International CyberEx 2023

#CyberEx23

cyberex_ INTERNATIONAL

OAS More rights for more people

incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD

CONTENTS

INTERNATIONAL CYBEREX 2023

1 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 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 these types of incidents. The exercise focuses directly on technical security profiles with strong knowledge in the fieldof Information and Communication Technologies (ICT).

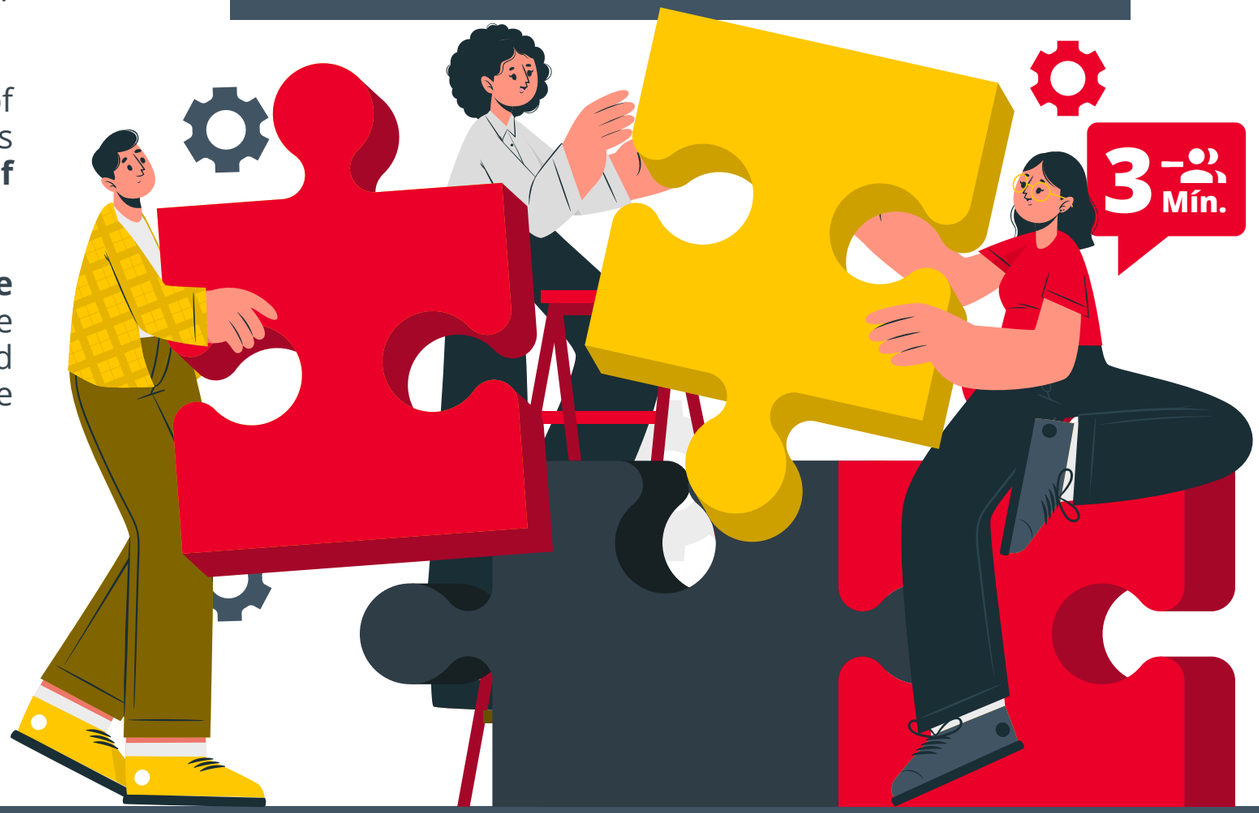
The cyber exercise will take place in form of a CTF (Capture the Flag) in small teams. This format is based on a model of cyber security competition and is designed to serve as a training exercise that allows participants to gain experience in tracking an intrusion, as well as to improve reaction capacities 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 differentvalues. Teams compete in an **8-hour session** to be **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 CTF (CAPTURE THE FLAG) IN SMALL TEAMS



2 PARTICIPATION REQUIREMENTS

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

◆ 2.1. TEAMS

Teams may consist of:

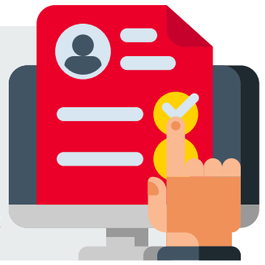
Each team can count with a maximum of 4 members and a minimum of 3 members according to the following distribution:

- ◇ **1 captain who will act as coordinator of the team** and will be the sole point of contact with the organizers.
- ◇ **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.

