# EC-Council Certified Incident Handler ( ECIH )

## Course Summary

### Description

The EC-Council Certified Incident Handler 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 policy related to incident handling. After attending the course, they will be able to create incident handling and response policies and deal with various types of computer security incidents. The comprehensive training program will make students proficient in handling and responding to various security incidents such as network security incidents, malicious code incidents and insider attack threats.

In addition, the students will learn about computer forensics and its role in handling and responding to incidents. The course also covers incident response teams, incident reporting methods and incident recovery techniques in detail.

The ECIH certification will provide professionals greater industry acceptance as the seasoned incident handler.

### Topics

- Introduction to Incident Response and Handling
- Risk Assessment
- Incident Response and Handling Steps
- CSIRT
- Handling Network Security Incidents
- Handling Malicious Code Incidents
- Handling Insider Threats
- Forensic Analysis and Incident Response
- Incident Reporting
- Incident Recovery
- Security Policies and Laws

### Audience

This course will significantly benefit incident handlers, risk assessment administrators, penetration testers, cyber forensic investigators, venerability assessment auditors, system administrators, system engineers, firewall administrators, network managers, IT managers, IT professionals and anyone who is interested in incident handling and response.

### Prerequisites

There are no prerequisites for this course.

### Duration

Two days

# EC-Council Certified Incident Handler

## Course Outline

**I. Introduction to Incident Response and Handling**
- A. Cyber Incident Statistics
- B. Computer Security Incident
- C. Information as Business Asset
- D. Data Classification
- E. Common Terminologies
- F. Information Warfare
- G. Key Concepts of Information Security
- H. Vulnerability, Threat, and Attack
- I. Types of Computer Security Incidents
- J. Examples of Computer Security Incidents
- K. Verizon Data Breach Investigations Report – 2008
- L. Incidents That Required the Execution of Disaster Recovery Plans
- M. Signs of an Incident
- N. Incident Categories
  1. Incident Categories: Low Level
  2. Incident Categories: Middle Level
  3. Incident Categories: High Level
- O. Incident Prioritization
- P. Incident Response
- Q. Incident Handling
- R. Use of Disaster Recovery Technologies
- S. Impact of Virtualization on Incident Response and Handling
- T. Estimating Cost of an Incident
- U. Symantec Global Disaster Recovery Survey – 2009
- V. Key Findings of
- W. Incident Reporting
- X. Incident Reporting Organizations
- Y. Vulnerability Resources

**II. Risk Assessment**
- A. Risk
- B. Risk Policy
- C. Risk Assessment
- D. NIST's Risk Assessment Methodology
  1. Step 1: System Characterization
  2. Step 2: Threats Identification
  3. Step 3: Identify Vulnerabilities
  4. Step 4: Control Analysis
  5. Step 5: Likelihood Determination
  6. Step 6: Impact Analysis
  7. Step 7: Risk Determination
  8. Step 8: Control Recommendations
  9. Step 9: Results Documentation
- E. Steps to Assess Risks at Work Place
  1. Step 1: Identify Hazard
  2. Step 2: Determine Who Will be Harmed and How
  3. Step 3: Analyze Risks and Check for Precautions
  4. Step 4: Implement Results of Risk Assessment
  5. Step 5: Review Risk Assessment
- F. Risk Analysis
  1. Need for Risk Analysis
  2. Risk Analysis: Approach
- G. Risk Mitigation
  1. Risk Mitigation Strategies
- H. Cost/Benefit Analysis
- I. NIST Approach for Control Implementation
- J. Residual Risk
- K. Risk Management Tools
  1. CRAMM
  2. Acuity STREAM
  3. Callio Secura 17799
  4. EAR / Pilar

