



UNIVERSITY OF
PUBLIC SERVICE
LUDOVIKA



Invitation to the **CYBER THREAT MANAGEMENT**

(ESDC Activity Number 24-25/264/1)

Budapest, Hungary, 7–10 October 2024

Under the auspices of the European Security and Defence College (ESDC), the Hungarian Ludovika University of Public Service (LUPS) and the Military Academy 'General Mihailo Apostolski' (MAGMA), in cooperation with the European Union Agency for Cybersecurity (ENISA), will run the Cyber Threat Management Course from Monday 7 to Thursday 10 October 2024, in Budapest.

Aligned with ESDC's Cyber ETEE platform, this course is specifically tailored for and offered to public sector employees from EU Member States, EU institutions, bodies and agencies, and is also open to public-sector employees from EU candidate countries who are responsible for and need to cover roles in cyber threat management.

The course aims to impart comprehensive knowledge of prevalent cyber threats and equip participants with the skills necessary to address contemporary and emerging cyber threats effectively. It will offer valuable insights into options available to security professionals for implementing and deploying efficient organisational and technical measures against the identified and analysed threats. Participants will gain a comprehensive understanding of each analysed threat, including its potential impact on organisational assets, exploitable vulnerabilities, and, most importantly, security measures that can be deployed to confront and mitigate the associated risks.

The overall objective of this course is to acquire substantial knowledge so as to be able to describe cyber-attack stages and CTI management practices and to understand security measures. It aims to enhance technical knowledge in cybersecurity by familiarising participants with generic attack methods and techniques; to improve skills and abilities to outline main cyber-attacks, analyse cyber threats; and to provide guidelines and recommend best practices in analysing levels of vulnerabilities, identifying and prioritising security measures, attack surfaces and vectors related to threats.

The course is structured in two parts:

1. An asynchronous self-learning component, which provides an introduction to understanding, analysing and mitigating a ransomware attack. This part is mandatory and requires 4 hours of self-study, if the attendee is already working in the field of incident response or cyber threat management.

2. A classroom course, which will be held from 7 to 10 October 2024. It will focus on contemporary and emerging cyber-threats and the organisational and technical measures that can be taken against the threats analysed.

At the end of the course, participants will be able to outline main cyber threats, participate in CTI tasks, effectively address security measures, and develop and implement best practices. They will also gain the capability to propose organisational and technical security measures and establish action plans within an organisation.

On behalf of the Hungarian Ludovika University of Public Service (LUPS) and the Military Academy 'General Mihailo Apostolski' (MAGMA) of the Republic of North Macedonia and European Union Agency for Cybersecurity (ENISA), we are pleased to invite you to nominate suitable participants for this ESDC course, which is an excellent opportunity to gain in-depth knowledge of major cyber threats and prepare to confront contemporary and emerging cyber-threats effectively.

Yours faithfully,



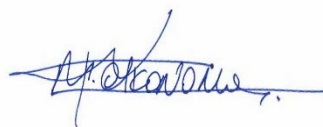
**Dóra
MOLNÁR**

Vice Director of
Cybersecurity Institute
Ludovika University of
Public Service
(LUPS)



**Prof Dr Mitko
BOGDANOSKI**

Dean
Military Academy
'General Mihailo
Apostolski'
(MAGMA)



**Dr. Demosthenes
IKONOMOU**

Head of Capacity
Building Unit
European Union
Agency for
Cybersecurity
(ENISA)



**Fergal
O' REGAN**

Acting Head
European Security and
Defence College
(ESDC)

Annexes:

- A – Course administrative instructions
- B – Tentative course agenda



UNIVERSITY OF
PUBLIC SERVICE
LUDOVIKA



Invitation to the **CYBER THREAT MANAGEMENT**

(ESDC Activity Number 24-25/264/1)

Budapest, Hungary, 7–10 October 2024

Annex A

Course administrative instructions

- **Target audience:** As part of ESDC's Cyber ETEE platform, this course is offered to public employees from EU Member States and EU institutions and also from the Candidate Countries who need to fulfil roles in cyber threat management.
- **Seats and nominations:** A maximum of 28 participants.
- **Application and deadline:** **The course is offered free of charge.** Applications should be submitted by designated nominators using the ESDC ENLIST Platform <https://esdc.europa.eu/enlist/login>, no later than 10 September 2024. A list with the relevant ENLIST nominators can be retrieved from the ESDC website at <https://esdc.europa.eu/nominators/>. **Late registration:** Subject to availability of seats, the course is open for late registration. Please contact the course administration: Ms Anna MALEC (ESDC Training Manager, Anna.MALEC@eeas.europa.eu) or the Course Directors, Ms Dora MOLNAR (Molnar.Dora@uni-nke.hu) or Goce STEVANOSKI (goce.stevanoski@ugd.edu.mk).
- **Registration will not be final until confirmed by the ESDC Secretariat.** Please do not book flights and accommodation before receiving confirmation.
- **Selection of participants** will be based on applicant backgrounds, experience, suitability, gender balance and country of origin. The decision on which applications are accepted remains solely with the Training Institutions and the ESDC Secretariat. When the participant list is finalised, the course administration will contact the selected participants and provide more detailed information about the course and logistics.
- **Mandatory e-learning and attendance:** The course consists of an e-learning preparatory phase, (online) to be completed using the ESDC e-Learning platform ILIAS, and a residential activity in Budapest (Hungary); both parts are compulsory. For the first part (i.e. the online modules), the ESDC will provide the relevant links to the selected participants. Participants must complete these online e-learning modules before the start of the residential part. The participants' attendance during the residential course in Budapest is mandatory on all days. A certificate will be awarded, on the last day, to those course participants who have completed both the e-learning phase and the residential course.
- **Course venue (location):** The course will be held mainly in the premises of the Hungarian Ludovika University of Public Service (2 Ludovika tér, H-1083 Budapest).
- **Language:** The working language is English, without translation.
- **Course (tuition) fees:** The course has no registration or tuition fees.

