European Security and Defence College
Doc: ESDC/2025/026
Date: 20 Feb 2025
Origin: ESDC Secretariat

Curriculum

To be reviewed by **Feb. 2027**	Activity number **257**	**Practical Cyber Threat Intelligence and Information Sharing using MISP**	ECTS **1**

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

Target audience	Aim
The course is intended for technical personnel (mid-ranking officials, engineers and technicians) employed in the field of cybersecurity from MS or EU institutions, bodies and agencies. Due to the technical nature of this course, attendees should be familiar with cybersecurity threats from a technical perspective.	This course aims to provide participants with a good understanding and technical skills of the overall process of threat intelligence in incident response, to create and share their own intelligence but also apply the information sharing concepts and improve their cyber security processes to gather more information and exercise it more efficiently. Participants will gain full access to a MISP instance where they will actively participate. Real cases from cyber security and intelligence will be given during the training session to allow realistic hands-on session.
Open to: ▪ EU member States, institutions and agencies	

Learning Outcomes

Knowledge	LO1. Understand the overview of MISP platform and administrating instructions LO2. Define Intelligence Data LO3. Define Information Sharing Community LO4. Perceive the features of the MISP software
Skills	LO5. Gather intelligence data LO6. Document intelligence data LO7. Analyse and contextualize intelligence using MISP LO8. Classify threat intelligence information LO9. Apply the information sharing concepts LO10. Build information sharing communities
Responsibility and Autonomy	LO11. Assess the potential impacts of cyber threats LO12. Assess data models in MISP and move from Taxonomies to Custom Objects LO13. Determine which data could be turned into actionable intelligence using APIs LO14. Integrate MISP with your tools and processes

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 three days.

Main Topic	**Suggested Residential Working Hours + (Hours required for individual learning E-Learning etc)**	**Suggested Contents**
1. MISP	6 + (2)	1.1 Introduction Cybersecurity Information Sharing - MISP Perspective 1.2 Usage and Features of the MISP software 1.3 Common Integration of MISP within an Organisation - from MISP Setup and Seizing to Situational Awareness 1.4 MISP Administration and Starting your Information Sharing Community
2.Practical OSINT exercises	8 + (2)	2.1 Practical OSINT exercise - Best Practices in Threat Intelligence 2.2 Practical OSINT exercise - Gather, document, analyse and contextualize intelligence using MISP
3.Information Sharing Communities	2 + (2)	3.1 Building Information Sharing Communities
4. MISP data models	4 + (2)	4.1 Extending Data Models in MISP - from Taxonomies to Custom Objects 4.2 Turning data into actionable intelligence using APIs 4.3 Integrating MISP with your tools and processes
TOTAL	**20 + (8)**	

Materials

Required:

- AKU 55 – EU Strategic Compass
- AKU 104a: Information Security Management Course Guide
- AKU 104b: Information Security Management Implementation Course Part 1_v1.1
- AKU 104c: Information Security Management Implementation Course Part 2_v1.1
- AKU 104d: Information Security Management Implementation Course Part 3_v1.1

Recommended:

- AKU 1 History and Context of the CSDP
- 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)

Methodology

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

Additional information

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".