Course code
50155/60155/70155

DV PLAN
C5i INTEGRATED SYSTEMS

Course From Zero to Hero

40 hours, 5 frontal sessions | 40 hours, 10 online sessions
40 hours, 9 hybrid sessions.

About the course

The profession of cybersecurity and information security is rapidly evolving due to the increasing number of hacking attempts, sophisticated hacking methods used by hackers, and the significant damage caused to organizations due to cyber threats, ransomware, scams, and other information security issues. The course was designed systematically and in accordance with the latest technologies in the fields of cyber, information security, communication, and computers, and tailored to the requirements of leading high-tech companies and organizations.

Course Objectives

Our leading and comprehensive Cyber course, where you will learn how to protect the organization by creating rules, defining different security profiles in all layers, from DNS to applications. You will learn how to configure IPS signatures to defend against anomalies and weaknesses in the organization, cope with denial-of-service attacks, data exfiltration, and advanced viruses. You will also learn advanced routing techniques, create Vdoms, define proxy servers, and create complete backups according to

target audience

The course is intended for anyone with an affinity for the world of technology who is interested in entering the field of information security and cybersecurity

Course code
50155/60155/70155

DV PLAN
C5i INTEGRATED SYSTEMS

Pre-requisites

Completion a course - Introduction to Cyber and Information Security.

Course content

First part

a) Understanding FW architecture
b) Installing FortiOS operating system on a virtual machine (VM)
c) Familiarity with protocols, sessions, and ports
d) Familiarity with the CLI
e) Basic settings
f) Administration, Backup
g) Interfaces - understanding and configuring different services (such as DHCP)
h) Routing and configurations
i) Policy configuration
j) Security profiles.

Second part

a) Remote work - IPSEC, SSL VPN
b) Routing
c) Vdoms

Third part

a) Familiarity with SD-WAN
b) Proxy mode configuration
c) Setting ports as layer2 devices
d) Introduction to Vlans
e) Working with HA (High Availability)

Fourth part

a) Diagnostics
b) Introduction to troubleshooting methodology in FortiGate
c) Diag commands
d) Logs
e) How to read logs
f) Deep analysis of logs
g) Structure and introduction to basic concepts
h) Forti Analyzer

Fifth part

a) Review of all the material we learned
b) Practice questions, and preparation for the exam
c) Familiarization with the new features of the operating system