- **Travel expenses, transfers, accommodation, meals and catering:** Participants should arrange their own travel and accommodation. All costs for travelling to/from Hungary, accommodation, catering and meals (including breakfast), daily allowances, transfers and local transport must be covered by the participants or by their sending authorities.

Hotel reservations: There are numerous hotels in the Budapest area, and participants are responsible for their own arrangements.

Participants should not make booking arrangements before receiving the confirmatory message on their complete course registration.

- **Liabilities, medical and life insurance:** In the event of medical emergencies or accidents, the costs will be covered directly by the health, life and accident insurance provided by the participants' sending countries, national authorities or organisations. The organiser does not provide health, life or accident insurance for participants at the event or during their stay in Hungary.
- **Dress code:** As far as the dress code is concerned, we recommend that participants wear business attire (or a dress) for the opening event and closing ceremony. Members of the armed forces, gendarmerie and police are not required to wear their uniforms. During the course, a networking social dinner will be offered to all course participants, experts and trainers. For this specific event, as well as course classes and field visits, comfortable business/smart casual attire will be appropriate.
- **Additional info:** The Critical Entities Resilience Advanced Course standard curriculum can be consulted on the ESDC website at <https://esdc.europa.eu/curricula/>.
- **Arrival/Departure:** Participants are invited to arrive in Budapest on Sunday 6 October 2024. The course will start around 08:00 on Monday 7 October 2024 and will finish around 13:00 on Thursday 10 October 2024.
- **Diversity and inclusion:** The ESDC is committed to an inclusive, gender-sensitive and discrimination-free environment. We do not and will not discriminate on the basis of race, colour, religion, gender, gender expression, age, national origin, disability, marital status, or sexual orientation in any of our activities or operations. Only in an inclusive environment can all people, and therefore the ESDC and its partners, realise their true potential. We therefore particularly encourage applicants from groups likely to be underrepresented to apply. The ESDC and the Training Institutions will not tolerate any conduct that violates these values.
- The final course agenda will be distributed to all selected participants. Nevertheless, for matters regarding the course programme and planned activities, please do not hesitate to contact the Course Director, Dóra MOLNÁR.
- **Additional information:** *Cybersecurity Risk Management (14-17 October)* versus *Cyber Threat Management (7-10 October)*. Both training activities are organised by LUPS under the auspices of the ESDC. These are two different training offers.

For more information about the classroom course and its structure, please contact the course directors, Dóra Molnár (Vice-Director, Institute of Cybersecurity, Ludovika University of Public Service, molnar.dora@uni-nke.hu) and Anna Molnár (Head of International Security Policy Department, molnar.anna@uni-nke.hu).

For more information about the e-learning material, please contact Fabio Di Franco, Cybersecurity Officer, ENISA (Fabio.DiFranco@enisa.europa.eu).



UNIVERSITY OF
PUBLIC SERVICE
LUDOVIKA



Invitation to the

CYBER THREAT MANAGEMENT course

(ESDC Activity Number 24-25/264/1)

Budapest, Hungary, 7–10 October 2024

Annex B

Tentative course agenda

The course is structured in two parts:

PART I: AN ASYNCHRONOUS SELF- LEARNING PART, which provides an introduction on **understanding, analysing & mitigating a ransomware attack**. This part is supported by the European Union Agency for Cybersecurity (ENISA). It is mandatory and requires 4 hours of self-study, if the attendee is already working in the field of incident response or cyber threat management.

The asynchronous self-learning is divided further into two parts:

- i. An eLearning segment presents how a ransomware incident happens and how to analyse it and identify mitigation measures in systematic way. The e-learning module is a storyline, which is based on a cyber-attack that uses Emotet malware. It consists of 4 modules and starts with one of our story's heroes, a government agency employee, being the victim of a ransomware attack. What follows is an analysis of the stages of the cyber-attack that took place against the government agency, using the Cyber Kill Chain Framework, and a presentation of all the appropriate technical countermeasures that the government agency could take to protect itself from such cyber-attacks.
- ii. A report with 3 case studies presents a mapping of MITRE ATT&CK's techniques as used in the three attack scenarios, to the Cyber Kill Chain methodology.

