2024

金砖国家职业技能大赛（金砖国家未来技能和技术挑战赛）

# 网络安全

# BRICS-FS-28-RU

# 技术规程 TD(仅供省级选拔赛参考)

2024 年 04 月

# 目录

# 1. 项目简介

## 1.1. 技能竞赛名称及说明

### 1.1.1. 技能竞赛的名称

2024 金砖国家职业技能大赛（金砖国家未来技能和技术挑战赛） 网络安全 (CyberSecurity)

赛项编号：BRICS-FS-28-RU

### 1.1.2. 技能竞赛描述

2024 金砖国家职业技能大赛（金砖国家未来技能和技术挑战赛） 网络安全赛项是培养与提升网络安全技术人才的重要平台，本赛项立足网络安全攻防实践，重点选拔网络安全实战人才，同时增加对新技术、新应用场景下产生的网络安全挑战，全面检验选手在网络安全管理、安全运维、网络安全应急响应、网络攻防渗透、数据安全以及新技术领域的专业能力。

报名资格：不设参赛组别，年龄在 16 周岁（2008 年 1 月 1 日以前出生）-35 周岁（1989 年 1 月 1 日以后出生）的职业院校（含高职本科、技工院校）及本科院校在校师生、企事业单位职工等均可报名参赛。应俄罗斯大赛组织方要求，出国参赛选手需年满 18 周岁。

组队方式：本赛项采用单人赛形式，每队由 1 名选手组成。

重点考核参赛选手网络安全实战能力，包括网络安全理论及职业能力考核、网络与数据安全基础技能应用、网络安全运营技能应用、新技术、新应用领域产生的网络安全挑战（如智能网联汽车、物联网、人工智能）安全技能应用，具体包括：

1） 参赛选手需要掌握网络安全相关理论知识，包括但不限于：《中华人民共和

国网络安全法》《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》《中华人民共和国密码法》《关键信息基础设施安全保护条例》以及其他网络和数据安全相关法律法规和标准规范等。

2) 参赛选手需要熟悉需要熟悉解题夺旗赛相关的技术要求， 具备网络与信息安全管理员基础能力，包括计算机硬件基础知识、.计算机软件基础知识、操作系统基础知识、数据库基础知识、网络协议基础知识等；

3) 参赛选手能够根据企业所发现的安全事件，展开网络安全事件的调查、 分析和取证工作，收集、保存、处理、分析和提供与计算机相关的证据，审计黑客的入侵行为，恢复被黑客破坏的文件。

4) 参赛选手可以利用一系列网络安全攻击渗透工具对所提供的网络安全 攻击靶场环境进行综合分析、挖掘和渗透。

5) 参赛选手具体应对新技术、新应用（如智能网联汽车、物联网、人工智能）网络安全挑战的安全检测、安全防护的专项能力。

## 1.2. 本文件的相关性和重要性

本文件包含本次技能竞赛所需的标准，以及管理竞赛的评测原则、方法和程序的信息。

每位专家和选手都必须了解和理解本技术说明。

如果不同语言的技术说明之间有任何冲突，以英文版本为准。

# 2. 技能标准

## 2.1. 技能标准的一般说明

技能标准明确界定了知识、理解和特定技能的要求，这些技能代表着国际上

在技术和职业表现方面的最佳实践。反映了全球对工作角色或职业在工业和企业中定位的共同认知。技能竞赛旨在体现这一技能标准所定义的国际最佳实践及其达到的水平，因此，该标准成为竞赛培训和准备的关键指南。

技能标准被划分为不同部分，每部分都附有标题和参考编号，并分配了相应的总分百分比，以反映其在整个标准体系中的相对重要性，这被称为“权重”。所有部分的权重百分比总和为 100，决定了评分标准中分值的分配。

评分方案通过具体的测试项目，仅对标准中列出的技能进行评测，旨在在竞赛规则允许的范围内尽可能全面地反映标准的要求。评分将严格按照标准中分配的分值进行，允许有 5%的变动范围，但不得改变标准规范所确定的权重。这样的安排确保了评分的公正性和准确性，同时也体现了对技能标准的尊重。

