河南省通信管理局
河南省通信行业协会

豫通局函〔2025〕203号

关于举办河南省第八届“天安杯”网络安全职业技能竞赛的通知

中国联合网络通信有限公司河南省分公司、中国移动通信集团河南有限公司、中国电信股份有限公司河南分公司、中国广电河南网络有限公司、中国铁塔股份有限公司河南省分公司、中移在线服务有限公司、联通（河南）产业互联网有限公司，相关单位:

为深入贯彻落实习近平总书记关于技能人才工作的重要指示批示精神，加快推进我省电信和互联网行业网络与信息安全人才队伍建设，根据《河南省人力资源和社会保障厅关于组织开展2025年河南省职业技能竞赛活动的通知》（豫人社函〔2025〕162

号）安排，现就举办河南省第八届“天安杯”网络安全职业技能竞赛（以下简称“竞赛”）有关事项通知如下：

一、组织机构

经省人社厅审定，本次竞赛为省级行业二类赛，由省通信管理局、省通信行业协会主办。竞赛成立组委会，全面负责竞赛的组织领导，统筹竞赛政策制定、组织协调、赛前培训安排、宣传报道等工作。组委会下设办公室。

各参赛单位负责牵头组织落实本单位选拔赛事宜，并在竞赛过程中接受组委会的指导。

二、竞赛项目

本次竞赛分为个人赛、团体赛和方案赛。

三、参赛对象

省各基础电信企业从事网络、信息安全管理和维护等相关岗位工作的在职职工，经本单位选拔后可报名参加。已获得“中华技能大奖”“中原技能大奖”“全国技术能手”“河南省技术能手”等荣誉人员，可以参加个人赛、团体赛、方案赛，并根据竞赛成绩参加全国行业职业技能竞赛，但不参与本次竞赛技师及高级工资格申请。各参赛单位要认真做好参赛人员身份审核工作。

每单位须报 1 名指导老师（不参与比赛），参赛队员身份一经上报，不得更改（报名表见附件 1、2、3），方案赛参赛团队的队长应由历届获奖者或资深专家担任。参赛单位名单及数量要求如下：

参赛单位	参赛队伍
中国联合网络通信有限公司河南省分公司	建议选拔12支队伍，每支队伍3名选手
中国移动通信集团河南有限公司	建议选拔12支队伍，每支队伍3名选手
中国电信股份有限公司河南分公司	建议选拔12支队伍，每支队伍3名选手
中国广电河南网络有限公司	建议选拔1支队伍，3名选手
中国铁塔股份有限公司河南省分公司	建议选拔1支队伍，3名选手
中移在线服务有限公司	建议选拔2支队伍，每支队伍3名选手
联通（河南）产业互联网有限公司	建议选拔1支队伍，3名选手

四、竞赛内容

竞赛内容涵盖电信网、互联网、工业互联网、物联网及5G、云计算、人工智能、大数据、低空经济、商用密码等新型融合领域网络和数据安全，结合典型网络安全问题和事件，围绕监测预警、漏洞挖掘、安全运维、团队协作、系统加固和应急响应等，模拟业务场景，加强实战攻防，重点考察参赛选手的网络攻防能力和技术业务能力。

