



IT MANAGEMENT AND CYBER SECURITY

Certified Cyber Security Specialist

Course code: IMCS-006

SPARK TRAINING

Professional training courses for leaders, specialists, and organizations seeking practical capability development.

info@sparktraining.eu

+31 85 115 0004 | sparktraining.eu

— Workshop Overview

Cyber threats continue to grow in complexity, frequency, and business impact. Organizations need skilled professionals who can protect systems, manage risks, respond to incidents, and build strong security frameworks. This course provides participants with practical knowledge in cyber security fundamentals, risk management, secure architecture, threat intelligence, business continuity, and incident response to strengthen organizational resilience.

Why Attend

This course uses an interactive and practical approach through presentations, case studies, security scenarios, risk assessments, group discussions, practical exercises, and real workplace examples.

Who Should Attend

Cyber Security Professionals
IT Managers
Network Administrators
Risk and Compliance Staff
IT Support Personnel
Security Officers
Anyone seeking professional cyber security

— Learning Objectives

- Understand core cyber security principles and standards
- Identify and manage cyber risks effectively
- Strengthen asset protection and secure architecture practices
- Apply technical, physical, and administrative controls
- Build security awareness and training programs
- Use threat intelligence to improve preparedness
- Support business continuity and disaster recovery planning
- Respond effectively to cyber incidents and investigations

Course Outline

DAY
1

Fundamentals of Cyber Security

- Definitions
- Security concepts and definitions
- Cyber security standards
- Importance of cyber resilience
- Security roles and responsibilities
- Current cyber threat environment

DAY
2

Risk Management and Asset Protection

- Risk and threat landscape
- Risk assessment, evaluation and analysis
- Risk response
- Risk monitoring and reporting
- Asset management
- Endpoint security

DAY
3

Secure Architecture and Security Controls

- Creating a secure architecture
- Secure by design
- System development lifecycle
- Device configuration
- Overview of cryptography
- Technical controls
- Physical controls
- Administrative controls

DAY
4

Security Education and Threat Management

- Security Education, Training, and Awareness (SETA)
- Developing a security education, training and awareness program
- Developing and measuring against SETA metrics
- Threat management principles
- Cyber Threat Intelligence
- Open-Source Intelligence overview

DAY
5

Business Continuity and Incident Management

- Business impact analysis
- Business continuity planning
- Disaster recovery planning
- Incident management and incident response overview
- Incident handling life cycle
- Digital forensics principles
- Final workshop: Build a cyber resilience action plan

— Upcoming Classroom Dates

DATE	LOCATION	FEE
5 - 9 October 2026	Paris - France	€2,200
12 - 16 October 2026	Barcelona - Spain	€2,100
9 - 13 November 2026	Munich - Germany	€2,125
16 - 20 November 2026	Kuala Lumpur - Malaysia	€1,400
7 - 11 December 2026	Amsterdam - Netherlands	€2,100
14 - 18 December 2026	London - United Kingdom	€2,125
21 - 25 December 2026	Paris - France	€2,200
4 - 8 January 2027	Kuala Lumpur - Malaysia	€1,400

— Certificate and Registration

Participants who attend and complete the full programme receive a SPARK Training Certificate of Completion. For registration, in-house delivery, or availability questions, contact info@sparktraining.eu or +31 85 115 0004.