## 2.2. 技能标准

### 2.2.1. 技能的一般规范

| 标准规范 | |
|---|---|
| 1 | **网络安全法律法规** |
| | **应知道并理解：** |
| | 《中华人民共和国网络安全法》 |
| | 《中华人民共和国数据安全法》 |
| | 《中华人民共和国个人信息保护法》 |
| | 《中华人民共和国密码法》 |
| | 《关键信息基础设施安全保护条例》 |
| | **应能够：** |
| | 在设计总体程序测试和记录评估过程时，应将网络安全和隐私原则应用于管理要求 |
| | (与保密性、完整性、可用性、身份验证、数字签名不可抵赖性相关) |
| | 对管理、操作和技术安全控制进行独立全面的评估，并对信息技术系统内部或继承的 |
| | 控制改进进行评估，以确定控制的整体有效性 |

| | |
|---|---|
| | 开发、创建和维护新的计算机应用程序、软件或专门应用程序 |
| | 修改现有的计算机应用程序、软件或专门应用程序 |
| | 分析新的或者现有计算机应用程序、软件或专业的应用程序的安全状况，提供可用的分析结果 |
| | 进行软件系统研究并开发新功能，确保有网络安全防护功能 |
| | 进行综合技术研究，对网络安全系统中可能存在的薄弱环节进行评估 |
| | 计划、准备和实施系统测试 |
| | 根据技术规范和要求，进行分析、评估并形成报告结果 |
| | 测试和评估信息系统的安全情况，涵盖系统开发生命周期 |
| **2** | **基础网络安全攻防实战** |
| | **应知道并理解：** |
| | 操作系统基础（如 Linux 文件和目录结构、环境安装部署）、操作系统基础命令、操作系统配置、操作系统管理、Linux 文件系统、操作系统 Shel、Linux 文本操作； |
| | 应用服务器工作原理、网页知识 |
| | 网络和链路层协议、传输层协议、应用层协议、组网和通信技术； |
| | 脚本语言开发基础、PHP 开发基础、Java 开发基础、前端语言开发基础。 |
| | **应能够：** |
| | 管理数据库或数据库管理系统 |
| | 管理并实施流程和工具，确保机构可以识别、存档、获取知识资产和信息内容 |
| | 处理问题，安装、配置、排除故障，并按照客户需求或咨询提供维护和培训 |
| | 完成采集数据的准确性验证 |
| | 安装、配置、测试、运行、维护和管理网络和防火墙，包括硬件和软件，确保所有信息 |
| | 的共享、传输，对信息安全和信息系统提供支持 |
| | 安装、配置、调试和维护服务器（硬件和软件），确保信息保密性、完整性和可用性 |
| | 管理账户、设置防火墙和安装操作系统补丁程序 |
| | 访问控制、账户和密码的创建和管理 |
| | 检查机构的现有计算机系统和流程，帮助该机构更安全、更快捷和更高效的运营 |
| **3** | **安全事件应急响应** |
| | **应知道并理解：** |
| | 行业技术标准和分析原则、方法和工具 |
| | 威胁调查、报告、调查工具和法律、法规 |
| | 网络安全事件类别、响应和处理方法 |
| | 网络防御和漏洞评估工具及其功能 |