竞赛试题由组委会办公室组织有关专家统一命制（具体竞赛考试大纲、竞赛内容、竞赛规则等详见附件4）。

五、竞赛安排

（一）竞赛报到时间：2025年10月13日9:00-13:00。

（二）竞赛时间：2025年10月13日13:00-10月14日18:00。

（三）竞赛地址：郑州数字化转型创新展示中心（郑州市金水区平安大道与中道东路交叉口东北角，地铁1号线/12号线龙子湖F出口）。

六、奖项设置

（一）金卫士个人奖

1.设一等奖3名、二等奖5名、三等奖7名及优胜奖10名，由竞赛组委会颁发获奖证书。

2.获奖选手按照有关规定晋升相应职业技能等级。

3.经竞赛组委会审核后对获奖选手授予“河南信息通信行业技术能手”荣誉称号。

4.竞赛选手成绩作为全国行业竞赛选拔赛成绩排名并代表河南参赛。

（二）金卫士团体合作奖

设金奖、银奖、铜奖各1名，由竞赛组委会颁发获奖证书。

（三）方案赛奖项

1.设一等奖1名，二等奖2名，三等奖3名（相同分数并列获奖），由竞赛组委会颁发证书。

2.排名前两位的获奖单位，在颁奖环节各有8分钟时间讲解获奖案例（若同一单位包揽前两名，则仅该单位进行一组分享，第三名获奖单位顺延获得讲解资格）。

七、有关要求

（一）各参赛单位要高度重视，在组委会的统一部署下，认真做好大赛各项组织工作，并紧密结合企业生产实际，加强协调和指导，把竞赛作为岗位练兵的重要举措和发现人才、选拔人才的重要参考。并利用各种宣传手段突出宣传“重视技能，尊重技能人才”理念。

（二）各参赛单位选拔工作要加强技术评判，做到科学、严谨、公平、公正。竞赛工作要聚焦高技能人才培养，突出岗位练兵、实战实用，充分调动网络信息安全管理人才的参赛热情，提升网络安全保障能力和水平。

（三）个人赛、团体赛参赛单位请于10月10日前将报名表发送至组委会指定邮箱，并电话联系组委会办公室确认参赛名单。

（四）方案赛参赛单位，请于9月29日17:00前将报名表及参赛案例申报材料提交至组委会指定邮箱，并电话联系组委会办公室确认参赛案例。

八、联系人及联系电话

河南省通信管理局：张南 0371-65898871

河南省通信行业协会：袁冰儿 18639551197

邮箱：hntxhxjs@163.com

附件：1.河南省第八届“天安杯”网络安全职业技能竞赛个人赛报名表

2.河南省第八届“天安杯”网络安全职业技能竞赛团

体参赛报名表

3. 河南省第八届“天安杯”网络安全职业技能竞赛方案赛报名表

4. 河南省第八届“天安杯”网络安全职业技能竞赛大纲

河南省通信管理局　　河南省通信行业协会

2025年9月26日

附件 1

河南省第八届“天安杯”网络安全职业技能竞赛个人赛报名表

序号	单位	姓名	性别	联系电话	身份证号码	证件照	是否住宿

附件 2

河南省第八届“天安杯”网络安全职业技能竞赛团体赛报名表

单位：　　领队姓名：　　联系电话：

序号	队名	团队口号	照片	队伍简介	姓名	性别	联系电话	身份证号码	是否住宿

附件 3

河南省第八届“天安杯”网络安全职业技能竞赛方案赛报名表

单位：　　领队姓名：　　联系电话：

序号	参赛方向	案例名称	案例简介	案例展示图片	姓名	性别	联系电话	身份证号码
					（队长姓名）			
					（队员姓名）			
					…			
					（队长姓名）			
					（队员姓名）			
					…			

附件 3-1 参赛案例模板

“天安杯”网络安全职业技能竞赛

参赛案例介绍表

案例名称：_____

案例方向：_____（公章）

参赛主体：_____

日期：_____年_____月_____日_____

填 表 须 知

一、请按照模板要求填写各项内容。

二、第一次出现外文名词时，要写清全称和缩写，再出现同一词时可以使用缩写。

三、参赛材料应客观、真实，尊重他人知识产权，遵守国家有关知识产权法律法规，对提供的全部材料的真实性负责。

四、参赛材料编写应避免过于理论化和技术化。

五、申报材料要求盖章处加盖部门公章，复印无效，并加盖骑缝章。

承 诺 书

单位名称:

项目名称:

