International CyberEx **2019**

#CyberEx19

cyberex_ INTERNATIONAL

OAS More rights for more people

incibe_ SPANISH NATIONAL CYBERSECURITY INSTITUTE

CNPIC CENTRO NACIONAL DE PROTECCIÓN DE INFRAESTRUCTURAS Y CIBERSEGURIDAD

INTERNATIONAL CYBEREX2019

CONTENTS

01_OBJECTIVE

The purpose of the International CyberEx is to carry out a cyber exercise among the Member States of the Organization of American States (OAS) and of the countries invited by the National Institute of Cybersecurity of Spain (INCIBE) in order **to strengthen the ability to respond to cyber incidents**, as well as **to improve collaboration and cooperation** in this type of incident. The exercise focuses directly on technical security profiles with strong knowledge in the field of Information and Communication Technologies (ICT).

The cyber exercise will take place in form of a CTF (Capture the Flag) in small teams. This format is based on a model of cyber security competition and is designed to serve as a training exercise that allows participants to gain experience in tracking an intrusion, as well as to improve reaction capacities to cyber attacks analogous to those that happen in the real world. There are two main styles for the CTF: attack/defense and jeopardy. The latter is suitable for **expanding technical capabilities.**

Jeopardy-style competitions are usually composed of several categories of problems, each containing a variety of questions of different values. Teams compete in an **8-hour session** for being **the first to solve the greatest number of challenges** but do not directly attack each other.

The countries that may participate are the **OAS Member States as well as the countries of the CSIRTs invited by INCIBE**. Each country may have 1 or more representative teams which shall include professionals from various fields and reinforce collaboration between institutions. The final selection of teams will be made by INCIBE and the Cybersecurity Program of the OAS.

The language used during the cyber exercise will be English.

THE CYBER EXERCISE WILL TAKE PLACE IN FORM OF A CTF (CAPTURE THE FLAG) IN SMALL TEAMS

02_PARTICIPATION REQUIREMENTS

Each country may have one or more representative teams that must meet the following requirements.

2.1. TEAMS

Teams may consist of:

CSIRTs Cyber Security Incident Response Teams (CSIRTs)

Experts from the public or private sector, military, academia, and civil society.

Each team can count with a **maximum of 4 members** and a **minimum of 3 members** according to the following distribution:

- **1 captain** who will act as coordinator of the team and will be the sole point of contact with the organizers. In addition, the captain will be in charge of delivering the flags captured and of requesting the clues that are available for each challenge.

- **From 2 to 3 team mates** who will support the captain to solve the different challenges.

The profile of the team members should be that of a **technician with experience and knowledge in ICT security** in at least one or more of the following fields:

- Knowledge in ICT security especially in the management of incidents in information security.

- Experience in managing security incidents and electronic fraud.

- Experience in analysis of compromised systems, SPAM, systems and security networks.

- Experience in malware analysis, both static and dynamic, and use of process automation tools such as behavior analysis, running analysis, etc.

- Experience in computer forensics. Experience in the use of tools that support the process of gathering and analyzing information.

- Experience in security audits: Methodologies, tools and technical experience in security audits or pentesting.

- Experience in administration and bastion of operating systems.

- Experience in network management and communications hardware, racks and applications and support services to security equipment.

02_PARTICIPATION REQUIREMENTS

2.2. REGISTRATION

In order to be eligible for participation in the cyber exercise, the team of each country must register at the online form

https://es.research.net/r/Registro_International

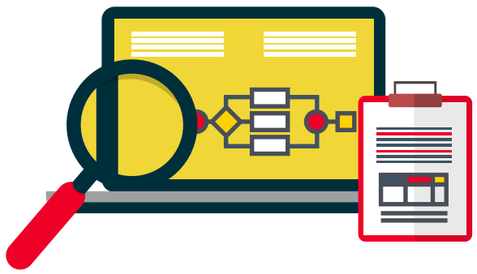
CyberEx19cyberex19_registro

Providing the following:

- Name, surname and contact information of the captain as well as the rest of the team members.
- Country and entity the team represents.
- Name of the team, taking into account that it will be public.
- IP addresses (with a maximum of 10) from which the participants are going to connect
- In addition, it will be possible to contribute an avatar or logo representative of the equipment, in format PNG 200x200 pixeles.

The contact information needs to be of the institution represented. Personal email addresses cannot be accepted.

Access to the platform will be restricted to the addresses provided during the registration, so it is important to ensure their availability for the day of the cyber exercise.



2.3. TECHNICAL REQUIREMENTS

The participating team is required to have at least the following resources:

Client server:

- Desktop PC or laptop.
- Browsers supported: Chrome (preferred) or Firefox (both in the latest versions).

Internet connection with sufficient bandwidth per user:

- Minimum: 1 Mbps download and 100Kbps upload.
- Recommended: 3 Mbps download and 1Mbps upload.

