Description:

The Certified Incident Handling Engineer course, C)IHE, is designed to help Incident Handlers, System Administrators, and Security Engineers understand how to plan, create and utilize their systems. Prevent, detect and respond to attacks through the use of hands-on labs in our exclusive Cyber Range.

With this in-depth training, you will learn to develop start to finish processes for establishing your Incident Handling team, strategizing for each type of attack, recovering from attacks and much more.

Annual Salary Potential $81,812 AVG/year

Key Course Information

Live Class Duration: 5 Days
CEUs: 40
Language: English
Class Formats Available:

    Instructor Led

    Self-Study

    Live Virtual Training

Suggested Prerequisites:

- 12 months network technologies

- Sound knowledge of networking and TCP/IP

- Linux knowledge is essential.

Modules/Lessons

Module 1: Incident Handling Explained
Module 2: Incident Response Policy, Plan and Procedures.
Module 3: Incident Response Team Structure
Module 4: Incident Response Team Services
Module 5: Incident Response Recommendations
Module 6: Preparation
Module 7: Detection and Analysis
Module 8: Containment, Eradication and Recovery
Module 9: GRR Rapid Response
Module 10: Request Tracker
Module 11: Post Incident Activity
Module 12: Recommendations
Module 13: References
Module 14: Information Sharing

Hands-On Labs

Lab 1: Identifying Incident Triggers
Lab 2: Drafting Incident Response Proceedures
Lab 3: Planning for Dependencies
Lab 4: Testing your plan
Lab 5: Drafting Security Policies
Lab 6: Practicing Attack Vectors
Lab 7: Deploy GRR Client
Lab 8: Create Request Tracker Workflow
Lab 9: Lessons Learned
Lab 10: Create a Checklist
Lab 11: Draft Response Improvement Recommendations
Lab 12: Sharing Agreements

Upon Completion

Upon completion, Certified Network Forensics Examiner students will have knowledge to perform network forensic examinations. Be able to accurately report on their findings, and be ready to sit for the C)NFE exam.

Who Should Attend

*   Penetration Testers
*   Microsoft Administrator
*   Security Administrators
*   Active Directory Administrators
*   Anyone looking to learn more about security

Accreditations

Exam Information

The Certified Incident Handling exam is taken online through Mile2's Learning Management System and is accessible on you Mile2.com account. The exam will take approximately 2 hours and consist of 100 multiple choice questions.

A minimum grade of 70% is required for certification.

Re-Certification Requirements

All Mile2 certifications will be awarded a 3-year expiration date.

There are two requirements to maintain Mile2 certification:

1) Pass the most current version of the exam for your respective existing certification
2) Earn and submit 20 CEUs per year in your Mile2 account.

Course FAQ's

Question: Do I have to purchase a course to buy a certification exam?

Answer: No

Question: Do all Mile2 courses map to a role-based career path?

Answer: Yes. You can find the career path and other courses associated with it at www.mile2.com.

Question: Are all courses available as self-study courses?

Answer: Yes. There is however 1 exception. The Red Team vs Blue Team course is only available as a live class.

Question: Are Mile2 courses transferable/shareable?

Answer: No. The course materials, videos, and exams are not meant to be shared or transferred.

Course and Certification Learning Options

Detailed Outline:

Course Introduction

Introduction

Chapter 1: Incident Handling Explained

  a. What is an incident?
  b. What is Incident Handling?
  c. Difference between IH and IR
  d. The Incident Response Process
  e. Seven reasons you must put together an incident response plan
  f. How to build an effective incident response team
  g. Considerations for Creating an Incident Response team
  h. Tips for incident response team members

Chapter 2: Incident Response Policy, Plan, and Procedure Creation

  a. Incident Response Policy
  b. Incident Response Plan
  c. Incident Response Procedures
  d. Sharing Information with Outside Parties

Chapter 3: Incident Response Team Structure

  a. Team Models
  b. Team Model Selection
  c. Incident Response Personnel
  d. Dependencies within Organizations

Chapter 4: Incident Response Team Services

  a. Intrusion Detection
  b. Advisory Distribution
  c. Education and Awareness
  d. Information Sharing

Chapter 11: Post-Incident Activity

    a. Lessons Learned
    b. Using Collected Incident Data
    c. Evidence Retention

Chapter 12: Incident Handling Checklist

    a. Building Checklists

Chapter 13: Incident Handling Recommendation

    a. Recommendations

Chapter 14: Coordination and Information Sharing

    a. Coordination
    b. Information Sharing Techniques
    c. Granular Information Sharing
    d. Sharing Recommendations

Detailed Lab Outline:

Lab Introduction – Recording IPs and Logging In

A. Lab 1 – Identifying Incident Triggers

    1. Explaining Centers of Gravity and how to Identify them
    2. Identifying Security Events within your Center of Gravity
    3. Defining Incident Triggers from the Security Events
    4. Lab 1 Worksheet

B. Lab 2 – Drafting Incident Response Procedures

    1. Logistics
    2. Required Actions
    3. Summary
    4. Lab 2 Worksheet

C. Lab 3 – Identifying and Planning for your dependencies

    1. Internal Dependencies
    2. External Dependencies
    3. Summary
    4. Lab 3 Worksheet

D. Lab 4 – Testing your plan and using a feedback loop to future proof your response

    1. Identifying metrics and implementing a feedback loop
    2. Lab 4 Worksheet

E. Lab 5 – Drafting General Security Policies

    1. Acceptable Use Policy

F. Lab 6 – Practicing Different Attack Vectors

    1. Brute Force
    2. Command Injection

G. Lab 7 – Deploy GRR Client and Gather Evidence

    1. Deploy GRR Client
    2. Gather Evidence from our GRR Client

H. Lab 8 – Creating Request Tracker Workflow

    1. Request Tracker
    2. Request Tracker for Incident Response

I. Lab 9 – Lessons Learned and Documentation

    1. Lessons Learned Presentation

J. Lab 10 – Creating an Incident Handling Checklist

    1. Create a Checklist

K. Lab 11 – Drafting Incident Response Recommendations for Improvements

    1. Create a Memo for Improvements and Changes

L. Lab 12 – Sharing Agreements and Reporting Requirements

    1. Questions about your organization's information sharing