| | |
|---|---|
| | 对于已知安全风险的应对措施 |
| | 身份验证、授权和访问方法 |
| | **应能够：** |
| | 使用防护措施和利用不同渠道收集的信息，以识别、分析和报告发生的、或可能发生的 |
| | 网络事件，以保护信息、信息系统和网络免于威胁 |
| | 测试、实施、部署、维护、检查、管理硬件基础架构和软件，按要求有效管理计算机网络防护服务提供商的网络和资源 |
| | 监控网络，及时记录未授权的活动 |
| | 在所属的领域对危机或者紧急状态做出有效响应，在自己的专业领域中降低直接和潜在 |
| | 的威胁 |
| | 使用缓解措施、准备措施，按照要求做出响应和实施恢复，以最大化存活率保障财产和 |
| | 信息的安全 |
| | 调查和分析相关网络安全应急响应活动 |
| | 对威胁和漏洞进行评估 |
| | 评估风险水平，制定在业务和非运营情况下采取适当的缓解措施 |
| **4** | **WEB 漏洞挖掘与防护** |
| | **应知道并理解：** |
| | 网络威胁行为者的背景和使用的方法 |
| | 用于检测各种可利用的活动的方法和技术 |
| | 网络情报信息收集能力和资源库 |
| | 网络威胁和漏洞 |
| | Web 漏洞原理知识 |
| | 服务器漏洞原理知识 |
| | 漏洞探测工具原理知识 |
| | SQL 注入漏洞基本利用方法、文件操作漏洞基本利用方法、CSRF 漏洞基本利用方法 |
| | 系统漏洞提权技术原理、数据库提权技术原理、系统配置错误提权原理 |
| | **应能够：** |
| | 使用漏洞探测工具成功探测到 Web 漏洞 |
| | 使用漏洞探测工具成功探测到网络服务脆弱性 |
| | 使用漏洞探测工具成功探测到服务器漏洞 |
| | 利用弱口令进行爆破 |
| | 利用文件类漏洞获取敏感文件 |
| | 利用 SQL 注入漏洞获取数据库信息 |
| | 利用 XSS 漏洞实现恶意代码注入和执行 |
| | 掌握常用渗透工具的使用 |

| | |
|---|---|
| 5 | **威胁分析与调查取证** |
| | **应知道并理解：** |
| | 威胁调查、报告、调查工具和法律、法规 |
| | 恶意软件分析的概念和方法 |
| | 收集、打包、传输和储存电子证据的过程，同时并维持监管链 |
| | 司法流程，包括事实陈述和证据 |
| | 持久性数据的类型和集合 |
| | 数字取证数据的类型和识别方法 |
| | 网络安全漏洞的具体操作性影响 |
| | **应能够：** |
| | 收集、处理、保存、分析和提供计算机相关的证据，以减轻网络脆弱性，支持犯罪、欺诈、反间谍或执法的调查 |
| 6 | 新技术、新应用领域产生的网络安全挑战 |
| | **应知道并理解：** |
| | 理解智能网联汽车中可能存在的安全挑战，如远程攻击、数据隐私泄露、车载系统漏洞等。 |
| | 了解人工智能在网络安全中的应用和挑战，如对抗对抗性攻击、隐私保护等问题。 |
| | 理解智能网联汽车、人工智能跨界融合所带来的安全挑战，如数据共享、系统兼容性等问题。 |
| | 了解智能网联汽车、人工智能领域的相关监管和标准化要求，确保安全实践符合法规要求。 |
| | **应能够：** |
| | 进行智能网联汽车、人工智能的安全评估和风险分析，识别潜在的安全风险。 |
| | 制定针对智能网联汽车、人工智能、安全策略和措施，保护系统和数据安全。 |
| | 实施各种安全措施，如网络防火墙、入侵检测系统、安全监控等，确保系统的安全性。 |
| | 持续学习和跟踪智能网联汽车、人工智能领域的最新安全技术和趋势，提高安全能力。 |
| | 快速响应和处理安全事件和紧急情况，确保系统的安全稳定。 |

## 2.2.2. 技能标准的详细文件

| 技能标准的详细文件 | | |
|---|---|---|
| 序号 | 标准号 | 中文标准名称 |
| 1 | GB / T22239-2019 | 《信息安全技术网络安全等级保护基本要求》 |
| 2 | GB / T28448-2019 | 《信息安全技术网络安全等级保护测评要求》 |

