**European Security and Defence College**
**Doc: ESDC/2022/074**
**Date: 1 April 2022**
**Origin:** ESDC Secretariat

# Curriculum

| | | | |
|---|---|---|---|
| To be reviewed by<br>**Feb. 2024** | Activity number<br>**264** | **Cyber Threat Management** | ECTS<br>**1** |

| | |
|---|---|
| Target audience<br>*The training is designed for personnel with an intermediate knowledge in cybersecurity. Participants could be technical experts (civilians or military personnel), from Member States (MS), EU Institutions and Agencies.* | Aim<br>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.<br>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. |
| Open to:<br>▪ EU Member States / EU Institutions Bodies and Agencies | |

| 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)]* |

## 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: it makes use of *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 feed-back* is given in the level 1 evaluation on the residential modules.

In order to complete the course, participants have to accomplish all learning objectives, which are evaluated based on their active contribution to the residential modules, including their syndicate sessions and practical activities as well as on their 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. **However, no formal verification of the learning outcomes is foreseen; proposed ECTS is based on participants' workload only**.

The Executive Academic Board takes these factors into account when considering the award of *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 residential module is held over 3 days.*

| Main Topic | Suggested Working Hours (required for individual learning) | Suggested Contents |
|---|---|---|
| **Day 1** | **14(6)** | |
| 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 | 4 | 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 | 8(4) | 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. (1st Part). |
| **Day 2** | **8** | |
| 5. Cyber security incidents | 1 | 51 Analysis of a cyber security incident (e.g. Malware – Emotet-based,<br>5.2 Web-based Attack – Capital One, Phishing – Ukrainian Power Grid) |
| 6. Technical Security Controls | 4 | 6.1 Analysis of technical controls used to counteract cyber threats |
| 7. Cyber exercise | 8(4) | 7.1 Analyze an attack related to a specific threat, using either the MITRE ATT&CK and Cyber Kill Chain frameworks or a combination thereof. (2nd Part). |
| **Day 3** | **8** | |
| 8. Technical Security Controls | 4 | 8.1 Analysis of technical controls used to counteract cyber threats |

| | | |
|---|---|---|
| 9. Cyber Threat Intelligence Management | 3 | 9.1 Cyber threat information, CTI formats, CTI sources, sharing with CERTs |
| 10. Cyber exercise | 2 | 10.1 Security measures for the analysed attack<br>Prioritise proposed measures. |
| **TOTAL** | **30(6)** | |

## Materials

**Required:**

**Recommended:**

- ELearning on Threat Management
- Presentations
- Case studies and cyber exercise (Table-top)

Prerequisites

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

## 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 supplemental (eLearning) study will reflect current developments in the field of cyber security/cyber defence in general and EU policies in particular.

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".