European Security and Defence College
Doc: ESDC/2025/031
Date: 20 February 2025
Origin: ESDC Secretariat

Curriculum

To be reviewed by **Feb. 2027**	Activity number **265**	**Cyber Incident Responder**	ECTS **1**

Target audience	Aim
Mid-ranking to senior military or civilian officials involved in cybersecurity incident response, as well as security operations center (SOC) and cybersecurity professionals from EU Institutions, Bodies, Agencies, and EU Member States, including the Western Balkans and other politically important regions in a base by base basis.	This course is designed to equip participants with the necessary skills to: • Analyze, evaluate, and mitigate the impact of cybersecurity incidents. • Identify root causes of cyber incidents and the malicious actors behind them. Participants will engage in exchanging views and sharing best practices regarding SOCs and Computer Security Incident Response Teams (CSIRTs). The course aims to enhance their knowledge, competencies, and capabilities to effectively tackle large-scale cyber-attacks within Windows network/domain environments. This course serves as an essential training module for cybersecurity personnel and officials, ensuring they are well-prepared to tackle the evolving threats in the cyber landscape effectively. By developing a comprehensive understanding of incident response strategies, best practices, and legal considerations, participants will enhance their capability to protect and secure cybersecurity infrastructures within their respective jurisdictions.
Open to: • EU Member States and EU institutions	

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)]* • *Supports the European Cybersecurity Skills Framework (ECSF) of ENISA Role profile 2. Cyber Incident Responder*

Learning Outcomes	
Knowledge	LO1: Identify incident handling tools. LO2: Understand incident handling communication procedures. LO3: Describe the response process for Windows cyber-attack incidents. LO4: Outline effective incident response steps. LO5: Describe the operation of Secure Operation Centers (SOCs). LO6: Identify best practices for effective incident response.

	LO7: Discuss relevant cybersecurity laws, regulations, and legislation.
Skills	LO8: Manage and analyze log files effectively. LO9: Collect, analyze, and correlate cyber threat information from various sources. LO10: Identify cyber threats through host, network, and log analysis. LO11: Develop an incident response plan. LO12: Utilize cyber incident response tools proficiently.
Responsibility and Autonomy	LO13: Apply incident response steps effectively. LO14: Adopt a dynamic approach to the incident response process. LO15: Use indicators of compromise for effective breach response in Windows environments. LO16: Assess and manage technical vulnerabilities. LO17: Measure the effectiveness of cybersecurity incident detection and response. LO18: Evaluate the resilience of cybersecurity controls and mitigation actions following incidents.

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

The residential course is held over 5 days.

Main Topic	Suggested Residential Working Hours + (Hours required for individual learning, E-Learning etc)	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 (included SOC services automation, UEBA, AI based tools)
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 (ex. MITRE ATT&CK, Lockheed Martin Cyber Kill Chain) • 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)**	

Material

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:

- *AKU 1 – History and context of the CSDP*
- *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)

Methodology

The course is based on the following methodology: lectures, panels, workshops, exercises and/or case studies

Additional information

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".