一、我单位对提供全部资料的真实性负责，如有不实，愿承担相应的责任。

二、我单位所涉及的案例内容皆符合国家有关法律法规及相关产业政策要求。

三、我单位对所提交的材料负有保密责任，按照国家相关保密规定，所提交的内容未涉及国家秘密、个人信息和其他敏感信息。在不涉及商业机密的情况下，自愿与其他企业分享经验。

四、我单位申报材料中涉及的产品无成果、权属（专利）争议或纠纷。

五、所填写的相关文字和图片已经由我单位审核，确认无误。我单位对违反上述承诺导致的后果承担全部法律责任。

负责人签字:　　单位盖章:

日期:

<table>
<tr><td colspan="4">一、参赛单位/团队基本情况</td></tr>
<tr><td>名　　称</td><td></td><td>统一社会信用代码</td><td></td></tr>
<tr><td>联 系 人</td><td></td><td>联系方式</td><td></td></tr>
<tr><td>参赛方向</td><td colspan="3">□数据安全方向　□物联网方向　□人工智能方向
□低空经济方向　□可信数据空间方向　□密码安全方向
□其他_____</td></tr>
<tr><td rowspan="3">团队简介</td><td>团队成员</td><td colspan="2">团队共*人，人员介绍（包括但不限于姓名、年龄、职务/职称、主要成果）。</td></tr>
<tr><td>应用案例</td><td colspan="2">解决方案应用实践的场景、行业领域及成效等情况。</td></tr>
<tr><td>获奖情况</td><td colspan="2">解决方案在国家、省层面获奖情况。</td></tr>
<tr><td colspan="4">二、参赛项目基本情况</td></tr>
<tr><td>参赛作品
整体描述</td><td colspan="3">1.背景和意义。
2.整体概述（描述应用场景、技术实现路径、核心产品以及预期效果）。
3.市场需求分析。
4.在河南乃至全国推广应用现状和推广应用场景设想。
5.预期带来的经济效益和社会效益。</td></tr>
<tr><td rowspan="3">创新性</td><td>技术概况</td><td colspan="2">关键技术介绍。</td></tr>
<tr><td>创新点</td><td colspan="2">技术创新和模式创新情况，解决技术难点情况，取得技术突破情况。</td></tr>
<tr><td>知识产权</td><td colspan="2">参赛作品及重要组成部件获取的专利数量和著作权登记情况。</td></tr>
</table>

实用性	应用情况	描述解决的实际问题，提供具体应用案例。
	可靠性	在实际运行中的稳定性、可靠性。
应用场景	可复制推广的行业、地区以及应用场景的描述。	
可推广性	竞争优势	是否具有技术壁垒，可复制性强弱、进入门槛高低、竞争优势劣势等。
	落地转化	落地转化计划、预期辐射带动情况。

附件4

河南省第八届“天安杯”网络安全职业技能竞赛大纲

一、管理部分

（一）法律

1.了解《网络安全法》主要内容，包括：网络运行安全、关键信息基础设施安全、网络信息安全、监测预警与应急处置、明确网络数据收集、存储、传输、处理的合法合规等要求。

2.了解《数据安全法》主要内容，包括：数据安全与发展、数据安全制度、数据安全保护义务、政务数据安全与开放、法律责任、数据分类分级保护制度（一般数据、重要数据、核心数据）等要求以及数据安全风险评估义务。

3.了解《个人信息保护法》主要内容，包括：个人信息处理规则、个人信息跨境提供的规则、个人在个人信息处理活动中的权利、个人信息处理者的义务以及敏感个人信息的特殊保护等要求。

4.了解《密码法》主要内容，包括：核心密码、普通密码、商用密码、法律责任、密码安全的基本策略等要求以及商用密码在数据加密、数字签名中的强制应用场景（政务数据、金融数据）。

（二）法规

1.了解《通信网络安全防护管理办法》（工信部令第 11 号）主要内容，包括：通信网络安全防护范围、管理主体、责任主体、同步要求、分级备案要求、符合性评测要求、风险评估要求、应急演练要求等内容。

