



European Security and Defence College (ESDC)

“Cyber Range – defensive capabilities”

(22-23/212/1)

DRAFT PROGRAMME

27 September – 29 September 2022 – Residential form

**Cyber Security Training Centre of Excellence
Warsaw, Poland
(Eksperckie Centrum Szkolenia Cyberbezpieczeństwa, Warszawa, Polska)**

Course Venue:

ul. gen. Sylwestra Kaliskiego 2
00-908 Warszawa 46

Director of CST CoE

Mr. Paweł DZIUBA

Course Director

COL Michał Majewski

DAY 1	Tuesday, 27 September 2022 (CEST)
08:30 – 09:00	<i>Registration</i> <i>Welcome coffee</i>
09:00 – 09:45	Course opening <ul style="list-style-type: none"> • Short presentation of CST CoE • Short presentation the European Security and Defence College (ESDC) and the Cyber ETEE Platform, Brussels
09:45 – 10:00	Welcome session – introduction of instructors and participants <i>Informal Tour-de-Table</i>
10:00 – 10:10	Introduction to the course – presentation of the course objectives. Brief overview of the competence of the team of specialists at CST CoE responsible for Cyber Range training, who organise advanced training and games
	SESSION 1 Overview of the CST CoE's CyberRANGE platform and its potential use.
10:10 – 10:45	<ul style="list-style-type: none"> • <i>Presentation</i>
10:45 – 11:00	<i>Coffee break</i>
	SESSION 2 Presentation of the technical aspects of the CyberRange platform design. Possibilities of using the CYBER RANGE tool for organising training for participants in various locations.
11:00 – 12:15	<ul style="list-style-type: none"> • <i>Demonstration</i>
12:15 – 13:30	<i>Lunch break</i>
	SESSION 3 Activities in the cyberspace domain in the escalation phase and during the conflict in Ukraine.
13:30 – 14:30	<ul style="list-style-type: none"> • <i>Presentation</i>
	SESSION 4 Case study. Groupwork.
14:30 – 15:30	<ul style="list-style-type: none"> • <i>Seminar</i>
15:30 – 15:45	Group photo
15:45 – 15:55	<i>Summary</i>

DAY 2	<u>Wednesday, 28 September 2022 (CEST)</u>
08:30 – 09:00	<i>Welcome coffee</i>
09:00 – 09:15	Introduction to the workshop, discussion of the concept and delivery
	SESSION 5 Kill Chain - explanation of the problem.
09:15 – 09:45	<ul style="list-style-type: none"> <i>Presentation</i>
09:45 – 11:30	SESSION 6 Presentation of the scenario prepared for the workshop. Background - embedding the discussed topics in reality, activities and techniques, discussion on the basis of the operation of APT groups.
	<ul style="list-style-type: none"> <i>Demonstration, Presentation</i>
11:30 – 11:45	<i>Coffee break</i>
	SESSION 7 Environment - presentation and description of the environment virtualised in CyberRange in which the workshop will be conducted.
11:45 – 12:15	<ul style="list-style-type: none"> <i>Demonstration</i>
12:15 – 13:30	<i>Lunch break</i>
	SESSION 8 Workshop - conducting a scenario, discussing the next steps and the steps performed by the attacker.
13:30 – 14:30	<ul style="list-style-type: none"> <i>Demonstration</i>
	SESSION 9 Mapping of selected techniques onto the MITRE ATT&CK matrix and discussion of mitigants.
14:30 – 15:30	<ul style="list-style-type: none"> <i>Demonstration</i>
15:30 – 15:40	<i>Summary</i>
15:40 – 16:00	<i>Questions and Answers</i>
19:30 – 21:00	<i>Icebreaker Dinner</i>

DAY 3	Thursday, 29 September 2022 (CEST)
08:30 – 09:00	<i>Welcome coffee</i>
09:00 – 09:05	Introduction to the third day of the course
	SESSION 10 Computer fraud as the most frequently handled incidents (86%), including phishing (77% of total incidents)
09:05 – 10:00	<ul style="list-style-type: none"> <i>Presentation</i>
	SESSION 11 How criminals work - phishing - the practical part
10:00 – 11:00	<ul style="list-style-type: none"> <i>Demonstration</i>
11:00 – 11:15	<i>Coffee break</i>
	SESSION 12 Presenting the course " <i>Pentester Tools - Basic Course</i> "
11:15 – 11:45	<ul style="list-style-type: none"> <i>Presentation</i>
	SESSION 13 Presenting the course " <i>Cyber Range - Cybersecurity in practice</i> "
11:45 – 12:00	<ul style="list-style-type: none"> <i>Presentation</i>
12:00 – 13:15	<i>Lunch break</i>
	SESSION 14 Cyber Range - Effectiveness of raising digital competence digital competence of staff responsible for cyber security
13:15 – 14:00	<ul style="list-style-type: none"> <i>Seminar</i>
14:00 – 14:10	<i>Summary</i>
14:10 – 14:20	Certificate Ceremony
14:20 – 14:40	<i>Closing Remarks - End of the Course</i>