Although not mandatory, it is recommended that each participant has access to an additional machine (virtual or physical) that has a distribution Kali Linux or similar.

2.4. RULES

The following rules must be met by participants given that violating this code of conduct will disqualify the entire team and lead to an exclusion of the competition:

1. Participants must behave in a professional manner at all times.
2. Participants will not manipulate or attempt to modify any element of the platform, including the rating system and the administration panel.
3. Denial of Service attacks are not allowed.
4. Brute force attacks are not allowed, unless specifically specified otherwise.
5. Do not restart, shut down or disable services or functions of target systems.
6. Offensive actions to attack or interfere with the systems of other participants are not allowed.
7. Participants will not attempt to deceive or collaborate with participants of other teams.
8. Participants must compete without help from people outside the competition.
9. It is not allowed to publish information about the competition, how to solve the objectives or the flags of the same, without written consent from INCIBE.
10. Only the ranking of the 10 best teams will be announced. The rest of the positions will be anonymous.

03_NEXT STEPS

The cyber exercise will consist of several phases with the following milestones and dates.

3.1. REGISTRATION

In order to participate in the cyber exercise, the captain of each team must register the team through the online form as indicated above.

The online form will be available from **Monday, July 15, 2019 at 10:00 (UTC) through Thursday, August 8, 2019 at 10:00 (UTC).**

3.2. SELECTION OF PARTICIPANTS

Once the registration window is closed, the organizers of the cyber exercise will contact the captains of the teams selected via e-mail to notify them that they have been chosen to participate.

The email notification will be send out on **Thursday, August 22, 2019**.

3.3. DELIVERY OF ACCESS CREDENTIALS

Before the test session, the organizers will contact each of the participants via e-mail to deliver the access credentials to the platform.

The delivery of the credentials by email will take place **between August 26 and August 30, 2019.**

3.4. TEST SESSION, INFORMATION ABOUT THE EXERCISE AND DOUBTS

Once the captains of the teams selected have been notified, there will be a test session in which all participants will be able to check their connectivity and access to the platform, and an information session in which an introduction to the use of the platform will be given. Subsequently, questions posed by the captains will be solved.

This session will take place by videoconference and online chat on **Monday, September 02, 2019 at 14:00 (UTC)** with an estimated duration of 1 hour.

3.6. EXECUTION OF THE CYBER EXERCISE

For the cyber exercise, all the participants must be connected to the platform. The captains must also use videoconference and chat to get information on the initial situation, at the beginning of the exercise, and to be able to contact the organizers during the course of the exercise.

The date of the exercise will be on **Wednesday, September 11, 2019 from 14:00 (UTC) and until 22:00 (UTC)**, with an estimated duration of 8 hours.

3.7. CLOSING SESSION

Once the exercise is completed, a session will be held by videoconference with all the participants in which the results of the cyber exercise will be presented. Moreover, the scenario as well as the processes that lead to obtaining the flags will be analyzed.

The closing session will take place on **Wednesday, September 11, 2019 at 22:00 (UTC).**

04_RESOURCES

The cyber exercise is developed on the basis of challenges in the CTF (Capture the Flag) jeopardy format and will include the following resources.

4.1. CYBER EXERCISE WEBSITE

The cyber exercise website https://www.incibe-cert.es/international-cyberex will be the reference point for the participating teams and will contain at least the following information:

Public:

• Explanatory summary of the cyber exercise and simple instructions for the execution.

• Technical requirements for participation.

• Frequently asked questions (FAQ).

• Calendars with the key dates of the cyber exercise.

• Online registration form.

Private:

• User manual of the platform.

• Access to the platform to solve the challenges.

4.2. CTF EXERCISE PLATFORM

INCIBE will provide the exercise platform and the necessary infrastructure for the execution of the challenges, the game system and the scoring.

The backend of the platform includes a provisioning system to create the virtual infrastructure according to the scenario. It further includes a monitoring system which verifies that virtual networks, systems and "flags" (target systems, services or processes, files, etc.) are available and functioning correctly. The platform also has access and account control functions, logging, security controls, manageability and performance of the infrastructure, etc.

In addition, it allows to start several copies of the same scenario, climbing horizontally. Load management and balancing allow for adjustment of performance and mitigation if the scenario is damaged as a result of players' actions (for example: improper use of an exploit that disables a system). This shared environment is reserved at a given point in order to avoid overlapping and allows for stability and adaptability to develop the challenges.

Once the user connects to the environment, she/he:

• Receives information on the challenges.

• Receives information about the flags to be captured.

• Sends the captured flags to be validated (captains only).

• Accesses the system of hints. Only the team captain can request the hints.

• Has all general information, as well as a help section.

• Will know her/his progress in the game as well as the relative position compared to other participants.

