



HS172: Advanced Security Training

Training Description:

This Advanced Security Training course provides security professionals with in-depth knowledge and hands-on experience in managing modern security threats. The training course covers advanced physical security practices, cyber threat intelligence, incident response strategies, risk management frameworks, and compliance requirements. Through case studies, simulations, and expert instruction, attendees will be equipped to lead security initiatives in complex environments.

Training Objectives:

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

- ✓ Analyze and mitigate sophisticated cyber and physical security threats
- ✓ Develop and manage security policies aligned with industry standards
- ✓ Implement incident response and recovery procedures
- ✓ Conduct risk assessments and apply security frameworks like NIST and ISO/IEC 27001
- ✓ Integrate physical and information security strategies

Training Designed for:

This course is intended for Senior Security Officers, Security Consultants, Cybersecurity Analysts, IT Security Managers, Incident Response Team Members, Risk Management Professionals and Physical Security Coordinators.

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.”

Content, location and duration 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:

DAY ONE:

- ❖ **Advanced Threat Landscape & Security Fundamentals**
 - Overview of current global threat landscape (cyber and physical)
 - Emerging trends in advanced persistent threats (APTs)
 - The role of threat intelligence in modern security
 - Review of security principles: CIA triad, defense in depth, zero trust
 - Case study: Recent security breach and lessons learned
- ❖ **Exercises:**
 - Threat mapping exercise
 - Group discussion on evolving security challenges

DAY TWO:

- ❖ **Risk Management & Security Frameworks**
 - Risk identification, analysis, and mitigation strategies

- Application of NIST Risk Management Framework (RMF)
- ISO/IEC 27001: Security management systems
- Business continuity planning (BCP) and disaster recovery (DR)
- Security policy development and lifecycle

❖ **Exercises:**

- Workshop: Create a basic risk assessment report
- Hands-on: Aligning policies with NIST and ISO standards

DAY THREE:

❖ **Cybersecurity & Technical Controls**

- Network security architecture and secure protocols
- Intrusion detection and prevention systems (IDS/IPS)
- Endpoint protection and patch management
- Security Information and Event Management (SIEM)
- Encryption, digital certificates, and PKI

❖ **Exercises:**

- Lab: Log analysis using a SIEM tool
- Hands-on: Configuring IDS rules and interpreting alerts

DAY FOUR:

❖ **Physical Security Integration**

- Physical access control systems (PACS)
- Video surveillance (CCTV), biometrics, and perimeter security
- Red teaming and penetration testing (physical and cyber)
- Insider threats and countermeasures
- Facility risk assessment and emergency response planning

❖ **Exercises:**

- Exercise: Physical security audit of a sample layout
- Role-play: Emergency response simulation

DAY FIVE:

❖ **Incident Response & Legal Compliance**

- Incident response lifecycle and playbooks
- Forensics fundamentals and evidence handling
- Data breach notification laws and regulatory compliance (e.g., GDPR, HIPAA)
- Security governance, audit, and reporting
- Final project: End-to-end incident simulation

❖ **Exercises:**

- Tabletop exercise: Coordinated incident response

❖ **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 Assessment

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) and wallet card(s) will be issued to each participant who successfully completed the course and passed the exam at the end of 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