

团体标准《网络安全测试能力（团队）评价规范》 编制说明

一、 工作简况

1.1 任务来源

《网络安全测试能力（团队）评价规范》由广东省计算机信息网络安全协会作为提出单位。该标准由广东省网络空间安全协会归口管理。

1.2 主要起草单位和工作组成员

本标准由广东省网络空间安全协会牵头，网安联认证服务有限公司、广州华南信息安全测评中心、广东关键信息基础设施保护中心、广东新兴国家网络安全和信息化发展研究院等多家单位共同参与编制。

1.3 主要工作过程

(1) 2021年5月，组织参与本标准编写的人员召开项目启动会，成立规范编制小组，确立各自分工，进行初步设计，并听取各协作单位的相关意见。

(2) 2021年6月，编制组召开组内研讨会并结合充分的调研结果，参考各类国家标准和相关政策文件，形成标准草案第一稿，后期经内部多次讨论研究，形成第二稿。

(3) 2021年7月，编制组召开组内研讨会，基于前期成果，经多次内部讨论研究，组织完善草案内容，形成征求意见稿。

二、标准编制原则和标准编制详细说明及解决的主要问题

2.1 编制原则

本标准的研究与编制工作遵循以下原则：

(1) 符合性原则

本标准符合法律法规和强制性标准要求，不损害人身健康和生命财产安全、国家安全、生态环境安全，符合国家相关主管部门的要求。

(2) 实用性原则

本标准规范是对实际工作成果的总结与提升，保持整体结果合理且维持原意和功能不变，针对不同的用户群体，做到可操作、可用与实用。

2.2 文档结构

《网络安全测试能力（团队）评价规范》标准文档分为前言、范围、规范性引用文件、术语和定义、评定原则、团队人员组成、团队的分级、团队评价指标、团队认证、团队评价方法、评价计分细则等部分。

2.3 整体格式

整体格式根据 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》的相关要求，对本标准的各要素进行编写和排版。

在标准内容汇总过程中，对各编写组成员提交过来的部分，根据 GB/T 1.1-2020 的编写要求进行了必要的增删改，以确保符合一致性、协调性、易用性等文件的表述原则及相关规定。

2.4 标准名称英文翻译

标准的名称“网络安全测试能力（团队）评价规范”翻译为 specification for the ability evaluation of cyber security testing teams。其中“Cyber security”在2017年中国网络安全法相关文件中，翻译为“网络安全”。

2.5 术语和定义

术语和定义中所列的术语的英文翻译，根据各部分编写成员提供的术语，如有类似术语的标准，参考了其翻译，没有类似术语标准翻译的，通过百度翻译和谷歌翻译后进行对比，并参考网络相关翻译后进行确定。

2.6 评定原则

本章阐述了网络安全测试团队能力的评定原则。评定原则是渗透测试团队能力评价的基本准则，贯穿整个评价过程。主要包括以下四项原则：自愿原则、公开原则、公平原则、公正原则。这四项原则为展开网络安全测试团队能力评价活动奠定了良好的基础。

2.7 团队人员组成

本部分介绍了在不同类型的网络安全竞赛中人员组成的差异。团队可按网络安全攻防与应急实战演练、CTF夺旗赛（解题模式、攻防模式、混合模式）靶场演练等赛事组成人员。渗透测试团队人员组合略有差异，体现在团队组成人数、团队人员主要技能等方面。

2.8 团队分级

本部分主要阐述了网络安全测试团队等级分类情况。网络安全测

试团队等级分为一星级、二星级、三星级、四星级、五星级。一星级级别最低，五星级级别最高。每个等级对应的要求各有不同，一星级要求最低，五星级要求最高，高级别要求涵盖低级别要求。

2.9 团队评价指标

团队评价指标包括基本条件、管理制度要求、能力要求、实战经验要求、业绩奖项。

基本条件是评定团队等级的起评条件，申请等级认证的团队所有人员应拥护中国共产党的领导，拥护中国特色社会主义制度；应具有中华人民共和国国籍，长期在境内居住，无境外永久居留权；应遵守相关法律法规的规定，无犯罪记录。

管理制度要求包括团队的成立背景、人员及资产管理制度、技能培训制度、接受主管部门监督等方面。

能力要求是指要求团队人员出示能证明其测试能力的凭证，如曾获得的国家级或省级网络安全相关认证证书、能力证书、荣誉证书（厅局级及以上政府部门发放的网络安全相关的嘉奖证书）等。

实战经验要求是对团队能力进行评价的重要指标之一，团队应有相关实战比赛经验，如参加过实战演练，CTF 类竞赛，职业技能竞赛，其它重大创新竞赛或演练等。

业绩奖项是指过去 2 年内，团队在相关比赛中获得荣誉奖项，可根据业绩奖项对团队进行等级评定。

2.10 团队认证

团队的等级认证主要对基本条件、管理制度要求、能力要求、实

战经验等指标进行综合评价，符合要求的团队可进行等级认证，颁发认证证书。

认证证书有效期为：2年。有效期内每年应进行年审以确保团队符合等级要求，不满足年审要求的团队将受到黄牌警告，有严重问题的将取消认定证书。有效期满或人员调整后应进行延期评审或重新等级认定，根据认定结果调整等级。

2.11 团队评价方法

团队评价方法包括各项评价指标的配比情况、综合评价计算公式、各等级综合得分要求等内容。

2.12 评价计分细则

评分细则详述了评价项目及其对应分值，具体评价内容及赋分情况。

2.13 解决的问题

此标准的发布，将填补网络安全行业关于团队测试能力评价规范的空白，对于规范网络安全行业测试团队的评价认证管理有着积极作用，有利于促进网络安全测试团队的培养，为网络安全行业发展提供人才资源。

三、知识产权情况说明

本标准不涉及专利。

四、采用国际标准和国外先进标准情况

无。

五、与现行相关法律、法规、规章及相关标准的协调性

建议本标准推荐性实施。本标准不触犯国家现行法律法规，不与其他强制性国标相冲突。

六、重大分歧意见的处理经过和依据

《网络安全测试能力（团队）评价规范》编制过程中未出现重大分歧。

七、标准性质的建议

建议《网络安全测试能力（团队）评价规范》作为推荐性团体标准发布实施。

八、贯彻标准的要求和措施建议

鉴于本标准是网络安全测试能力（团队）评价规范，用于评价网络安全相关测试团队的能力，在网络安全领域首次提出测试团队能力评价的标准，建议在标准贯彻执行过程中，各单位应当起到协调以及推广的作用。

九、替代或废止现行相关标准的建议

无替代或废止。

十、其他应予说明的事项

无。

《网络安全测试能力（团队）评价规范》标准编制组

2021年07月