2.了解《关键信息基础设施安全保护条例》（国令第 745 号）主要内容，包括：关键信息基础设施认定、运营者责任义务、保障和促进、法律责任等内容。

3.了解《网络数据安全管理条例》主要内容，包括：网络数据安全管理、网络数据跨境安全管理、网络数据监督管理、供应链安全以及数据流转中的安全保护等要求。

4.了解《电信和互联网用户个人信息保护规定》（工信部令第 24 号）主要内容，包括：用户个人信息的收集和使用规范要求、安全保障措施、责任和义务等内容。

5.了解《网络产品安全漏洞管理规定》（工信部联网安〔2021〕66 号）主要内容，包括：管理对象、管理职责、主体责任、漏洞发布要求、漏洞收集平台相关要求等内容。

6.了解《数据出境安全评估办法》，明确数据出境安全评估的触发条件、流程和豁免情形。

7.了解《工业和信息化领域数据安全管理办法》，熟悉行业数据分类等级、重要数据目录以及备案要求。

（三）政策文件

1.了解通信网络安全防护工作总体思路、基本原则、主要任

务、实施及监督检查要求、安全服务机构管理等政策文件。

2.熟悉通信网络安全防护定级范围、评审要求、备案等政策要求，熟悉通信网络单元安全防护定级方法、定级对象命名规则、定级报告内容、定级备案相关信息等。

3.了解通信行业网络和数据安全管理体系相关工作。

4.了解数据安全综合治理政策（如《全国数据资源调查工作方案》）。

（四）通信网络安全防护标准

1.熟悉各专业网络单元安全防护标准中技术要求内容。

2.了解安全风险评估要素及关系、工作形式、不同生命周期要求和实施要点等要求。

3.了解灾难备份原则、灾难备份资源要素、实施过程、灾难恢复预案等要求。

4.了解安全管理制度、安全管理机构、人员安全管理、安全建设管理、安全运维管理等内容。

5.了解安全风险评估工作的国际标准名称（ISO/IEC TR 13335、ISO/IEC 17799、ISO/IEC 27001 等），了解《信息系统安全等级保护定级指南》、《信息系统安全等级保护实施指南》等国家标准总体情况。

二、技术部分

（一）操作系统安全检测与防护

了解操作系统（Windows、Linux、Unix 等）的常规安全防护

机制。熟悉系统日志、应用程序日志等溯源攻击途径。掌握系统账号、权限、文件系统、文件共享、网络参数、端口和服务、日志审计、漏洞补丁等项目的安全检测与安全加固方法；掌握系统加密、系统防火墙、安全策略、杀毒软件的安装和配置方法。

（二）数据库安全检测与防护

了解数据库（Mssql、Mysql、Oracle、MongoDB、Redis 等）的库表管理、数据访问、权限控制等基础安全防护机制。熟悉数据存储加密不当、数据库访问与权限管理配置不当、SQL 注入攻击、数据库漏洞攻击等常见安全问题。掌握数据库运维管控、数据存储加密、数据脱敏、风险发现、日志审计等安全防护方法。

（三）网络层攻击与防护

了解网络层的网络架构、传输方式、传输协议和控制措施；了解针对有线和无线的攻击方式和安全防护机制。熟悉常见的网络层攻击，包括：DoS 和 DDoS、窃听、假冒/伪装、重放攻击、篡改、针对 DNS 的工具（欺骗、投毒和劫持）、ARP 攻击、DHCP 攻击以及无线攻击等。掌握通过使用网络层安全工具和设备（如：NMAP、防火墙、Web 防火墙、IDS/IPS、抗拒绝服务攻击系统、网络扫描器、SOC、SIEM、EDR 等）发现和阻断网络层攻击的方法和技术；掌握对网络层设备（如：路由器、交换机等）的安全配置和加固技术；掌握验证各种安全防护手段（如密码强度、访问控制）有效性和强度的方法。

