€TRAINING

Cyber Security

20 - 24 May 2024
London (UK)
Landmark Office Space

Cyber Security

REF: B2488 DATE: 20 - 24 May 2024 Venue: London (UK) - Landmark Office Space Fee: 5850 Euro

Introduction:

Cybersecurity is extremely important because it helps protect critical information systems in countries. Cybersecurity is also important for safeguarding the security of vital facilities and important information within countries. Additionally, it is important for protecting the security of important state institutions, such as government offices and military bases, as well as securing important systems within significant companies and other organizations.

Program Objectives:

At the end of this program, the participants will be able to:

- Understand the fundamentals of cybersecurity and the surrounding threats and how to deal with them.
- Understand international and national mechanisms for cybersecurity protection.
- Understand cyber attacks, how they are carried out, and the strengths and weaknesses of information systems.
- Understand ransomware attacks and how to handle them.
- Analyze famous cyber attacks and their consequences.

Targeted Audience:

- Police officers working in criminal investigation and information analysis.
- Public prosecutors and judges.
- Government and private sector employees.
- Information security officers in the police and military sectors.
- Security officers in institutions and companies.

Program Outlines:

Unit 1:

Definition of cybersecurity, its aspects, and legal protection:

- Concept of cybersecurity.
- Basic elements of cybersecurity.
- Legal aspects of cybersecurity protection.

Unit 2:

Cybersecurity rules in institutions:

- Technical assets for dealing with information systems in institutions.
- Cybersecurity threats in industrial and vital institutions.
- Cyber wars and attacks targeting information systems.
- Safe use rules for information systems in institutions.

Unit 3:

Analytical study of famous cyber attacks:

- Analytical study of the Aramco cyber attacks.
- Analytical study of the Estonia cyber attacks and their aftermath.
- Analytical study of various attacks worldwide.
- Analysis of the most important statistical sites for cyber attacks.

Unit 4:

Ransomware attacks and how they work and strategies for dealing with them:

- Definition of ransomware.
- Mechanism of ransomware and the objectives of the attacks committed by it.
- Most famous ransomware attacks and their consequences.
- How to deal with and prevent attacks.

Unit 5:

International and national efforts to protect cybersecurity:

- International protection of cybersecurity and regulation of cyber warfare rules by the Tallinn Manual for Cybersecurity.
- Role of the International Telecommunication Union in assessing cyber readiness to deal with cyber attacks.
- Interpol's efforts in protecting cybersecurity.