Web: www.secureninja.com
Phone: 703.535.8600
Email: info@secureninja.com

ECIH - EC Council Certified Incident Handler

Course Description and Overview

Overview

SecureNinja's two (2) day Authorized EC-Council Certified Incident Handler training and certification boot camp is designed to provide the fundamental skills to handle and respond to the computer security incidents in an information system. The course addresses various underlying principles and techniques for detecting and responding to current and emerging computer security threats. Students will learn how to handle various types of incidents, risk assessment methodologies, and various laws and policy related to incident handling. After attending the course, they will be able to create incident handling and response policies and deal with various types of computer security incidents. The comprehensive training program will make students proficient in handling and responding to various security incidents such as network security incidents, malicious code incidents, and insider attack threats.

In addition, the students will learn about computer forensics and its role in handling and responding to incidents. The course also covers incident response teams, incident reporting methods, and incident recovery techniques in detail. When a student leaves this intensive 2-day class they will have hands-on understanding and experience in Incident Handling.

This course prepares you for EC-Council Certified Incident Handler exam 212-89

Topics Covered

Introduction to Incident Handling and Response

- Incident Handling and Response Process
- Forensic Readiness and First Response
- Handling and Responding to Malware Incidents
- Handling and Responding to Email Security Incidents
- Handling and Responding to Network Security Incidents
- Handling and Responding to Web Application Security Incidents
- Handling and Responding to Cloud Security Incidents
- Handling and Responding to Insider Threats
- Handling and Responding to Endpoint Security Incidents

Who Would Benefit

This course will significantly benefit incident handlers, risk assessment administrators, penetration testers, cyber forensic investigators, venerability assessment auditors, system administrators, system engineers, firewall administrators, network managers, IT managers, IT professionals and anyone interested in incident handling and response.

Web: www.secureninja.com
Phone: 703.535.8600
Email: info@secureninja.com

Prerequisites

Have a prior networking foundation.

ECIH Exam Info

- **Exam Title**: EC-Council Certified Incident Handler (ECIH)
- **Exam Code**: 212-89
- **Number of Questions**: 100
- **Exam Format**: Multiple Choice
- **Duration**: 3 hours
- **Passing Score**: The passing score varies between 60% to 78%, depending on the specific exam form.
- **Test Delivery**: EC-Council Exam Portal

Course Length

- 2 Days
- 16 Hours

Course Outline

Foundational Understanding:

- Grasp core incident handling principles within information systems.
- Identify and analyze emerging computer security threats.
- Understand the incident response workflow and processes.

Incident Classification and Response:

- Classify and respond effectively to various security incidents like network threats, malicious code, and insider attacks.
- Develop strategies to mitigate and manage different incident types.
- Understand time and cost metrics and difficulties to resolve incidents.
- See examples of modern attacks and current approaches done to respond.

Risk Assessment and Compliance:

- Utilize risk assessment methodologies specific to incident handling.
- Understand the impact of laws, regulations, and policies on incident response.

Policy Development and Implementation:

- Formulate and implement incident-handling policies based on industry standards.
- Ensure alignment and integration of policies within organizational frameworks.

Team Roles, Reporting, and Recovery:

- Define roles within incident response teams and establish effective reporting methods.

Web: www.secureninja.com
Phone: 703.535.8600
Email: info@secureninja.com

- Apply recovery techniques to restore systems and ensure business continuity post-incidents.

Practical Proficiency:

- Apply learned skills in simulated incident handling scenarios.
- Demonstrate proficiency in managing security incidents practically.

Ethical Conduct:

- Uphold ethical standards throughout incident handling procedures.
- Address ethical dilemmas that may arise during incident response.

Follow On Courses

- CEH
- EDRP
- CISSP