BLACKBIRD FOR TRAINING

Comprehensive Information Security & Cyber Security

26 July – 6 August 2027
Kuala Lumpur (Malaysia)



Comprehensive Information Security & Cyber Security

Ref: 321503_141087 **Date:** 26 July – 6 August 2027 **Location:** Kuala Lumpur (Malaysia) **Fees:** 8800 GBP

Introduction

In today's increasingly connected world, cybersecurity is more critical than ever. Organizations face a growing array of cyber threats, from data breaches to advanced cyber-attacks. This course provides participants with a comprehensive understanding of how to protect their organization from cyber-attacks. It covers everything from the basic principles of information security to the most advanced cyber defense strategies, ensuring that all participants leave with a clear understanding of how to safeguard their infrastructure.

Through this course, you will learn about the latest threat trends, cybersecurity risk management techniques, and how to design and implement a comprehensive cyber security policy. By examining real-world cybersecurity simulations, you will gain hands-on experience mitigating common cyber threats.

Course Objectives

By the end of this course, participants will:

- Understand the key cyber threats and vulnerabilities facing organizations today, and the need for a comprehensive cybersecurity strategy.
- Learn information security techniques and controls to protect organizations from cyber-attacks, ensuring they align with a comprehensive information security program.
- Grasp the fundamentals of an Information Security Management System ISMS, and how it supports overall security goals.
- Explore various data protection principles, including techniques to safeguard data in motion and at rest.
- Dive into social engineering threats, methods, and the importance of cyber defense tactics to counteract them.
- Analyze software vulnerabilities and discover security solutions to reduce the risk of exploitation.
- Examine physical and IT security controls and understand their interconnectedness in maintaining a robust defense.



Course Outlines

Day 1: Cybersecurity Awareness

- What is Security? Defining the fundamental principles of cybersecurity.
- Confidentiality, Integrity, and Availability: The cornerstones of information security.
- Security Baselining: Setting standards for securing systems.
- Security Concerns: Humans: Understanding the role of employees in cybersecurity.
- Types of Threats: Exploring various cyber-attacks and their implications.
- Security Controls: Implementing security measures to reduce risk.
- What is Hacking?: Understanding the methods used by attackers.
- Risk Management: Establishing a comprehensive cyber security strategy.

Day 2: Network Discovery

- Networking Review: Key concepts for understanding network security.
- Discovery, Footprinting, and Scanning: Techniques attackers use to assess systems.
- Common Vulnerabilities and Exposures: Identifying vulnerabilities that affect network security.
- Security Policies: The importance of creating robust cybersecurity policies.

Day 3: Security Architecture

- Security Architecture: Understanding the structure of secure systems.
- Network Devices & Zones: How to protect your network's perimeter and internal areas.
- Network Segmentation & NAT: Techniques for securing communication channels.
- Network Access Control: Safeguarding access points and communication paths.

Day 4: Data Security

- Cryptography: Securing data through encryption.
- Principles of Permissions: How to implement proper access control.
- Steganography: Hiding information within other data forms.

Day 5: Identity Management

- What is Identity Management?: The role of authentication in cybersecurity.
- Personally Identifiable Information PII: How to protect sensitive data.
- Authentication Factors & Directory Services: Securing user identities and credentials.
- Password Policies: Implementing strong password controls to prevent unauthorized access.



Day 6: Network Hardening

- Limiting Remote Admin Access: Reducing attack surfaces through access controls.
- Network Segmentation: The best practices for protecting network traffic.
- Limiting Physical Access: Strengthening security with physical control mechanisms.

Day 7: Software Security

- Software Engineering: Developing secure applications.
- Security Guidelines & Vulnerabilities: How to prevent flaws in software systems.
- Environment Monitoring: Using tools to track and protect system activity.

Day 8: Physical Security

- What is Physical Security?: The importance of physical protection in cybersecurity.
- Defense in Depth: A multi-layered approach to physical and IT security.

Day 9: Incident Response

- Disaster Types & Business Continuity: Preparing for potential cyber disasters.
- Incident Investigation & Forensic Response: Understanding how to respond to breaches.

Day 10: Trends in Cybersecurity

- Cybersecurity Design Constraints: How modern systems shape cybersecurity strategies.
- Cyber Driving Forces: Understanding the major factors driving cybersecurity evolution.
- Cybersecurity Standards & Training: The importance of compliance and cybersecurity training for all employees.

Why Attend This Course: Wins & Losses!

- Comprehensive Knowledge of Cybersecurity: Gain a high-level understanding of comprehensive cyber security practices and how they can be integrated into your organization.
- Effective Risk Management: Learn how to assess and manage cyber risks through structured cybersecurity risk management training.
- Real-World Application: Through cybersecurity simulation training, you will practice responding to real-world cyber threats, preparing you to defend your organization in a constantly evolving cyber landscape.
- Hands-On Experience: Learn how to develop a comprehensive cybersecurity strategy and implement cyber defense operations, using practical, real-world scenarios.



Conclusion

This advanced course is designed to provide a comprehensive understanding of how to build, implement, and manage comprehensive cyber security strategies. Through cybersecurity training and real-world case studies, you will gain the skills needed to protect your organization against the growing threats in today's cyber environment.

Whether you are looking to enhance your leadership capabilities in cybersecurity or improve the technical resilience of your infrastructure, this course is an essential resource for cybersecurity professionals and leaders alike.

