



European Cyber Security Challenge 2015

# Info-Sheet

Coordinator:



Local Organizer:



Local Partners:



GOLD Sponsor:



# European Cyber Security Challenge

Today, most countries lack sufficient IT security professionals to protect their IT infrastructure. To help mitigate this problem, many of them setup national cyber security competitions for finding young cyber talents and for encouraging them to pursue a career in cyber security.

The European Cyber Security Challenge leverages these competitions in that it adds a pan-European layer to them: The top cyber talents from each country meet to network and collaborate and finally compete against each other to determine which country has the best cyber talents. To find out who's countries team is the best, contestants have to solve security related tasks from domains such as web security, mobile security, crypto puzzles, reverse engineering and forensics and collect points for solving them.

The European Cyber Security Challenge is an initiative from ENISA and organizations from six countries involved in the implementation of the first European Cyber Security Challenge in 2015 in Lucerne, Switzerland. The countries and organizations involved are:

- **Austria — Cyber Security Challenge Austria**

- Organization: Cyber Security Austria
- Webpage: <http://www.verbotengut.at/>
- Contact: Joe Pichlmayer, [joe.pichlmayr@cybersecurityaustria.at](mailto:joe.pichlmayr@cybersecurityaustria.at)



- **Germany — Cyber Security Challenge Germany**

- Organization: if(is), Heise Medien, TeleTrust, Compass Security (Consortium)
- Webpage: <http://www.cybersecuritychallenge.de>
- Contact: Prof. Norbert Pohlmann, [pohlmann@internet-sicherheit.de](mailto:pohlmann@internet-sicherheit.de)



- **Romania — D-CTF**

- Organization: National CYBERINT Center from Romania
- Webpage: (work in progress)
- Contact: Gabriela Matei, [gabriela.matei@cyberint.ro](mailto:gabriela.matei@cyberint.ro)



- **Spain — Cyber Camp Wargame**

- Organization: Instituto Nacional de Ciberseguridad, Ministerio de Industria, Energía y Turismo
- Webpage: <https://cybercamp.es/>
- Contact: Raúl Riesco Granadino, [raul.riesco@incibe.es](mailto:raul.riesco@incibe.es)



- **Switzerland — Swiss Cyber Storm Cyber Security Challenge**

- Organization: Swiss Cyber Storm
- Webpage: <http://challenge.swisscyberstorm.com>
- Contact: Bernhard Tellenbach, [president@swisscyberstorm.com](mailto:president@swisscyberstorm.com)



- **United Kingdom — Cyber Security Challenge UK**

- Organization: Cyber Security Challenge UK
- Webpage: <http://cybersecuritychallenge.org.uk/>
- Contact: Debbie Tunstall, [dtunstall@Cybersecuritychallenge.org.uk](mailto:dtunstall@Cybersecuritychallenge.org.uk)



# European Cyber Security Challenge 2015

In 2015, Swiss Cyber Storm and its local partners, the Swiss Federal department of Foreign Affairs, the Swiss Federal Department of Finance and the Swiss Academy of Engineering Sciences, host the European Cyber Security Challenge (ECSC). Swiss Cyber Storm is the organizer of Switzerland's national cyber security challenge.

## How to join the European Cyber Security Challenge

Countries and organizers of national challenges are invited to contact ENISA if they are interested in participating in 2016 or later. Contact: **Cosmin Ciobanu**, [Cosmin.Ciobanu@enisa.europa.eu](mailto:Cosmin.Ciobanu@enisa.europa.eu)

## What is the language of the competition?

The competition and all material related to it is in English. The language spoken with the officials/staff and the jury is English. Team-internal communication does not have to be in English.

## Who can participate?

Participants selected by their country's organization responsible for running the ECSC qualification. In 2015, the following countries can assemble and send a team:

- Austria, Germany, Romania, Spain, Switzerland, and United Kingdom.

The selected participants should be the top participants from the national challenge and must meet the following criteria:

- They are between 14 and 30 years old
- They are a citizen of the country for which they participate or they live or study there
- They do not (yet) have a master degree or similar
- They do not have a higher education related to cyber security (e.g., Certified Ethical Hacker, Bachelor in Forensics, ...)

Staff and other people involved in the development of the challenges for the ECSC final are excluded from participation.

## Team composition and categories

Teams consist of two (max. 3) coaches/staff members and a maximum of ten (10) contestants from two categories: Junior and Senior. The senior category might not contain more than five (5) members.

**Junior:** Between 14 and 20 years old

**Senior:** Between 20 and 30 years old

Note that categories in the national challenges might differ. In these cases, the countries assemble a team from the top participants that meets the above age criteria.

*Example: A country has a Junior category with participants between 14-18 years old. The country wants to send four members below 18 years, two members that are 19 years old and four members above 20 years.*

## What is the age cut-off date?

Cut-off date for the age criteria is the start of the national qualification phase in the respective country. Example: If someone turns 30 the day after this cut-off date, the person is eligible even though at the ECSC final, the person is already 30 years old.

