Incident Response & Handling Training

Overview

This 3-day course teaches you the tools and methods for responding to computer incidents and the methods used by hackers to undermine systems, so you can prepare, detect, and respond to them. The gives you hands-on experience for discovering holes before hackers do. The course also explores the legal issues associated with responding to computer attacks.

Who Should Attend?

- Incident Handling Personnel/Manager
- System Administrators and security personnel
- IT Security Officers
- IT Professionals

Objective

- To learn the method for responding to computer incident.
- To learn the method that being used by the hackers to undermine the system
- To learn how to prevent, detect and respond to the attack.

Programme Outline

- **Introduction to Incident handling**

    - Definition of incident
    - Criteria for Incident
    - Categories of incidents
    - Types of incidents
    - Response level to incidents
    - Definition of incident handling
    - Purpose of incident handling
    - 6 steps in incident handling
        a. Preparation
        b. Identification
        c. Containment
        d. Eradication
        e. Recovery
        f. Follow up

- **Request Tracker for Incident Handling**

    - The need and importance of an automated helpdesk system for incident handling.
    - Brief description of the RTIR automated helpdesk system
    - The usage and benefits of the RTIR
    - Hands-on on using the RTIR

- **Log and Malicious Code Analysis**
    - Log Analysis

- Network Devices
    - Router log
        a. Cisco
        b. 3COM
    - Firewall log
        a. BSD
        b. Checkpoint
        c. Zone Alarm
    - IDS log
        a. Snort
        b. RealSecure
    - Antivirus log
        a. Trendmicro
        b. Symantec

- **System Devices**
    - Windows Server
        a. Windows 2000
        b. Windows XP
    - Unix Server
        a. Solaris
        b. BSD
        c. Linux

- **Malicious Code Analysis**
    - Trojan
    - Worm
    - Virus

Prerequisites:

This course is particularly is suited to individuals who lead or form a part of an incident handling team

Trainer:

1. En Adli Abdul Wahab
2. En. Mahmud Abd Rahman
3. En. Mohamad Nasir Che Embee

Fees

This programme is priced at **RM2000.00** per person, inclusive of 3-days trainer's fee, course materials, meals and refreshments, venue, parking and certificate of attendance

Venue

Training Room, CyberSecurity Malaysia, Level 4, Block C, Mines Waterfront Business Park, No. 3, Jalan Tasik, The Mines Resort City, 43300 Seri Kembangan, Selangor Darul Ehsan

Duration

3 days (9:00am -5:00pm)

Registration

Download form: http://www.cybersecurity.my

Complete the registration form and fax to **+603 - 8946 0844**

Contact us
Tel: **+603 – 8946 0999** Email : **training [at] cybersecurity.my**