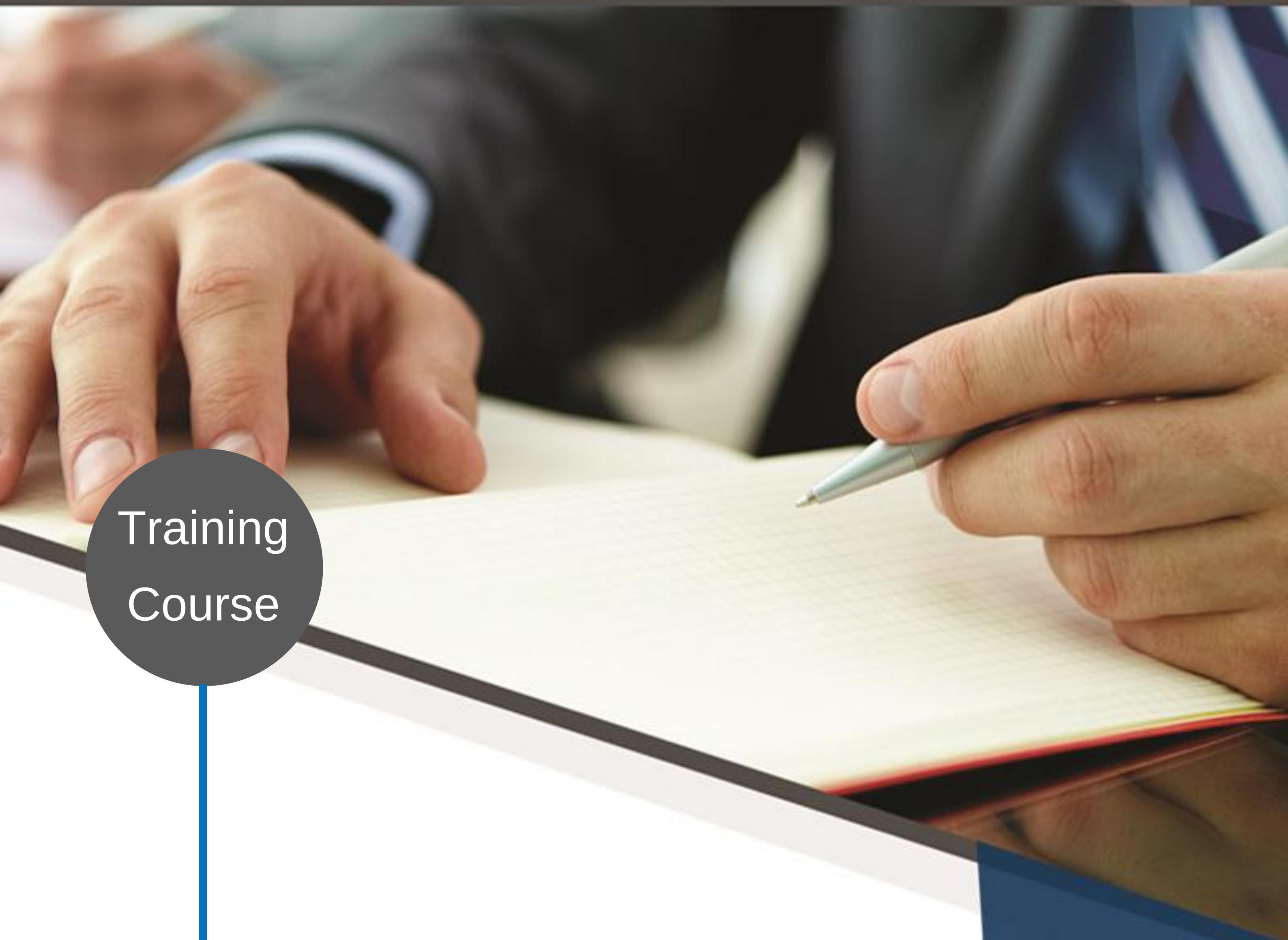
Skills International for Training & Consulting



Training Course

Security Incident Management & Investigation

Skills International for Training & Consulting

سكلز الدولية للتدريب والإستشارات

Course Plan

Introduction

Effective security incident management and investigation are critical components of protecting an organization's assets, reputation, and continuity. This "Security Incident Management & Investigation" course provides participants with the tools and methodologies needed to efficiently manage and respond to security incidents while conducting thorough investigations. The course covers the entire incident lifecycle, from detection and response to investigation, documentation, and post-incident analysis. Participants will gain practical knowledge of various security incident scenarios and learn how to apply investigative techniques to uncover the root cause of security breaches.

Course Objectives:

- ✓ Understand the principles and best practices for managing security incidents.
- ✓ Learn how to identify and classify different types of security incidents.
- ✓ Develop effective strategies for incident response and escalation.
- ✓ Master investigative techniques for collecting and analyzing security incident data.
- ✓ Understand legal and regulatory requirements in security investigations.
- ✓ Build a systematic approach to documenting and reporting security incidents.

- ✓ Strengthen organizational security by learning from past incidents through analysis and lessons learned.

Who Should Attend?

- ○ Security Managers and Officers
- ○ Incident Response Teams
- ○ Cybersecurity Professionals
- ○ Law Enforcement and Investigators
- ○ Risk and Compliance Managers
- ○ IT Security Specialists
- ○ Operational and Facility Security Staff
- ○ Anyone involved in managing or investigating security incidents within their organization

Training Methods:

- ✓ Online Video material.
- ✓ Presentation.
- ✓ Live Interactive sessions.
- ✓ Course presenter will make extensive use of all tools that will be needed for the virtual environment.
- ✓ Questions & Answers

Course Outline:

Day One

- Introduction to Security Incident Management and Investigation
- The Security Incident Lifecycle: Detection, Response, Investigation, and Recovery
- Types of Security Incidents (Physical, Cybersecurity, Internal, External)
- Incident Identification and Classification Criteria
- The Importance of a Security Incident Response Plan (SIRP)

Day Two

- Roles and Responsibilities of Incident Response Teams
- Communication Strategies During a Security Incident
- Immediate Actions: Containment, Eradication, and Recovery
- Tools and Technologies for Security Incident Detection
- Security Incident Escalation Procedures

Day Three

- Evidence Collection and Chain of Custody
- Conducting Initial Incident Assessments and Damage Control
- Investigative Techniques: Interviews, Surveillance, and Data Collection

- Cybersecurity Incident Investigations: Specific Techniques and Tools
- Physical Security Incident Investigations: Evidence and Procedures

Day Four

- Data Analytics and Forensic Tools for Investigations
- Identifying and Handling Insider Threats
- Legal Aspects of Security Incident Investigations
- Understanding Data Breach and Privacy Laws
- Post-Incident Reporting and Documentation Requirements

Day Five

- Incident Root Cause Analysis and Problem-Solving
- Implementing Corrective and Preventive Actions Post-Incident
- Lessons Learned: Improving Security Based on Incident Analysis
- Crisis Management and the Role of Security Investigations in Organizational Recovery
- Case Studies: Real-Life Examples of Security Incident Management and Investigations

Training Details

Course Duration	5 Days
Pre-Schedule	17 – 21 Aug 2025
Venue	Dubai – The H Hotel
Training Fees Per Person	KWD 1600 (One Thousand Six Hundred Only)
Course Fees Include	✓ Tuition documentation ✓ Curriculum and Training Handout ✓ Five star Lunch ✓ Completion Certificates