TLP - AMBER

EUROPEAN UNION AGENCY
FOR CYBERSECURITY

Player Guide

Cyber Europe 2026

WHAT TO EXPECT FOR THE UPCOMING EXERCISE

Table of Contents

1. Cyber Europe 2026 in a nutshell

Cyber Europe is a series of pan-European exercises aimed at testing cybersecurity, business continuity and crisis management capabilities, for both the public and private sectors from the EU and EFTA Member States. The exercises are simulations of large-scale cybersecurity incidents inspired by real-life events, that escalate to become cyber crisis. Under its new mandate, ENISA will strengthen the existing preventive operational capabilities thanks to exercises like Cyber Europe.

The goals of Cyber Europe focus on:

- **TEST** and **IMPROVE** the readiness-preparedness of the EU to deal with large-scale cybersecurity incidents and crises
- **BUILD TRUST** between the actors in the EU cybersecurity *ecosystem*
- Provide participants a **TRAINING OPPORTUNITY** that is unique because of the intensity, magnitude and pressure generated by the simulated crisis

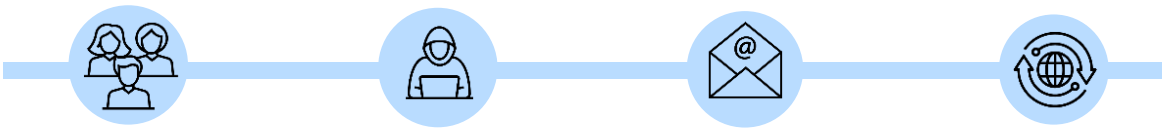
Cyber Europe 2026 will be the **8th edition** of this pan-European series of exercises, happening on 10th, 11th June 2026. The scenario of the exercise envisions attacks to the **railway and maritime sectors** all across EU, targeting as well digital infrastructure and public administration as secondary objectives to increase the pressure.

A series of technical and operational incidents that will require, technical knowledge, cooperation at various levels (intra-organisation, cross-organisation, national-level, cross-country) to resolve, as well as dynamic media pressure tasks will complement the operational aspects of the scenario. Cooperation and information exchange is expected to take place between National and European level as well as between participating players from the private sector and relevant Member State and EU authorities.

2. Conduct

2.1 During the exercise – what to expect

The exercise will last 48 hours: from **10th June 2026 at 09:00h CEST** until **11th June at 17:00h CEST**



Take part in a **cyber exercise** designed for **over 5000 European Entities**.

Playing from your **usual place of work**, using normal means of communication and operational procedures.

Respond/react to exercise injects (received by email) which contain details of **simulated cyber incidents** (= no real impact on systems).

Consult **the Exercise Universe** platform, which simulates media pressure.

- In order to contain communications linked to the exercise to only teams participating, but also to facilitate the players' cooperation and communication during the execution, an **Exercise Address Book** is created and shared with you in the STARTEX (first inject of the exercise). Please limit the communications to external teams to the entries of this Address Book.

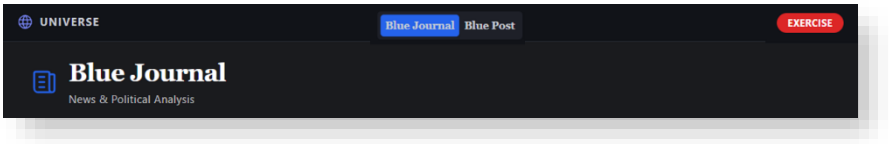
- Players will receive injects via email coming from noreply@exercises.cyberskills.eu
- The players respond to the Injects as in reality according to the **processes and procedure in place**.
- The players also promote **communication and collaboration with the other Exercise participants** if and when found necessary based on the Injects – via email, chat rooms, VCs, phone or other usable tools
- For every Exercise message **at the beginning** and **at the end** of the content (and at the beginning of the title if applicable/possible) the following marking will be added.

*****EXERCISE**EXERCISE**EXERCISE*****

- Please inform your teams/colleagues about the Exercise markings and use, together with the date of the exercise (so they are aware in case they receive by mistake a message marked as part of the Exercise)

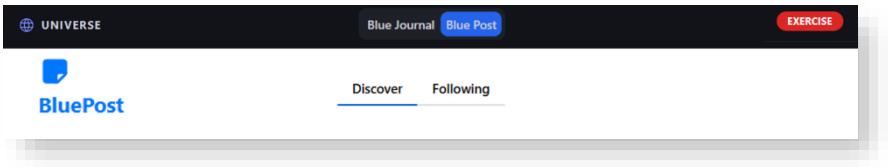
During the exercise you will have access the universe via two different platforms:

- **Blue Journal**: On this platform, you will find news articles and videos related to the events taking place during the exercise. Please make sure to stay up to date with the latest information, as new content may be published regularly.



