Certified Cyber Security Specialist (CCSS)

Meirc Training & Consulting | 65 +years

PLUS SPECIALTY TRAINING

Call us
+971 4 556 7171
800 7100 (within UAE)

Email us
meirc@meirc.com

Website
www.meirc.com

Why Attend

Participants on this Certified Cyber Security Specialist course will engage in an immersive learning experience that covers cybersecurity definitions, principles, practices, and industry standards. The aim of this course is to go beyond just theory, and equip participants with practical skills to tackle organizational risks effectively. This includes understanding asset security, using endpoint security, and learning about secure design principles and cryptography.

The course provides a holistic approach to security, in which participants will learn how to manage different types of controls (technical, physical, and managerial) to ensure their organizations are secure. Participants will gain skills in designing security programs, and will learn about to utilize cyber threat intelligence and Open-Source Intelligence (OSINT) to detect and respond to cyber threats. Participants will also gain insight and practice into business impact analysis, by creating plans for business continuity and disaster recovery, and will learn the basics of incident management, in order to handle cyber security incidents effectively.

Course Methodology

The course will include practical sessions, presentations, group work and demonstrations in order to enhance the learning experience.

Course Objectives

By the end of the course, participants will be able to:

- Apply skills for identifying, assessing, analyzing, responding to, and monitoring risks and threats within the organization, facilitating informed decision-making and proactive risk mitigation
- Master principles of asset security, including endpoint security, resilient architectures, secure design, SDLC practices, configuration management, and cryptography
- Implement a holistic security approach by deploying and managing technical, physical, and managerial controls to ensure a robust and comprehensive security posture
- Utilize knowledge and skills in leveraging cyber threat intelligence and Open-Source Intelligence (OSINT) for proactive identification, response, and mitigation of potential cyber threats
- Conduct business impact analyses, create business continuity plans, and craft disaster recovery plans to ensure effective organizational sustainability and recovery from disruptive incidents

Target Audience

This course is suitable for anyone already familiar and involved with IT / Cyber / Digital Security, and seeking to build on their fundamental principles of security. This includes, but is not limited to, IT professionals, security professionals, auditors, system administrators, general management, and anyone who is tasked with managing and protecting the integrity of the network/organizational infrastructure.

Target Competencies

- Information security management
- Development of IT policies and procedures
- Applications of cyber security solutions
- Threat Intelligence
- Incident management and response

Course Outline

- Fundamentals of Cyber Security
    - Definitions
    - Security concepts and definitions
    - Cyber security standards
- Risk Management
    - Risk and threat landscape
    - Risk assessment, evaluation and analysis
    - Risk response
    - Risk monitoring and reporting

- Asset Management
    - Endpoint security
    - Creating a secure architecture
    - Secure by design
    - System development lifecycle
    - Device configuration
    - Overview of cryptography
- Security Controls
    - Technical controls
    - Physical controls
    - Administrative controls
- Security Education, Training, and Awareness (SETA)
    - Developing a security education, training and awareness program
    - Developing and measuring against SETA metrics
- Threat Management
    - Cyber Threat Intelligence
    - Open-Source Intelligence overview
- Business Continuity and Disaster Recovery
    - Business impact analysis
    - Business continuity planning
    - Disaster recovery planning
- Incident Management
    - Incident management and incident response overview
    - Incident handling life cycle
    - Digital forensics principles

Meirc Professional Certificate (MPC)

MPC certified courses by Meirc Training & Consulting are designed for those willing to challenge themselves and go the extra distance. Participants who fully attend an MPC course and successfully complete the test on the last day, will receive a Meirc Professional Certificate (MPC), in addition to the one they receive for full attendance. MPC certificates are regionally recognized and can be quite valuable when applying for more senior roles within the organization or outside.

1st Floor, Building 13, Bay Square,
Business Bay P.O. Box 5883
Dubai, UAE

+971 4 556 7171

800 7100 (within UAE)

meirc@meirc.com

www.meirc.com

65 +years

Meirc Training & Consulting | 65 +years

CONNECT WITH US