MINISTRY OF COMMUNICATIONS AND MULTIMEDIA MALAYSIA

CyberSecurity MALAYSIA

Accredited by:

GLOBAL ACE CERTIFICATION

Certified IoT Security Analyst (CISA)

Certification

This training exposes participants with skills to assess IoT environment which includes robotic technology, web application, wireless network, and cloud. Participants will be able to identify, perform and mitigate security issues as part of securing IoT environment.

Terminal Objectives

- To analyse the main components in IoT environment and technology
- To understand the capabilities of components in IoT environment
- To conduct Network Security Assessment involving assessing the security protocol
- To identify possible mitigation processes
- To defend the communication in IoT environment
- To perform application security assessment
- To provide remediation strategies
- To defend the applications in IoT environment
- To determine security risk and incident management plan of IoT environment

Target Participants

- IT developer, security analyst, engineer, and cloud security analyst.

Certified Examination

The CISA examination is certified by the Global ACE Certification. The examination framework is designed to align with a set of relevant Knowledge, Skills and Attitudes (KSA) that are necessary for a Secure Application Professional. Candidates will be tested via a combination of either continual assessment (CA), multiple choice (MC), theory/ underpinning knowledge assessment (UK), practical assessment (PA), assignments (AS) and case studies (CS) as required.

Candidates can take the examination at authorized examination centres in participating member countries. Candidates who have successfully passed the CISA examination will be eligible to apply as an associate or professional member by fulfilling the membership criteria defined under the Global ACE Certification.

Program Outline

Module 1: Introduction to IoT	
Module 1.1 Introduction to IoT Security	Component of IoT Security 1. Robotic 2. Wireless 3. Web Application 4. Cloud Computing 5. IoT Security Guideline 6. Outcome from IoT Security
Module 1.2 IoT Technology	1. History of IoT Technology 2. Current IoT Technology 3. IoT In Security 4. Previous Incident in IoT
Module 2: Robotic Technology	
Module 1.2 Introduction to Robotic Technology	1. Introduction to robotic components 2. Introduction to robotic communications
Module 2.2 Case Study	1. Case Study 1: Manufacturing 2. Case Study 2: Autonomous System
Module 2.3 Introduction to type of robotics	1. Collaborative Robot 2. Industrial Robot
Module 3: Wireless Network Assessment	
Module 3.1 Introduction to Wireless Network	1. Wi-Fi network fundamentals 2. Wireless network standard and organization 3. Wireless threats and attacks
Module 3.2 Information Gathering	1. Case Study 1: Manufacturing 2. Case Study 2: Autonomous System
Module 3.3 Introduction to type of robotics	1. Active and Passive Scanning 2. Using tool: Kismet
Module 3.4 Wireless Network Defense	1. Mitigation process

Program Outline

Module 4: Web Application Security	
Module 4.1 Introduction to Web Application Security	1. Use of web applications 2. Importance of web applications in IoT
Module 4.2 Web Application Threat in IoT	1. OWASP Top 10 2019 2. SQL Injection 3. Cross Site Scripting (XSS)
Module 4.3 Penetration Testing	4. SQL Injection on Vulnerable Web Site 5. Cross Site Scripting on Vulnerable Web Site
Module 4.4 Web Application Defense	1. Mitigation process
Module 5: Cloud	
Module 5.1 Introduction to Cloud	1. Introduction to Cloud 2. Type of Cloud Computing 3. Public, Private vs Hybrid Cloud
Module 5.2 Cloud as a Services	1. Infrastructure as a Services 2. Platform as a Services 3. Software as a Services
Module 5.3 Concept and Architecture	1. Importance of Cloud Computing in IoT 2. Secure Cloud Architecture 3. Secure Cloud Implementation
Module 6: Security in IoT	
Module 6.1 Introduction to IoT Security Guideline	1. The importance of IoT Security
Module 6.2 Introduction to IoT Security Infrastructure	
Module 6.3 Introduction to IoT Security layer	
Module 6.4 IoT Security Requirement	1. Guideline on IoT Security Requirement

For additional information, please visit www.cybereducationscheme.org. You can also contact us at training@cybersecurity.my or call at 03 8800 7999

CyberSecurity Malaysia,
Level 7, Tower 1, Menara Cyber Axis,
Jalan Impact, 63000 Cyberjaya,
Selangor Darul Ehsan, Malaysia

Tel: +603 8800 7999 **Fax:** +603 8008 7000
Email : info@cybersecurity.my
Customer Service Hotline: 1 300 88 2999
Website: www.cybersecurity.my