At the end of the asynchronous eLearning, the trainee must go through a short assessment and complete it successfully in order to be admitted to the classroom course.

PART II: A CLASSROOM COURSE, which will be held at the Ludovika University of Public Service (2 Ludovika Tér, H-1083 Budapest) from 7 to 10 October 2024. The course will take a blending approach, mixing online lectures and exercises, and so facilitate achieving the learning objectives. It will focus on contemporary and emerging cyber-threats and the organisational and technical measures that can be taken against the threats analysed. The scheduled activities and related topics are indicated below in the table:



UNIVERSITY OF
PUBLIC SERVICE
LUDOVIKA



TIME	DAY 1 (7 OCTOBER 2024) LOCATION: JOHN LUKACS HALL (SIDE BUILDING)
8:15 – 08:30	<i>Registration</i>
8:30 - 9:00	Opening ceremony Dr László Kovács, Vice-Rector for Academic Affairs (UPS Ludovika) Goce Stevanoski (Military Academy 'General Mihailo Apostolski')
9:00 – 11.15	The Cyber Threat Landscape. Introduction to vulnerabilities. tbd
11:15 – 11:30	Coffee break
11.30 – 13.00	Analysis of major threats and cyber security incidents Lecturer: Kire Jakimovski (Military Academy 'General Mihailo Apostolski')
13:00 – 14:00	Lunch
14:00 – 15:30	Analysis of major threats and cyber security incidents Lecturer: Kire Jakimovski (Military Academy 'General Mihailo Apostolski')
15:30-15:45	Coffee break
15:45 – 17:00	Web-based attacks: Capital One, phishing – Ukrainian power grid and Western Balkan case studies Lecturer: Goce Stevanoski (Military Academy 'General Mihailo Apostolski')
TIME	DAY 2 (8 OCTOBER 2024) LOCATION: INFORMATION LAB (EDUCATION BUILDING)
08:30 – 10:45	Cyber exercise (analysing an attack related to a specific threat) Lecturer: Sándor Magyar (LUPS)
10:45 – 11:00	Coffee break
11:00 – 12:30	Cyber exercise (analysing an attack related to a specific threat) Lecturer: Sándor Magyar (LUPS)
12:30 – 13:30	Lunch
13:30 – 15:45	Cyber threat information, CTI formats and sources, sharing with CERTs Location: John Lukacs hall (Side Building) Lecturer: Mádi-Nátor Anett (CYEX)
17.00 – 19.00	Guided tour of the Castle of Buda Ibolya Horváthné Szalóczy



**UNIVERSITY OF
PUBLIC SERVICE**
LUDOVIKA



TIME	DAY 3 (9 OCTOBER 2024) LOCATION: JOHN LUKACS HALL (SIDE BUILDING)
08:30 – 10:00	Analysis of technical controls used to counteract cyber threats I Lecturer: Csaba Krasznay (LUPS)
10:00 – 10:15	Coffee break
10:15 – 11:45	Analysis of technical controls used to counteract cyber threats II Lecturer: Csaba Krasznay (LUPS)
12:00 – 13:00	Lunch
13:00 – 13:30	Visit of the Ludovika Museum
13:30 – 16:45	Cyber exercise (analysing an attack related to a specific threat) Location: Information lab (Education building) Lecturer: András Szabó (LUPS)

TIME	DAY 4 (10 OCTOBER 2024) LOCATION: INFORMATION LAB (EDUCATION BUILDING)
08:30 – 10:00	Cyber exercise (analysing an attack related to a specific threat) Lecturer: András Szabó (LUPS)
10:00 – 10:15	Coffee break
10:15 – 11:45	Cyber exercise (security measures for the attack analysed; prioritising proposed measures) Lecturer: András Szabó (LUPS)
12:00 – 13:30	Certificate ceremony - closing remarks (ESDC) TBD (LUPS)
12:30 – 13:30	Lunch



UNIVERSITY OF
PUBLIC SERVICE
LUDOVIKA



LEARNING OUTCOMES	
Knowledge	<ul style="list-style-type: none"> Describe top cyber threats organisations face today. Define generic attack methods and techniques. Describe cyber-attack stages related to a threat. Understand security measures. Define the importance of organisational and technical security measures. Describe cyber threat intelligence management practices.
Skills	<ul style="list-style-type: none"> Outline main cyber threats. Analyse a cyber threat. Apply MITRE ATT@CK and Cyber Kill Chain frameworks.
Competences	<ul style="list-style-type: none"> Analyse the importance of vulnerabilities. Propose the use of specific security measures. Identify, and prioritise security measures. Identify attack surfaces and vectors related to a threat. Describe security measures contributions against threats.

The main profile of this course, according to the **European Cybersecurity Skills Framework (ESCF)**, is the Cyber Threat Intelligence Specialist. Other ESCF roles like Cybersecurity Architect, Cyber Incident Responder, Cybersecurity Researcher and Chief Information Security Officer (CISO) can also benefit from this course.