EC-Council Certified Incident Handler

Learn via: **Classroom/AFA**

Duration: **3 Day**

Overview

The EC-Council Certified Incident Handler (ECIH) program 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 policies related to incident handling. After attending this course, they will be able to create incident handling and response policies as well as deal with various types of computer security incidents.
The IT incident management training program will enable students to be proficient in handling and responding to various security incidents such as network security incidents, malicious code incidents, and insider attack threats. In addition, students will learn about computer forensics and its role in handling and responding to incidents. The course also covers incident response teams, incident management training methods, and incident recovery techniques in detail.
The ECIH certification will provide professionals greater industry acceptance as the seasoned incident handler.
Target Audience
This course will significantly benefit incident handlers, risk assessment administrators, penetration testers, cyber forensic investigators, vulnerability assessment auditors, system administrators, system engineers, firewall administrators, network managers, IT managers, IT professionals and anyone who is interested in incident handling and response.

Training Outline

Module 01: Introduction to Incident Response and Handling

- Cyber Incident Statistics
- Computer Security Incident
- Information as Business Asset
- Data Classification
- Common Terminologies
- Information Warfare
- Key Concepts of Information Security
- Vulnerability, Threat, and Attack
- Types of Computer Security Incidents
- Examples of Computer Security Incidents
- Verizon Data Breach Investigations Report – 2008
- Incidents That Required the Execution of Disaster Recovery Plans
- Signs of an Incident
- Incident Categories
- Incident Categories: Low Level
- Incident Categories: Middle Level
- Incident Categories: High Level

    Incident Prioritization
    Incident Response
    Incident Handling

- Use of Disaster Recovery Technologies
- Impact of Virtualization on Incident Response and Handling
- Estimating Cost of an Incident
- Key Findings of Symantec Global Disaster Recovery Survey - 2009
- Incident Reporting
- Incident Reporting Organizations
- Vulnerability Resources

Module 02: Risk Assessment

- Risk
- Risk Policy

- Risk Assessment
- NIST's Risk Assessment Methodology

    Step 1: System Characterization
    Step 2: Threats Identification
    Step 3: Identify Vulnerabilities
    Step 4: Control Analysis
    Step 5: Likelihood Determination
    Step 6: Impact Analysis
    Step 7: Risk Determination
    Step 8: Control Recommendations
    Step 9: Results Documentation

- Steps to Assess Risks at Work Place

    Step 1: Identify Hazard
    Step 2: Determine Who Will be Harmed and How
    Step 3: Analyze Risks and Check for Precautions
    Step 4: Implement Results of Risk Assessment
    Step 5: Review Risk Assessment

- Risk Analysis

    Need for Risk Analysis
    Risk Analysis: Approach

- Risk Mitigation

    Risk Mitigation Strategies

- Cost/Benefit Analysis
- NIST Approach for Control Implementation
- Residual Risk
- Risk Management Tools

    CRAMM
    Acuity STREAM
    Callio Secura 17799
    EAR / Pilar

Module 03: Incident Response and Handling Steps

- How to Identify an Incident
- Handling Incidents
- Need for Incident Response
- Goals of Incident Response
- Incident Response Plan

    Purpose of Incident Response Plan
    Requirements of Incident Response Plan
    Preparation

- Incident Response and Handling Steps

    Step 1: Identification
    Step 2: Incident Recording
    Step 3: Initial Response
    Step 4: Communicating the Incident
    Step 5: Containment
    Step 6: Formulating a Response Strategy
    Step 7: Incident Classification
    Step 8: Incident Investigation
    Step 9: Data Collection
    Step 10: Forensic Analysis
    Step 11: Evidence Protection
    Step 12: Notify External Agencies
    Step 13: Eradication
    Step 14: Systems Recovery
    Step 15: Incident Documentation
    Step 16: Incident Damage and Cost Assessment
    Step 17: Review and Update the Response Policies

- Training and Awareness
- Security Awareness and Training Checklist
- Incident Management

Purpose of Incident Management
Incident Management Process
Incident Management Team

- Incident Response Team

Incident Response Team Members
Incident Response Team Members Roles and Responsibilities
Developing Skills in Incident Response Personnel
Incident Response Team Structure
Incident Response Team Dependencies
Incident Response Team Services

- Defining the Relationship between Incident Response, Incident Handling, and Incident Management

Incident Response Best Practices
Incident Response Policy
Incident Response Plan Checklist
Incident Handling System: RTIR
RPIER 1st Responder Framework

Module 04: CSIRT

- What is CSIRT?
- What is the Need of an Incident Response Team (IRT)
- CSIRT Goals and Strategy
- CSIRT Vision
- Common Names of CSIRT
- CSIRT Mission Statement
- CSIRT Constituency
- CSIRT Place in the Organization
- CSIRT Relationship with Peers
- Types of CSIRT Environments
- Best Practices for creating a CSIRT

