INTRODUCTION TO CYBERSECURITY

COURSE OVERVIEW

This course is designed to introduce participants to the fundamentals of cybersecurity, equipping them with the essential knowledge and skills needed to protect information systems and networks from cyber threats. Participants will explore the core concepts of cybersecurity, network security, cryptography, threat detection and response, and security best practices. Through a combination of lectures, case studies, and hands-on labs, students will gain practical experience in implementing cybersecurity measures and understanding the latest security trends.

DATES, VENUES AND FEES

20 – 24 April 2025 – Dubai
05 – 09 October 2025 - Dubai
(5 Days)

Fees US$ 4500

Note: Fee is per participant + 5% VAT (if applicable).
Groups from the same company can enjoy a **discounted** price.

WHO SHOULD ATTEND?

This course is appropriate for a wide range of professionals but not limited to:

- Beginners in Cybersecurity
- IT Professionals
- Business and Organization Leaders
- Aspiring Security Analysts
- Students and Career Changers

CONTACT US NOW

+971 (4) 4539841 – 42 – 43
WhatsApp: +971 52 398 7781

Millennium Solutions Training Center FZ-LLC
First Floor, Office #134, Knowledge Park, Block 2B, Dubai, UAE
Email: info@mstcme.com
Website: www.mstcme.com

ACCREDITATION

This training course is certified by CPD.

The CPD Certification Service is the leading independent CPD accreditation institution operating across industry sectors to complement the Continuing Professional Development policies of professional institutes and academic bodies. The CPD Certification Service provides support, advice, and recognised independent CPD accreditation compatible with global CPD principles. CPD is the term used to describe the learning activities professionals engage in to develop and enhance their abilities and keep skills and knowledge up to date. CPD Units are only awarded to programmes after each programme is scrutinised to ensure integrity and quality according to CPD standards and benchmarks.

COURSE CERTIFICATE

MSTC certificate will be issued to all attendees completing a minimum of 80% of the total tuition hours of the course.

CPD internationally recognized certificate will be issued for all participants who will meet the course requirements.
CPD certificates will be issued within a month of the successful completion of the course.

TRAINING METHODOLOGY

- Expert instructor lecture, input using numerous visual aids
- Supportive comprehensive course manual enabling practical application and reinforcement
- Participant discussion and involvement regarding their specific projects and challenges
- Real-world case studies and best practices

LEARNING OBJECTIVES

By the end of this course, participants should be able to:

- Understand the key concepts of cybersecurity, including the CIA triad (Confidentiality, Integrity, Availability) and the different types of cyber threats.
- Identify and describe the various types of cyberattacks, including malware, phishing, and DoS/DDoS attacks.
- Understand basic networking concepts and apply network security techniques, such as firewalls, VPNs, and IDS/IPS.
- Understand cryptographic principles and methods for encrypting and securing data.
- Recognize the phases of a cyber attack and understand the role of threat detection systems, such as SIEM.
- Implement incident response strategies to handle security breaches effectively.
- Identify best practices for securing cloud environments, IoT devices, and applications.
- Explore emerging trends in cybersecurity, including AI, machine learning, and future challenges in the field.

CONTACT US NOW

+971 (4) 4539841 – 42 – 43
WhatsApp: +971 52 398 7781

Millennium Solutions Training Center FZ-LLC
First Floor, Office #134, Knowledge Park, Block 2B, Dubai, UAE
Email: info@mstcme.com
Website: www.mstcme.com

COURSE OUTLINE

DAY 1

Introduction to Cybersecurity and Basic Concepts

- **Understanding Cybersecurity**
  - What is cybersecurity?
  - Importance of cybersecurity in the modern world
  - Key principles of cybersecurity: Confidentiality, Integrity, and Availability (CIA Triad)
  - Types of cybersecurity threats (malware, phishing, DDoS, etc.)
  - Real-world examples of cyberattacks and their impact
- **Key Terminologies and Cybersecurity Frameworks**
  - Common cybersecurity terminology (e.g., vulnerabilities, exploits, attacks, etc.)
  - Introduction to cybersecurity frameworks and standards (NIST, ISO 27001, etc.)
  - Cybersecurity roles and responsibilities (CISO, Security Analyst, etc.)
- **Types of Cyberattacks**
  - Malware: Viruses, worms, trojans, ransomware, etc.
  - Phishing and social engineering attacks
  - Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS) attacks
  - Insider threats and their risks
- **Case Study and Discussion**
  - Review of a major cyberattack case study (e.g., WannaCry ransomware attack)
  - Group discussion on how these attacks could have been prevented