| | | |
|---|---|---|
| 3 | GB17859-1999 | 《计算机信息系统安全保护等级划分准则》 |
| 4 | GB/T20271-2006 | 《信息安全技术信息系统通用安全技术求》 |
| 5 | GB/T20270-2006 | 《信息安全技术网络基础安全技术要求》 |
| 6 | GB/T20272-2006 | 《信息安全技术操作系统安全技术要求》 |
| 7 | GB/T20273-2006 | 《信息安全技术数据库管理系统安全技术要求》 |
| 8 | GA/T671-2006 | 《信息安全技术终端计算机系统安全等级技术要求》 |
| 9 | GB/T20269-2006 | 《信息安全技术信息系统安全管理要求》 |
| 10 | ISO/IEC27001 | 《信息安全管理体系》 |
| 11 | GB/T43697-2024 | 《数据安全技术数据分类分级规则》 |
| 12 | GB/T40856-2021 | 《车载信息交互系统信息安全技术要求与试验方法》 |
| 13 | GB/T40857-2021 | 《汽车网关信息安全技术要求与试验方法》 |
| 14 | GB/T 35679-2017 | 《智能网联汽车信息安全保护技术要求》 |

# 3.3 评分方案

## 3.1. 评分流程及方法

- 本赛项四个阶段均实行计算机自动评分，确保评分客观公正。在评分过程中，为保障信息安全，赛场内需进行两次加密操作。选手提交的成绩还需进行三次加密处理。加密工作由专门的加密裁判负责，确保加密过程规范、准确。
- 第一组加密裁判负责首次抽签，产生参赛编号，替换选手个人身份信息，并记录加密过程，将相关证件装入密封袋单独保管。
- 第二组加密裁判组织第二次抽签，确定赛位号，替换参赛编号，并记录加密过程，将相关编号装入另一密封袋单独保管。
- 第三组加密裁判负责对选手各阶段成绩进行第三次加密，加密后的结果交由裁判长组织评分裁判进行评分汇总。第三次加密的文件也由加密裁判密封保存。
- 所有加密结果均须经加密裁判和监督人员签字确认，确保加密过程的透明性

和可追溯性。

- 四个阶段成绩汇总解密后，由裁判长进行复核并签字确认，确保成绩的准确性和公正性。最后，成绩由工作人员录入系统，完成整个评分流程。

## 3.2. 评分规则

- **裁判评分方式**

现场裁判组严密监督机考评分过程，确保公正公平。评分裁判负责各阶段成绩的加密工作，确保信息安全。裁判长则负责成绩的解密汇总，并全程把控竞赛进展。

竞赛现场配备监督员、裁判员和技术支持队伍，各司其职。裁判员负责与选手沟通，收发试卷等材料，处理设备问题；技术支持工程师则负责工位设备的应急处理，确保比赛顺利进行。

整个竞赛流程分工明确，团队协作紧密，为选手提供了良好的竞赛环境。

- **成绩产生办法**

赛按任务评分，满分为 1000 分，详细评分要求见下表。

| 竞赛阶段 | 阶段名称 | 任务阶段 | 评分方式 |
|---|---|---|---|
| 第一阶段<br>权重 25% | 职业素养与理论技能 | 题 1…N | 机考自动化评分 |
| 第二阶段<br>权重 30% | 网络与数据安全技能应用，包括基础网络攻防渗透与漏洞挖掘、数据安全分析与应用 | 任务 1…N | 机考自动化评分 |
| 第三阶段<br>权重 35% | 网络安全运营技能应用，包括安全事件响应、安全加固与溯源分析 | 任务 1…N | 机考自动化评分 |
| 第四阶段<br>权重 10% | 新技术、新应用领域产生的网络安全挑战（如智能网联汽车、物联网、人工智能）安全技能应用 | 任务 1…N | 机考自动化评分 |

### 3.3. 排名规则

对参赛选手提各阶段绩进行第三次加密，将加密后的结果，交由裁判长组织评分裁判进行评分汇总。第三次加密过程文件由加密裁判密封保存，单独保管。按照四个阶段汇总成绩。按照成绩排名，如果分数相同，比对第四阶段成绩，成绩高者排名靠前。若总分相同、第四阶段成绩相同，比对第三阶段成绩，成绩高者排名靠前，依次类推。

