2025

BRICS SKILLS COMPETITION

(BRICS+ FUTURE SKILLS & TECH CHALLENGE)

Cyber Security

BRICS-FS-28

Technical Description
(International Finals_Online)

September 2025

Catalogue

1. About the competition

1.1. Name of competition

Cyber Security of the 2025 BRICS Skills Competition (BRICS Future Skills and Technology Challenge).

Item number: BRICS-FS-28

1.2. Aims of the competition

The Cyber Security Competition of the 2025 BRICS Skills and Technology Challenge (BRICS Future Skills and Technology Competition) serves as a crucial platform for cultivating cybersecurity professionals. Aligned with real-world attack-defense scenarios in cyberspace, this competition aims to precisely identify skilled talents with practical capabilities. It focuses on assessing cybersecurity risks arising from new technologies integrated into digital transformation processes, comprehensively evaluating participants' competencies in security planning and design, vulnerability management, emergency response, and governance of cutting-edge technologies.

1.3. Eligibility

The 2025 BRICS Skills Competition will not set any age categories. Participants can be vocational college students (including higher vocational colleges, undergraduate institutions, and technical colleges), university students aged between 16 (born before January 1, 2009) and 35 (born after January 1, 1990), as well as

employees from enterprises and public institutions.

1.4. Match system model

The competition is a two-player game, with each team consisting of two players.

2. Player ability requirements

The focus is on assessing the practical network security ability of the contestants, including the assessment of network security theory and professional ability,

Application of basic skills in network and data security, application of network security operation skills, new technologies, new application fields

Cyber security challenges in life (such as trusted data space security) and application of security skills, including:

（1）Participants should have an understanding of network security regulations and standards

Master core laws, regulations and standards, including but not limited to the Cybersecurity Law of the People's Republic of China, Data Security Law of the People's Republic of China, Personal Information Protection Law of the People's Republic of China, Cryptography Law of the People's Republic of China, Regulations on the Security Protection of Critical Information Infrastructure, and National Occupational Standard for Network and Information Security Administrators (Data Security Administrators).

（2）Participants should have a solid basic knowledge of information technology and basic security competition skills

Master the basic knowledge of computer hardware, software, operating system,

database, network protocol; have the basic literacy of network and information security management; be familiar with the form and technical requirements of problem solving flag competition (CTF).

（3）Participants should have the ability to respond to network security incidents and analyze evidence

It can investigate, analyze and collect security incidents discovered by enterprises, including: collection, preservation, processing, analysis and provision of electronic evidence; audit tracking of intrusion behaviors; and recovery of damaged files or systems.

（4）Participants should have practical skills in penetration testing and vulnerability mining

Proficient in using various penetration testing tools, security analysis, vulnerability mining and comprehensive penetration of preset network target environment, so as to discover and verify security risks from the perspective of attackers.

（5）Participants should have the ability to detect and protect against emerging technology security threats

It has special security detection and protection capabilities for the security challenges in new technologies/applications represented by trusted data space security.

3. Skills standards

3.1. A general description of the skill standard

The skill standards identify the requirements for knowledge, understanding and specific skills that represent international best practices in technical and occupational performance and reflect global consensus on relevant work roles or occupations in industry and business.

Skills competitions are skill standard oriented and designed to demonstrate the contestants' mastery of international best practices. Training and preparation for competitions are based on this standard to ensure that the contestants can achieve the required level of skills.

The standard comprises multiple sections, each with a clear title and reference number. Each section carries a specific percentage (weight) in the total score, reflecting its importance within the standard. The total weight of all sections adds up to 100%. The weighting system directly determines how scores are allocated within the evaluation framework, ensuring fairness and accuracy in competition assessments.

The competition questions and scoring criteria are meticulously designed around the skills outlined in the standards, aiming to comprehensively reflect the requirements under competitive conditions. During evaluation, scores will be assigned as specified in the standards with a permissible 5% margin of error. However, the original weighting coefficients must remain unchanged to ensure the reliability and validity of the competition outcomes.

3.2. Detailed requirements of skill standards

(1) Network security laws and regulations

Participants should understand the Cybersecurity Law of the People's Republic of China, Data Security Law of the People's Republic of China, Personal Information Protection Law of the People's Republic of China, Cryptography Law of the People's Republic of China, Regulations on the Security Protection of Critical Information Infrastructure and National Occupational Standards for Network and Information Security Administrators (Data Security Administrators), etc.

