enisa
EUROPEAN UNION AGENCY FOR CYBERSECURITY

What are Cyber Europe Exercises?

Cyber Europe exercises are large-scale cybersecurity incident simulations that escalate to EU-wide cyber crises.

The exercises offer the opportunity to analyse advanced cybersecurity incidents and deal with complex business continuity and crisis management situations.

Cyber Europe exercises are developed by European cybersecurity experts and feature exciting scenarios, inspired by real-life events.

The exercises are prepared by civil servants from most European countries and the ENISA exercises team.

As most European countries participate, cross-border cooperation is a key part of the exercises.

The Cyber Europe exercises offer adaptable learning experiences: from a single analyst to an entire organization, opt-in or opt-out scenarios – you can customize the exercise to your needs.

Why should I participate?

It is a unique opportunity to test internal business continuity and IT security policies.

Exercises provide IT security teams with hands-on incident handling experiences.

You can develop a strong collaboration with competent national authorities and private stakeholders.

You get connected to the persons in charge at national and European level in case of cyber crises.

Be part of the growing EU community of IT security specialists. You will a have a fun time while getting prepared for a real emergency!

How do I get involved?

Contact us at exercises@enisa.europa.eu

ENISA will connect you with the local planner to get you on-board.

The scenario

Cyber Europe 2022 planners developed a scenario revolving around Healtcare which can include, Ministries of Health, Healthcare Providers, eHealth service providers with potential impacts in other sectors.

The scenario will contain real life inspired technical incidents to analyse, from forensic and malware analysis, open source intelligence, and of course non-technical incidents.

The incidents will build up into a crisis at all levels: local, organization, national, European. Business continuity plans and Crisis management procedures will be put at test.

When and where?

In June 2022, for two days. The exact dates will be communicated upon registration.

Participants will stay at their usual work environment, connect to the ENISA Cyber Exercise Platform (CEP) and access the exercise information.

The exercise will rely upon the CEP offering an integrated environment, the Universe for the virtual world, including incident material, simulated news websites, social media channels, file sharing platforms and security blogs.

CYBER EXERCISE PLATFORM

Who is the target group?

The exercise is suited for IT security, business continuity and crisis management teams.

The scenario will require knowledge of cybersecurity issues such as network analysis, malware analysis, forensics, source code analysis, etc., as well as business continuity and crisis management, including media crisis communication.

Since the exercise can be tailored to the participants needs, the individual teams do not need to have expertise in all the above mentioned topics.

Public sector:
National/Governmental CSIRTs, Cyber Security Authorities, Ministries of Health, Healthcare Organisations (e.g. hospitals, clinics), eHealth Service Providers, Health insurances.

Private sector:
Healthcare Organisations (e.g. hospitals, clinics, labs), Health industry, Insurance companies.

European Union Agency for Cybersecurity (ENISA)

Agamemnonos 14
Chalandri 15231
Attiki, Greece
Tel: +30 28 14 40 9711

#CyberEurope

www.cyber-europe.eu
www.enisa.europa.eu

Contact us
exercises@enisa.europa.eu