JUNE 2023 LETRA TRAINING WEEK

INVITATION & AGENDA

EVENT 19- 21 JUNE 2023
LOCATION ENISA ATHENS FACILITY, AGAMEMNONOS 14, CHALANDRI 15231, ATTIKI, GREECE

LETRA TRAINING WEEK

We are pleased to invite you to the inaugural Learning, Exercises and Training (Letra) event, hosted by the European Union Agency for Cybersecurity (ENISA), as part of the 2023 European Year of Skills and the Cybersecurity Skills Academy. This exclusive training event will take place in ENISA's facilities in Athens and offer two distinct courses focused on crucial aspects of cybersecurity.

Course 1: Cyber Awareness Program Development
Date: June 19, 2023
Description: This course, based on ENISA's "awareness raising in a box"[1] concept, aims to equip participants with the skills necessary to develop effective cyber awareness programs within their organizations.

Course 2: Zero-Trust Architecture Training
Dates: June 20-21, 2023 (2-day course)
Description: This comprehensive two-day course will provide an in-depth understanding of the zero-trust security model, its logical components, network requirements, and essential security measures that can be implemented to enhance the maturity of a Zero Trust Architecture.

Both courses adhere to a 'train-the-trainer' approach and will be conducted exclusively in-person in Athens. Please note that there will be no hybrid delivery option for these sessions.

We are delighted to offer these courses free of charge. To apply, please email Fabio.DiFranco@enisa.europa.eu with your desired course selection no later than May 30, 2023. As the number of places is limited, we encourage you to confirm your attendance as soon as possible. Successful applicants will receive a confirmation email detailing their registration status.

[1] https://www.enisa.europa.eu/topics/cybersecurity-education/awareness-raising-in-a-box

ENISA LETRA TRAINING WEEK JUNE 2023

We look forward to your participation in this valuable learning experience as we strive to advance cybersecurity skills and knowledge across Europe.

TENTATIVE DAILY AGENDA

09.30 - 09.45	coffee break & (on the first day of each course) registration
09.45 - 11:00	Training session
11:15 - 11.30	coffee break
11:30 - 13:00	Training session
13.00 - 14.15	lunch
14:15 - 15.30	Training session
15.30 - 15.45	coffee break
15.45 - 17:00	Training session

Please note that coffee breaks and lunch will be provided free of charge during the event. However, participants are responsible for their own travel and accommodation expenses.

COURSE DETAILS: CYBER AWARENESS PROGRAM DEVELOPMENT AWARENESS RAISING IN A BOX (AR-IN-A-BOX)

During this course, participants will explore various methodologies for developing an Awareness Raising Program tailored to organizations of different types and sizes. The distinctions between custom and ready-made programs will be highlighted, and ENISA's AR-in-a-box project will be thoroughly discussed, including guidance on maximizing the use of the provided materials. Additionally, an introduction to designing a small tabletop exercise will be offered. To conclude, participants will engage in a real-time cyber awareness game, allowing them to apply their newly acquired skills and suggest enhancements.

Target audience, under the European Cybersecurity Skills Framework (ECSF)[2]:

- Cybersecurity Educators.

Learning Outcomes & Prerequisites:

Knowledge	Design and Implementation of a fully-fledged Cyber Security Awareness Program; Define key target audiences & dissemination channels for a Cyber Security Awareness Program; Define implementation steps towards the establishment of a Cyber Security Awareness Program; Identify maturity levels a Cyber Security Awareness Program; Define key steps towards the evaluation of a Cyber Security Awareness Program.
Skills	Design and Implementation of a Cyber Awareness Program; Select the right dissemination channels for your Cyber Awareness Program; Create engaging and gamified Cyber Awareness related content; Assess the maturity levels of a Cyber Awareness Program; Evaluation skills on Cyber Awareness Program Components.
Competences	Enhance Cyber Awareness & Capacity Building Skills; Awareness Program Management & Implementation.
Prerequisite	English: Common European Framework of Reference for Languages (CEFR) Level B2; Intermediate knowledge in: Cyber security awareness topics.

[2] https://www.enisa.europa.eu/topics/education/european-cybersecurity-skills-framework

COURSE DETAILS: ZERO-TRUST ARCHITECTURE

This two-day training is designed for information security officers and security architects seeking to transition to a zero-trust architecture model. Through this module, participants will:

1. Gain insight into the fundamental principles and components of a zero-trust architecture;
2. Learn about the controls that contribute to establishing a zero-trust architecture;
3. Determine the key steps for evaluating the maturity of a zero-trust architecture;
4. Identify controls that enhance the maturity of a zero-trust architecture.

By the end of the training, participants will have a solid understanding of the security measures that can be employed to address major threats and minimize associated risks through the implementation of a zero-trust security model.

Target audience, under the European Cybersecurity Skills Framework (ECSF):

- Cyber Security Architects;
- Chief Information Security Officers.

Learning Outcomes & Prerequisites:

Knowledge	Recognise best practices and standards in zero trust modules; Define key principles and elements of a zero-trust architecture; Define controls that contribute towards the establishment of a zero-trust architecture; Identify zero-trust architecture maturity levels; Define key steps towards the evaluation of the zero-trust architecture maturity; Identify controls towards the maturity of a zero-trust architecture.
Skills	Design a zero-trust architecture; Establish an implementation plan towards a mature zero-trust architecture; Select controls towards a zero-trust architecture; Assess the maturity levels of a zero-trust architecture; Identify zero-trust architecture's contribution to mitigate malicious activities.
Competences	Enhance architecture's zero-trust maturity; Development of a migration plan towards a ZTA; Evaluate security controls' contribution towards a ZTA.
Prerequisite	English: Common European Framework of Reference for Languages (CEFR) Level B2; Intermediate knowledge and experience in IT or networking; Intermediate knowledge in some of these topics: Basic information security controls, Basic cryptography concepts, Secure communications.