European Security and Defence College
Doc: ESDC/2024/055
Date: 21 Feb 2024
Origin: ESDC Secretariat

Curriculum

To be reviewed by	Activity number	**Implementation of Cybersecurity technical controls**	ECTS
Feb. 2026	**272**		**1**

CORRELATION WITH CTG / MTG TRAs	EQUIVALENCES
CTG / MTG TRA on Cyber	•Support ECSF Role 8. Cybersecurity Implementer •Specialised cyber course, at technical level •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 civilian or military personnel in IT who want to gain essential understanding and practical tools needed to perform actions to successfully mitigate the most common threats in order to better support their Organization's mission.

Prerequisites:

- good work/administration experience in the Linux and Windows environments, especially command line
- intermediate knowledge and experience in IT or networking.
- intermediate knowledge in some of these topics: Basic Information Security Controls, Cryptography concepts, Secure communications.

Open to:

- EU member States, institutions and agencies
- Candidate countries

Aim

This course aims to:

- reinforce the necessity and the exact scope of the most critical security controls;
- perform essential cyber security functions and basic incident response;
- enhance the understanding of the difference in performance between various devices and provide some important tips for handling the common threats;
- provide hands-on training on cyber security issues with lab execution.

Learning Outcomes

Knowledge	L01. List best practices and standards in critical cyber security controls L02. Examine methodologies for performing essential cyber security functions L03. Outline fundamental methodology for basic incident response L04. Examine common tools for handling common cyber threats L05. Outline Defense in Depth Techniques L06. Point Endpoint Detection and Response L07. Show Management and monitoring L08. Show Endpoint investigation L09. Show Network traffic analysis

Skills	L10. Define the basic notions and concepts related to cyber security controls L11. Recognize the procedure of performing essential cyber security functions L12. Recognize the procedure and methodology for instance response L13. Implement Defence in Depth , Detection and Response techniques L14. Apply Network traffic analysis
Responsibility and Autonomy	L15. Implement essential cyber security functions and basic incident response techniques. L16. Enhance understanding of the difference in performance of various devices implemented in cyber security. L17. Familiarisation with First Responder processes for the most popular client-side attacks.

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 accomplish 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

Residential module is held over 3 days

Main topic	Suggested working hours (required for individual learning)	Suggested content
1. Cybersecurity Introduction	1	• Introduction • Policy basics • IT cybersecurity Fundamentals
2. Defense in Depth Techniques	1	• Basic techniques of Defense in depth • Security functions & Networking
3. Endpoint Detection and Response	1	• Modern endpoint detection and response technologies • Next generation Anti-Virus
4. Log management and monitoring	1	• Logging techniques • Log sources evaluation Correlation and Alerts
5. Perimeter Protection – Firewalls& IDS	1	• Network security fundamentals • Applied security controls • Next generation Firewalls
6. Access Control	1	• Authentication mechanisms • From Windows authentication to Multi Factor Authentication, Authorization and audit
7. Incident Handling	1 (2)	• Incident handling phases • Management and processes
8. First Response	1 (1)	• After ALARM actions

		• First action items
9. Lab Preparation	1 (3)	Familiarization with First Responder processes regarding most popular client-side attacks.
10. Lab execution	7	• Endpoint investigation with Sys-internals • Memory acquisition with FTK • Volatile data acquisition with Triage-IR • Attachment online analysis • Attachment offline analysis • Network traffic analysis with Wireshark • IOCs - Threat Hunting • Mitigation activities across enterprise
TOTAL	**16 (6)**	

<u>Materials</u>

Required:

- AKU 112 – Linux Fundamentals
- AKU 113 – Pentester tools Basic course
- AKU 118 Incident response fundamentals
- In course case studies and exercises
  - AKU 104D
-

Recommended:

- AKU 55 - Strategic Compass

- AKU 114 – Cyber range – cybersecurity in practice
- 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 from 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".

Developed by: ESDC Secretariat