Participants must demonstrate the following capabilities: 1) The ability to integrate cybersecurity and privacy principles into the design and documentation of overall program testing and evaluation processes, covering critical elements such as confidentiality, integrity, availability, authentication, and non-repudiation of digital signatures; 2) The capacity for independent and comprehensive assessment of management, operational, and technical security controls, with precise judgment of the effectiveness of internal information technology systems and their integrated controls; 3) Proficiency in developing and maintaining computer applications and software (including new development and modification), coupled with the ability to analyze security conditions and deliver reliable assessments; 4) Competence in conducting software system research, including developing new features with cybersecurity protection functions and evaluating vulnerabilities in network security systems; 5) The capability to plan and implement system testing according to technical specifications, conduct analysis and evaluations, produce reports, and comprehensively test information system security throughout the entire system development lifecycle.

（2）Practical attack and defense of basic network security

Participants should master: fundamental operating system knowledge (including Linux file and directory structures, system installation and configuration), command-line operations, system configuration and management, along with Linux file systems, Shell environments, and text manipulation; application server principles and web development fundamentals; network layer protocols and communication technologies; as well as scripting languages, PHP, Java, and front-end language development basics.

Participants should demonstrate the following capabilities: 1) Database and database management system administration proficiency; 2) Process and tool management implementation to ensure effective protection of organizational knowledge assets and information; 3) Problem-solving competencies including system installation, configuration, troubleshooting, and maintenance training delivery based on operational needs; 4) Data accuracy verification expertise; 5) Full lifecycle management of network infrastructure and firewall systems (both hardware/software) to guarantee secure information sharing; 6) Server (hardware/software) management proficiency to maintain information integrity, availability, and confidentiality; 7) Account, firewall, and system patch management proficiency; 8) Access control and account password management skills; 9) Ability to evaluate and optimize organizational computer systems and workflows.

（3）Emergency response to security incidents

Participants should understand: industry technical standards, analysis principles and methods tools; threat investigation report tools and regulations; network security incident classification and processing methods; network defense vulnerability

assessment tools functions; known security risk response; identity authentication and authorization access methods.

Participants should demonstrate: proficiency in implementing protective measures and multi-source information analysis for network incident reporting; capability to manage hardware/software infrastructure infrastructure to ensure network security services; ability to monitor network logs for unauthorized activities; proficiency in crisis response and threat mitigation within professional domains; capacity to execute recovery protocols through preparedness measures; competence in investigating emergency response operations; proficiency in assessing threat vulnerabilities; and the ability to develop business continuity measures based on risk levels.

（4）WEB vulnerability mining and protection

Participants should understand: the background and methods of cyber threat actors; detection of available activity techniques; network intelligence collection capabilities and resources; network threat vulnerabilities; Web, server vulnerabilities and the principle of detection tools; various vulnerability exploitation methods and the principle of power enhancement.

Participants should have the ability to accurately detect various vulnerabilities with vulnerability detection tools; the ability to use technical means to crack weak passwords, sensitive files, extract database information, inject and execute malicious code; and the ability to master and use common penetration tools.

(5) Threat analysis and investigation

Participants should understand: threat investigation report tools and regulations; malware analysis; electronic evidence processing process and regulatory chain

maintenance; judicial process and evidence requirements; data types and forensics methods; specific impact of vulnerabilities.

Participants should have the ability to collect, process, preserve and analyze computer evidence in a standardized manner to facilitate investigation and reduce network vulnerability.

(6) Cyber security challenges in new technologies and new application fields

Participants should understand the core challenges of data security in new technologies and application scenarios, including: risks of unauthorized access, theft, and leakage of data in complex environments (such as multi-source and cross-system/region flows); challenges in permission control, isolation, and auditing caused by blurred trust boundaries in new architectures (e.g., cloud-native and edge computing); risks of covert data theft, misuse, and sophisticated data tampering in advanced persistent threats (APT); privacy violations and de-identification risks from large-scale data aggregation and correlation analysis; as well as risks of sensitive raw data leakage through model outputs or system characteristics (e.g., model reverse engineering and membership inference attacks). Additionally, participants must grasp key compliance requirements such as identification and management of critical data, data classification standards (core, important, general data), and the fundamental principles of core regulations including the Data Security Law of the People's Republic of China and the Personal Information Protection Law of the People's Republic of China (data security obligations, personal information processing rules, data outbound security assessments), along with the applicability of relevant national/industry standards in new scenarios.