（四）数据安全与保护

了解电信和互联网行业数据分级分类方法；了解同态加密、安全多方计算、联邦学习、差分隐私等隐私计算技术；熟悉容灾备份、持续数据保护等技术和应用方法；熟悉数据安全的全流程管控、追溯技术，以及动态行为分析和数据安全加密保护技术；熟悉数据安全特性，了解数据全生命周期安全威胁类型及安全防护技术，了解数据安全技术体系，包括数据防泄漏、数据溯源和审计以及数据匿名化等，了解数据全生命周期防护，包括采集、存储、传输、处理以及销毁等阶段的技术方法。

（五）Web 应用安全

了解 Web 应用安全架构，风险分析及常规防护思路。熟悉框架和组件漏洞、权限绕过、弱口令、注入、跨站、文件包含、非法上传、非法命令执行、任意文件读取和下载等常见安全问题。掌握常见 Web 环境的安全配置方法和检测方法和安全防护手段。

（六）渗透测试技术

熟悉渗透基本思路、方法和流程，熟悉各种常见渗透测试工具。掌握常规的渗透测试技术，包括：信息收集、漏洞发掘、常规漏洞利用、常见应用入侵、服务器提权、远程溢出攻击、内网渗透、身份隐藏、暗网挖掘等。

（七）应急响应与恢复

熟悉应急响应与恢复的基本方法和流程。掌握应急响应和恢复的调查、取证、恢复等相关技术，包括：入侵取证分析、日志审计分析、反取证技术、文件删除恢复、中毒文件恢复等。

（八）软件开发安全

了解软件安全开发生命周期、软件安全架构和设计、软件威胁建模原理和方法；了解常见编程环境（C/C++、JAVA、PHP、JSP 等）的构建以及语言的编写。熟悉常见的软件安全漏洞的产生原理和加固方法；熟悉软件安全开发过程中有关参数化查询、输入验证、输出编码、访问控制、身份验证、安全日志、API 接口安全、使用安全的第三方组件等安全开发规范；熟悉代码审计（包括人工审计和工具审计）和代码加固技术。

（九）恶意代码与逆向

熟悉恶意代码的分类、特点和运行机制，熟悉常见的恶意代码，包括：后门、僵尸网络、启动器、感染病毒、勒索病毒、远程控制木马、Rootkit 等。熟悉发现、隔离、清除常见恶意代码的相关工具及技术手段。熟悉常见的恶意代码保护措施以及清除手段。熟悉对常见恶意代码进行静态与动态的分析、源定位以及修复的方法。

（十）商用密码安全

了解信息系统密码应用基本要求、商用密码应用安全相关标准要求，熟悉商用密码设计、应用、测评的基本流程、技术，熟悉服务器密码机、签名验签服务器、密钥管理系统等常见密码安全设备的技术原理及日常使用。

（十一）移动应用安全

了解智能终端操作系统（安卓系统、苹果 IOS）的安全机制；

了解移动应用软件的安全机制和调试分析、代码审计技术。熟悉移动互联网联网应用和应用商店的架构组成与技术实现；熟悉移动应用软件的越权访问、信息泄露、上传漏洞、业务逻辑错误等安全问题的检测与处理技术；熟悉针对移动应用程序的安全防护技术。掌握移动互联网恶意程序的监测与处置方法。

（十二）工业互联网安全

熟悉工业互联网体系架构，了解工业互联网的特征及常见安全威胁类型和安全防护技术等。熟悉常见的工控协议、工控安全漏洞、恶意代码病毒、安全威胁信息等，了解常见工业互联网安全防护措施及实现原理，掌握典型工业互联网安全监测、应急处置、安全事件取证、溯源分析等技术。

