European Security and Defence College
Doc: ESDC/2024/64
Date: 21 February 2024
Origin: ESDC Secretariat

Curriculum

To be reviewed by	Activity number	**Cyber Incident Responder**	ECTS
Feb. 2025	**265**		**1**

Target audience	Aim
The participants should be mid-ranking to senior military or civilian officials dealing with cyber incident response, security operations centre and cybersecurity professionals from EU Institutions, Bodies and Agencies as well as EU Member States and the Western Balkans. Open to: • EU Member States / EU Institutions Bodies and Agencies • Candidate Countries	The aim of the course is to prepare the participants to analyse, evaluate and mitigate the impact of cybersecurity incidents and to identify the root causes of cyber incidents and malicious actors. Furthermore, this course will allow the mid-ranking to senior officials to exchange their views and share best practices on security operation centres (SOCs) and computer security incident response teams (CSIRTs) topics by improving their knowledge, skills and competencies. By the end of this course, the participants will learn how to acquire and use specific tactics, techniques, procedures and tools and will develop skills to deal with large-scale cyber-attacks in a windows network/domain.

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

Learning Outcomes	
Knowledge	LO1- Identify incident handling tools LO2- Identify incident handling communication procedures LO3- Describe a Windows cyber-attack (incident) response process LO4- Describe the steps to effectively conduct incident response LO5- Describe Secure Operation Centres (SOCs) operation LO6- Describe best practices for effective incident response LO7- Discuss cybersecurity related laws, regulations and legislations

Skills	L08- Manage and analyse log files LO9- Collect, analyse and correlate cyber threat information originating from multiple sources LO10- Identify cyber threats using host, network and log analysis LO11- Build an incident response plan LO12- Use cyber incident response tools
Responsibility and Autonomy	LO13- Apply effectively the incident response steps LO14- Apply a dynamic approach to incident response process LO15- Use indicators of compromise to effectively respond to breaches affecting Windows LO16- Assess and manage technical vulnerabilities LO17- Measure cybersecurity incidents detection and response effectiveness LO18- Evaluate the resilience of the cybersecurity controls and mitigation actions taken after a cybersecurity or data breach incident

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, the 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 5 days.

Main Topic	Suggested Working Hours (required for individual learning)	Suggested Contents
1. Introduction to incident response	6(4)	• Event • Alert • Incident • Indicators of compromise (IOCs)
2. Security Operation Centre (SOC)	12(6)	• Develop a security operations centre (SOC) strategy • Create processes, procedures, and training • Manage and analyse log files • Collect, analyse and correlate cyber threat information originating from multiple sources • Identify cyber threats using host, network and log analysis
3. Steps of a cybersecurity incident response	12(6)	• Preparation • Identification • Containment • Eradication • Recovery • Lessons learned
4. Build and apply an incident response plan	10(5)	• Build an incident response plan • Use cyber incident response tools

5. Windows cyber-attack response process	12(6)	• Technical response best practices • Operations response best practices • Technical recovery best practices • Operations recovery best practices • Incident response process for Security and Operations (SecOps) • Post-incident clean-up
6. Risk Management	6(3)	• Identify risks • Assess risks • Risk treatment • Monitor and report
9. Communication procedures of a cybersecurity incident	6(4)	• Procedures to communicate a cybersecurity incident • Cybersecurity related laws, regulations and legislations
TOTAL	64 (34)	

<u>Material</u>

Required:

AKU 104: Module 3 – Experience a security incident
AKU 104: Module 5 – Introduction to Risk Management
AKU 104: Module 6 – Conduct Risk Assessment
AKU 104: Module 7 – Risk Treatment
AKU 104: Module 8 – Review Organisational Controls
AKU 104: Module 9 – Review Technical Controls
AKU 112: Linux fundamentals
AKU 118: Incident response fundamentals

Recommended:

- *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**)*
- *EU Policy on Cyber Defence, JOIN(22) 49 final, 10.11.2022*
- *The EU's Cybersecurity Strategy for the Digital Decade (December 2020)*
- *The EU Cybersecurity Act (June 2019)*
- *The EU Cyber Diplomacy Toolbox (June 2017)*
- *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)*
- *Council conclusions on Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry (November 2016)*

<u>Methodology</u>

The course is based on the following methodology: Presentations, Panels talks, Q&A and/or workshops

<u>Additional information</u>

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).