European Security and Defence College
Doc: ESDC/2023/058
Date: 16 February 2023
Origin: ESDC Secretariat

Curriculum

To be reviewed by	Activity number	**Cyber Threat Intelligence (CTI) Specialist**	ECTS
Feb. 2025	**267**		**1**

Target audience	Aim
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	The aim of the course is to provide understanding of the Cyber Threat Intelligence (CTI) in tactical, operational, and strategic-level, supporting a robust establishment of security skillset and to develop existing skills. It focuses on organizations' personnel awareness of actionable threats, which empowers them to implement protective and detective measures. This helps to eliminate potentially damaging effects through prevention. Furthermore, this course will allow the mid-ranking to senior officials to exchange their views and share best practices on CTI-related topics by improving their knowledge, skills and competencies. By the end of this course, the participants will develop skills to recognize adversary tactics, techniques, and procedures, creating structured analytical techniques to be successful in any security role.

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)]*

Learning Outcomes	
Knowledge	LO1- Describe Cyber Threat Intelligence (CTI) Mechanism 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: 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, the 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
1. Introduction to CTI and Requirements	4 (2)	• Intelligence Lexicon and Definitions • Structured Analytical Techniques
2. Threat Intelligence Consumption	4 (2)	• Consuming Intelligence for Different Goals • 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: Open Source Intelligence (OSINT) Introduction Course

Recommended:

- *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 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)*

<u>Methodology</u>

The course is based on the following methodology: Presentations, Panels talks, Q&A and/or workshops

<u>Additional information</u>

The Chatham House Rule is applied during all residential modules of the HLC: "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".

The mandatory EU security clearance to "Confidential" level should be valid for the entire duration of the HLC and participants must prove that they have an EU clearance certificate before the start of the first residential module (September).