Participants must demonstrate the following capabilities: Conduct systematic

data security risk assessments for emerging technologies and application scenarios, identifying potential vulnerabilities and critical data asset threats throughout the entire data lifecycle (collection, transmission, storage, processing, sharing, publication, and destruction). Based on risk assessments and compliance requirements, design and implement comprehensive security strategies covering the full data lifecycle, including but not limited to: implementing minimal data collection with desensitization/anonymization; establishing granular, auditable access controls (e.g., RBAC/ABAC) and permission management; deploying appropriate data transmission protocols (e.g., TLS) and static encryption; applying integrity-preserving technologies (e.g., hashing, signatures); developing secure data transfer and sharing mechanisms; defining data retention and destruction policies. Participants should possess the ability to configure or integrate mainstream data security technologies (e.g., DLP, database auditing, key management, security gateways, log analysis) to effectively execute these strategies and ensure data confidentiality, integrity, and availability. They must continuously monitor evolving security technologies, emerging threats, and regulatory updates, proactively adapt to changes, and enhance capabilities. Additionally, participants should demonstrate rapid identification, analysis, and response to data breaches, unauthorized access, tampering, or destruction incidents, effectively executing emergency response procedures for incident containment and recovery.

3.3. Related knowledge points reference files

order number	knowledge point
1	General Secretary Xi Jinping's important thoughts on building China into a

	cyber power and his important instructions on cyber security
2	Cyber Security Law of the People's Republic of China
3	Data Security Law of the People's Republic of China
4	Cryptography Law of the People's Republic of China
5	Personal Information Protection Law of the People's Republic of China
6	The Criminal Law of the People's Republic of China and the Law of the People's Republic of China on Punishment of Public Security Administration contain relevant provisions on cyber security violations
7	Measures for Data Export Security Assessment
8	Regulations on the Security Protection of Critical Information Infrastructure
9	"GB/T 39786-2021 Information Security Technology Basic Requirements for Password Application in Information Systems"
10	"GB/T 22240-2020 Information Security Technology Network Security Level Protection Guidelines"
11	"GB/T 25058-2019 Information Security Technology Network Security Level Protection Implementation Guide"
12	"GB/T 22239-2019 Information Security Technology Basic Requirements for Network Security Level Protection"
13	"GB/T 28448-2019 Information Security Technology Network Security Level Protection Evaluation Requirements"
14	"GB/T 25070-2019 Information Security Technology Network Security Level Protection Security Design Technical Requirements"
15	"GB/T 20984-2022 Information Security Technology Information Security

	Risk Assessment Methods"
16	"GB/T 41391-2022 Information Security Technology Basic Requirements for Collection of Personal Information by Mobile Internet Applications (App)"
17	"GB/T 41479-2022 Information Security Technology Network Data Processing Security Requirements"
18	"GB/T 36626-2018 Information Security Technology-Information System Security Operation and Maintenance Management Guide"
19	"GB/T 37094-2018 Information Security Technology-Security Management Requirements for Office Information Systems"
20	"GB/T 40652-2021 Information Security Technology Guidelines for Prevention and Handling of Malicious Software Events"
21	"GB/T 38645-2020 Information Security Technology Emergency Drill Guide for Network Security Events"
22	"GB/T 30279-2020 Information Security Technology Network Security Vulnerability Classification and Grading Guide"
23	"GB/T 30276-2020 Information Security Technology Network Security Vulnerability Management Specification"
24	"GB/T 28458-2020 Information Security Technology Network Security Vulnerability Identification and Description Specification"
25	"GB/T 37973-2019 Information Security Technology Big Data Security Management Guide"
26	"GB/T 37027-2018 Information Security Technology Definition and Description Specification of Network Attack"

27	"GB/T 39204-2022 Information Security Technology-Security Protection Requirements for Critical Information Infrastructure"
28	National Occupational Standard for Network and Information Security Administrator (Data Security Administrator)
29	Other relevant network security laws, regulations and standards

4. Knowledge outline

The "Cyber Security" competition is divided into four stages. The schedule and score weight of the competition are shown in the following table:

Competition phase	Phase name	Competition time (minutes)	weight	Scoring method
stage Ⅰ	Professional quality and theoretical skills	Thirty minutes on the first morning	25%	Computerized automated scoring
stage Ⅱ	Network and data security skills application, including basic network attack and penetration and vulnerability mining, data security analysis and application	60 minutes on day one	30%	Computerized automated scoring
phase III	Application of network security operations skills,	80 minutes on the first day	35%	Computerized automated

	including security incident response, security hardening and traceability analysis			scoring
Phase IV	Cyber security challenges arising from new technologies and new areas of applications (trusted data space) Security skills applied	40 minutes on the first morning	10%	Computerized automated scoring
amount to		210 minutes	100%	

（1）**Phase 1: Theoretical knowledge**

knowledge point	explain
professional quality	It covers the awareness of network security norms, security awareness and discipline. Participants are required to be familiar with the norms and best practices of the network security industry, actively prevent security risks, strictly abide by work and competition discipline, and complete tasks on time.
Vulnerability mining knowledge points	This course covers fundamental web security principles, including SQL injection, cross-site scripting (XSS), and cross-site request forgery (CSRF), along with server vulnerability analysis. Students will master practical

	exploitation techniques such as brute-force attacks using weak passwords, leveraging file vulnerabilities to upload sensitive data, executing malicious commands through command execution vulnerabilities, and extracting database information via SQL injection attacks.
Data security knowledge points	The competition covers data security regulations, foundational theories, technical frameworks, management processes, risk assessment methodologies, and individual data security awareness. Participants must understand relevant regulatory policies, master core concepts like data integrity, confidentiality, and availability, be familiar with encryption techniques, access control protocols, and backup systems, comprehend data lifecycle management and classification/gating processes, develop strategies to assess data risks and implement protective measures, while enhancing personal data security consciousness.
Emergency response knowledge points	Participants are required to master the principles, procedures, and troubleshooting methods of emergency response. They must be capable of account investigation in both LINUX and Windows systems, including privileged accounts and shadow accounts; network communication and port investigation using relevant tools to monitor network connections; process analysis through command-line system process monitoring; startup item analysis to examine system boot configurations;

	scheduled task investigation by reviewing crontab and other scheduled tasks; service analysis of system services; Webshell detection through examining Webshell files; and system backdoor investigation to identify unauthorized access points. Additionally, they should be able to recognize common web vulnerability attack patterns, sensitive information exploitation characteristics, and SQL injection exploit features.
Points to reinforce security	In Windows systems, security policy configurations involve account and password management, including enforcing strong password policies, managing user and group permissions through proper authorization allocation, enabling audit functions to track system activities, and analyzing computer configurations using logs and security templates. For Linux systems, proficiency in account and group management is essential. This includes understanding the risks of weak passwords and their detection methods, mastering techniques for identifying empty passwords and zero-uid users, as well as being familiar with file format classification within the Linux file system.

（2）Phase 2: Application of network and data security skills

knowledge point	explain
Network attack and penetration and vulnerability mining	Participants must demonstrate proficiency in using vulnerability detection tools to accurately identify Web vulnerabilities, network service weaknesses, and server flaws.

	Competitors should demonstrate practical attack capabilities through multiple exploitation methods: brute-force password cracking, file access via vulnerabilities for sensitive data extraction or malicious code injection, command execution through SQL injection exploits, database credential theft using XSS vulnerabilities, directory traversal attacks for arbitrary file access, XXE vulnerability exploitation for reconnaissance operations, CSRF spoofing attacks, SSRF attack simulations, and sensitive data retrieval through information leakage exploits.
Data security analysis and application	The main focus is on the candidate's data packet analysis and data forensics ability, including detection and prevention of sensitive information leakage, classification and management of data, application of digital watermark technology to protect digital content copyright and integrity, as well as mastery of common encryption and decryption algorithms such as AES, RSA, etc.

（3）Phase 3: Application of network security operational skills

knowledge point	explain
Cyber Security Incident Response	Participants are required to master core competencies in intrusion detection, containment protocols, system recovery, and forensic evidence collection, with practical application capabilities. They must demonstrate the ability to promptly identify intrusion attempts, implement effective

	countermeasures to halt attacks, swiftly restore normal system operations, while properly documenting and preserving evidence to support subsequent analysis.
Security hardening and traceability analysis	In terms of security reinforcement, participants are required to master methods for enhancing system defense capabilities, such as properly configuring security policies, updating system patches, and strengthening access controls. For traceability analysis, contestants must possess the ability to track attack sources and analyze attack paths. This involves reconstructing the attack process through analysis of system logs, network traffic, and other information to identify the origin of attacks, thereby providing evidence for preventing similar threats.

