Certified Incident Handling Engineer

Modality: On Demand

Duration: 5 Hours

About this course:

The Certified Incident Handling Engineer (CIHE) course is designed, aiming for individuals who are interested in effectively and efficiently handle incidents. Through the course, an individual will learn to properly utilize resources while preventing, detecting and mitigating attacks over data or network infrastructure. The Certified Incident Handling Engineer course also covers concepts, which are required in planning, creating, and implementing effective incident responses. Moreover, the course also teaches individuals the common exploits and techniques, which can be used by hackers to penetrate into the system. Therefore, individuals are in a better position to respond to any such attacks on IT infrastructure.

The Certified Incident Handling Engineer course will cover the following topics.

- Threats
- Vulnerabilities in the network
- IH preparation
- Request trackers for incident handling
- Preliminary responses
- Identification and initial responses
- Sysinternals
- Containment
- Eradication
- Follow-up
- Recovery
- Virtualization security
- Malware incident handling.

The average salary for a Certified Incident Handling Engineer skills is **$78,662** per year.

Course Objectives:

The objectives of the Certified Incident Handling Engineer course are following

- To enable individuals to detect security threats, risks and weaknesses.
- To enable an individual to prevent, detect, and respond to security breaches.
- To enable an individual to report on findings.
- To enable an individual to take and clear the Certified Incident Handling Engineer examination successfully.

Audience:

Anyone who is already on the job and is responsible for incident handling or is interested in pursuing a career in this regard

Prerequisites:

Knowledge and understanding of the Certified Information System Security Office course.

Suggested prerequisite course:

Certified Information Systems Security Officer

Course Outline:

- Module 01 - Course Introduction
- Module 02 - Threats, Vulnerabilities and Exploits
- Module 03 - IH Preparation
- Module 04 - Request Tracker for Incident Handling
- Module 05 - Preliminary Response
- Module 06 - Identification and Initial Response
- Module 07 - Sysinternals
- Module 08 - Containment
- Module 09 - Eradication
- Module 10 - Follow-up
- Module 11 - Recovery
- Module 12 - Virtualization Security
- Module 13 - Malware Incident Handling