European Security and Defence College
Doc: ESDC/2021/074
Date: 17/03/2021
Origin: Executive Academic Board

Curriculum

To be reviewed by *February 2023*	Activity Number **210**	**Cyber Incident Handling process**	ECTS **2**

Target audience

Participants should be junior to senior ranking officials dealing with aspects in the field of cyber security from third States. They should have basic to good knowledge of Windows and Linux operating systems and bash commands.

Course participants must be available during the entire course and should be ready to participate with their specific field of expertise and experience.

Aim

This course aims to enable participants to comprehend the main notions of cyber incident handling and system forensics both in Windows and in Linux using widely available tools.

Furthermore, this course will help to build trust measures on cyber incident handling and system forensics, enabling officials to exchange their views, share best practices by improving their knowledge, skills and competencies in the cyber domain.

By the end of this course, the participants will be familiar with the terminology; concepts and tools used in cyber incident handling process and system forensics, and share views on how to detect attacks and find evidences that proves it.

Learning outcomes	Knowledge	K1 – Identify and understand the cyber threat K2 – Describe Incident handling process K3 – Distinguish between Memory, Registry, File System and Application forensics K4 – Describe Incident report
	Skills	S1 – Analyse the cyber threat S2 – Produce evidence from incident handling process S3 – Apply forensics methods in Memory, Registry, File system and Applications in Windows S4 – Apply forensics methods in Memory, File system in Linux
	Competences	C1 – Combine incidents to define a cyber-attack C2 – Evaluate the seriousness of an attack C3 – Produce Incident report C3 – Propose ways to secure the system after a forensics analysis C4 – Justify a cyber-attack C5 – Reconstruct a cyber-attack

Evaluation and verification of learning outcomes

The course is evaluated according to the Kirkpatrick model: it makes use of level 1 evaluation (based on participant's satisfaction with the course).

In order to complete the course, participants have to accomplish all learning objectives, which are evaluated based on the active contribution in the residential Module, including their syndicate sessions and practical activities as well as on the completion of the eLearning phases: course participants finalise the autonomous knowledge units (AKUs) and pass the tests (mandatory), scoring at least 80% in the incorporated out-test/quiz. At the end of the course, there is active observation by the course director/lead instructor and a feedback questionnaire is filled by the course participants.

However, no formal verification of learning outcome is foreseen; proposed ECTS is based on participants' workload only

Course Structure

Main Topic	Recommended Working Hours (of that eLearning)	Contents
Incident Handling	20(10)	Understanding the cyber threat Analyse the incident handling process Report an incident Specify evidences
System Forensics	30(15)	Windows • Memory forensics • Registry forensics • File system forensics • Application forensics Linux • Memory forensics • File system forensics
TOTAL	**50(25)**	

Materials

Essential eLearning:
AKU 104a: Information Security Management Implementation Course
AKU 104b: Information Security Management Implementation Course
AKU 104c: Information Security Management Implementation Course

Reading material [examples]:

- *The EU Cyber Diplomacy Toolbox (June 2017)*
- *The EU Cybersecurity Act (June 2019)*
- *EU Security Union Strategy: connecting the dots in a new security ecosystem*
- *The EU's Cybersecurity Strategy for the Digital Decade.*

Additional information

Pre-course questionnaire on learning expectations and possible briefing topic from the 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 supplemental (eLearning) study will reflect current developments in the field of cyber security/cyber defence in general and EU policies in particular.

In order to facilitate discussion between course participants and trainers/experts/guest speakers, the **Chatham House Rule** is used during the residential Module: "*participants to the CSDP HLC 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*"**.**