ACTIVITY UNDER THE CYBER ETEE PLATFORM

COURSE ON CYBER THREAT MANAGEMENT

INVITATION & AGENDA

DATE 13 – 15 OCTOBER, 2021

LOCATION PALACE OF PARLIAMENT - BUCHAREST INTERNATIONAL CONFERENCE CENTRE (ROMANIA)

INFORMATION ABOUT THE COURSE

Under the auspices of the European Security and Defence College (ESDC), ENISA has the honour of organising a blended course dedicated to Cyber Threat Management.

As part of ESDC's Cyber ETEE platform, this course is offered to 15 public employees from EU Member States and EU institutions working in CSIRTs or SOCs, which want to enrich their methodological and tactical skills on how to analyse threats and incidents and how to defend from it.

The course is structured in 2 parts:

1. An asynchronous eLearning part and a complementary report provide an analysis of malware-based cyber-attacks, look at the associated threats and the measures needed to confront it. This part is mandatory and requires at least 5 hours of self-study for trainees that fulfil the course's prerequisites (Page 5). An assessment on the knowledge acquired during this phase, must be successfully completed to be admitted to the second part of the course.
2. A three-day residential course which will be held in Bucharest's International Conference Centre on the 13-15 of October 2021 will focus on putting into practise cyber threat management aspects and controls.

The main objective of the course is to provide participants an in-depth knowledge on top cyber threats and prepare them to efficiently confront contemporary and emerging threats by providing insights on the options they have in deploying efficient organizational and technical countermeasures.

The participants will also gain significant knowledge on regulatory and technical aspects of cyber threat information lifecycle and sharing and will indulge in the analysis of cyber-security incidents utilizing existing de facto cyber-attack methodologies and details of cyber threats that advanced groups utilize.

The course is offered free of charge. The nomination of the suitable candidates for attending the course should be done via the ENLIST registration system of the ESDC by the designated EU ENLIST Nominators. A

ACTIVITY UNDER THE CYBER ETEE PLATFORM

COURSE ON CYBER THREAT MANAGEMENT

list with relevant ENLIST nominators can be retrieved from the ESDC website at https://esdc.europa.eu/nominators/.

Deadline for registration is **13th September 2021** and will not be final until confirmed by the ESDC Secretariat.

For more information about the course structure, please contact Dr. Fabio Di Franco - Fabio.difranco@enisa.europa.eu

ASYNCHRONOUS ELEARNING AND COMPLEMENTARY MATERIAL

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 heroes, a Government Agency's 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 countermeasures that the Government Agency could take to protect itself from such cyber-attacks.

E-LEARNING MODULES	DESCRIPTION
1. Character Introduction	This section introduces the characters of the story as well as their roles and responsibilities regarding information security in the Government Agency.
2. Ransomware Experience	This section presents an information security incident that will occur in the agency.
3. Analysis of Attack	This section describes in detail all the stages of the cyber-attack against the agency, utilising the Cyber Kill Chain Framework
4. Mitigation Measures	This section presents all the appropriate countermeasures that the agency can take to protect itself from such cyber-attacks.

A complementary report will provide an analysis of three reported and well-studied cyber attacks, using the Lockheed Martin's Cyber Kill Chain methodology. It will help the trainees to consolidate the knowledge and prepare for the mandatory assessment.

At the end of his phase, the trainee must go through a short assessment and complete it successfully in order to be admitted to the residential course.

3-DAY RESIDENTIAL COURSE

The residential course is scheduled for the 13th to 15th of October 2021. The course will follow a blended approach, mixing lectures and an extended table-top exercise to achieve the learning objectives.

Half of the residential course is devoted to the table-top cyber exercise which gives the trainees the opportunity to learn from peers, put into practise the knowledge gained in the first phase of the course and during the morning's lectures. In particular,

ACTIVITY UNDER THE CYBER ETEE PLATFORM

COURSE ON CYBER THREAT MANAGEMENT

the trainees will experience on cyber threats, acquire skills on analyzing threats and the role these play in a cybersecurity incident, and apply MITRE ATT&CK and Cyber Kill Chain frameworks.

The scheduled activities and the related topics are indicated below.