**III. Incident Response and Handling Steps**
- A. How to Identify an Incident
- B. Handling Incidents
- C. Need for Incident Response
- D. Goals of Incident Response
- E. Incident Response Plan
  1. Purpose of Incident Response Plan
  2. Requirements of Incident Response Plan
  3. Preparation
- F. Incident Response and Handling Steps
  1. Step 1: Identification
  2. Step 2: Incident Recording
  3. Step 3: Initial Response
  4. Step 4: Communicating the Incident
  5. Step 5: Containment
  6. Step 6: Formulating a Response Strategy
  7. Step 7: Incident Classification
  8. Step 8: Incident Investigation
  9. Step 9: Data Collection
  10. Step 10: Forensic Analysis
  11. Step 11: Evidence Protection
  12. Step 12: Notify External Agencies
  13. Step 13: Eradication
  14. Step 14: Systems Recovery
  15. Step 15: Incident Documentation
  16. Step 16: Incident Damage and Cost Assessment

# EC-Council Certified Incident Handler

## Course Outline (con't)

17. Step 17: Review and Update the Response Policies

G. Training and Awareness
H. Security Awareness and Training Checklist
I. Incident Management
   1. Purpose of Incident Management
   2. Incident Management Process
   3. Incident Management Team
J. Incident Response Team
   1. Incident Response Team Members
   2. Incident Response Team Members Roles and Responsibilities
   3. Developing Skills in Incident Response Personnel
   4. Incident Response Team Structure
   5. Incident Response Team Dependencies
   6. Incident Response Team Services
K. Defining the Relationship between Incident Response, Incident Handling and Incident Management
L. Incident Response Best Practices
M. Incident Response Policy
N. Incident Response Plan Checklist
O. Incident Handling System: RTIR
P. RPIER 1st Responder Framework

**IV. CSIRT**

A. What is CSIRT?
B. What is the Need of an Incident Response Team (IRT)
C. CSIRT Goals and Strategy
D. CSIRT Vision
E. Common Names of CSIRT
F. CSIRT Mission Statement
G. CSIRT Constituency
H. CSIRT Place in the Organization
I. CSIRT Relationship with Peers
J. Types of CSIRT Environments
K. Best Practices for creating a CSIRT
   1. Step 1: Obtain Management Support and Buy-in
   2. Step 2: Determine the CSIRT Development Strategic Plan
   3. Step 3: Gather Relevant Information
   4. Step 4: Design your CSIRT Vision
   5. Step 5: Communicate the CSIRT Vision
   6. Step 6: Begin CSIRT Implementation
   7. Step 7: Announce the CSIRT
   8. Step 8: Evaluate CSIRT Effectiveness
L. Role of CS IRTs
M. Roles in an Incident Response Team
N. CSIRT Services
   1. Reactive Services
   2. Proactive Services
   3. Security Quality Management Services
O. CSIRT Policies and Procedures
   1. Attributes
   2. Content
   3. Validity
   4. Implementation, Maintenance and Enforcement
P. How CSIRT Handles a Case
Q. CSIRT Incident Report Form
R. Incident Tracking and Reporting Systems
   1. Application for Incident Response Teams (AIRT)
   2. BMC Remedy Action Request System
   3. PGP Desktop Email
   4. The GNU Privacy Guard (GnuPG)
   5. Listserv
S. CERT
T. CERT-CC
U. CERT(R) Coordination Center: Incident Reporting Form
V. CERT:OCTAVE
   1. OCTAVE Method
   2. OCTAVE-S
   3. OCTAVE Allegro
W. World CERTs
   1. Australia CERT (AUSCERT)
   2. Hong Kong CERT (HKCERT/CC)
   3. Indonesian CSIRT (ID-CERT)
   4. Japan CERT-CC (JPCERT/CC)
   5. Malaysian CERT (MyCERT)
   6. Pakistan CERT (PakCERT)
   7. Singapore CERT (SingCERT)
   8. Taiwan CERT (TWCERT)
   9. China CERT (CNCERT/CC)
   10. Government Forum of Incident Response and Security Teams (GFIRST)
   11. Canadian CERT
   12. Forum of Incident Response and Security Teams
   13. CAIS/RNP
   14. NIC BR Security Office Brazilian CERT
   15. EuroCERT
   16. FUNET CERT
   17. SURFnet-CERT

