DESCRIPTION OF THE COURSE

Technology is at the core of our daily life and, in this vein, cyberattacks are on the rise. In this regard, cybersecurity knowledge is essential to protect our assets.

With this 22 hours online free course you will:

- learn the main concepts of cybersecurity.

- how information and network can be protected.

- advanced ways to protect information and network, as well as some cyberattack techniques and legal issues.

Pre-requisites: Computer basics

You can sign up for one or more modules for free. Upon completion, you will get an achievement certificate.

This programme is focused on:

- Professionals working in Defence and AeroSpace Industry (up-skilling and re-skilling activities) and
- Engineering Degree/Master student

IMPORTANT: This prototyped programme is **EXCLUSIVE FOR** partners of the **ASSETs+ consortium** and **associated stakeholders.**

If you want to join the ASSETs+ Stakeholders Group and become part of our ecosystem, please, **click here**.

General information

- **Format: Online**

- **Language: English**

- **EQF level:** 5

- **Instructor: Lorena González, Rafael Estepa, Antonio Estepa, José M. De Fuentes**

- **Hours: 6**

- **Host institution: Universidad de Sevilla, Universidad Carlos III de Madrid**

Programme schedule: Module 1 CYBERSECURITY BASICS

21 /feb/2023 16:30 – 18:30	Introduction to cybersecurity: the need for cybersecurity -Main threats (interception, modification...) and Malware types in the defense sector
22 /feb/2023 16:30 – 18:30	Network security basics: TCP/IP stack, MAC address, IP address, DNS
23 /feb/2023 16:30 – 18:30	Good Practices and Main countermeasures: Encryption and secure passwords, the need of antivirus/Endpoint security, the importance of backups

General information

- **Format: Online**

- **Language: English**

- **EQF level:** 6

- **Instructor: Lorena González, Rafael Estepa, Antonio Estepa, José M. De Fuentes**

- **Hours: 8 (1 ECTS)**

- **Host institution: Universidad de Sevilla, Universidad Carlos III de Madrid**

Programme schedule: Module 2 TECHNICAL FOUNDATIONS OF CYBERSECURITY

27 / Feb/2023 16:30 – 18:30	Data Protection I (Cryptography basics, Public Key Infrastructure, Access control, Providing integrity)
28 / Feb/2023 16:30 – 18:30	Data Protection II (Cryptography basics, Public Key Infrastructure, Access control, Providing integrity)
1 / March /2023 16:30 – 18:30	Network protection Basics: Firewalls, DMZ, Subnet protection
2 / March /2023 16:30 – 18:30	Network Protection Tools (Secure Networking/auditing, IDS/IPS, …)

General information

- **Format: Online**

- **Language: English**

- **EQF level:** 5

- **Instructor: Lorena González, Rafael Estepa, Antonio Estepa, José M. De Fuentes**

- **Hours: 8** (1 ECTS)

- **Host institution: Universidad de Sevilla, Universidad Carlos III de Madrid**

Programme schedule: Module 3 ADVANCED CYBERSECURITY

6 /March/2023 16:30 – 18:30	Advanced crypto + Cyber threat intelligence and information sharing
7 /March/2023 16:30 – 18:30	Cyberattack techniques and defences (Main attacks, Pentesting)
8 /March/2023 16:30 – 18:30	Advanced network security
9 /March/2023 16:30 – 18:30	Regulation, management and guidelines

Learning outcomes:

Module 1- Cybersecurity basics: Use access control software, Identify data supporting strategies, Collect data from cyberdefense resources, Secure network communications

Module 2- Technical foundations of cybersecurity: Identify data supporting strategies, Secure network communications, Use of event correlation tools, Use access control software, Identify data supporting strategies

Module 3- Advanced cybersecurity: Collect data from cyberdefense resources Identify data supporting strategies, Identify vulnerabilities of a cyber infrastructure Secure network communications, Use of event correlation tools, Identify data , supporting strategies, Risk management

More information & registrations:
http://waine.us.es/assets

www.assets-plus.eu

The European Commission's support for the production of this publication does not constitute an endorsement of the contents, which reflect the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.