Curriculum

To be reviewed by **Feb. 2024**	Activity number **264**	**Cyber Threat Management**	ECTS **1**
			EAB.CYBER **N/A**

Target audience	Aim
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.	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.
Open to: ▪ EU Member States / EU Institutions Bodies and Agencies	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

The course corresponds to the strategic objectives of The EU's Cybersecurity Strategy for the Digital Decade [16.12.2020 JOIN(2020) 18 final] and the objectives of the CTG / MTG TRA

Knowledge	L01– Describe top cyber threats organizations face today L02- Define generic attack methods and techniques L03- Describe cyber-attack stages related to a threat L04- Understand security measures L05- Define the importance of organizational and technical security measures L06- Describe cyber threat intelligence management practices
Skills	L07- Outline main cyber threats L08- Analyse a cyber-threat L09- Apply MITRE ATT@CK and Cyber Kill Chain frameworks.
Responsibility and Autonomy	L10- Analyze the importance of vulnerabilities L11- Propose the use of specific security measures L12- Identify, and prioritize security measures L13- Identify attack surfaces and vectors related to a threat L14- 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. It is a specialised course, at tactical/technical levels. link with the Pillars 1 and 2 of the EU's Cybersecurity Strategy for the Digital Decade [16.12.2020 JOIN(2020).
Furthermore the course gives an overview of the CFSP/CSDP and the related EU policies and concepts and focuses on the foundations of the CFSP/CSDP [preparatory eLearning phase].

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 Attack frameworks (MITRE ATT&CK and Cyber Kill Chain) 1.2 ENISA Threat Landscape
2. An introduction to vulnerabilities	1	2.1 Main categories 2.2 Sources (NIST NVD, MITRE) 2.3 Scoring (CVSS)
3. Analysis of major threats	1	3.1 Analysis of 1-2 major threats identified by ENISA, e.g., 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, 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, 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 Prioritise proposed measures.
TOTAL	**30(6)**	

Materials	Methodology

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:
  o Basic Information Security Controls,
  o Cryptography concepts
  o Secure communications.
	The course is based on the following methodology: lectures, panels, workshops, exercises
	
	Additional information
	
	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).