(4) The fourth stage: network security challenges in new technologies and new application fields

knowledge point	explain
Secure trusted data space	To address emerging technologies and new application scenarios, we conduct systematic data security risk assessments to identify potential vulnerabilities and critical threats to data assets throughout the entire lifecycle (collection, transmission, storage, processing, sharing, publication, and destruction). Based on risk assessments and compliance requirements, we design and implement comprehensive security strategies covering the entire data

	lifecycle. These include: implementing minimal data collection with desensitization/anonymization; establishing granular audit trails through access control systems (RBAC/ABAC); deploying secure protocols like TLS for data transmission and static encryption; applying integrity-preserving technologies such as hashing and digital signatures; developing secure data transfer mechanisms; and establishing data retention protocols with proper destruction procedures. We configure or integrate mainstream security technologies including Data Loss Prevention (DLP), database auditing, key management systems, secure gateways, and log analysis tools to ensure data confidentiality, integrity, and availability. Continuously monitoring evolving threats, regulatory updates, and technological advancements, we proactively adapt our capabilities through adaptive learning. Our rapid response system enables swift identification, analysis, and handling of data breaches, unauthorized access, tampering, and destruction incidents, effectively executing emergency procedures for incident recovery.

5. Skills management and communication

5.1. Experts and referees

The skills expert group, composed of chief experts, deputy chief experts and

expert members, is responsible for further revising the technical documents related to this competition.

Be responsible for the officiating, scoring, monitoring and result verification of the competition, report the results to the organizing committee office and the judging committee in time, and release the results on site.

5.2. Competitive exchanges

This event can be used to provide feedback in the QQ group of the event.

6. marking scheme

6.1. Scoring process and method

- All four stages of this competition will be assessed by computerized scoring systems to ensure objective and fair evaluation. To safeguard information security during the scoring process, two encryption procedures must be implemented within the venue. These encryption operations are managed by specialized encryption officers who guarantee standardized and accurate implementation throughout the entire process.
- The first group of encryption judges is responsible for the first lottery, generating the participant number, replacing the personal identity information of the players, recording the encryption process, and putting the relevant certificates into a sealed bag for separate storage.
- The second group of encryption referee organizations will conduct a second lottery to determine the race number, replace the participant number, record the

encryption process, and put the relevant numbers into another sealed bag for separate storage.

- All encryption results must be signed and confirmed by encryption judges and supervisors to ensure the transparency and traceability of the encryption process.
- After the summary of the four stages of the results is decrypted, the chief referee will review and sign to confirm the accuracy and fairness of the results. Finally, the staff will input the results into the system to complete the whole scoring process.

6.2. the code of points

- **Method of judging scores**

The on-site judging panel closely monitored the machine evaluation and scoring process to ensure fairness and impartiality. The scoring judges were responsible for encrypting the scores at each stage to ensure information security. The chief judge was responsible for decrypting and summarizing the scores, and kept a close watch on the progress of the competition throughout.

The competition site is equipped with supervisors, referees and technical support teams, each performing their respective duties. Referees are responsible for communicating with contestants, collecting and distributing test papers and other materials, and handling equipment issues; technical support engineers are responsible for emergency handling of equipment at workstations to ensure the smooth progress of the competition.

The whole competition process has a clear division of labor and close teamwork, which provides a good competition environment for the players.

- **Method of determining results**

The competition is scored according to the task, with a full score of 1000 points.

Detailed scoring requirements are shown in the table below.

Competition phase	Phase name	Task phases	Scoring method
stage Ⅰ weight 25%	Professional quality and theoretical skills	Question 1...N	Computerized automated scoring
stage Ⅱ weight 30%	Network and data security skills application, including basic network attack and penetration and vulnerability mining, data security analysis and application	Task 1...N	Computerized automated scoring
phase III weight 35%	Application of network security operations skills, including security incident response, security hardening and traceability analysis	Task 1...N	Computerized automated scoring
Phase IV weight 10%	Cyber security challenges arising from new technologies and new areas of application (trusted data space) Security skills applied	Task 1...N	Computerized automated scoring

6.3. Ranking rules

According to the ranking of scores, if the scores are the same, the higher score in

the fourth stage will be ranked higher. If the total score is the same and the fourth stage score is the same, the higher score in the third stage will be ranked higher, and so on.