**Can you give some examples of people meeting the above criteria?**

- 16 years old support technician apprentice
- 14 years old high-school / secondary education student
- 20 years old math student
- 26 years old software developer at Example.com with a BSc in electrical engineering.

# How does the ECSC final work (Program)?

The teams of the participating countries travel to Switzerland to compete against the other teams. The schedule looks as follows:

## October 19<sup>th</sup> before 13:00: Arrival Day

- Arrival at Zurich Airport and transportation to your Hotel in Lucerne.

Hotel: <http://www.radissonblu.com/hotel-lucerne>

By default, each team gets 6 double-rooms with two beds.

## October 20<sup>th</sup>: Acclimatize

- Intro and game rules and ethics instructions
- Setup of your team's infrastructure
- Solve some trial challenges to know how everything works
- From 18:30 on: VIP-Event in rooftop-bar in Lucerne.
  - Networking event with decision makers, government officials and other VIPs with the moto: "Meet the future cyber talents!"
  - By default, contestants <18 years old will be marked. They are not allowed to consume alcohol.

## October 21<sup>th</sup>: Acclimatize

- From 8:00: Challenge in challenge room.
- From approx. 17:00: Presentations in front of the Jury

## October 22<sup>th</sup>: Compete

- Transportation to Bern
- Hotel: <http://baerenbern.ch/default/en/index.html>
- By default, each team gets 6 double-rooms with two beds.
- Social Event for the teams
- Sightseeing in Bern
- Starting from approx. 17:00: Award Ceremony

## October 23<sup>th</sup>: Voyage home

- Transportation to Zurich Airport

# What do you have to bring with you?

## Non-Technical Equipment:

- Team-Clothing
  - for the VIP-Event, the challenge day and the award ceremony
- Clothing for 5 days
- Toiletris (toothbrush etc.)
- Writing utensils

## Technical Equipment:

- Your own **laptop** meeting the following minimum requirements:
  - 8GB of RAM, 20GB of free HD Space
  - Wired and wireless network access should be possible
  - You have to have admin rights on your laptop
- An **Ethernet network cable**, at least 3 meters long
- A **travel adapter** to plug in and power your equipment in Switzerland

## What tasks do I have to solve in the challenge?

Swiss Cyber Storm won't release detailed information on the challenges. However, the contest will be scenario based where you will have to (partially) setup and fix/defend an infrastructure. You'll also have the chance to collect points by attacking other teams. However, finding and fixing problems with your own infrastructure and keeping it up and running will be the most important part of the challenge.

Furthermore, it is important that you know the strengths and weaknesses of your team so that you can distribute the tasks appropriately. There will be three difficulty levels of tasks: Hard, Medium and Easy. Usually, Easy tasks are suitable for the Juniors in your team.

### **Tasks are related to the following topics:**

- Web Security
- Crypto Puzzles
- Reverse Engineering and Forensics
- (Secure) Programming
- Penetration Testing
- Attack & Defense
- Linux/Windows/MacOSX Security
- Mobile Security
- Presentation / Communication / Soft-Skills

## What can I do to prepare myself and my team?

- Register your Hacking-Lab account
- Download the LiveCD from:
- Get familiar with Hacking-Lab
- Try to solve some free challenges in Hacking-Lab
- Learn how to use the Hacking-Lab LiveCD
- Learn how to connect with VPN (using the LiveCD)
- Carefully read the "How it Works" section in Hacking-Lab

# Organization and Roles

The following main parties are involved in the organization of the European Cyber Security Challenge:

- ENISA organization committee consisting of one member per participating country
  - Definition of jury composition and selection criteria
  - Definition of the eligibility criteria for ECSC participants
  - Review of the participants: Online meeting on September 14th
  - Coordination of (supranational) press releases
- Local Organizer—Swiss Cyber Storm
  - Design, setup and operation of the challenge platform and the competition
  - Responsible for organizing transportation, challenge rooms, food and accommodation
  - Planning and supervision of the challenge and related events

Members of the local organization committee involved in the challenge design, setup and operation are not allowed to be a jury member or team tutor.

- Delegations: Team Tutors and Staff (max. of 2 per team. 3 on request)
  - They accompany a nation's team
  - They have to make sure that their team sticks to the schedule and rules
  - The leader of the delegation is the main point of contact with the local organizer

## Rules of the Challenge

The gaming rules specifying what participants are allowed to do and what not are published in a separate document. The document is handed out to the participants at the gaming rules and ethics instructions on site.

## Jury Composition

The Jury is composed as follows:

- One member from each participating country
- One representative per challenge sponsor

This is a benefit for Challenge sponsors to see the finalists in action

Selection Criteria for Jury Members are:

- Jury members must be older than 30 years
- Jury members should have more than 5 years of practical experience in the IT security domain
- Jury members should be able to assess presentation and communication skills
- Jury members must not have any professional relationship to any of the team members; a "No conflict of interest" note needs to be signed by each member of the jury.