European Security and Defence College
Doc: ESDC/2020/035
Date: 14/02/2020
Origin: ESDC Secretariat

Curriculum

To be reviewed by *February 2022*	Activity Number ***204***	**Cybersecurity Organisational, Defensive Capabilities**	ECTS **1**

Target audience	Aim
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 clear background related to the technical and tactical aspects of cyber security. Course participants must be available during the entire course and should be ready participate with their specific field of expertise and experience.	This course will cover topics related to capabilities that need to be developed, implemented and provided by a Computer Security Incident Response Team. Furthermore, this course will allow cyber security experts to exchange their 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.

Learning outcomes	Knowledge	K1- Identify the EU institutions and Agencies involved in cyber security, cyber defence and their respective roles K2 - Identify the challenges of cyber security at a European level K3 - Recognise the extensive nature of the information society we live in K4 - Recognise the nature of the different cyber threats we are experiencing K5 - Define the basic notions and concepts related to cyber security and cyber defence K6 - Reflect on different trends among cyber threats K7 - Identify concepts related to hybrid threats on cyber K8 - Identify different trends of hybrid threats related to cyber security K9 - Discern the challenges of industrial and public planning needed to face cyber threats K10 - Identify the best practices and standards in information security management
	Skills	S1- Analyse information related to Cyber Threat Intelligence and Information Gathering S2- Analyse security incidents S3- Classify the technical as well as organisational tools related to cyber security S4- Classify the potential impacts of cyber threats in public policies S5- Classify the potential impacts of cyber security on public policies S6- Classify the critical risks for information security management S7- Use of security detection and preventing techniques S8- Apply concepts and techniques related to malware, forensic analysis and risk management
	Competences	C1 - Assess the potential impact of cyber threats on cyber policies and systems C2 - Assess the potential impact of cyber incidents on cyber policies and systems C3 - Determine cyber countermeasures on cyber policies and systems

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
Risk Management	8 (4)	• Risk management process, Roles, responsibilities • Risk identification, assessment, and response o Relevant definitions, Risk assessment process and steps o Risk register and assessment tables o Assessing risk, recording results in the risk register; different assessment approaches o Risk response strategies, developing risk response plans and actions o Examples of "actionable" risk responses • Risk Monitoring o Tracking and reporting risks o Monitoring existing risks and execution of risk response plans and actions o Business impact analysis (BIA)
Cyber Threat Intelligence	8	• Identification of cyber threat actors • Analysis of the cyber threats • Threat assessment and Hybrid threats • Threat Intelligence Tools • Incident handling and Threat Intelligence
Malware Analysis	5	• Methodology on malware analysis, types, techniques and best practices • Incident response on malware
Forensic Analysis	6	• Methodology on forensic analysis, types, techniques and best practices • •Incident response on forensic analysis
TOTAL	**27 (4)**	

Materials

Essential eLearning:
AKU 2 on European Global Strategy
AKU 104b Information Security Management Implementation Course

Reading material [examples]:
Council conclusions on Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry (November 2016)
European Parliament: Directive on security of network and information systems by the European Parliament (2016)

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*"**.**