- **Blue Post:** This platform functions as a social media application. While you cannot create or publish posts, you are able to view content published by simulated users, as well as their reactions.

  The top page of the Blue Post platform will resemble the screenshot provided. Please note that any content appearing under the *Following* tab is considered out of scope for this exercise and should be disregarded.



Access to the aforementioned platforms will be provided **on the day of the exercise.**

Do not fight the scenario and have fun 😊!

2.2 Important considerations

- **Do not post exercise content** on an online platform or on social networks
- **Do not share important information about the exercise** (scenario details, dates, player entities) in a public place or with non-participating entities/people.

2.2.1 Inform about a no-play situation

➢ **No-play situation** means, when a playing team decides that the exercise, as a whole, needs to be aborted for them.

This might happen for example when there is a fire alarm, when the building has to be evacuated, or when real crisis happens and people are needed for real situations.

In case a no play situation happens during the exercise the players must:

- **Send NO-PLAY email to Planner**

Simple template for no-play situation (please replace the fields in brackets):

To: *[YOUR PLANNER]*
Subject: (*EXERCISE* CE26): NO-PLAY for team *[YOUR TEAM]*

*** EXERCISE ** EXERCISE ** EXERCISE ***

Dear Planner,

We need to abort the exercise, NO-PLAY SITUATION for *[YOUR TEAM]*.

Short justification:

[Provide in a few words what happened]
*** EXERCISE ** EXERCISE ** EXERCISE ***

2.2.2 Use of AI and External Tools During the Exercise

Participants are expected to approach this exercise as they would a real-world incident, including careful consideration of how and when to use artificial intelligence tools and other external platforms.

Any decision to input, upload, or process information related to a potential compromise, such as logs, system data, or sensitive organisational details, should reflect the policies, legal constraints, and risk appetite of their organisation.

The same level of diligence applies to the use of third-party services more broadly. Participants must ensure that their actions align with internal security policies, data protection requirements, and established incident response procedures at all times.

3. Pre-exercise tests

3.1 Communication checks

A Communication-check is a verification test performed to ensure that all participants can receive exercise injects reliably and on time via the specific delivery methods used during the exercise.

Participants will receive a single, short verification inject via email. They will be required to acknowledge receipt by following the instructions within that inject (usually a quick link or survey).

This allows the exercise organisation to validate the player list and confirm deliverability for every individual recipient.

The Comm-check will arrive in your inbox as a standard email. Please ensure it has not been redirected to your junk or spam folder. The communication-check email will appear as follows:

*** EXERCISE ** EXERCISE ** EXERCISE ***

From: Cyber Europe 2026 Exercise Control
Sent at: 2026-05-18 10:00
To: ['All']
Subject: (*EXERCISE* CE26-ComCheck): Communication Check - Cyber Europe 2026

Dear participant,

You receive this email because you have been registered for the upcoming Cyber Europe 2026 exercise.

We perform this communication check in order to make sure you can receive the exercise injects (i.e. emails).