# EC-Council Certified Incident Handler

## Course Outline (con't)

18. DFN-CERT
19. JANET-CERT
20. CERT POLSKA
21. Swiss Academic and Research Network CERT

X. http://www.first.org/about/organization/teams/
Y. http://www.apcert.org/about/structure/members.html
Z. IRTs around the World

**V. Handling Network Security Incidents**

A. Denial-of-Service Incidents
B. Distributed Denial-of-Service Attack
C. Detecting DoS Attack
D. Incident Handling Preparation for DoS
   1. DoS Response Strategies
   2. Preventing a DoS Incident
   3. Following the Containment Strategy to Stop DoS
E. Unauthorized Access Incident
   1. Detecting Unauthorized Access Incident
   2. Incident Handling Preparation
   3. Incident Prevention
   4. Following the Containment Strategy to Stop Unauthorized Access
   5. Eradication and Recovery
   6. Recommendations
F. Inappropriate Usage Incidents
   1. Detecting the Inappropriate Usage Incidents
   2. Incident Handling Preparation
   3. Incident Prevention
   4. Recommendations
G. Multiple Component Incidents
   1. Preparation for Multiple Component Incidents
   2. Following the Containment Strategy to Stop Multiple Component Incidents
   3. Recommendations
H. Network Traffic Monitoring Tools
   1. Ntop
   2. EtherApe
   3. Ngrep
   4. SolarWinds: Orion NetFlow Traffic Analyzer
   5. Nagios: op5 Monitor
   6. CyberCop Scanner
I. Network Auditing Tools
   1. Nessus
   2. Security Administrator's Integrated Network Tool (SAINT)
   3. Security Auditor's Research Assistant (SARA)
   4. Nmap
   5. Netcat
   6. Wireshark
   7. Argus - Audit Record Generation and Utilization System
   8. Snort
J. Network Protection Tools
   1. Iptables
   2. Proventia Network Intrusion Prevention System (IPS)
   3. NetDetector
   4. TigerGuard

**VI. Handling Malicious Code Incidents**

A. Count of Malware Samples
B. Virus
C. Worms
D. Trojans and Spywares
E. Incident Handling Preparation
F. Incident Prevention
G. Detection of Malicious Code
H. Containment Strategy
I. Evidence Gathering and Handling
J. Eradication and Recovery
K. Recommendations
L. Antivirus Systems
   1. Symantec: Norton AntiVirus 2009
   2. Kaspersky Anti-Virus 2010
   3. AVG Anti-Virus
   4. McAfee VirusScan Plus
   5. BitDefender Antivirus 2009
   6. F-Secure Anti-Virus 2009
   7. Trend Micro AntiVirus plus AntiSpyware 2009
   8. HijackThis
   9. Tripwire Enterprise
   10. Stinger

**VII. Handling Insider Threats**

A. Insider Threats
B. Anatomy of an Insider Attack
C. Insider Risk Matrix
D. Insider Threats Detection
E. Insider Threats Response
F. Insider's Incident Response Plan
G. Guidelines for Detecting and Preventing Insider Threats

# EC-Council Certified Incident Handler

## Course Outline (con't)

1. Human Resources
2. Network Security
3. Access Controls
4. Security Awareness Program
5. Administrators and Privileged Users
6. Backups
7. Audit Trails and Log Monitoring

H. Employee Monitoring Tools
1. Activity Monitor
2. Net Spy Pro
3. Spector Pro
4. SpyAgent
5. Handy Keylogger
6. Anti Keylogger
7. Actual Spy
8. IamBigBrother
9. 007 Spy Software
10. SpyBuddy
11. SoftActivity Keylogger
12. Elite Keylogger
13. Spy Sweeper