7. Competition requirements

7.1. matters need attention

- Mobile storage devices, calculators, communication tools and reference materials are strictly prohibited during the competition.
- Please check the hardware, software and material list for completeness according to the competition environment provided by the competition, and ensure that the computer is running normally.
- Before you begin, read all the task requirements in detail and pay attention to possible correlations between tasks.
- Please save the results in time according to the requirements when operating. After the competition, the equipment will be kept running, and the final results will be submitted as the basis for evaluation.
- After the competition is over, please keep the equipment, software and questions on your seat. Do not take any items away from the venue.
- The submission is prohibited from adding any marks unrelated to the competition, and the violator will be deemed to have a zero score.

7.2. Competition schedule and score weight

The "Cyber Security" competition is divided into four stages. The schedule and

score weight of the competition are shown in the following table:

Competition phase	Phase name	Competition time (minutes)	weight	Scoring method
stage Ⅰ	Professional quality and theoretical skills	Thirty minutes on the first morning	25%	Computerized automated scoring
stage Ⅱ	Network and data security skills application, including basic network attack and penetration and vulnerability mining, data security analysis and application	60 minutes on day one	30%	Computerized automated scoring
phase III	Application of network security operations skills, including security incident response, security hardening and traceability analysis	80 minutes on the first day	35%	Computerized automated scoring
Phase IV	Cyber security challenges arising from new technologies and	Forty minutes a morning	10%	Computerized automated scoring

	new areas of application (trusted data space) Security skills applied			
amount to		210 minutes	100%	

8. Proposition principles and matters description

8.1. Propositional principles

(1) The competition questions are all original, and fully combine the theoretical and technical requirements of the actual environment.

(2) The competition supports anti-cheating mechanisms such as random attachments, dynamic FLAG, and random order and options of theoretical questions.

(3) In order to ensure the fairness, fairness and safety of the competition, the proposition work must be strictly in accordance with the relevant requirements of the organizing committee office, and the whole process should be kept confidential.

8.2. Method of answering questions

(1) Platform login

Participants need to use the assigned account and password to log in the competition platform and confirm that the account can log in the competition platform normally. After entering the platform, you can click the competition notice to view the

competition rules. (It is recommended to use Chrome browser)

(2) Answer theoretical questions

Click the entry button for the theoretical question competition to begin answering. After submitting your answer to each question, you can proceed to the next one. Contestants may freely choose any question number to answer and modify their answers within the specified time limit. Once all questions are completed, click Submit to finish the theoretical question competition.

(3) CTF answers

Click the CTF competition entrance to enter the answer section. Each CTF question needs to solve the correct flag value and submit it before you can get the corresponding score. You can click the next question to continue answering, and the system will automatically add the score of the questions you have obtained.

8.3. Competition announcement

The competition questions will be announced about one month before the competition through the official website of the competition.

8.4. Changes to competition questions

About 30 percent of the competition questions are changed before the official competition.

9. Infrastructure for the competition

9.1. Hardware configuration of competition operator

Paramount contestants do not need to bring their own computer, the organizing committee office will provide competition operation machine.

equipment	device name	quantity	remarks
Contestant client machine	PC machine	According to the configuration of the participating team	General purpose desktop (minimum configuration) Processor: i5/i7 Memory: 16G Solid state drive: 256G Graphics card: RTX4060 USB interface: 3.0 Network card: Gigabit

9.2. Competition operator software configuration

order number	software	introduce
1	Windows10	operating system
2	MicrosoftOffice2016/2019	Document editing tools
3	VMware17 or later	Virtual machine operating environment
4	Super Terminal SecureCRT/putty	Equipment debugging

		connection tool
5	Google Chrome	browser

9.3. Competition platform and other equipment

hardware	quantity	Specific configuration	remarks
Cyber security competition platform	2	(1) The competition platform system adopts B/S architecture, with built-in modules such as topic management, event management, team management, data statistics, large screen display and data operation and maintenance; (2) The platform scoring mechanism supports two modes of FLAG submission and CHECK verification, and the whole process of event scoring is completed automatically; (3) The platform supports Chinese and English interface display, the operation interface and topic description can be displayed in Chinese and English, which can support international competitions, or third language can be supported through extension; (4) The platform supports a variety of competition types, including theoretical competition, CTF flag capture competition, AWD/AWDP attack and defense competition,	The main configuration can be increased according to the number of teams

