Certified Incident Handling Engineer

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 $91,546 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
Module 2 - Policy, Plan & Procedure
Module 3 - Team Structure
Module 4 - Team Services
Module 5 - Recommendations
Module 6 - Preparation
Module 7 - Detection and Analysis
Module 8 - Contain, Eradicate, and Recover
Module 9 - GRR Rapid Response
Module 10 - Request Tracker
Module 11 - Post Incident Activity
Module 12 - Checklist
Module 13 - Incident Handling Recommendations
Module 14 - Coordination and Information Sharing

Hands-On Labs

Lab 1: Identifying Incident Triggers
Lab 2: Drafting Incident Response Procedures
Lab 3: Planning for Dependencies
Lab 4: Testing your plan
Lab 5: Acceptable Use Policy
Lab 6: Practicing Attack Vectors
Lab 7: Deploy GRR Client
Lab 8: Create Request Tracker Workflow
Lab 9: GRR Rapid Response
Lab 10: Create a Checklist
Lab 11: Drafting Response Improvement Recommendations
Lab 12: Sharing Agreements

Certified Incident Handling Engineer

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

Chapter 1: Incident Handling Explained

Section 1 - Introduction
Section 2 – What is an Incident?
Section 3 – What is Incident Handling?
Section 4 – Difference Between IH and IR
Section 5 – The Incident Response Process
Section 6 – Seven Reasons You Must Put Together an Incident Response Plan
Section 7 – How to Build an Effective Incident Response Team
Section 8 – Considerations for Creating an Incident Response Team
Section 9 – Tips for Incident Response Team Members

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

Section 1 - Introduction
Section 2 – Incident Response Policy
Section 3 – Incident Response Plan
Section 3 – Incident Response Procedures
Section 5 – Sharing Information with Outside Parties

Chapter 3: Incident Response Team Structure

Section 1 - Introduction
Section 2 – Team Models
Section 3 – Team Model Selection
Section 4 – Incident Response Personnel
Section 5 – Dependencies within Organizations

Chapter 4: Incident Response Team Services

Section 1 - Introduction
Section 2 – Intrusion Detection
Section 3 – Advisory Distribution
Section 4 – Education and Awareness
Section 5 – Information Sharing

Chapter 11: Post-Incident Activity

Section 1 - Introduction
Section 2 – Lessons Learned
Section 3 – Using Collected Incident Data
Section 4 – Evidence Retention

Chapter 12: Incident Handling Checklist

Section 1 - Introduction
Section 2 - Building Checklists

Chapter 13: Incident Handling Recommendation

Section 1 - Introduction
Section 2 - Recommendations

Chapter 14: Coordination and Information Sharing

a. Section 1 - Introduction
b. Section 2 - Coordination
c. Section 3 – Information Sharing Techniques
d. Section 4 – Granular Information Sharing
e. Section 5 – 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