International CyberEx 2016

CNPIC
CENTRO NACIONAL PARA LA PROTECCIÓN
DE LAS INFRAESTRUCTURAS CRÍTICAS

10 incibe_
2006-2016
TRABAJANDO POR
LA CONFIANZA DIGITAL

Organization of
American States

More rights
for more people

INTERNATIONAL CYBEREX2016

CONTENTS

01_PURPOSE

02_TEAM PROFILE

03_PLANNING

04_CYBEREXERCISE ASSETS

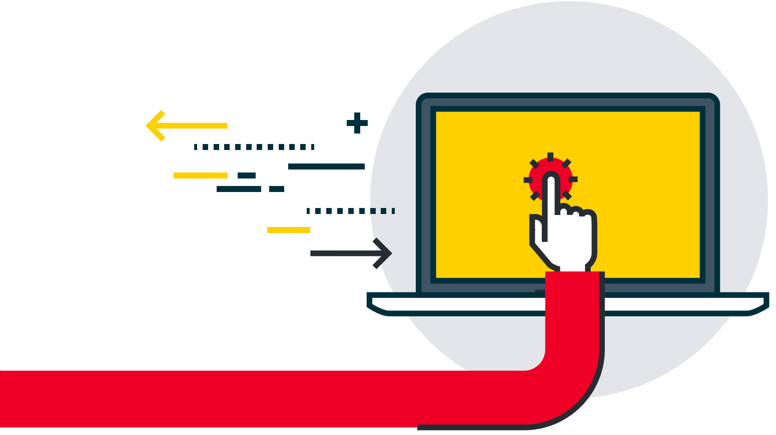
04.1_Cyberexercise website

04.2_CTF Execution Platform

04.3_Technical Team

04.4_Eligibility

01_PURPOSE



The purpose of International CyberEx is to run a cyberexercise within the Member States of the Organization of American States (OAS) that will allow the strengthening of the capacities to respond to cyber incidents, as well as increase and improve collaboration and cooperation against such incidents. This exercise focuses directly on a technical safety profile with high expertise in the field of Information and Communications Technology (ICT).

The cyberexercise will be conducted in "Capture The Flag" (CTF) format. This format is based on a cyber security competition model and is designed to serve as a training exercise that allows providing participants with experience in monitoring intrusion and working on reaction capabilities to similar cyber attacks that happen in the real world. There are two main types of CTFs: offense/defense and jeopardy. The latter has been chosen for this case because it is the most appropriate to expand technical capabilities.

Jeopardy style competitions usually involve several categories of problems, each of which contains a variety of questions with different values. The teams, at an 8-hour session compete to be the first to solve the most challenges, but they do not directly attack each other.

Potential participating countries are the 35 OAS Member States and OAS observer countries that could become guests. Participation by countries (with a maximum total of 45 teams) will allow the internal configuration by each country of a team that includes professionals from various fields and strengthening collaboration between institutions. The final selection of the teams will be made by INCIBE and the OAS Cyber Security Program.

The default language for the cyberexercise will be English.

This year, international CyberEx will take place concurring with the Summer Bootcamp event (https://cybercamp.es/summer-bootcamp). Therefore, attendees of the Summer Bootcamp could participate in person if desired.

Summer BootCamp 2016 is designed as a free and international event which is intended to offer general and advanced training in the latest techniques of fighting against cybercrime and cybersecurity incident managing. This training is offered to specialists from Law Enforcement Authorities and public CERTs and staff from public organizations working in areas directly related to cybersecurity. The event will take place in the city of Leon (SPAIN) from July 17th through July 29th.

Members not attending Summer Bootcamp could participate in the cyberexercise remotely from each location.

THE CYBEREXERCISE WILL BE CONDUCTED IN "CAPTURE THE FLAG" (CTF) FORMAT

02_TEAM PROFILE

Each team will consist of a maximum of 8 members. Some cases will involve the participation of more than two teams per country.

Teams may be composed of Cybersecurity Incident Response Teams (CSIRTs/CERTs – Computer Emergency Response Teams) or experts from the public or private sector and civil society.

The profile of the team members is a technician with expertise and knowledge in ICT security in at least one or more of the following fields:

- ICT security training and especially in management of information security incidents.

- Experience in managing security incidents and wire fraud.

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

- Experience in analyzing malware, both static and dynamic analysis and using tools that automate processes such as behavioral analysis, performance analysis, etc.

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

- Experience in security audits: methodologies, tools and technical expertise on security audits or pentesting.

