Certified Incident Handling Engineer (CIHE)

Modality: Virtual Classroom

Duration: 5 Days

SATV Value:

CLC:

NATU:

SUBSCRIPTION: No

About this course:

Our Training program of Cyber Security is intended to help Incident Handling Engineers in increasing total information on security ruptures in the system of an association. Regardless of whether you are a General Security Engineer or a System Administrator, this program will help you massively. We have relegated exceptionally prepared certify experts to instruct fundamental to ace level security basics to engineers needing to show signs of improvement comprehension of detecting, planning, and containing security ruptures that represent a significant danger to the system of IT in associations.

This program is planned remembering the ever-changing security requirements of companies. That is the explanation this course gives great preparation to Incident Handling Engineers. Additionally, understudies selected the course get an opportunity to find out about shrouded procedures utilized by programmers around the world to get into profoundly secure frameworks. Our experts will train you through activities on how you can set out a solid security system to keep hackers from causing significant misfortune.

Also, you will become familiar with a broad scope of incident handling procedures through virtual lab practices using various methods including reconnaissance, malware, vulnerability assessment, and web application manipulation with Netcat, Nexus, and that's only the tip of the iceberg. Every last bit of it in addition to much more will be covered in the course on both Windows and Linux operating systems.

This Training program of Cyber Security is fitting for the graduates of the mile2 Certified Incident Handling Engineer. Our expert teachers assist engineers with learning security points in detail so they can devise related methodologies easily. The fundamental reason for this program is to offer training of SANS Security 504. Understudies ready to take the certification exams of CIHE and GCIH can profit greatly from this program.

Course Objective:

- Have the information to recognize security risks, dangers, and weaknesses.
- Have the information to get ready for detection, prevention, and reactions to security breaks.
- Have information to precisely provide details regarding their discoveries from assessments.
- Be prepared to sit for the Certification Exam of CIHE

Audience:

This course is perfect for Incident Handling engineers who need to figure out how to distinguish, plan, manage, and eradicate security dangers. Understudies need to have fundamental to the information of intermediate-level on CISSO. You are more likely than not finished our CISSO course to have the option to enlist for this course. Regardless of whether you have significant experience, this course is perfect for you.

Prerequisites:

- At least a year's involvement with the technologies of systems administration
- Information on Microsoft packages
- A sound information of networking
- Basic understanding of Linux is essential
- A sound information of TCP/IP

Suggested prerequisites courses:

Enterprise Linux Network Services (L-275)

Linux Fundamentals (L-120)

Course Outline:

- **Module I -** Incident Handling Explained
- **Module II -** Threats, Vulnerabilities, and Exploits
- **Module III –** Preparation
- **Module IV -** First Response
- **Module V –** Containment
- **Module VI –** Eradication
- **Module VII –** Recovery
- **Module VIII -** Follow-Up

Lab Outline

- **Module I Lab -** Attacks Under The Microscope
- **Module II Lab -** Ticketing System
- **Module III Lab -** SysInternals Suite
- **Module IV Lab -** Examine System Active processes
- **Final Scenario –** 4 hours

Advanced Labs

- **Advanced Module I Lab -** Computer Security Incident Response Team
- **Advanced Module II Lab -** Log File Analysis: Analyzing a Shell History File
- **Advanced Module III Lab –** Log File Analysis: Searching Attacks in your Apache Logs
- **Advanced Module III Lab -** Rootkits and Botnets: How to Crash your Roommate's Windows

7 PC

- **Advanced Module III Lab -** Rootkits and Botnets: Exploit MS Word to Embed a Listener
- **Advanced Module III Lab -** Rootkits and Botnets: Zeus Trojan
- **Advanced Module IV Lab -** Artifact Analysis: Processing and Storing Artifacts