## 4.4 竞赛项目要求

### 4.1. 注意事项

- 竞赛期间严禁携带移动存储设备、计算器、通信工具和参考资料。
- 请根据大赛提供的竞赛环境，检查硬件设备、软件及材料清单是否完整，确保计算机正常运行。
- 在操作前，请详细阅读所有任务要求，注意任务间可能存在的关联。
- 操作时请按答题要求及时保存结果。竞赛结束后，设备保持运行，最终提交成果为评判依据。
- 竞赛完成后，请保留设备、软件和赛题在座位上，禁止携带任何物品离场。
- 禁止在提交资料上添加与竞赛无关的标记，违规者将视为零分。

### 4.2. 竞赛时间安排与分值权重

“网络安全”竞赛共分四个阶段，竞赛时间安排和分值权重见下表：

| 竞赛阶段 | 阶段名称 | 竞赛时间（分钟） | 权重 | 评分方式 |
|---|---|---|---|---|
| 第一阶段 | 职业素养与理论技能 | 第一天上午 60 分钟 | 25% | 机考自动化评分 |
| 第二阶段 | 网络与数据安全技能应用，包括基础网络攻 | 第一天上午 90 分钟 | 30% | 机考自动化评分 |

| | | | | |
|---|---|---|---|---|
| | 防渗透与漏洞挖掘、数据安全分析与应用 | | | |
| 第三阶段 | 网络安全运营技能应用，包括安全事件响应、安全加固与溯源分析 | 第一天下午 90 分钟 | 35% | 机考自动化评分 |
| 第四阶段 | 新技术、新应用领域产生的网络安全挑战(如智能网联汽车、物联网、人工智能）安全技能应用 | 第一天下午 60 分钟 | 10% | 机考自动化评分 |
| 合计 | | 300 分钟 | 100% | |

## 4.3. 各模块作业及要求

| 赛项涉及知识点与技能点 | | |
|---|---|---|
| **序号** | **内容模块** | **说明** |
| 第一阶段（理论） | 职业素养 | 网络安全规范意识、安全意识、纪律意识等; |
| | 法律法规 | 《中华人民共和国网络安全法》《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》《中华人民共和国密码法》《关键信息基础设施安全保护条例》以及其他网络和数据安全相关法律法规和标准规范等。 |
| | 漏洞挖掘知识点 | Web 漏洞原理知识、服务器漏洞原理知识、SQL 注入漏洞基本利用方法、文件操作漏洞基本利用方法、CSRF 漏洞基本利用方法、SSRF 漏洞基本利用方法、XSS 漏洞基本利用方法、XXE 漏洞基本利用方法、无恶意特征漏洞基本利用方法、信息泄漏漏洞利用方法、目录遍历漏洞利用方法、反序列化漏洞基本利用方法、未授权漏洞基本利用方法、命令/代码执行类漏洞利用方法; |
| | 数据安全知识点 | 数据安全法规政策、数据安全基础理论、数据安全技术理论、数据安全管理流程、数据安全评估、个人数据安全意识 |
| | 应急响应知识点 | 应急响应原理流程与排查、LINUX/windows 应急响应过程中所涉及的排查点,包括账户排查（特权账户、影子账户）、网络通信与端口排查、进程分析、启动项分析、定时任务排查、服务分析、Webshell 排查、系统后门排查、常见 web 漏洞攻击特征判断、敏感信息漏洞利用特征、sql 注入漏洞利用特征; |
| | 安全加固知识点 | Windows 账户与密码的安全策略设置，用户和用户组的权限管理、审核，日志的启用使用安全模版来分析配置计算机。、Linux 系统中的账号和组、弱口令密码带来的风险、检查空 |

| | | |
|---|---|---|
| | | 口令的方法、检查系统中是否存在其它 id 为 0 的用户的方法、Linux 文件系统的文件格式分类； |

| 赛项涉及知识点与技能点 | | | |
|---|---|---|---|
| 序号 | 竞赛阶段 | 内容模块 | 说明 |
| 第二阶段 | 网络与数据安全技能应用，包括基础网络攻防渗透与漏洞挖掘、数据安全分析与应用 | 网络攻防渗透与漏洞挖掘 | 使用漏洞探测工具探测到 Web 漏洞、使用漏洞探测工具成功探测到网络服务脆弱性、使用漏洞探测工具成功探测到服务器漏洞；利用弱口令进行爆破、利用文件类漏洞获取敏感文件、利用文件类漏洞上传恶意代码、利用命令执行漏洞运行恶意命令、利用 SQL 注入漏洞获取数据库信息、利用 XSS 漏洞实现恶意代码注入和执行、利用目录遍历漏洞访问任意文件、利用 XXE 漏洞执行探测和攻击、利用 CSRF 漏洞伪造请求、利用 SSRF 漏洞伪造请求、通过信息泄露漏洞访问敏感信息。 |
| | | 数据安全分析与应用 | 主要考察选手数据包分析、数据取证等能力；敏感信息泄露、数据分类、数字水印技术、常见加解密算法等内容 |
| 第三阶段 | 网络安全运营技能应用，包括安全事件响应、安全加固与溯源分析； | 网络安全事件响应 | 主要考查学生对入侵检测、抑制处置、系统恢复、证据收集等知识点的掌握和运用能力。 |
| | | 安全加固与溯源分析 | 安全加固考查学生如何增强系统防御能力，而溯源分析则检验学生追踪攻击来源、分析攻击路径的能力。 |
| 第四阶段 | 新技术、新应用领域产生的网络安全挑战（如智能网联汽车、物联网、人工智能）安全技能应用 | 智能网联安全靶场挑战 | 通过虚拟环境中模拟的车辆车机功能，尝试利用多种痛惜协议对车辆实现指令发送并通过指令实现控制车辆要求。 |

# 5.5 技能管理与沟通

## 5.1. 专家组

技能专家组由首席专家 1 名、副首席专家 2 名及若干名专家组成员构成，负责共同修订本赛项技术文件及日常技能管理工作。

## 5.2. 竞赛交流

比赛前若有软硬件准备、考试环境部署等疑问，参赛方可通过网络安全竞赛公众号与大赛赛项 QQ 群进行反馈。本赛项的训练交流、赛前、赛中及赛后交流等也通过公众号与 QQ 群开展。

# 6. 安全要求

参照金砖国家职业技能大赛组委会制定的健康、安全及环境政策与规范，确保竞赛全程严格遵守相关规定：

- 在健康方面，重视参赛者和工作人员的身体健康，预防疾病传播，确保比赛环境清洁卫生。
- 在安全方面，加强场地安全管理，预防火灾、电气事故等安全隐患，确保比赛过程安全无虞。
- 在环境方面，倡导环保理念，减少比赛对环境的负面影响，促进可持续发展。

# 7. 基础设施与竞赛设备

## 7.1. 竞赛设备

赛项执委会提供不少于 3 台三层交换机、12 台二层交换机、10 台信号屏蔽

仪和一台 LED 展示大屏，支撑竞赛系统的搭建，通过高可用技术架构支撑参赛选手的高并发访问，为参赛选手提供性能良好，运行稳定的竞赛平台。

| 资源名称 | 关键参数 | 作用 | 数量 |
|---|---|---|---|
| 三层交换机 | 24 个千兆以太网电口+4 个复用千兆 SFP 光口+4 个 10G SFP+光口。 | 网络互联、路由 | 3 |
| 二层交换机 | 24 个千兆以太网电口 | 网络互联 | 12 |
| 网线跳线 | 六类工业级跳线 | 连接线路 | 140 |
| PC 主机 | 多核 CPU，CPU 主频>=3.5GHZ,>=四核心八线程，内存>=8G，具有串口或者配置 USB 转串口的配置线，支持硬件虚拟化。 | 大屏呈现 | 2 |
| 信号屏蔽仪 | 控制范围：40 米左右 | 屏蔽无线信号和手机信号 | 10 |
| LED 屏 | 24 平米左右 | 提供比赛的监控和展示 | 1 |

## 7.2. 竞赛操作终端机软件配置

| 序号 | 软件 | 介绍 |
|---|---|---|
| 1 | Windows10 | 操作系统 |
| 2 | MicrosoftOffice2016/2019 | 文档编辑工具 |
| 3 | VMware15 或以上版本 | 虚拟机运行环境 |
| 4 | 超级终端 SecureCRT/putty | 设备调试连接工具 |
| 5 | 谷歌 Chrome | 浏览器 |

