

Knowledge of Cyber Security technologies

This course will provide you with a good understanding and perception of cybersecurity, and knowledge of security technologies related to the network architecture.

Who would benefit:

This course is designed for ICT engineers

Content :

1. Cyber Security Evolution and Basic Concepts

2. Cybersecurity History
3. What is Cyber Security?
4. Software Vulnerability
5. Security Intelligence

2. Most Common Network Threats

- 1) Brute-force
- 2) DoS and DDoS
- 3) Botnet
- 4) Fishing and Social Engineering
- 5) Ransomware
- 6) Data Breach
- 7) "National Team"

3. Main Means of Protection

- 1) Best Practices for Individuals and Businesses
- 2) IPDRR Cybersecurity Framework
- 3) Security Tools

4. Network Architecture and Security

- 1) Basics of Network Protocol Models
- 2) Firewall Isolation and Filtering
- 3) VPN and Tunneling
- 4) Network Traffic Identification

5. Cryptography and PKI

- 1) What is Cryptography?
- 2) Cryptographic Algorithms and Keys
- 3) Symmetric Key Algorithms
- 4) Digital Certificate and PKI
- 5) Cryptographic Protocol

6. Identity and Access Management (IAM) Technology

- 1) Definition of IAM
- 2) Definition of Account Management
- 3) Authentication Factors and Method of Selection
- 4) Authorization Principle and Access Control

7. Security Detection and Response Technology

- 1) Basic Principles of Security Detection and Response
- 2) DoS Attack and Detection
- 3) Security Vulnerability and Intrusion Detection
- 4) Application of Security Detection and Response Technology