		security operation and maintenance competition and other common questions, which can be flexibly selected according to the requirements of the competition; (5) The platform supports user management functions, providing account management, team management and role permission management. Administrators can perform batch operations on accounts and teams, including import, export, add, delete and disable operations; (6) The platform supports the simultaneous management of multiple competitions, and supports the operation of new construction, editing, searching, publishing, environment deployment, in-process management, and results of competitions; (7) The platform supports individual and group participation in theoretical competition, problem solving competition, attack and defense competition mode, and can be freely combined according to the needs of the competition; (8) The platform supports the simultaneous management of multiple competitions, and supports the operation of new competition,	

		editing, searching, publishing, environment deployment, in-competition management, competition results and other processes.	

9.4. Layout of competition venues

The competition venue features well-lit facilities with complete lighting systems, stable power and water supply, and a clean environment. Isolation barriers are installed to restrict non-competition personnel from entering the area, ensuring safety and order in the competition zone. Security personnel, firefighters, medical teams, and equipment maintenance crews are on standby to handle emergencies. Safety corridors and warning lines are established to restrict access for spectators, journalists, and inspectors entering the venue, guaranteeing the smooth and orderly conduct of the event.

10. Competition discipline

Contestants should strictly observe the discipline of the competition, obey the command, wear the competition card uniformly, dress decently, and be polite. Observe the discipline of the competition, obey the command and arrangement of the staff, and take good care of the equipment and equipment of the competition site.

All competitors must register with their real names and bring their id cards. Those who take the exam on behalf of others or falsify information will be disqualified and notified.

(1) Participants must enter the venue within the specified time and take their seats according to the designated machine number. After entering the venue, they

must obey the unified arrangement of the competition organizers. After entering the venue, they will be disqualified from the competition.

(2) Contestants must complete the competition project at the designated seat. They are not allowed to leave the seat without permission from the judges. If they need to go to the bathroom or have other matters, they should raise their hands and indicate that they can leave the seat only after being confirmed and accompanied by the staff.

(3) During the competition, participants must strictly prohibit any attacks on the competition system or other contestants 'personal computers that could disrupt gameplay. Contestants are required to adhere to operational protocols, ensure equipment and personal safety, and comply with referees' supervision and warnings. If equipment malfunctions or damage occur due to participant-related factors, resulting in inability to continue the game, the chief referee reserves the right to terminate the contestant's participation. For equipment failures caused by non-participant factors, the chief referee will make decisions based on specific circumstances.

(4) Participants must strictly abide by the rules and regulations of the competition, obey the judges, play in a civilized manner, and strictly prohibit all kinds of cheating, communication with the outside world and other serious violations of competition discipline.

(5) Before the end of the competition, the contestants shall not leave the stage in advance; when the referee announces the end of the competition, all the contestants shall immediately stop the operation related to the answer.

(6) The competition adopts automatic scoring system. During the competition, the operation shall be carried out according to the requirements of the judges. Any

violation of operation shall be treated as cheating.

(7) To ensure the fairness and integrity of the competition, the expert panel and judging committee from the organizing committee will monitor real-time updates on contestants' scores and rankings throughout the event. They will randomly verify problem-solving approaches based on anti-cheating monitoring results. Contestants must document critical solution steps (writeup) during problem-solving and upload complete writeups of all key steps to the competition system.

(8) During the competition, the arbitration opinion of the chief referee shall be the final decision. Any uncivilized behavior such as disobedience to the referee or disturbance of the order of the court shall be strictly dealt with in accordance with relevant regulations.

(9) Violators of the above regulations will face penalties from the on-site referee team based on the severity of their actions. Penalties may include, but are not limited to: warnings, point deductions, disqualification from competitions, and public notifications to relevant authorities. Those who damage the competition environment or disrupt normal operations will be held legally accountable by the organizing committee office.

(10) When the end of the competition is heard, the participants should stop all operations immediately and shall not delay the time of the competition for any reason. When leaving the competition site, they shall not take away the items related to the competition.

11. Information about the competition

11.1. Safety operating instructions

(1) Participants shall confirm the safety and integrity of their work stations, equipment and tools according to the regulations, strictly abide by the rules and regulations of the competition, pay attention to personal and equipment safety, accept the supervision and warning of the judges, and compete in a civilized manner.