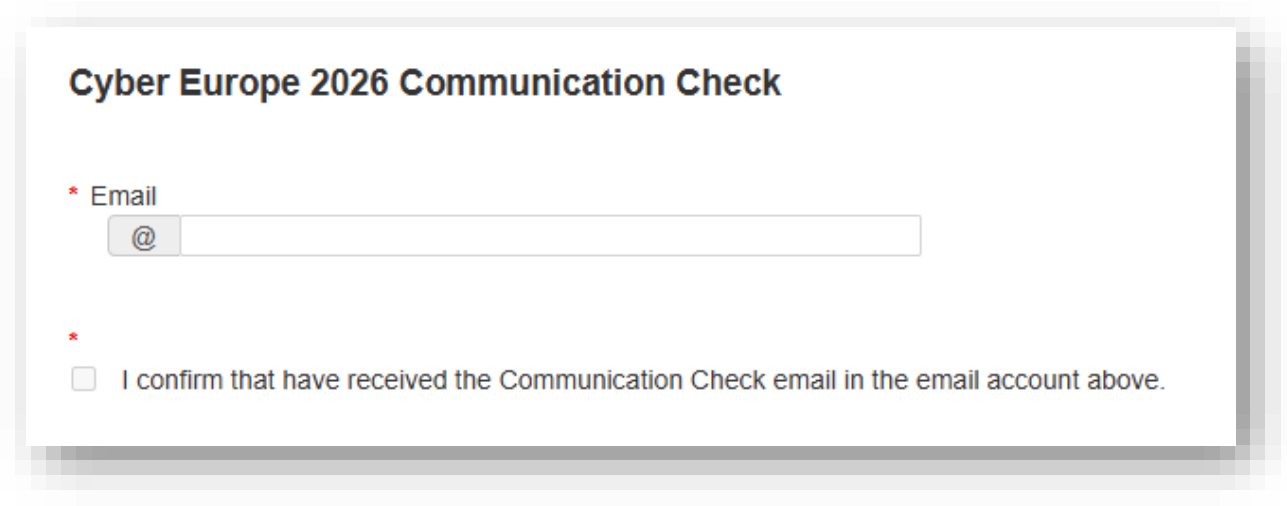
To help us verify this, please fill in this quick survey (less than 1 minute):
[survey link]

Please answer the survey by **Tuesday 19 of May**.

Regards,
Cyber Europe 2026 Exercise Control

*** EXERCISE ** EXERCISE ** EXERCISE ***

Once you open the email, click the provided link to access the verification survey, which will consist of the following fields:



3.1.1 Communication checks schedule

The CE26 organisation plans to perform 3 communication checks:

Communication check	When	Deadline to reply	Who does it apply to
Comm-check-1	11 May, 10h CEST	12 May (end of day)	All registered participants
Comm-check-2	18 May, 10h CEST	19 May (end of day)	Participants with issues in comm-check-1
Comm-check-3	25 May, 10h CEST	26 May (end of day)	All registered participants

If you do not receive the Comm-check inject as per the schedule, please reach out to your planner.

4. Resource requirements

The resources described below refer to an average security team that would like to participate in CE26. Teams can respond operationally and/or technically to incidents of the exercise depending on their needs, skills and availability of personnel. Below there are two different team setups; one describing the **optimal** and one describing the **minimal** human resource allocation in order to participate in CE26. Any intermediate setup is also acceptable.

In any given setup, teams should be aware that they would be occupied for two full days (8 hours each), which is the official length of the exercise. Teams can continue resolving incidents outside the 8-hour-per-day window of the exercise, as in real life, in order to mitigate the virtual crisis.

4.1 Team setup

	Optimal	Minimal
Benefit	Benefit from all aspects of the exercise	Benefit from selected aspects of the exercise
Operational players	2 x **IT/Security Team Coordinator**(s) and/or **Manager**(s)	1 x **IT/Security Team Coordinator** and/or **Manager**
Technical players	3 x **Cyber Security Analysts** with the following skills/level of expertise on more than one of the following: • Network Forensics (Skill Level Medium) • System Forensics (Windows / LINUX) (Skill Level High) • Artifact / Malware Analysis (Skill Level High) • Mobile Malware Analysis (Skill Level Medium) • Incident handling / IOC extraction (Skill Level Medium) • Cryptography (Skill Level High)	1 x **Cyber Security Analyst** with the following skills/level of expertise on one or more of the following: • System Forensics (Windows/Linux) (Skill Level Medium) • Programming (Skill Level Low) • Artifact / Malware Analysis (Skill Level High) • ICS Network Protocols (Skill Level High) Incident handling / Event Logs Analysis (Skill Level Medium)
Other players	1 x or more members of a **PR team** (for the media and communication incident response) 1 x **Data Protection Officer** (DPO) Specialist responsible for handling any issues that may arise related to data privacy and potential breaches.	1 x member of a **PR team** (for the media and communication incident response)

4.2 Tools and other resources

In order for the teams to perform their various operational and technical tasks, access to specific infrastructure will be needed. The CE26 exercise can be played with minimal technical/material resources in hand. Below is an indicative list of other resources needed for the exercise.