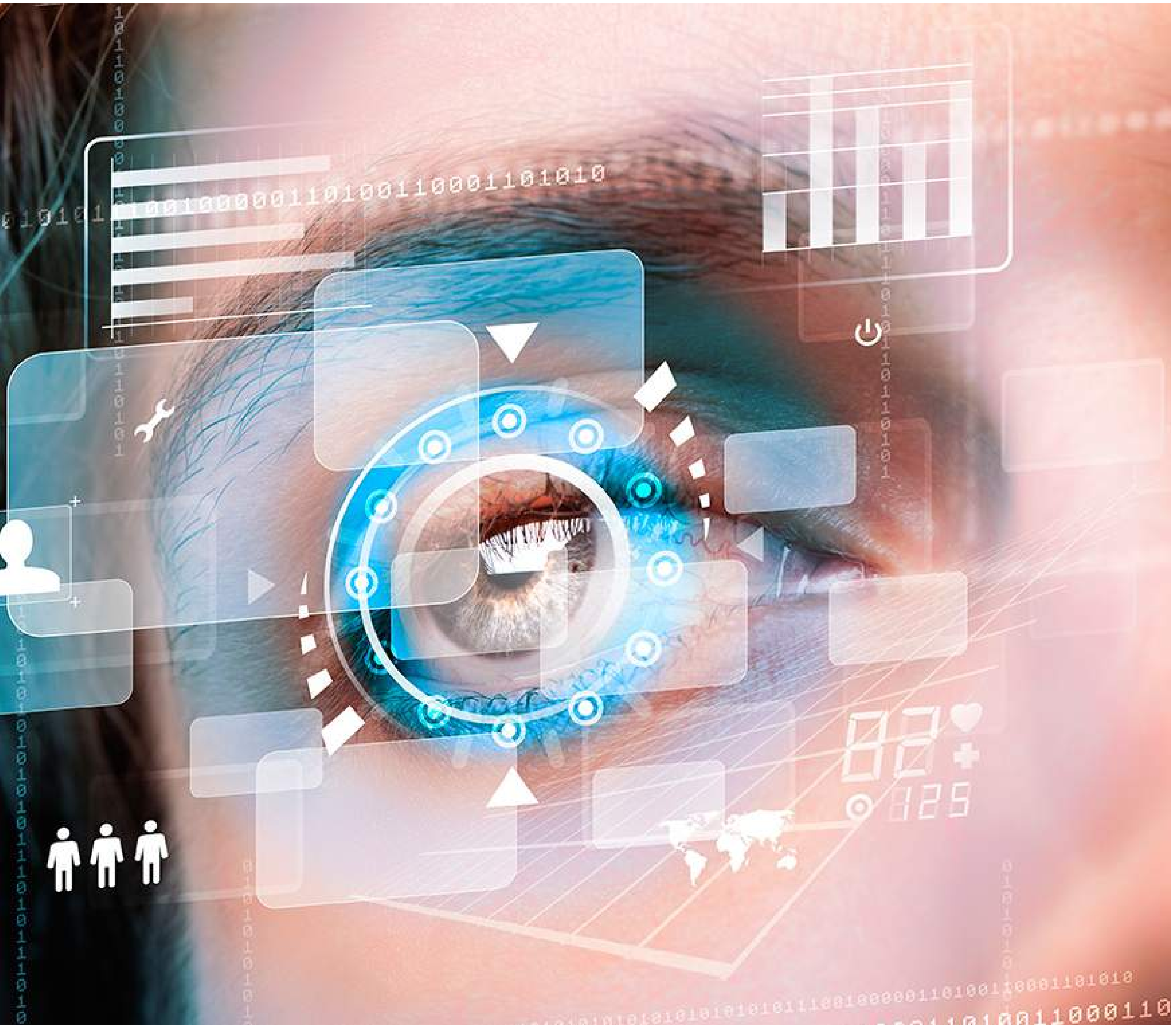
- Experience in administration and bastions of operating systems.

- Experience in administration of networks and communications hardware, racks and applications and safety equipment support services.

Each team must identify a captain, who will be responsible to discuss with the coordination team.

In order to join the cyberexercise, each team must complete a PDF form that specifies profile information and captain's point of contact.

03_PLANNING



The cyberexercise will have several phases, to be completed with the following schedule.

1. INTRODUCTORY SESSION

The cyberexercise will begin with an introductory meeting with all participants, where the initiative will be transferred and it will allow establishing the cooperation framework, both technical and organizational between the entities.

This session will take place by videoconference on July 7th, 2016 at 10.00 (GMT-4).

