European Security and Defence College

European Security and Defence College
Doc: ESDC/2025/039
Date: 20 February 2025
Origin: ESDC Secretariat

Curriculum

To be reviewed by	Activity number	**Cyber Threat Intelligence (CTI) Specialist**	ECTS
Feb. 2027	**267**		**1**

<u>Target audience</u>

The participants should be mid-ranking to senior military or civilian officials dealing with cyber threat intelligence (CTI), national intelligence, security operations centre and cybersecurity professionals from EU Institutions, Bodies and Agencies as well as EU Member States.

Open to:

- EU Member States / EU Institutions Bodies and Agencies

<u>Aim</u>

The goal of this course is to equip participants with a comprehensive understanding of Cyber Threat Intelligence (CTI) across tactical, operational, and strategic levels. By focusing on enhancing the security skill set of organizational personnel, the course aims to raise awareness of actionable threats and empower individuals to implement effective protective and detective measures. This proactive approach is essential for mitigating potential damage through prevention.

Moreover, the course serves as a platform for mid-ranking to senior officials to engage in meaningful discussions and share best practices on CTI-related topics. By fostering knowledge exchange, participants will improve their competencies in dealing with cyber threats.

Upon completion of the course, participants will possess the skills necessary to recognize adversary tactics, techniques, and procedures (TTPs). They will also learn to apply structured analytical techniques, enabling them to succeed in various security roles. This will ultimately contribute to a more robust organizational defense against cyber threats.

CORRELATION WITH CTG / MTG TRAs	EQUIVALENCES
CTG / MTG TRA on Cyber and on EU's Policy on Cyber Defence	• *Specialised cyber course, at tactical, operational, and strategic level.* • *Linked with the strategic objectives of Pillar 2 of the EU's Cybersecurity Strategy for the Digital Decade [16.12.2020 JOIN (2020)]* • *Supports the European Cybersecurity Skills Framework (ECSF) of ENISA 'Cyber Threat Intelligence Specialist' profile*

Learning Outcomes	
Knowledge	LO1- Describe Cyber Threat Intelligence (CTI) Mechanisms LO2- Describe CTI elements and state of the art tools and techniques LO3- Describe threat intelligence consumption LO4- Describe dissemination and attribution LO5- Define fallacies and biases LO6- Identify CTI methodologies LO7- Identify incident handling procedure from the CTI's point of view
Skills	LO8- Apply structured analytic OSINT / CTI techniques LO9- Apply the kill chain and diamond model L10- Build a CTI custom procedure LO11 - Practice intrusion analysis LO12- Recognise fallacies and biases LO13- Use Threat Analysis and Open Sources LO14- Use CTI tools LO15- Use relative tools (open source or commercial) and frameworks
Responsibility and Autonomy	LO16- Analyse collected information from various sources LO17- Analyse and Produce Intelligence LO18- Select the most accurate and appropriate information LO19- Select CTI Sources LO20- Create an intelligence requirement through a structured approach LO21- Create formal reports to present the results of analysis LO22- Create custom CTI procedure for an organization

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 fulfil 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 residential course is held over 3 days.		
Main Topic	**Suggested Residential Working Hours +**	**Suggested Contents**

	(Hours required for individual learning E-Learning etc)	
1. Introduction to CTI and Requirements	4 + (2)	• Intelligence Lexicon and Definitions • Differences between data, information, and intelligence • Structured Analytical Techniques
2. Threat Intelligence Consumption	4 + (2)	• Consuming Intelligence for Different Goals • Sliding scale of cybersecurity
3. Generate Intelligence	5 + (3)	• Prerequisites for Intelligence Generation • Building an Intelligence Team
4. Intrusion Analysis	6 + (3)	• Methods to Performing Intrusion Analysis • MITRE ATT&CK
5. Kill chain and Diamond model	6 + (3)	• Kill Chain • Diamond Model
6. CTI Collection Sources	4 + (2)	• Collection Source: Malware • Collection Source: Domains • External Datasets
7. Analysis and Production of Intelligence	6 + (3)	• Storing Threat Data • Threat Information Sharing
8. Fallacies and Biases	3 + (2)	• Logical Fallacies • Cognitive Biases
9. Dissemination and Attribution	4 + (2)	• Understanding the Audience and Consumer • Different Methods of Campaign Correlation • STIX and TAXII
TOTAL	**42 + (22)**	

<u>Material</u>

Required:
- AKU 109: Open Source Intelligence (OSINT) Introduction Course

Recommended:
- AKU 1 – History and Context of the CSDP
- 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**)
- EU Policy on Cyber Defence, JOIN(22) 49 final, 10.11.2022
- The EU's Cybersecurity Strategy for the Digital Decade (December 2020)
- The EU Cybersecurity Act (June 2019)
- The EU Cyber Diplomacy Toolbox (June 2017)
- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal

<u>Methodology</u>

The course is based on the following methodology: lectures, panels, workshops, exercises and/or case studies

<u>Additional information</u>

Pre-course questionnaire on learning expectations and possible briefing topic form 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. 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 modules 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".

data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) • Council conclusions on Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry (November 2016)	