- A properly **configured lab** with a number of analysis machines (running your favourite OS) in order to download related artifacts and perform artifact analysis, with the following requirements
    - Windows:
        - minimum: CPU Cores 2 - RAM 4GB - Storage 60GB
        - optimal: CPU Cores 4 - RAM 8GB - Storage 60GB
    - Linux/Debian:
        - minimum: CPU Cores 1 - RAM 4GB - Storage 60GB
        - optimal: CPU 2 - Cores 4 - RAM 8GB - Storage 60GB
- **Software tools** that will be useful for analysis of the different incidents (examples):
    - VMware, Virtual Box Player (or any other Virtualization Solution)
    - Python or C
    - Hex Viewer such as HxD
    - PEStudio
    - Detect-It-Easy
    - radare2
    - IDA Free Debugger
    - Ghidra at least version 12.0.1
    - Android Emulator of your choice
    - Jadx
    - MobSF
    - Medusa framework
    - Frida tool
    - Docker
    - John The Ripper
    - MFT Explorer
    - Windows Sysinternals Utilities
    - A Windows VM for dynamic analysis
    - A Debian/Kali VM for static analysis (optional but recommended)

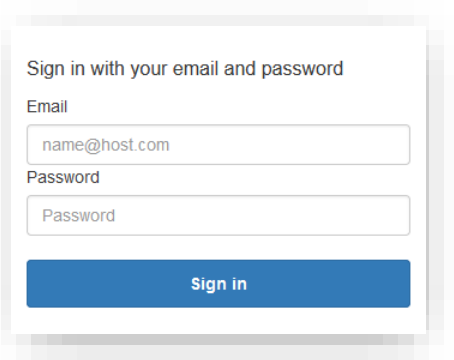
4.3 Technical Artifacts

If you are a technical player, as part of the exercise you will receive injects that include links to technical artifacts associated to the specific incidents composing the exercise. This section includes some useful information regarding how to access the different artifacts to analyse.

4.3.1 Encryption approach

The exercise has **one general set of credentials** that will allow you to download the different elements of the exercise, including the Technical Artifacts:

- **Username:** CE26-Player@cyberskills.eu
- **Password:** ItisTime-to-Play_CE26!



These credentials will be also provided in the STARTEX inject.

Furthermore, the **artifact-level password** will be provided during the course of the exercise in order to decrypt / unzip the files for analysis.

IMPORTANT: Use **7-Zip** to extract these files. Other software may fail to unzip the technical artifacts correctly due to file path lengths or formatting.

You can see here an example of inject bearing a technical artifact:

*** EXERCISE ** EXERCISE ** EXERCISE ***

From: CE26 Team
Sent at: 2026-06-10 09:45
To: Recipient Group
Subject: Sample inject

Dear all,

This is an illustrative inject with artifact include, take a look at the 'Related links' section below. Thank you.

CE26 team

Related links:

Artifact password: [password here]
Artifact SHA512: [integrity validation string here]
Download artifact from: [link to download]

*** EXERCISE ** EXERCISE ** EXERCISE ***

4.3.2 Early download

The following table includes the artifact links for early download (in order to avoid delays during the exercise):

Technical artifact ID	Download link
TA11	https://d156thhod767r2.cloudfront.net/ce26/artefacts/e1/inc11/e1-ransomware.zip
TA12	https://d156thhod767r2.cloudfront.net/ce26/artefacts/e1/inc12/Artifact_1.2.zip
TA13	https://d156thhod767r2.cloudfront.net/ce26/artefacts/e1/inc13/File-exfiltration-2026-May-04_13_01_02.pcap.zip
TA21	https://d156thhod767r2.cloudfront.net/ce26/artefacts/e2/inc21/comlogs.zip
TA22.1	https://d156thhod767r2.cloudfront.net/ce26/artefacts/e2/inc22/e2-train-firmware_part1.zip
TA22.2	https://d156thhod767r2.cloudfront.net/ce26/artefacts/e2/inc22/e2-train-firmware_part2.zip
TA24	https://d156thhod767r2.cloudfront.net/ce26/artefacts/e2/inc24/24-Supply-chain.zip
TA25	https://d156thhod767r2.cloudfront.net/ce26/artefacts/e2/inc25/railway-artifact-3.zip
TA26	https://d156thhod767r2.cloudfront.net/ce26/artefacts/e2/inc26/railway-artifact-1.zip
TA27	https://d156thhod767r2.cloudfront.net/ce26/artefacts/e2/inc27/workstation-evidence.zip
TA31	https://d156thhod767r2.cloudfront.net/ce26/artefacts/e3/inc31/soc-logs.zip
TA32	https://d156thhod767r2.cloudfront.net/ce26/artefacts/e3/inc32/pcs-image.zip
TA33	https://d156thhod767r2.cloudfront.net/ce26/artefacts/e3/inc33/E3-Ransomware.zip
TA34	https://d156thhod767r2.cloudfront.net/ce26/artefacts/e3/inc34/vts-malware.zip
TA41.1	https://d156thhod767r2.cloudfront.net/ce26/artefacts/e4/inc41/vulnticketing.vmdk.zip
TA41.2	https://d156thhod767r2.cloudfront.net/ce26/artefacts/e4/inc41/e41-web-compromise.zip
TA42	https://d156thhod767r2.cloudfront.net/ce26/artefacts/e4/inc42/ransomware.zip
TA43	https://d156thhod767r2.cloudfront.net/ce26/artefacts/e4/inc43/ddos.zip
TA44	https://d156thhod767r2.cloudfront.net/ce26/artefacts/e4/inc44/exfiltration.zip