(2) When installing the equipment for the competition, the contestants should understand the performance parameters of the equipment in advance to ensure the correct use of the equipment.

(3) When installing sensors and other equipment, the contestants must pay attention to the short circuit of the positive and negative poles of the power supply to avoid burning out the equipment and safety accidents.

(4) When installing equipment, the contestants should keep the power supply of the work station off and do not connect the equipment with electricity. If leakage is found, they should report to the judges in time and contact technicians to check the equipment.

(5) Contestants should pay attention to anti-static safety during the installation of equipment, and should not put the circuit board on a metal surface or without protective stacking.

(6) Participants should not touch or open the power distribution box of the training station, and pay attention to the safety of using 220V strong power behind the station.

(7) Contestants shall not enter the work station of other teams or interfere with the competition of other teams during the competition.

11.2. Information for Teams

(1) Each team shall purchase personal accident insurance for the participants during the competition.

(2) Each team shall manage and educate the participants and team leaders for safety, and the team leaders shall keep communication open during the competition.

(3) All participating teams shall obey and implement the arbitration results. Any malicious appeal, once verified, the organizing committee will investigate the responsibility of relevant personnel.

(4) The team leader is responsible for the management and organization of the team during the competition.

11.3. Leader's Notes

(1) The team leader shall resolutely implement the competition and various rules, obey the arrangement and management of the event executive committee, strengthen the management of the participants, and make all preparations.

(2) The team leader is responsible for drawing the number of the participating team and shall not enter the competition site during the competition.

(3) The team leader is responsible for coordinating and communicating with the executive committee of the competition during the event.

(4) If the team considers that there is any non-compliance with the competition rules, the team leader shall submit the written appeal materials signed to the arbitration group of the event within 2 hours after the end of the competition. Oral appeal is invalid and the arbitration group will not accept it.

11.4. Information for participants

(1) Participants should strictly abide by the rules and regulations of the competition, ensure personal and equipment safety, accept the supervision and warning of the judges, and compete in a civilized manner.

(2) Participants shall enter the competition with the entry certificate issued by the organizing committee and valid identification documents (ID card or passport).

(3) Participants shall enter the competition venue within the specified time, confirm the on-site conditions and sign. They shall operate according to the unified instructions. Each team shall independently determine the division of labor, workflow, and schedule for participants, as stipulated.

Complete the competition at the designated workstation within the time limit. Do not enter the workstation of other teams at will.

(4) After entering the competition, the participants shall confirm whether the equipment and tools are safe and intact according to the regulations, strictly abide by the rules and regulations of the competition and operating procedures, and ensure the safety of their own person and equipment.

(5) During the competition, if there is a failure of the competition equipment caused by factors other than the players, please inform the on-site referee in time, and the technical staff will repair or replace the competition equipment. The referee team may give additional time according to the specific situation of the time spent to eliminate the failure.

(6) When installing and deploying the competition equipment, the contestants should understand the performance parameters of each equipment in detail, such as power supply input, so as to ensure the normal use of the equipment.

(7) When connecting sensors and other equipment, contestants should pay attention to prevent short circuit between positive and negative poles and avoid burning out the equipment. Do not touch or open the power distribution box of the training station, and pay attention to the safety of using 220V strong electricity behind the station.

(8) Food and drinking water will be provided in the stadium during the competition. The rest, food and toilet time of the competitors will be counted in the competition time.

(9) After the end of the competition, the participating team shall clean up the site and restore the venue to the state before the competition.

(10) During the competition, if the participants do not obey the instructions of the referee or disrupt the order of the court, the chief expert will deduct the score of the team at will; in serious cases, the team will be disqualified. Those who cheat will be disqualified directly.

11.5. Staff information

(1) The competition staff shall be uniformly employed and assigned by the competition executive committee.

(2) Obey the leadership of the organizing committee, observe professional ethics, adhere to principles and act in accordance with regulations. Do a good job with a high degree of responsibility, serious attitude and meticulous style.

(3) Be familiar with the Competition Rules and implement the competition rules carefully.

(4) Stick to the post, do not be late, do not leave early, do not leave without permission.

(5) The staff of the competition should actively maintain the order of the competition, so as to facilitate the normal performance of the competitors.

(6) The staff shall not answer any technical questions raised by the contestants during the competition. In case of any dispute, it shall be reported to the executive committee.

(7) Those who bring influence or losses to the competition due to violation of regulations will be given necessary treatment.