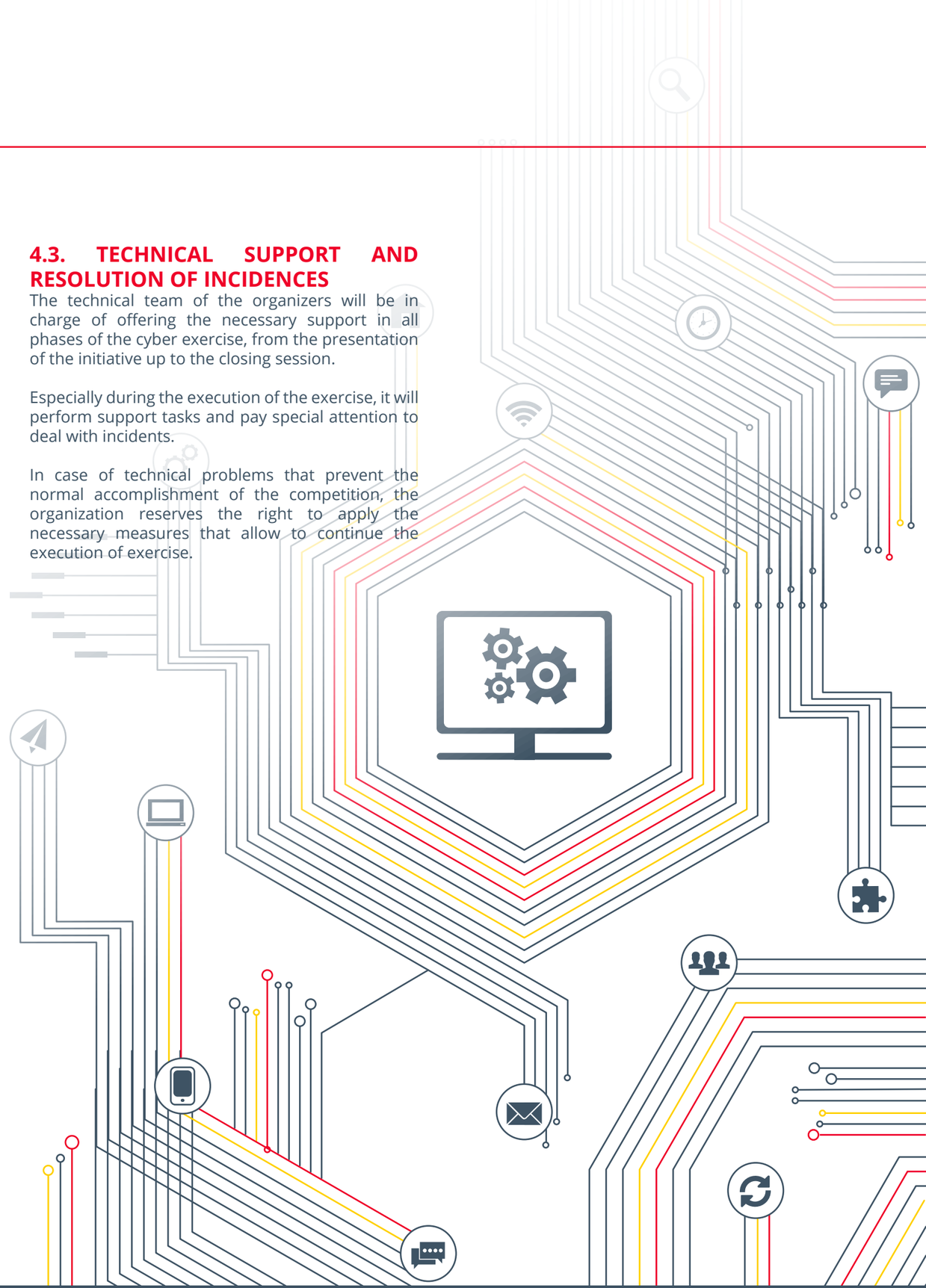
A good coordination between team members and their captain is a fundamental part of the cyber exercise, and should be strengthened. INCIBE reserves the right to limit the access to the platform only to certain users (for example, only to captains), or to modify the flow of the exercise during the execution of the same if the circumstances require it. Participants should be prepared for such events.

4.3. TECHNICAL SUPPORT AND RESOLUTION OF INCIDENCES

The technical team of the organizers will be in charge of offering the necessary support in all phases of the cyber exercise, from the presentation of the initiative up to the closing session.

Especially during the execution of the exercise, it will perform support tasks and pay special attention to deal with incidents.

In case of technical problems that prevent the normal accomplishment of the competition, the organization reserves the right to apply the necessary measures that allow to continue the execution of exercise.



International CyberEx **2019**

#CyberEx19

cyberex_ INTERNATIONAL

OAS More rights for more people

incibe_ SPANISH NATIONAL CYBERSECURITY INSTITUTE

CNPIC CENTRO NACIONAL DE PROTECCIÓN DE INFRAESTRUCTURAS Y CIBERSEGURIDAD