MINISTRY OF DIGITAL

CyberSecurity MALAYSIA

Accredited by:

GLOBAL ACE CERTIFICATION

Certified Incident Handling and Network Security Analyst (CIHNSA)

Certification

This training is specially conducted for the participating agencies and Sector Leads to equip them with the intermediate knowledge in Incident handling and Network Security.

Participants will be exposed to the security environment through practitioners' experience sharing, case studies and hands on exercises by doing relevant analysis with the related tools. Participants will be exposed to the actual drill environment where the previous drill scenario will be simulated. Rephrase to – Participants will be provided with the actual incident scenario, malware samples and handling vulnerabilities.

Terminal Objectives

- Recognize the importance of following well-defined processes, policies, and procedures;
- Understand technical, communication, and coordination issues involved;
- Analyze and assess the impact of computer security incidents;
- Build and coordinate response strategies for various types of computer security incidents;
- Gain practical understanding of various methods for analyzing artefacts left on a compromised system;
- Obtain practical experience in the analysis of vulnerabilities and the coordination of vulnerability handling tasks.

Target Participants

- Computer network incident handling and incident responder professionals
- Computer security incident response team members and technical staff
- System and network administrators with incident handling experience
- IT professionals from private and public sectors

Certified Examination

The CIHNSA 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 CIHNSA 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

Day 1	
Module 1 Introduction Security Incident, Incident Handling	1. Introduction: Security Incident 2. Introduction: Security Incident 3. Six Steps of Incident Handling 4. Sample Incidents ▪ Handling Phishing ▪ Handling Intrusion Incident ▪ Handling Malware Incident ▪ Handling DDOS
Day 2	
Module 2 Malware Analysis	1. Introduction: Malware analysis 2. Malware Analysis Tools 3. Malware Analysis Technique ▪ Static Analysis ▪ Dynamic Analysis ▪ Behavioural Analysis 4. Malware Analysis Hands-On
Day 3	
Module 3 Web Security Module	1. Introduction: Web Security 2. Introduction: Linux Environment & HTTP Request 3. Web Application Vulnerability ▪ Remote/Local File Inclusion (RFI/LFI) ▪ SQL Injection (SQLi) ▪ Cross Site Scripting (XSS) 4. Web Incident Analysis

For additional information, please visit www.cyberguru.my. 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