2 PARTICIPATION REQUIREMENTS

◆2.2. REGISTRATION



In order to be elegible for participation in the cyber exercise, the team of each country must register at the online form:
https://www.surveymonkey.com/r/CYBEREX2023

◆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 band width per user:

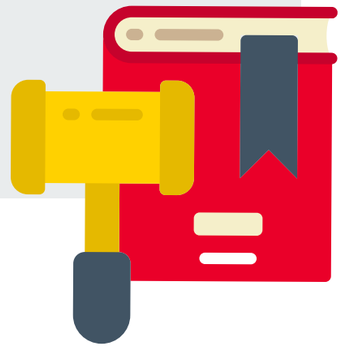
- ◇ Minimum: 1 Mbps download and 100kbps upload
- ◇ Recommended: 3 Mbps download and 1Mbps upload

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 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 permited. allowed.
4. Brute force attacks are not allowed, unless specifically requested 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 flagsof 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.



3 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 it through the online form at the following web address:
https://www.surveymonkey.com/r/CYBEREX2023.

The online form will be available **from May 15, 2023 to June 9, 2023 at 16:00 (UTC).**

◆3.2. SELECTION OF PARTICIPANTS

Once the registration phase is closed, the organizers of the cyber-exercise will contact the captains of the selected teams via email to notify them if they have been selected to participate.

Given that the maximum number of teams in the cyberexercise is limited, the OAS and INCIBE will make a selection of participants among all registered teams based on criteria to be defined between both organizations, among which may take into account the participation of as many countries as possible, and the prioritization of national reference CSIRT teams.
The notification by email will be made on **June 19, 2023.**

◆3.3. DELIVERY OF ACCESS CREDENTIALS

Prior to the test session, the organizers will contact each participant via email to deliver the credentials to access the platform.
The credentials will be delivered by email **on June 22, 2023.**

◆3.4. TEST SESSION, INFORMATION ABOUT THE EXERCISE AND DOUBTS

Once the captains of the selected teams have been notified, a test of connectivity to the platform and credentials will be carried out, as well as an informative session with all the participants in which an introduction to the use of the platform will be given. After the explanation, any doubts and questions raised by the captains will be answered.
This session **will take place by videoconference and online chat on June 28, 2023 at 14:00 (UTC)** with an estimated duration of 1 hour

◆3.5. EXECUTION OF THE CYBER EXERCISE

For the execution of the cyber-exercise, all participants must connect to the platform. The captains must also use videoconferencing and chat to be informed, at the beginning, of the starting situation and to be able to contact the organizers during the execution.
The date of the exercise will be **July 11, 2023 from 14:00 (UTC) to 22:00 (UTC)**, with an estimated duration of 8 hours.

◆3.5. CLOSING SESSION

Once the execution has been completed, a videoconference session will be established with all the participants in which the results of the cyberexercise will be reported. The closing session will take place on **July 11, 2023 at 22:00 (UTC).**

4 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.es/en/events/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 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 includes 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.
◇ Accesses the system of hints. Only the team captain can request hints
◇ Has all general information, as well as access to 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.

The technical team will pay particular attention during the execution of the exercise to perform support tasks and 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.

◆ 4.4. AWARDS

Teams that rank at the top of the cyber-exercise will be eligible for a number of rewards, which will be reported during the execution of the cyber-exercise and during the closing session of the cyber-exercise. To inquire about these rewards after the end of the exercise, please contact the organization at the following address: **cybersecurity@oas.org**

International

CyberEx 2023

#CyberEx23

cyberex_ INTERNATIONAL

OAS More rights for more people

incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD