INCIDENT HANDLING & RESPONSE | COURSE OUTLINE

CYBER ZONES
Cyber Security Services

Course Title:

Incident Handling & Response | IHR

Duration:

5 days,20 Hrs
4 hours per day

Class Format Options:

Instructor-led classroom – Practical Training.

Who Should Attend:

- Cyber Security Professionals
- SOC Managers
- SOC Engineers
- IT Auditors
- Security Consultants
- System Administrators
- IS Managers
- IT Departments

Prerequisites:

A general knowledge of information systems and security

Provided Materials:

- Softcopy Materials.
- Incident handling tools.

This training course is practical training course on which each trainee will learn the proper technique to incident handling furthermore, this training course contains how to investigate a cyber attack.

Course Overview

The **incident handling & response course (IHR)** is an advanced **defensive cyber security course** from **BLUE Team** training path aims to teach trainees to manage security incidents by understanding common attack techniques as well as defending against and/or responding to such attacks when they occur. The **IHR** training course focuses on preparing, detecting, responding, and resolving security incidents.

Incident Handling and Response training course is designed for those people who wish to become cyber security professionals, SOC engineers, SOC Managers, Information Security Assurance specialists, the course covers:

- The steps of the incident handling process.
- Detecting malicious applications and network activity.
- Common attack techniques that compromise hosts.
- Detecting and analyzing system and network vulnerabilities.
- Continuous process improvement by discovering the root causes of incidents.

Upon completion trainees will be able to:

- Apply incident handling processes in-depth, including preparation, identification, containment, eradication, recovery and follow up to protect environments.
- Analyze the structure of common attack techniques to be able to evaluate an attackers spread through a system and network, anticipating further attacker activities.
- Tracing emails originating and detect (Spoofing) fake emails from real emails.
- Use built-in command-line tools such as Windows task Manager as well as netstat, PID and system internals utilities to detect attacker presence on a machine.
- Run port scanners and find out the use of scripting used by attackers.
- Run vulnerability scanners to find vulnerabilities on target systems to detect and analyze the impacts on the systems.

IHR Course Content

Course Content

- **Module 1:** Introduction
- **Module 2:** Preparation for Threats, Vulnerabilities and Exploits.
- **Module 3:** Identification and Initial Response.
- **Module 4:** Preliminary Response
- **Module 5:** Sysinternals
- **Module 6:** Containment
- **Module 7:** Eradication
- **Module 8:** Follow-Up
- **Module 9:** Recovery

.

IHR Course LABS

- **Lab 1:** Security Events Lab
- **Lab 2:** Built in command in windows
- **Lab 3:** Using wire shark
- **Lab 4:** Ping Sweep & Detection
- **Lab 5:** Port Scanning & Detection
- **Lab 6:** ARP Cache Poisoning advanced
- **Lab 7:** Virus Total
- **Lab 8:** Computer Monitoring & detection
- **Lab 9:** Vulnerability Assessment
- **Lab 10:** SysInternal Tools