2. DOUBT SOLVING SESSION

This session will take place on Tuesday, July 19th, 2016 at 10:00 (GMT-4), and will serve, remotely via audio or video conferencing, for participants to submit questions and for the organization to respond to all of them as prior step to the execution of the exercise.

3. EXECUTION OF THE EXERCISE

The exercise date will be July 21st, 2016. The exercise will last for 8 hours and it will take place in a single day.

Given the amount of time zones of the OAS countries (as shown in Annex I), It is proposed that the reference time zone be GMT-4 (New York Time). This time zone allows including most countries, with a difference of one hour.

The cyberexercise will commence at 10:00 (GMT-4) and will end at 18:00 (GMT-4). It will include a time at the beginning to explain the scenario as well as time at the end for analysis.

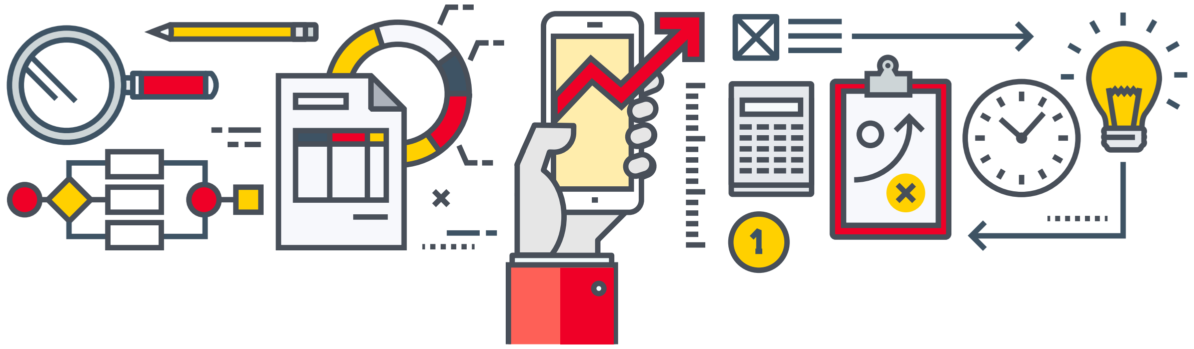
Each country team will participate remotely from each location or in person in the Summer Bootcamp event.

4. CLOSING SESSION

The closing session will serve to analyze the scenario executed as well as the processes that lead to the achievement of flags.

Also, participants will have the floor so they can give their opinion to improve future editions of cyberexercise.

The closing session will take place as a workshop of Summer Bootcamp on July 22, 2016 at 11:00 time of SPAIN (GMT+2). Also, once finished it will be uploaded to the private zone, so that all the participating members could access and view the session.



04_CYBEREXERCISE ASSETS

The cyberexercise will be developed based on the realization of challenges in jeopardy CTF format and will include the following assets..

04.1. Cyberexercise website
The cyberexercise website (https://www.cyberex.es/international/) will be the benchmark for the participating countries and willcontain at least the following information:

• Explanatory summary about the cyberexercise and basic instructions for implementation (public).

• Technical details for participation (public).

• Platform User Manual (private).

• Dates for the implementation of the cyberexercise (public).

• Management of users who will participate in the cyberexercise (private).

• Access to the platform to solve the challenges (private).

04.2. CTF Execution Platform
INCIBE will host the execution platform and the necessary infrastructure for the implementation of the challenges, the gameplay and scoring.

The backend of the platform includes a provisioning system to form the virtual infrastructure according to the scenario. It also includes a monitoring system that verifies that the virtual networks, systems and the “flags” (target systems, services or processes, files, etc.) are available and with adequate performance.

The platform also includes access and account control functions, logging, security controls, management capacity and performance of the infrastructure etc. It also allows starting multiple copies of the same scenario, scaling horizontally. Management and load balancing to adjust the performance and mitigating factor if the scenario is damaged as a result of the actions of the players (e.g. misuse of an exploit to disable a system).

This shared environment is reserved at some point to avoid overlap and it allows stability and scalability set out to develop challenges.

Once connected to the environment, the user:
- Receives the information on challenges.
- Receives the information of flags to be captured.
- Sends the flags captured for validation.
- Accesses the system tracks.
- Has an overview, a support section and the possibility of setting up the profile.
- Knows his or her progress in the game as well as the position relative to other participants.

04.3. Technical Team
The cyberexercise technical team is responsible for providing the necessary support for the realization of all the cyberexercise phases, since the submission of the initiative to the closing session.

It will perform support tasks, in particular and with greater emphasis, during the execution of the exercise to address incidences.

