European Security and Defence College
Doc: ESDC/2024/043
Date: 21 Feb 2024
Origin: ESDC Secretariat

Curriculum

To be reviewed by	Activity number	CSIRT Fundamentals	ECTS
Feb. 2026	**204**		**1**

CORRELATION WITH CTG / MTG TRAs	EQUIVALENCES
CTG / MTG TRA on Cyber	•Specialised cyber course, at technical and tactical levels •Linked with the strategic objectives of Pillar 1 and 2 of the EU's Cybersecurity Strategy for the Digital Decade [16.12.2020 JOIN (2020)]

Target audience

Participants should be mid-ranking to senior officials dealing with technical and tactical aspects in the field of cyber security and cyber defence from EU MSs, relevant EU institutions and agencies. They should have a background clearly related to technical and tactical aspects of cyber security.

(Information Technology (IT) or Information Security (IS) professionals)

Course participants must be available throughout the course and should be ready to participate with their specific fields of expertise and experience.

Open to:

- EU member States, institutions and agencies

Aim

This course will cover topics related to capabilities that need to be developed, implemented and provided by a Computer Security Incident Response Team.

The educational material combines the theoretical framework and innovative interactive e-learning methods and provides the materials to cover the fundamental knowledge required for cybersecurity incident response, as well as a comprehensive introduction to risk management.

Furthermore, this course will allow cyber security experts to exchange views and share best practices on cyber-related topics by improving their knowledge, skills and competencies. By the end of this course the participants will be able to assess the potential impacts and incidents on cyber policies and systems and determine cyber countermeasures on cyber policies and systems. Also, learners will acquire or develop specific knowledge, skills and attitudes which will allow them to investigate, analyse, and respond to cyber incidents within the network environment.

Learning Outcomes

Knowledge	LO1. Identify the EU institutions and agencies involved in cyber security and cyber defence and their roles LO2. Identify the challenges of cyber security at European level LO3. Recognise the extensive nature of the information society we live in LO4. Recognise the natures of the different cyber threats we are experiencing LO5. Define basic notions and concepts related to cyber security and cyber defence LO6. Incident handling standards, methodologies and frameworks LO7. Reflect on different cyber threat trends. LO8. Identify concepts related to hybrid threats on cyber LO9. Identify different trends of hybrid threats related to cyber security

	L010. Discern the challenges of industrial and public planning needed to face cyber threats LO11. Reporting Findings L011. Identify best practices and standards in information security management
Skills	LO11. Analyse information related to Cyber Threat Intelligence and Information Gathering LO12. Analyse security incidents LO13. Classify the technical and organisational tools related to cyber security LO14. Define in public policies the potential impacts of cyber threats LO15. Define in public policies the potential impacts of cyber security LO16. Classify the critical risks for information security management LO17. Understand the use of security detection and preventing techniques LO18. Apply concepts and techniques related to malware, forensic analysis and risk management
Responsibility and Autonomy	LO19. Assess the potential impact of cyber threats on cyber policies and systems LO20. Assess the potential impact of cyber incidents on cyber policies and systems LO21. Determine cyber countermeasures on cyber policies and systems

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

Main Topic	Suggested Working Hours (required for individual learning)	Suggested Contents
1. Incident Response and Management	4	1.1 Incident response terminology and definitions 1.2 An introduction to cyber threats 1.3 Cybersecurity attack procedures 1.4 Incident handling and incident management – an overview 1.5 Incident handling standards, methodologies and frameworks 1.6 Incident handling recommendations and best practices 1.7 Incident handling tools 1.8 Methodology on malware analysis, types, techniques and best practices 1.9 Incident response on malware
2. Risk Management	4(2)	2.1 Risk management as a fundamental component of building up a comprehensive cybersecurity posture 2.2 Overall context – what is risk and why is it important? 2.3 Risk management and its position in an overall organisational approach to cybersecurity 2.4 Main risk management concepts and terminology 2.5 Relevant standards and frameworks 2.6 Risk management process 2.6.1 Context Establishment 2.6.2 Risk Identification

		2.6.3 Risk Analysis 2.6.4 Risk Evaluation 2.6.5 Risk Treatment 2.6.6 Monitoring and Communication 2.7 Exercises
2. Cyber Threat Intelligence	6(2)	3.1 Indroduction Threat Intelligence 3.2 Identification of cyber threat actors 3.3 Analysis of cyber threats 3.4 Threat assessment and Hybrid threats 3.5 Threat Intelligence Tools 3.6 Incident handling, roles, report modules and communication plan
3. Malware Analysis	6	4.1 Methodology 4.2 Static vs Dynamic Analysis 4.3 Reverse Engineering/Debugging 4.4 Extracting Indicators of Compromise 4.5 Malware Incident Response Procedure
4. Forensic Analysis	6	5.1 Forensic Investigation Process 5.2 Forensic Analysis Methodology 5.3 Artefact analysis (memory, hard disk, network, etc other log analysis) 5.4 Reporting Findings
TOTAL	**26(4)**	

<u>Materials</u>

Required:

- AKU 55 - Strategic Compass
- AKU104-Information security management from ENISA
- AKU106- Hybrid modules

Recommended:

- AKU106 Hybrid modules
- 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)
- The EU Cyber Diplomacy Toolbox (June 2017)

<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'.