EUROPEAN SECURITY AND DEFENCE COLLEGE
COLLÈGE EUROPÉEN DE SÉCURITÉ ET DE DÉFENSE

**European Security and Defence College**
**Doc: ESDC/2024/053**
**Date: 21 February 2024**
**Origin:** ESDC Secretariat

# Curriculum

| To be reviewed by | Activity number | **Cyber Threat Management** | ECTS |
|---|---|---|---|
| **Feb. 2026** | **264** | | **1** |

| CORRELATION WITH CTG / MTG TRAs | EQUIVALENCES |
|---|---|
| CTG / MTG TRA on Cyber | • *Specialised cyber course, at tactical/technical levels*<br>• *Linked with the strategic objectives of Pillar 1 and Pillar 2 of the EU's Cybersecurity Strategy for the Digital Decade [16.12.2020 JOIN (2020)]* |

Target audience

*The training is designed for personnel with an intermediate knowledge in cybersecurity. Participants sould be technical experts (civilians or military personnel), from Member States (MS), EU Institutions and Agencies.*

Open to:

- EU Member States / EU Institutions Bodies and Agencies
- Candidate countries

Aim

This course aims to provide an in-depth knowledge on top cyber threats and prepare participants to efficiently confront contemporary and emerging cyber-threats. It provides insights on the options security experts have in deploying efficient organizational and technical measures against the analysed threats.

Participants will be able to get a good understanding about each of the analysed threats, the way they can harm the organisation's assets, vulnerabilities that they can exploit, and most importantly, security measures that can be deployed to confront them and reduce the associated risks.

| Learning Outcomes | |
|---|---|
| Knowledge | LO1– Describe top cyber threats organizations face today<br>LO2- Define generic attack methods and techniques<br>LO3- Describe cyber-attack stages related to a threat<br>LO4- Understand security measures<br>LO5- Define the importance of organizational and technical security measures<br>LO6- Describe cyber threat intelligence management practices |
| Skills | LO7- Outline main cyber threats<br>LO8- Analyse a cyber-threat<br>LO9- Apply MITRE ATT@CK and Cyber Kill Chain frameworks. |

| | |
|---|---|
| Responsibility and Autonomy | LO10- Analyze the importance of vulnerabilities<br>LO11- Propose the use of specific security measures<br>LO12- Identify, and prioritize security measures<br>LO13- Identify attack surfaces and vectors related to a threat<br>LO14- Describe security measures contributions against threats |

## Evaluation and verification of learning outcomes

The course is evaluated according to the Kirkpatrick model, particularly level 1 evaluation (based on participants' satisfaction with the course) and level 3 evaluation (assessment of participants' long-term change in behaviour after the end of the course). Evaluation feedback is given in the level 1 evaluation of the residential modules.

In order to complete the course, participants have to accomplish all the learning objectives, and are evaluated on the basis of their active contribution to the residential modules, including their teamwork sessions and practical activities, and on their completion of the eLearning phases. Course participants must complete the autonomous knowledge units (AKUs) and pass the tests (mandatory), scoring at least 80% in the incorporated test/quiz. However, no formal verification of the learning outcomes is provided for; the proposed ECTS is based solely on participants' coursework.

The Executive Academic Board takes these factors into account when considering whether to award certificates to participants. Module leaders provide an evaluation report for each residential module. The Course Director is responsible for overall coordination, with the support of the ESDC Secretariat, and drafts the final evaluation report, which is presented to the Executive Academic Board.

## Course structure

*The recommended residential module is held over 4 days.*

| Main Topic | Suggested Working Hours (required for individual learning) | Suggested Contents |
|---|---|---|
| 1. The Threat Landscape | 2 | 1.1 Tactics, Techniques and Procedures<br>Attack frameworks (MITRE ATT&CK and Cyber Kill Chain)<br>1.2 ENISA Threat Landscape |
| 2. An introduction to vulnerabilities | 1 | 2.1 Main categories<br>2.2 Sources (NIST NVD, MITRE)<br>2.3 Scoring (CVSS) |
| 3. Analysis of major threats | 1 | 3.1 Analysis of 1-2 major threats identified by ENISA, e.g.,<br>3.2 Malware, Web-based attacks, Phishing |
| 4. Cyber security incidents | 5(2) | 4.1 Analysis of a cyber security incident (e.g. Malware – Emotet-based,<br>4.2 Web-based Attack – Capital One, Phishing – Ukrainian Power Grid) |
| 5. Cyber exercise 1 | 12 | 5.1 Analyze an attack related to a specific threat, using either the MITRE ATT&CK and Cyber Kill Chain frameworks or a combination thereof. |
| 6. Technical Security Controls | 4(2) | 6.1 Analysis of technical controls used to counteract cyber threats |
| 7. Cyber Threat Intelligence Management | 3 | 7.1 Cyber threat information, CTI formats, CTI sources, sharing with CERTs |
| 8. Cyber exercise 2 | 2 | 8.1 Security measures for the analysed attack<br>Prioritise proposed measures. |
| **TOTAL** | **30(4)** | |

## Materials

**Prerequisites**

- Intermediate knowledge and experience in IT or networking.
- Intermediate knowledge in some of these topics:
  - Basic Information Security Controls,
  - Cryptography concepts
  - Secure communications.

**Required:**

- AKU 55 - Strategic Compass
- AKU 104 - eLearning module developed by ENISA

**Recommended:**

- The ENISA Threat Landscape (ETL) report
- AKU 2: European Global Strategy
- Council Conclusion on EU Policy on Cyber Defence (22.05.2023)
- EU Policy on Cyber Defence, JOIN(22) 49 final (10.11.2022)
- Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 concerning measures for a high common level of cybersecurity across the Union (NIS 2)
- COUNCIL DECISION (CFSP) 2020/1127 of 30 July 2020 amending Decision (CFSP) 2019/797 concerning restrictive measures against cyber-attacks threatening the Union or its Member States
- EU's Cybersecurity Strategy for the Digital Decade (December 2020)
- The EU Cybersecurity Act ( June 2019)
- The EU Cyber Diplomacy Toolbox (June 2017)

## Methodology

- The course is based on the following methodology: lectures, panels, workshops, exercises and/or Case studies and cyber exercise (Table-top)

## 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 supplemental (eLearning) study will reflect current developments in the field of cyber security/cyber defence in general and EU policies in particular. Course participants must be willing to contribute with their specific expertise and experience throughout the course.

The Chatham House Rule is applied during all 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".