Cyber Defense and Countermeasures – C842

Course Feedback

Overview

Traditional defenses such as firewalls, security protocols, and encryption sometimes fail to stop attackers determined to access and compromise data. This course provides 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 learn how to handle various types of incidents, risk assessment methodologies, and various laws and policy related to incident handling. This course prepares students for the Certified Incident Handler (EC-Council ECIH) certification exam.

Competencies

- **Information Security and Incident Categories**
  The graduate identifies key concepts of information security and incident categories.

- **Risk Assessment**
  The graduate applies NIST’s risk assessment methodology to conduct IT risk assessment.

- **Incident Response and Handling Steps**
  The graduate describes steps in incident response and handling procedures.

- **CSIRT**
  The graduate defines the purpose, protocol, and functions of a Computer Security Incident Response Team (CSIRT).

- **Handling Network Security Incidents**
  The graduate describes security incident types and procedures for handling them.

- **Handling Malicious Code Incidents**
The graduate describes steps in detecting and preventing insider threats.

- **Forensic Analysis and Incident Response**
  The graduate describes the role of forensics analysis in incident response and prevention plan.

- **Incident Reporting**
  The graduate describes the purpose, key elements, and procedure for creating an incident report.

- **Incident Recovery and Continuity Planning**
  The graduate describes the principles of incident recovery and continuity planning in order to evaluate business impact.

- **Security Policies and Laws**
  The graduate distinguishes the purpose and elements of a security policy in order to comply with the laws and regulations related to handling a security incident.

**Learning**

**Getting Started**
Welcome to Cyber Defense and Countermeasures. This course uses Soomo learning resources that contain all of the necessary reading materials, labs, videos, and knowledge checks needed to prepare you for EC-Council's Certified Incident Handler certification exam.

For the best understanding of the course content, complete each lesson. To help you track your progress, we suggest you follow the pacing guide identified at the beginning of the course.

Your competence will be demonstrated by the successful completion of the EC-Council Certified Incident Handler (ECIH) 212-89 exam. See the EC-Council Certification Process link within the Course Information section below for a complete explanation of details.

Select the ‘Go to Course Material’ button to begin.

**Assessments**

https://my.wgu.edu/courses/course/9040003
A score of **Competent** or **Exemplary** is required to pass all assessments. Passing a preassessment does not guarantee you will pass the high stakes assessment. On objective assessments, you will be charged a retake fee for the third attempt and every attempt thereafter. For more information [click here](https://my.wgu.edu/courses/course/9040003).

**Course Information**

- The Writing Center
- WGU Library
- Accessibility Policy
- Student Success Center
- EC-Council Incident Handler Certification Process