London TDM

Information Technology and Digital Transformation Training Courses

Course Venue: Malaysia - Kuala Lumpur

Course Date: From 05 July 2026 To 09 July 2026

Course Place: Royale Chullan Hotel

Course Fees: 6,000 USD

Introduction

In today's digital landscape, cybersecurity incidents are inevitable, making a robust incident response and recovery strategy critical for organizations. This 5-day professional course is designed to equip cybersecurity professionals with the knowledge and skills necessary to effectively manage and mitigate the impact of cybersecurity incidents, ensuring a swift recovery and minimizing damage.

Objectives

- Understand the fundamentals of cybersecurity incident response and recovery.
- Develop the ability to identify and assess cybersecurity incidents effectively.
- Gain essential skills in incident containment, eradication, and recovery processes.
- Learn to design and implement a comprehensive incident response plan.
- Master communication and collaboration strategies during and after an incident.

Course Outlines

Day 1: Introduction to Cybersecurity Incidents

- Overview of cybersecurity incidents and their impact on organizations.
- Types of cybersecurity threats and vulnerabilities.
- The cybersecurity incident response lifecycle.
- Key roles and responsibilities in incident response.
- Case studies of notable cybersecurity incidents.

Day 2: Preparing for Incident Response

- Designing an incident response plan.
- Establishing an incident response team.
- Tools and technologies for incident detection and response.
- Setting up an incident response infrastructure.
- Conducting regular training and simulations.

Day 3: Identifying and Assessing Incidents

- Incident detection and monitoring techniques.
- Using threat intelligence to identify incidents.
- Incident severity classification and prioritization.
- Forensic data collection and analysis.
- Reporting and documentation of incidents.

Day 4: Incident Containment, Eradication, and Recovery

- Strategies for incident containment.
- Methods for eradicating threat actors and malware.
- Data and system recovery best practices.
- Ensuring business continuity during incidents.
- Post-incident analysis and lessons learned.

Day 5: Post-Incident Activities and Improvement

- Effective communication during and after incidents.
- Conducting a post-incident review and debriefing.
- Updating incident response plans and policies.
- Building a culture of continuous improvement.
- Enhancing organizational resilience against future incidents.