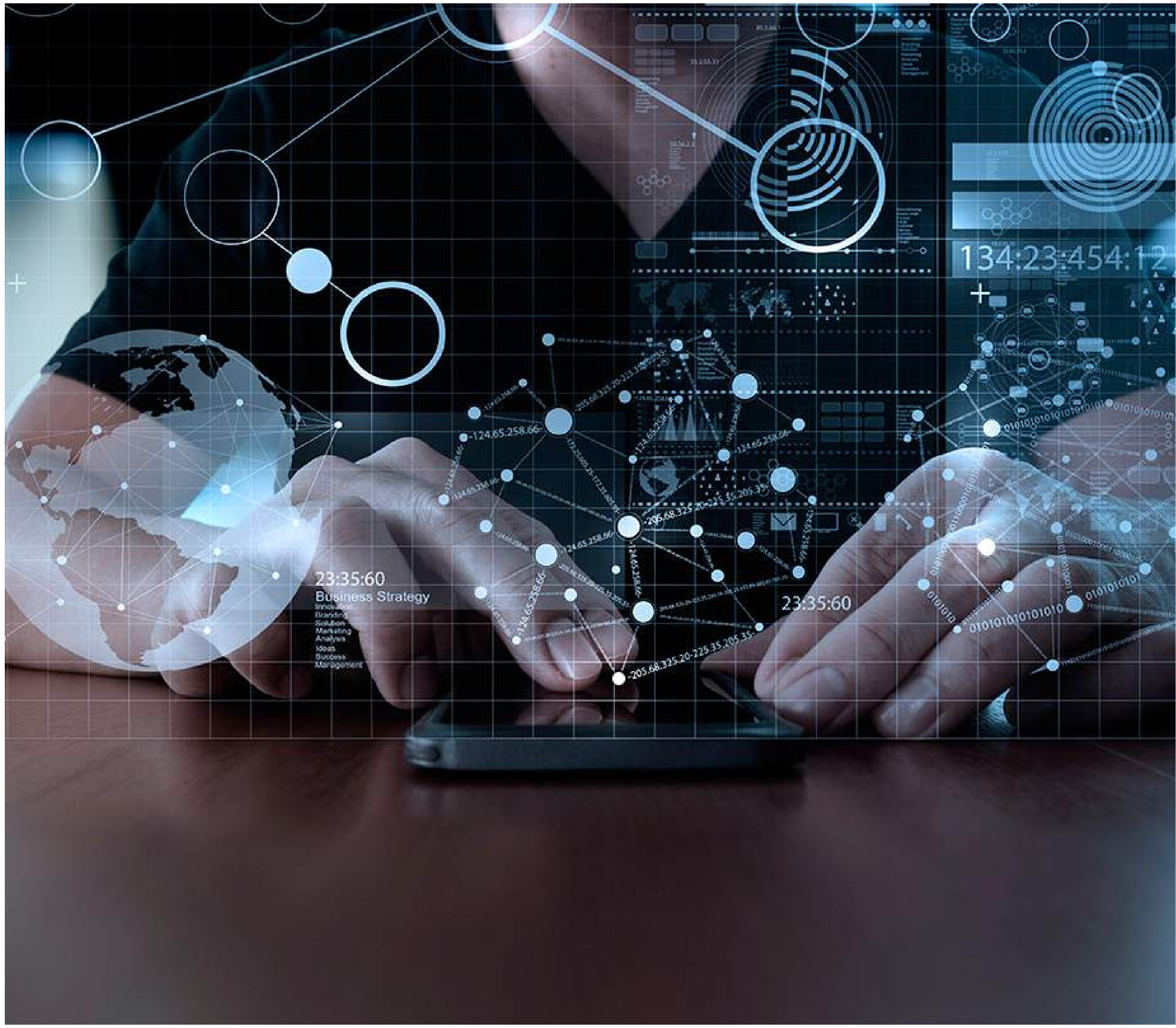
04.4. Eligibility
The participating team must have at least the following elements:

• Unfiltered Internet connection with minimum bandwidth: 256kbp/s.

• PCs with hacking tools such as:
  - Kali Linux
  - Backtrack

• A team captain responsible for team coordination and communication with the technical team of the cyberexercise organization.

• OpenVPN client to connect to the platform.



International CyberEx 2016

CNPIC
CENTRO NACIONAL PARA LA PROTECCIÓN DE LAS INFRAESTRUCTURAS CRÍTICAS

10 incibe_
2006-2016
TRABAJANDO POR LA CONFIANZA DIGITAL

Organization of American States | More rights for more people