IMPORTANT: The general set of credentials will be needed to download the artifacts; please take into account that the artifact-level password(s) and hash information will be provided to the players during the execution of the exercise in the “Related Links” section of the corresponding inject.

5. Evaluation & feedback

As part of CE26 Evaluation Plan, and in order to produce a valuable and insightful After-Action Report, we will ask you, before and after Cyber Europe 2026, to share your expectations towards the exercise (before) and to evaluate your participation and provide feedback (after). This will be done through two survey phases (maximum 15 minutes to complete) that will capture all these aspects.

5.1 Before

Before Cyber Europe 2026, you will receive a link to an **anonymous evaluation survey** to reflect your expectations. The evaluation consists of two distinct parts:

The General Survey: The aim of this survey is to capture your expectations about what you hope to gain through the experience and your confidence in completing specific tasks during the exercise.

The Role-specific Survey(s): The aim of this survey is to capture your baseline confidence for specific tasks you will perform during the exercise.

- The specific link will appear at the end of the general survey, dynamically tailored to you based on your answers to the player scoping questions. Please follow that link to complete the survey.
- If you are going to play multiple roles during the exercise, you may be asked to complete more than one role-specific survey.

Please fill in both surveys before the exercise execution, specifically **by 8th June 2026**. It will take maximum 15 minutes to complete.

Link to the pre-exercise survey(s): https://ec.europa.eu/eusurvey/runner/CE26-Players-Expectations

5.2 During

During exercise players are expected to interact with monitoring emails that will be flagged accordingly. Responses sent to this monitoring emails can be used for evaluation purposes. Players might be requested to submit analyses of technical artifacts to these email accounts. An example monitoring email could be '*enisa-monitor-[country]-ce2026@get.cyberskills.eu*'.

5.3 After

After the Cyber Europe 2026 comes to an end, containing a link to our **anonymous evaluation surveys**. Your insights are incredibly valuable for refining the exercise and assessing our objectives.

The evaluation consists of two distinct parts:

The General Survey: this section focuses on your overall experience and suggestions for improving future iterations of the exercise.

- The link will be provided directly in the **post-ENDEX inject**

- Upon completion, you will get access to the **Certificate of Participation**, which you can post on social media.

The Role-specific Survey(s): this section deep-dives into the specific challenges faced by your team, helping us evaluate whether the exercise's core objectives were met.

- The link(s) will appear automatically **at the end of the General Survey**, dynamically tailored to you based on your answers to the player scoping questions.
- If you played multiple roles during the exercise, you may be asked to complete more than one role-specific survey.
- After completing these final surveys, you will get access to the official **Exercise Solutions** of Cyber Europe 2026.

You will have to fill in this survey before **19th June 2026**. It will take maximum 15-20 minutes to complete.

6. Social media engagement

As part of our Cyber Europe 2026 Communication Plan, we have created a Social Media Pack for Players, which you can access through this link:

Link to the Player social media pack: https://d156thhod767r2.cloudfront.net/ce26/CE26-Player-SM-pack.zip

Inside, you will find:

- **Social media guidelines**: for you to read and follow carefully when communicating about Cyber Europe 2026 in social media
- **Social media copy suggestions**: including ready-to-use text and suggestions for your posts
- **Ready-to-use visual material**: ready-to-use image to include in your posts