DAY 2

Network Security

- **Introduction to Networking and Network Security**
  - Basic networking concepts (IP addresses, DNS, routers, firewalls, etc.)
  - Importance of securing networks
  - Types of networks: Local Area Network (LAN), Wide Area Network (WAN), Virtual Private Network (VPN)
- **Network Security Devices and Tools**
  - Firewalls: Types (hardware, software) and configurations
  - Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS)
  - Network segmentation and its importance in security
  - Virtual Private Networks (VPNs) and secure tunneling protocols
- **Securing Network Communication**
  - Encryption protocols (SSL/TLS, HTTPS, etc.)
  - Public Key Infrastructure (PKI) and certificates
  - Network security best practices
- **Practical Hands-on Lab**
  - Setting up a basic firewall on a virtual machine
  - Using Wireshark to monitor network traffic
  - Introduction to VPN setup

DAY 3

Cryptography and Data Protection

- **Introduction to Cryptography**
  - What is cryptography and why is it important?
  - Basic concepts: Symmetric vs Asymmetric encryption
  - Common cryptographic algorithms (AES, RSA, SHA-256, etc.)
- **Key Management and Digital Signatures**
  - Importance of secure key management
  - Public Key Infrastructure (PKI)
  - Digital signatures and their role in ensuring integrity and authenticity
- **Data Protection Strategies**
  - Data at rest vs data in transit
  - Encryption methods to protect sensitive data
  - Data masking, tokenization, and hashing
- **Practical Hands-on Lab**
  - Encrypting and decrypting data using open-source tools
  - Generating and managing digital certificates
  - Using hashing algorithms to ensure data integrity

CONTACT US NOW

+971 (4) 4539841 – 42 – 43
WhatsApp: +971 52 398 7781

Millennium Solutions Training Center FZ-LLC
First Floor, Office #134, Knowledge Park, Block 2B, Dubai, UAE
Email: info@mstcme.com
Website: www.mstcme.com

COURSE OUTLINE

DAY 4

Threat Detection and Response

- **Cyber Threats and Attack Lifecycle**
  - The Cyber Kill Chain: Phases of an attack
  - Techniques used by attackers (reconnaissance, exploitation, installation, etc.)
  - Identifying and understanding threat intelligence
- **Security Information and Event Management (SIEM)**
  - Overview of SIEM systems and their role in cybersecurity
  - Common SIEM tools and technologies (Splunk, ELK Stack, etc.)
  - Collecting and analyzing logs for anomaly detection
- **Incident Response and Handling**
  - Phases of incident response: Preparation, Detection, Containment, Eradication, Recovery, Lessons Learned
  - Key roles in an incident response team
  - Creating an incident response plan
- **Practical Hands-on Lab**
  - Using a SIEM tool to detect network anomalies
  - Building a simple incident response plan
  - Simulating a security incident and responding to it

DAY 5

Security Best Practices and Future Trends

- **Best Practices in Cybersecurity**
  - Secure coding practices and application security
  - Password management: Strong passwords, multi-factor authentication (MFA)
  - Patching and vulnerability management
  - Regular security audits and penetration testing
- **Securing the Cloud and IoT**
  - Cloud security principles (e.g., AWS, Azure, Google Cloud)
  - IoT security challenges and considerations
  - Best practices for securing cloud and IoT environments
- **Future of Cybersecurity**
  - Emerging threats: AI and machine learning in cybersecurity, deepfakes
  - The role of automation and orchestration in cybersecurity
  - Cybersecurity career opportunities and growth areas
- **Final Review and Certification Preparation**
  - Recap of key concepts covered in the course
  - Discussion of resources for further learning (websites, books, certifications)
  - Q&A session and course feedback
- **Capstone Project or Quiz**
  - Option for a capstone project where students assess a hypothetical organization's cybersecurity posture and make recommendations
  - Alternatively, a final quiz covering the topics taught

CONTACT US NOW

+971 (4) 4539841 – 42 – 43
WhatsApp: +971 52 398 7781

Millennium Solutions Training Center FZ-LLC
First Floor, Office #134, Knowledge Park, Block 2B, Dubai, UAE
Email: info@mstcme.com
Website: www.mstcme.com