（十三）新技术应用安全

1.了解云计算的概念及特征。熟悉云计算常见的安全问题，包括：虚拟机安全、容器安全、应用程序安全、数据安全、网络隔离、微隔离、接口安全等。

2.了解大数据的概念及特征。熟悉利用大数据分析技术提升网络系统安全隐患发现和防护能力。

3.了解物联网的概念及相关基础技术，了解智能摄像头、ID/IC卡、智能卡、智能家居、可穿戴智能设备等常见安全威胁，熟悉物联网应用环境中典型的安全攻击，如RFID攻击等。

4.了解5G技术的概念及特征。熟悉5G网络架构和关键技术，了解5G关键技术存在的安全风险以及安全框架。

5.了解 AI 大模型数据安全的相关基础技术，例如训练数据投诉攻击防御、模型输出隐私保护等。

6.了解人工智能的典型应用及安全风险。结合人工智能在电信和互联网行业的应用，了解其可能导致的数据隐私泄露、深度伪造、智能钓鱼等安全风险以及安全措施。

7.了解低空经济的概念及特征。熟悉低空经济的核心技术、应用场景以及面临的安全挑战和应对措施。

8.了解可信数据空间的概念及特征。熟悉可信数据空间实现的技术原理及实施关键点，了解其典型的风险场景以及安全防护措施。

三、参考资料

【管理部分】

1.中华人民共和国网络安全法

2.中华人民共和国数据安全法

3.中华人民共和国个人信息保护法

4.中华人民共和国密码法

5.数据出境安全评估办法

6.工业和信息化领域数据安全管理办法

7.关键信息基础设施安全保护条例（国令第 745 号）

8.信息系统安全等级保护定级指南

9.信息系统安全等级保护实施指南

10.信息系统密码应用设计指南

11.信息系统密码应用基本要求

12.通信网络安全防护管理办法（工信部令第 11 号）

13.电信和互联网用户个人信息保护规定（工信部令第 24 号）

14.网络产品安全漏洞管理规定（工信部联网安〔2021〕66 号）

15.公共互联网网络安全突发事件应急预案

16.公共互联网网络安全威胁监测与处置办法

17.工业和信息化部关于加强电信和互联网行业网络安全工作的指导意见（工信部保〔2014〕368 号）

18.电信网和互联网网络安全防护系列标准

19.通信网络安全管理文件与标准汇编

【技术部分】

1.黑客攻防技术宝典-Web 实战篇（第 2 版）

2.安全实战之渗透测试

3.黑客攻防从入门到精通实战篇（第 2 版）

4.Python 黑帽子：黑客与渗透测试编程之道（第 2 版）

5.信息安全原理与实践（第 3 版）

6.应用密码学（第 3 版）

7.恶意代码逆向分析基础详解

8.恶意代码原理、技术与防范

9.Android 应用安全实战

10.Android 应用安全测试与防护

11.iOS 应用逆向与安全之道

12.iOS 黑客攻防秘籍（第 2 版）

13.无线网络威胁和移动安全隐私

14.大数据安全：技术与管理

15.物联网安全（第 2 版）

16.云原生安全：攻防实践与体系构建

17.数据安全实践指南

18.数据安全与隐私计算

19.工业互联网安全：架构与技术

20.工业互联网安全：架构与防御

四、竞赛规则

（一）个人赛竞赛规则

1.个人赛由大赛组委会统一集中举行，采用“个人理论赛+个人夺旗赛”的方式，参赛选手在相同比赛环境中根据竞赛系统提示完成相应的关卡考题，通过提交正确答案后获得相应分数，总计 3 小时。