## 7.3. 竞赛系统及监控设备

| 硬件 | 数量 | 具体配置 | 备注 |
|---|---|---|---|

| | | | |
|---|---|---|---|
| 网络安全竞赛沙箱 | 2 | 系统采用 B/S 架构，内置题目管理、赛事管理、队伍管理、数据统计、大屏展示、数据运维等模块；<br>沙箱评分机制支撑 FLAG 提交与选手 CHECK 验证两种模式，全程自动化完成赛事评分；<br>沙箱支撑中英文界面展示，操作界面与题目描述都可以中英文展示，可支撑国际赛，也可以通过扩展支持第三种语言；<br>沙箱支持多种大赛类型，包括理论赛，CTF 夺旗赛，AWD/AWDP 攻防赛，安全运维赛等常见题型，可根据赛事要求灵活选择；<br>沙箱支持用户管理功能，提供账号管理、队伍管理、角色权限管理，管理员可对账户、队伍进行批量操作，包括导入、导出、新增、删除和禁用等操作；<br>沙箱支持多场竞赛同时管理，支持对竞赛新建、编辑、搜索、发布、环境部署、竞赛中管理、竞赛结果等流程进行操作；<br>沙箱支持个人及团体参赛方式的理论赛、解题赛、攻防赛竞赛模式，并可根据需求进行竞赛形式自由组合；<br>沙箱支持多场竞赛同时管理，支持对竞赛新建、编辑、搜索、发布、环境部署、竞赛中管理、竞赛结果等流程进行操作； | 主备配置，根据队伍数量可增加 |
| 智能网联汽车竞赛仿真环境 | 若干 | 智能网联汽车竞赛仿真台架是模拟真实车辆环境的关键设施，其核心零部件涵盖了车身控制域、车载终端、整车控制器等众多关键部分；零部件通过 CAN 通信网络进行高效连接，确保通信信息的实时传输与交互。竞赛台架不仅模拟了车辆的基本硬件结构，更内置了多种车联网安全漏洞，为参赛选手提供了真实且富有挑战性的竞赛环境。<br>竞赛仿真台架漏洞类型多样，包括 Web 安全、协议安全、无线安全、内核安全等多个方面，覆盖了车辆零部件、车载娱乐系统以及车辆控制系统等多个关键领域。这种设计使得选手能够全面、深入地了解车联网安全领域的各个方 | 依据队伍数量而定 |

| | | | |
|---|---|---|---|
| | | 面，从而提升他们的技术能力和实战经验。<br>通过与竞赛平台的紧密联动，参赛选手能够便捷地链接竞赛台架，进行车辆漏洞挖掘。漏洞挖掘过程中，选手不仅能够运用所学知识进行实际操作，还能够将挖掘到的漏洞提交到竞赛平台，展现参赛选手技术实力和安全技能。 | |
| 交换机 | 若干 | 为各参赛队 PC 提供网络管理。 | 依据队伍数量而定 |
| 横幅或大屏 | 1 | CCVR2024***分赛场”（***为学校的全称） | |
| 备用配件 | 若干 | 电脑、摄像头、U 盘等 | 场地内部工位硬件损坏可随时进行更换 |
| 监控 | 1 | 手机或者录像机 | 比赛全程录制 |
| 电脑或者手机 | 1 | Zoom 会议 | 用于与主赛场联络 |

## 7.4. 网络配置

| 项目 | 具体配置 |
|---|---|
| 网络配置 | （线上赛可以联网，线下赛不支持联网）<br>工位电脑均支持连接互联网，带宽大于 4M |

## 7.5. 竞赛场地布局

竞赛场地光线明亮，照明设备完善；供电供水设施稳定可靠，场地保持整洁。设置隔离带，限制非竞赛人员进入比赛场地，确保比赛区域的安全与秩序。赛场配备保安、消防、医疗及设备维修团队，随时待命，以应对突发状况。设立安全通道与警戒线，对进入赛场的参观、采访、视察人员进行区域限制，确保大赛安全有序进行。