Step 1: Obtain Management Support and Buy-in
Step 2: Determine the CSIRT Development Strategic Plan
Step 3: Gather Relevant Information
Step 4: Design your CSIRT Vision
Step 5: Communicate the CSIRT Vision
Step 6: Begin CSIRT Implementation
Step 7: Announce the CSIRT
Step 8: Evaluate CSIRT Effectiveness

- Role of CSIRTs
- Roles in an Incident Response Team
- CSIRT Services

Reactive Services
Proactive Services
Security Quality Management Services

- CSIRT Policies and Procedures

Attributes
Content
Validity
Implementation, Maintenance, and Enforcement

- How CSIRT Handles a Case
- CSIRT Incident Report Form
- Incident Tracking and Reporting Systems

Application for Incident Response Teams (AIRT)
BMC Remedy Action Request System
PGP Desktop Email
The GNU Privacy Guard (GnuPG)
Listserv

- CERT
- CERT-CC
- CERT(R) Coordination Center: Incident Reporting Form
- CERT:OCTAVE

OCTAVE Method
OCTAVE-S

OCTAVE Allegro

- World CERTs

  Australia CERT (AUSCERT)
  Hong Kong CERT (HKCERT/CC)
  Indonesian CSIRT (ID-CERT)
  Japan CERT-CC (JPCERT/CC)
  Malaysian CERT (MyCERT)
  Pakistan CERT (PakCERT)
  Singapore CERT (SingCERT)
  Taiwan CERT (TWCERT)
  China CERT (CNCERT/CC)
  US-CERT
  Government Forum of Incident Response and Security Teams (GFIRST)
  Canadian CERT
  Forum of Incident Response and Security Teams
  CAIS/RNP
  NIC BR Security Office Brazilian CERT
  EuroCERT
  FUNET CERT
  SURFnet-CERT
  DFN-CERT
  JANET-CERT
  CERT POLSKA
  Swiss Academic and Research Network CERT

- http://www.first.org/about/organization/teams/
- http://www.apcert.org/about/structure/members.html
- IRTs Around the World

Module 05: Handling Network Security Incidents

- Denial-of-Service Incidents
- Distributed Denial-of-Service Attack
- Detecting DoS Attack
- Incident Handling Preparation for DoS

  DoS Response Strategies
  Preventing a DoS Incident
  Following the Containment Strategy to Stop DoS

- Unauthorized Access Incident

  Detecting Unauthorized Access Incident
  Incident Handling Preparation
  Incident Prevention
  Following the Containment Strategy to Stop Unauthorized Access
  Eradication and Recovery
  Recommendations

- Inappropriate Usage Incidents

  Detecting the Inappropriate Usage Incidents
  Incident Handling Preparation
  Incident Prevention
  Recommendations

- Multiple Component Incidents

  Preparation for Multiple Component Incidents
  Following the Containment Strategy to Stop Multiple Component Incidents
  Recommendations

- Network Traffic Monitoring Tools

  Ntop
  EtherApe
  Ngrep
  SolarWinds: Orion NetFlow Traffic Analyzer
  Nagios: op5 Monitor
  CyberCop Scanner

- Network Auditing Tools

Nessus
Security Administrator's Integrated Network Tool (SAINT)
Security Auditor's Research Assistant (SARA)
Nmap
Netcat
Wireshark
Argus - Audit Record Generation and Utilization System
Snort

- Network Protection Tools

Iptables
Proventia Network Intrusion Prevention System (IPS)
NetDetector
TigerGuard

Module 06: Handling Malicious Code Incidents

- Count of Malware Samples
- Virus
- Worms
- Trojans and Spywares
- Incident Handling Preparation
- Incident Prevention
- Detection of Malicious Code
- Containment Strategy
- Evidence Gathering and Handling
- Eradication and Recovery
- Recommendations
- Antivirus Systems

Symantec: Norton AntiVirus 2009
Kaspersky Anti-Virus 2010
AVG Anti-Virus
McAfee VirusScan Plus
BitDefender Antivirus 2009
F-Secure Anti-Virus 2009
Trend Micro AntiVirus plus AntiSpyware 2009
HijackThis
Tripwire Enterprise
Stinger

Module 07: Handling Insider Threats

- Insider Threats
- Anatomy of an Insider Attack
- Insider Risk Matrix
- Insider Threats Detection
- Insider Threats Response
- Insider's Incident Response Plan
- Guidelines for Detecting and Preventing Insider Threats

Human Resources
Network Security
Access Controls
Security Awareness Program
Administrators and Privileged Users
Backups

- Audit Trails and Log Monitoring
- Employee Monitoring Tools

Activity Monitor
Net Spy Pro
Spector Pro
SpyAgent
Handy Keylogger
Anti Keylogger
Actual Spy
IamBigBrother
007 Spy Software
SpyBuddy
SoftActivity Keylogger
Elite Keylogger
Spy Sweeper

