Certified Incident Handling

Description:

The C)IHE - Certified Incident Handling Engineer course, is designed to help Incident Handlers, System Administrators, and Security Engineers understand how to plan, create, and utilize their systems to prevent, detect, and respond to attacks through the use of mile2's live hands-on Cyber Range.

Mile 2 C)IHE strictly follows NIST's 800-61 to identify the four phases of incident response: (1) preparation for a cybersecurity incident, (2) detection and analysis of a security incident, (3) containment, eradication, and recovery, and (4) post-incident analysis. With C)IHE's in-depth certification training, the student will learn to develop start-to-finish processes for establishing an incident-handling team, strategizing for potential attack types, recovering from attacks, and much more.

Annual Salary **$91,546**

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.

Module 01: Incident Handling Explained
Module 02: Incident Response Policy, Plan and Procedure Creation
Module 03: Incident Response Team Structure
Module 04: Incident Response Team Services
Module 05: Incident Response Recommendations
Module 06: Preparation
Module 07: Detection and Analysis
Module 08: Containment, Eradication and Recovery
Module 09: Post Incident Activity
Module 10: Incident Handling Checklist
Module 11: Incident Handling Recommendations
Module 12: Coordination and Information Sharing

Lab 01: Identifying Incident Triggers
Lab 02: Drafting Incident Response Procedures
Lab 03: Identifying and Planning for Your Dependencies
Lab 04: Testing Your Plan and Using a Feedback Loop to Future Proof Your Response
Lab 05: Drafting General Security Policies
Lab 06: Leveraging SIEM for Advanced Analytics
Lab 07: Use Velociraptor and Gather Evidence
Lab 08: Creating Request Tracker Workflow
Lab 09: Lessons Learned and Documentation
Lab 10: Creating and Incident Handling Checklist
Lab 11: Drafting Incident Response Recommendations for Improvements
Lab 12: Sharing Agreements and Reporting Requirements

Upon Completion

Upon completion, Certified Incident Handling Engineer students will know NIST's 800-61 four incident handling phases, be able to accurately report on their findings, and be ready to sit for the C)IHE 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 coursesassociated with it at www.mile2.com.

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

Answer: Yes.

Question: Are Mile2 courses transferable/shareable?

Answer: No. The course materials, videos, and exams arenot meant to be shared or transferred.

Course and Certification Learning

Detailed Outline

Module 00: Course Introduction

Module 01: 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

Module 02: Incident Response Policy, Plan and Procedure Creation

Section 1: Introduction
Section 2: Incident Response Policy
Section 3: Incident Response Plan
Section 4: Incident Response Procedures
Section 5: Sharing Information with Outside Parties

Module 03: 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

Module 04: Incident Response Team Services

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

Module 05: Incident Response Recommendations

Section 1: Introduction
Section 2: Establish a formal Incident Response Capability
Section 3: Establish Information Sharing Capabilities
Section 4: Building an Incident Response Team

Chapter 06: Preparation

Section 1: Introduction
Section 2: Threat Hunting
Section 3: Threat Analysis Frameworks
Section 4: Tools and Toolkits
Section 5: Policy
Section 6: Procedures

Section 7: Preventing Incidents

Module 07: Detection and Analysis

Section 1: Attack Vectors

Section 2: Signs of an Incident

Section 3: Sources of Precursors and Indicators

Section 4: Incident Analysis

Section 5: Incident Documentation

Section 6: Incident Prioritization

Section 7: Incident Notification

Module 08: Containment, Eradication and Recovery

Section 1: Selecting the Right Containment Strategy

Section 2: Gathering and Handling Evidence

Section 3: Identifying the Attacking Hosts

Section 4: Eradication and Recovery

Module 09: Post Incident Activity

Section 1: Introduction

Section 2: Lessons Learned

Section 3: Using Collected Incident Data

Section 4: Evidence Retention

Module 10: Incident Handling Checklist

Section 1: Introduction

Section 2: Building Checklists

Module 11: Incident Handling Recommendations

Section 1: Introduction

Section 2: Recommendations

Section 3: Implement Threat Intel

Module 12: Coordination and Information Sharing

Section 1: Introduction

Section 2: Coordination

Section 3: Purple Teaming

Section 4: Information Sharing Techniques

Section 5: Granular Information Sharing

Section 6: Sharing Recommendations