Tel No:+97126654546 | Fax No:+97126654182 | Email: training@cmc-me.com | www.cmc-me.com

IT209K:
Security Tools and Systems Training

Tel No:+97126654546 | Fax No:+97126654182 | Email: training@cmc-me.com | www.cmc-me.com

Training Description:

In this intensive training course, you will gain the foundational knowledge and skills to analyze and assess network risks and then select and deploy appropriate countermeasures.

Training Objectives:

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

- ✓ Evaluate methods for strong authentication.
- ✓ Search for possible vulnerabilities in operating systems.
- ✓ Reduce your organization's exposure to dangers in enterprise-wide and virtual private networks (VPNs).
- ✓ Analyze your exposure to security threats.
- ✓ Protect your organization's systems and data.
- ✓ Deploy firewalls and data encryption to minimize threats.
- ✓ Assess alternative user and host authentication mechanisms.
- ✓ Manage risks originating from inside the organization and from the internet.
- ✓ Leverage continued support with after-course one-on-one instructor coaching and computing sandbox

Training Designed for:

This course is intended for Business Development Managers, Corporate Planning Professionals, Geoscience & Engineering Professionals, Supply Planners & Scheduling Professionals, Government Regulators, Law Professionals, Tax & Finance Advisors, Auditing Personnel, Compliance Officers, Equity Analyst and Bankers, Joint Venture Officers, Negotiators and Contracting Professionals and Trading Professionals.

Training Requirement:

"Hand's on practical sessions, equipment and software will be applied during the course if required and as per the client's request."

Contents can be adapted to your specific wishes. It is therefore possible to focus on specific modules of the training course as per client's learning needs and objectives. Further, it should be forwarded to us a month prior to the course dates.

Training Program:

FIVE DAYS:

- ❖ Module 1: Building A Secure Organization
- ❖ Real threats that impact cybersecurity
  - Hackers, internal and external
  - Eavesdropping
  - Spoofing
  - Sniffing
  - Trojan horses
  - Viruses
  - Wiretaps

- A cyber security policy: the foundation of your protection
  - Defining your information assurance objectives
  - Assessing your exposure
- Module 2: A Cryptography Primer
- Securing data with symmetric encryption
  - Choosing your algorithm: DES, AES, Rc4, and others
  - Assessing key length and key distribution
- Solving key distribution issues with asymmetric encryption
  - Generating keys
  - Encrypting with RSA
  - Explore PGP and GnuPG
  - Evaluating Web of Trust and PKI
- Ensuring integrity with hashes
  - Hashing with Md5 and SHA
  - Protecting data in transit
  - Building the digital signature
- Module 3: Verifying User and Host Identity
- Assessing traditional static password schemes
  - Creating a strong password policy to prevent password guessing and cracking
  - Protecting against social engineering attacks
  - Encrypting passwords to mitigate the impact of password sniffing
- Evaluating strong authentication methods
  - Preventing password replay using one-time and tokenized passwords
  - Employing biometrics as part of multi-factor authentication
- Authenticating hosts
  - Distrusting IP (Internet Protocol) addresses
  - Mitigating address-spoofing issues and implementing countermeasures
  - Implementing solutions for wireless networks
- Module 4: Preventing System Intrusions
- Discovering system vulnerabilities
  - Searching for operating system vulnerabilities
  - Discovering file permission issues
  - Limiting access via physical security
- Encrypting files for confidentiality
  - Encrypting with application-specific tools
  - Recovering encrypted data
- Hardening the operating system
  - Locking down user accounts
  - Securing administrator's permissions
  - Protecting against viruses
- Module 5: Guarding Against Network Intrusions
- Scanning for vulnerabilities
  - Searching for rogue servers
  - Profiling systems and services

- Reducing Denial of Service (DoS) attacks
  - Securing DNS (Domain Name System)
  - Limiting the impact of common attacks
- Deploying firewalls to control network traffic
  - Preventing intrusions with filters
  - Implementing a cyber security policy
  - Deploying personal firewalls
- Protecting web services and applications
  - Validating user input
  - Controlling information leakage
- Module 6: Ensuring Network Confidentiality
- Threats from the LAN
  - Sniffing the network
  - Mitigating threats from connected hosts
  - Partitioning the network to prevent data leakage
  - Identifying wireless LAN vulnerabilities
- Confidentiality on external connections
  - Ensuring confidentiality with encryption
  - Securing communication with IPsec
- Course Conclusion
- POST-ASSESSMENT and EVALUATION

Training Methodology:

This interactive training course includes the following training methodologies as a percentage of the total tuition hours:

- 30% Lectures, Concepts, Role Play
- 70% Workshops & Work Presentations, Techniques, Based on Case Studies & Practical Exercises, Gamification, Software & General Discussions
- Pre and Post Test

Training Fees:

TBA as per the course location - This rate includes participant's manual, hand-outs, buffet lunch, coffee/tea on arrival, morning & afternoon of each day.

Note: The 5% VAT (Value Added Tax), will be effective starting 01st of January 2018 as per the new regulation from the UAE Government. The VAT applies for all quotation both for local and abroad.

Training Certificate(s):

CMCT Internationally recognized certificate(s) will be issued to each participant who completed the course.

Training Timings:

Daily Timings:

07:45 - 08:00	Morning Coffee / Tea
08:00 - 10:00	First Session
10:00 - 10:20	Recess (Coffee/Tea/Snacks)
10:20 - 12:20	Second Session
12:20 - 13:00	Recess (Prayer Break & Lunch)
13:00 - 14:00	Last Session

For training registrations or in-house enquiries, please contact:

Aisha Relativo - Training & Career Development Manager
aisha@cmc-me.com / training@cmc-me.com
Tel.: +971 2 665 3945 or +971 2 643 6653 | Mob.: +971 52 2954615