Module 08: Forensic Analysis and Incident Response

- Computer Forensics
- Objectives of Forensics Analysis
- Role of Forensics Analysis in Incident Response
- Forensic Readiness
- Forensic Readiness And Business Continuity
- Types of Computer Forensics
- Computer Forensic Investigator
- People Involved in Computer Forensics
- Computer Forensics Process
- Digital Evidence
- Characteristics of Digital Evidence
- Collecting Electronic Evidence
- Challenging Aspects of Digital Evidence
- Forensic Policy
- Forensics in the Information System Life Cycle
- Forensic Analysis Guidelines
- Forensics Analysis Tools

    Helix

    - Tools Present in Helix CD for Windows Forensics

    Windows Forensic Toolchest
    Knoppix Linux
    The Coroner's Toolkit (TCT)
    EnCase Forensic
    THE FARMER'S BOOT CD (FBCD)
    DumpReg
    DumpSec
    DumpEvt
    Foundstone Forensic ToolKit
    Sysinternals Suite
    NSLOOKUP
    dig – DNS Lookup Utility
    Whois
    VisualRoute
    Netstat Command
    Linux: DD Command
    Linux: Find Command
    Linux: Arp Command
    Linux: ps, ls, lsof, and ifconfig Commands
    Linux: Top Command
    Linux: Grep Command
    Linux: Strings Command

Module 09: Incident Reporting

- Incident Reporting
- Why to Report an Incident
- Why Organizations do not Report Computer Crimes
- Whom to Report an Incident
- How to Report an Incident
- Details to be Reported
- Preliminary Information Security Incident Reporting Form
- CERT Incident Reference Numbers
- Contact Information

    Sample Report Showing Contact Information

- Summary of Hosts Involved

    Sample Report Showing Summary of Hosts Involved

- Description of the Activity

    Sample Report Showing Description of the Activity

- Log Extracts Showing the Activity

    Example Showing the Log Extracts of an Activity

- Time Zone
- Federal Agency Incident Categories

- Organizations to Report Computer Incident

    United State Internet Crime Task Force
    Internet Crime Complaint Center (IC3)
    Computer Crime & Intellectual Property Section
    Internet Watch Foundation (IWF)

- Incident Reporting Guidelines
- Sample Incident Reporting Form
- Sample Post Incident Report Form

Module 10: Incident Recovery

- Incident Recovery
- Principles of Incident Recovery
- Incident Recovery Steps
- Contingency/Continuity of Operations Planning
- Business Continuity Planning
- Incident Recovery Plan
- Incident Recovery Planning Process

    Incident Recovery Planning Team
    Business Impact Analysis
    Incident Recovery Plan Implementation
    Incident Recovery Training
    Incident Recovery Testing

Module 11: Security Policies and Laws

- Security Policy
- Key Elements of Security Policy
- Goals of a Security Policy
- Characteristics of a Security Policy
- Design of Security Policy
- Implementing Security Policies
- Acceptable Use Policy (AUP)
- Access Control Policy

    Sample Access Control Policy
    Importance of Access Control Policies

- Asset Control Policy
- Audit Trail Policy

    Sample Audit Trail Policy 1
    Importance of Audit Trail Policy

- Logging Policy

    Importance of Logging Policies

- Documentation Policy
- Evidence Collection Policy
- Evidence Preservation Policy
- Information Security Policy

    Information Security Policy: University of California
    Information Security Policy: Pearce & Pearce, Inc.
    Importance of Information Security Policy

- National Information Assurance Certification & Accreditation Process (NIACAP) Policy

    Importance of NIACAP Policy

- Physical Security Policy

    Sample Physical Security Policy 1
    Sample Physical Security Policy 2
    Importance of Physical Security Policies

- Physical Security Guidelines
- Personnel Security Policies & Guidance
- Law and Incident Handling

    Role of Law in Incident Handling
    Legal Issues When Dealing With an Incident
    Law Enforcement Agencies

- Laws and Acts

  Searching and Seizing Computers without a Warrant

  - A: Fourth Amendment's "Reasonable Expectation of Privacy" in Cases Involving Computers: General Principles
  - A.4: Private Searches

  The Privacy Protection Act
  Federal Information Security Management Act (FISMA)
  Mexico
  Brazilian Laws
  Canadian Laws
  United Kingdom's Laws
  Belgium Laws
  German Laws
  Italian Laws
  Cybercrime Act 2001
  Information Technology Act
  Singapore Laws
  Sarbanes-Oxley Act
  Social Security Act
  Gramm-Leach-Bliley Act
  Health Insurance Portability and Accountability Act (HIPAA)

- Intellectual Property Laws

  Intellectual Property
  US Laws for Trademarks and Copyright
  Australia Laws For Trademarks and Copyright
  UK Laws for Trademarks and Copyright
  China Laws for Trademarks and Copyright
  Indian Laws for Trademarks and Copyright
  Japanese Laws for Trademarks and Copyright
  Canada Laws for Trademarks and Copyright
  South African Laws for Trademarks and Copyright
  South Korean Laws for Trademarks and Copyright
  Belgium Laws for Trademarks and Copyright
  Hong Kong Laws for Intellectual Property