DAY 1: WEDNESDAY, 13 OCTOBER 2021	
9.00 – 9.30	Introduction to the course and Ice breaking session
9.30 – 18.00	The Threat Landscape • Tactics and Techniques, • Attack frameworks (MITRE ATT&CK and Cyber Kill Chain), • ENISA Threat Landscape. • Threat Actors Vulnerabilities • Main categories of vulnerabilities, • NIST NVD (CVSS), • Vulnerabilities lifecycle Analysis of major threats • Malware, • Web-based attacks, • Phishing Cybersecurity incidents • Analysis of the first stages of an attack Cyber exercise • First-day run of the cyber-exercise - Analysis of a cyber incident
DAY 2: THURSDAY, 14 OCTOBER 2021	
9.00 – 18.00	Cyber security frameworks • NIST CSF, CIS Controls, ENISA NCAF Technical Security Controls • Analysis of technical controls used to counteract cyber threats Cyber security incidents • Analysis of the final stages of an attack Cyber exercise • Second-day run of the cyber-exercise – work on the final stages of the attack scenario
DAY 3: FRIDAY, 15 OCTOBER 2021	
9.00- 16.00	Technical Security Controls • Analysis of further technical controls used to counteract cyber threats Cyber Threat Intelligence Management • CTI collection, intelligence and sharing units • Regulatory framework • CTI sharing challenges Cyber exercise • Third-day run of the cyber-exercise (use of analysed controls for the first two days' attack scenario) Final Discussion

ACTIVITY UNDER THE CYBER ETEE PLATFORM

COURSE ON CYBER THREAT MANAGEMENT

MEET THE TRAINERS

Kostas Papadatos (Cyber Noesis) is an Information Security Executive and Entrepreneur with over twenty years of experience in a multitude of cross-functional roles, including the establishment and fostering of a successful Information Security enterprise. Extensive executive background combined with strong information security expertise (in both management & technical areas) and cross-industry exposure (in sectors like financial, telecoms, manufacturing, lottery, healthcare, transportation, retail, government, army etc.).He holds an MSc in Information Security from Royal Holloway (University of London) and a number of industry certifications including CISSP-ISSMP, CISM, ISO 27001 Lead Auditor, ISO 27005 Risk Manager, Certified DPO, PMP and MBCI.

Konstantinos Rantos is an Associate Professor at the Computer Science Department and Director of the Web Services and Information Security Lab at the International Hellenic University. In the past, he held information security positions in the private and public sector. He participated in many national as well as research and development projects under EU ACTS, CIP LSPs, ARTEMIS JU, FP7, and H2020 programmes. He has been a representative of Greece in European working groups on issues of authentication, digital signatures and e-government. He has more than 50 publications in journals, books and international conferences, and acts as a reviewer to a number of conferences and scientific journals. His research interests are in the areas of cybersecurity, Internet of Things security, authentication systems, and privacy.

Fabio Di Franco (ENISA) is currently leading the activities in ENISA on cyber skills and cyber education. He is also responsible for developing and delivering trainings to EU member states and EU institutions on information security management and IT security. He also advises the European Union and the Member States on research needs in cybersecurity with a view to enabling effective responses to the current and emerging threats. Fabio has a PhD in telecommunication engineering and is a Certified Information Systems Security Professional (CISSP).

Athanasios Vasileios Grammatopoulos (ENISA) has a joined B.Sc. and M.Sc. degree in Electrical and Computer Engineering from Technical University of Crete, Greece (2018). He is completing a M.Sc. in Digital Systems Security and works as a Cybersecurity Operational Assistant at ENISA. He has experience with web technologies and web applications.

ACTIVITY UNDER THE CYBER ETEE PLATFORM

COURSE ON CYBER THREAT MANAGEMENT

LEARNING OUTCOMES & PREREQUISITE

Knowledge	K1.	Describe top cyber threats organizations face today
	K2.	Define generic attack methods and techniques
	K3.	Describe cyber-attack stages related to a threat
	K4.	Understand security measures
	K5.	Define the importance of organizational and technical security measures
	K6.	Describe cyber threat intelligence management practices
Skills	S1.	Outline main cyber threats
	S2.	Analyse a cyber-threat
	S3.	Apply MITRE ATT&CK and Cyber Kill Chain frameworks.
Competences	C1.	Analyze the importance of vulnerabilities
	C2.	Propose the use of specific security measures
	C3.	Identify, and prioritize security measures
	C4.	Identify attack surfaces and vectors related to a threat
	C5.	Describe security measures contributions against threats

Prerequisite	P1. English: Common European Framework of Reference for Languages (CEFR) Level B2 P2. A master degree in cybersecurity or related topic followed by at least 3 years' experience in IT Security at technical and tactical level