专家
保障组织设计
统筹管理设计
防御能力评估
安全策略优化
监控能力构建
安全保障专家
安全运维体系设计
安全运维架构师
安全运维
威胁狩猎
应急响应
应急演练
安全应急专家
攻击溯源
攻击取证
攻击取证与溯源专家
威胁情报管理
样本分析
样本分析与情报专家
安全应急
新领域安全评估
风险评估
安全风险评估专家
数据安全体系设计
数据模型设计
数据安全顾问
信息安全风险管理咨询
安全风险管理专家
数据安全治理
数据安全治理专家
安全评估
安全架构分析
安全开发全管控
安全开发管控专家
架构安全评审
安全架构管理
安全架构师
安全开发
岗位关键技能
NSFOCUS