2.个人理论赛与个人夺旗赛分开进行，个人理论赛在开赛 30 分钟后关闭答题环境，个人夺旗赛在开赛 30 分钟后开始，开赛 3 小时后关闭答题环境。

3.个人赛时长 180 分钟，包括个人理论赛 30 分钟和个人夺旗赛 150 分钟。

4.赛事期间严禁以任何形式进行的交换答案等行为，一经发

11.iOS 应用逆向与安全之道

12.iOS 黑客攻防秘籍（第 2 版）

13.无线网络威胁和移动安全隐私

14.大数据安全：技术与管理

15.物联网安全（第 2 版）

16.云原生安全：攻防实践与体系构建

17.数据安全实践指南

18.数据安全与隐私计算

19.工业互联网安全：架构与技术

20.工业互联网安全：架构与防御

四、竞赛规则

（一）个人赛竞赛规则

1.个人赛由大赛组委会统一集中举行，采用“个人理论赛+个人夺旗赛”的方式，参赛选手在相同比赛环境中根据竞赛系统提示完成相应的关卡考题，通过提交正确答案后获得相应分数，总计 3 小时。

2.个人理论赛与个人夺旗赛分开进行，个人理论赛在开赛 30 分钟后关闭答题环境，个人夺旗赛在开赛 30 分钟后开始，开赛 3 小时后关闭答题环境。

3.个人赛时长 180 分钟，包括个人理论赛 30 分钟和个人夺旗赛 150 分钟。

4.赛事期间严禁以任何形式进行的交换答案等行为，一经发

（二）团队赛竞赛规则

1.团队赛由大赛组委会统一集中举行，采用“团队攻防赛+应急响应赛”的方式，参赛选手在相同比赛环境中根据竞赛系统提示完成相应的关卡考题，通过提交正确答案后获得相应分数，总计6小时。

2.团队攻防赛与应急响应赛分开进行，团队攻防赛 3 小时，应急响应赛3小时。

3.团队赛成绩总分为每支参赛队伍在团队攻防赛与应急响应赛中得分的相加值。团队赛总成绩=团队攻防赛成绩+应急响应赛团队成绩

4.团队赛以总得分为依据降序进行排名，得分相同时，以较早达到该分数的团队名次为先。

团队攻防赛

1.团队攻防赛采用 AWD 网络混战模式，参赛队伍互相进行攻击和防守，通过漏洞获取相应的 flag 得分，修补己方主机漏洞进行防御避免失分。

2.题目类型涵盖 WEB 类、PWN 类等。

3.每个队伍维护的主机环境完全一致。

4.比赛时长 180 分钟，采用回合制，每回合 10 分钟，每回合更新 flag。

5.每个队伍每小时可申请 1 次赛题重置，申请机会不可累积，每次重置将扣分，请各队伍提前备份相关文件以备自行恢复。

应急响应赛

1.应急响应赛采用综合防御形式，参赛团队在一个独立的防御场景中。题目环境预设多个漏洞点，选手需要自行发现并修复漏洞点，选手自行 check，若 check 通过达成目标的获得对应分值，未达成目标的不得分，可继续修复。

2.每个队伍维护的主机环境完全一致。

3.比赛时长 180 分钟，需要选手自行 check，检测运维的环境是否完成修复。

5.采用累加计分方式，参赛者须在不影响服务正常运行的条件下修复漏洞，并自行完成漏洞点的检查检测。检测通过后，参赛者将获得该漏洞点预设的分数。

（三）方案赛竞赛规则

1.团队方案赛分为初赛和决赛两部分，参赛案例方向包括但不限于数据安全方向、物联网方向、人工智能方向、低空经济方向、可信数据空间方向、密码安全方向等。

2.初赛为线上比赛，由评审专家组根据各参赛单位提交比赛报名表和参赛案例申报表进行评审并公布初赛排名，排名前 80%（若经计算确定的晋级队伍数量为小数，则依据四舍五入原则取整数）自动入围决赛。

3.决赛为线下比赛，每支参赛队伍需进行方案展示，形式为 PPT 讲解、系统演示等；展示结束后，专家评委将进行提问并现场打分。

4.专家评委根据评分说明现场为参赛案例打分，每个案例去掉一个最高分和一个最低分，其余所有分数的平均值即为该案例的最终得分。

河南省通信管理局办公室　　2025年9月26日印发