European Security and Defence College
Doc: ESDC/2022/219
Date: 12/10/2022
Origin: ESDC Secretariat

Curriculum

To be reviewed by	Activity number	Cyber Range – defensive capabilities	ECTS
Feb. 2025	**212**		**2**

Target audience

This course is intended for mid-ranking to senior officials employed in the field of cybersecurity from MS or EU institutions, bodies and agencies. Course participants' duties should relate to cybersecurity. Attendees should need to understand cybersecurity threats from a technical perspective.

Open to:

- EU Member States and EU institutions

Aim

The paramount objective of this course is to develop a more comprehensive approach to advanced exercises and training using new cyber defence technologies and scenarios. By bringing together civilian and military officials, it aims to improve understanding of how efficient and useful competences could be gained using the CyberRange (CR) platform.
Cyber Range is a complex virtual environment that reflects, models and simulates part of a cyber sphere. It offers organisations an opportunity to simulate cyber combat training and network and system development testing and benchmarking. Consequently, it is a multipurpose environment in support of three primary processes: knowledge development, assurance and dissemination.

It will translate into enhanced skills of digital professionals and contribute to building cyber-resilience and strategic autonomy – a pillar of CSDP.

The course is based on the CR platform and creates an opportunity to assess and discuss the importance of CR as a virtual training environment.

CORRELATION WITH CTG / MTG TRAs	EQUIVALENCES
CTG / MTG TRA on Cyber	• *Specialised at strategic, tactical and technical levels* • *Linked with the strategic objectives of Pillar 2 of the EU's Cybersecurity Strategy for the Digital Decade [16.12.2020 JOIN (2020)]*

Learning outcomes

Knowledge	LO01 – Describe the basic principles of Cyber Range (CR). LO02 – List the technical aspects of the CR platform design. LO03 – Identify the importance of CR as a virtual training environment. LO04 – List benefits of using the CR platform. LO05 – Identify the nature of the various cyber threats affecting an organisation.

Skills	LO06 – Define the required digital competence of staff responsible for cybersecurity. LO07 – Outline the opportunities offered by CR with regard to the capability development process within the cybersecurity field. LO08 – Use the CR platform in cyber-related professional training.
Responsibility and Autonomy	LO09 – Assess the potential impacts of cyber threats on an organisation. LO10 – Support the professional development of personnel dealing with cybersecurity.

Evaluation and verification of learning outcomes

The course is evaluated in accordance with the Kirkpatrick model, with level 1 evaluation (based on participants' satisfaction with the course).

In order to complete the course, participants have to accomplish all learning objectives, which are evaluated based on their active contribution to the residential module, including syndicate sessions and practical activities, as well as on the completion of the eLearning phases: course participants must finalise the autonomous knowledge units (AKUs) and pass the tests (mandatory), scoring at least 80% in the incorporated out-test/quiz. There is active observation by the course director/lead instructor and a feedback questionnaire is filled in by participants at the end of the course.

However, no formal verification of learning outcomes is planned; the proposed ECTS is based on participants' workload only.

Course structure

The residential module is held over three days.

Main topic	Suggested working hours (required for individual learning)	Suggested content
1. Cybersecurity within the EU	1(4)	1. Current EU regulations on cybersecurity, including the Cyber Defence Policy Framework (CDPF)
2. Various cyber threats that can potentially affect an organisation	6(4)	2.1. Cyberspace domain activities in Ukraine 2.2. Computer fraud 2.3. How criminals work - phishing - the practical part 2.4. Related case studies 2.5. Mapping of selected techniques onto the MITRE ATT&CK matrix and discussion of mitigants
3. Cyber Range platform	4(0)	3.1. Overview of the CyberRange platform and its potential use 3.2. Presentation of the technical aspects of the Cyber Range platform design 3.3. Possibilities for using the Cyber Range tool for organising training for participants in various locations 3.4. Pentester Tools Basic Course and Cyber Range Cybersecurity in Practice course content presentation 3.5. Cyber Range - effectiveness in enhancing the digital competence of staff responsible for cybersecurity
4. Kill Chain - scenario demonstration run on the Cyber Range platform	6(0)	4.1. Kill Chain - explanation of the problem 4.2. Presentation of the scenario prepared for the workshop 4.3. Background - embedding the discussed topics in reality, activities and techniques, discussion on the basis of the operation of APT groups 4.4. Environment 4.5. Presentation and description of the environment virtualised in CyberRange in which the workshop will be conducted 4.6. Workshop

		4.7. Conducting a scenario, discussing the next steps and the steps performed by the attacker
TOTAL	**17(8)**	

Materials required: • **AKU108** - The Cyber Defence Policy Framework (CDPF) Recommended: • Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union • Council Conclusions on Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry (November 2016) • The EU Cybersecurity Act (June 2019) • The EU's Cybersecurity Strategy for the Digital Decade (December 2020)	Methodology The course is based on the following methodology: lectures, panels, workshops, exercises Additional information Pre-course questionnaire on learning expectations and possible briefing topic from the specific area of expertise may be used. All course participants have to prepare for the residential module by going through the relevant eLearning preparatory phase, which is mandatory. The materials proposed for supplementary (eLearning) study will reflect current developments in the field of cybersecurity/cyber-defence in general and EU policies in particular. The Chatham House rule is applied during the residential phase of the course: "participants are free to use the information received, but neither the identity nor the affiliation of the speaker(s), nor that of any other participant, may be revealed".