**VIII. Forensic Analysis and Incident Response**
A. Computer Forensics
B. Objectives of Forensics Analysis
C. Role of Forensics Analysis in Incident Response
D. Forensic Readiness
E. Forensic Readiness and Business Continuity
F. Types of Computer Forensics
G. Computer Forensic Investigator
H. People Involved in Computer Forensics
I. Computer Forensics Process
J. Digital Evidence
K. Characteristics of Digital Evidence
L. Collecting Electronic Evidence
M. Challenging Aspects of Digital Evidence
N. Forensic Policy
O. Forensics in the Information System Life Cycle
P. Forensic Analysis Guidelines
Q. Forensics Analysis Tools
1. Helix
2. Tools Present in Helix CD for Windows Forensics
3. Windows Forensic Toolchest
4. Knoppix Linux
5. The Coroner's Toolkit (TCT)
6. EnCase Forensic
7. THE FARMER'S BOOT CD (FBCD)
8. DumpReg
9. DumpSec
10. DumpEvt
11. Foundstone Forensic ToolKit
12. Sysinternals Suite
13. SLOOKUP
14. dig – DNS Lookup Utility
15. Whois
16. VisualRoute
17. Netstat Command
18. Linux: DD Command
19. Linux: Find Command
20. Linux: Arp Command
21. Linux: ps, ls, lsof, and ifconfig Commands
22. Linux: Top Command
23. Linux: Grep Command
24. Linux: Strings Command

**IX. Incident Reporting**
A. Incident Reporting
B. Why to Report an Incident
C. Why Organizations do not Report Computer Crimes
D. Whom to Report an Incident
E. How to Report an Incident
F. Details to be Reported
G. Preliminary Information Security Incident Reporting Form
H. CERT Incident Reference Numbers
I. Contact Information
1. Sample Report Showing Contact Information
J. Summary of Hosts Involved
1. Sample Report Showing Summary of Hosts Involved
K. Description of the Activity
1. Sample Report Showing Description of the Activity
L. Log Extracts Showing the Activity
1. Example Showing the Log Extracts of an Activity
M. Time Zone
N. Federal Agency Incident Categories
O. Organizations to Report Computer Incident
1. United State Internet Crime Task Force
2. Internet Crime Complaint Center (IC3)
3. Computer Crime & Intellectual Property Section
4. Internet Watch Foundation (IWF)

# EC-Council Certified Incident Handler

## Course Outline (con't)

P. Incident Reporting Guidelines
Q. Sample Incident Reporting Form
R. Sample Post Incident Report Form

**X. Incident Recovery**
A. Incident Recovery
B. Principles of Incident Recovery
C. Incident Recovery Steps
D. Contingency/Continuity of Operations Planning
E. Business Continuity Planning
F. Incident Recovery Plan
G. Incident Recovery Planning Process
1. Incident Recovery Planning Team
2. Business Impact Analysis
3. Incident Recovery Plan Implementation
4. Incident Recovery Training
5. Incident Recovery Testing

**XI. Security Policies and Laws**
A. Security Policy
B. Key Elements of Security Policy
C. Goals of a Security Policy
D. Characteristics of a Security Policy
E. Design of Security Policy
F. Implementing Security Policies
G. Acceptable Use Policy (AUP)
H. Access Control Policy
1. Sample Access Control Policy
2. Importance of Access Control Policies
I. Asset Control Policy
J. Audit Trail Policy
1. Sample Audit Trail Policy 1
2. Importance of Audit Trail Policy
K. Logging Policy
1. Importance of Logging Policies
L. Documentation Policy
M. Evidence Collection Policy
N. Evidence Preservation Policy
O. Information Security Policy
1. Information Security Policy: University of California
2. Information Security Policy: Pearce & Pearce, Inc.
3. Importance of Information Security Policy
P. National Information Assurance Certification & Accreditation Process (NIACAP) Policy
1. Importance of NIACAP Policy
Q. Physical Security Policy
1. Sample Physical Security Policy 1
2. Sample Physical Security Policy 2
3. Importance of Physical Security Policies
R. Physical Security Guidelines
S. Personnel Security Policies & Guidance
T. Law and Incident Handling
1. Role of Law in Incident Handling
2. Legal Issues When Dealing With an Incident
3. Law Enforcement Agencies
U. Laws and Acts
1. Searching and Seizing Computers without a Warrant
2. § A: Fourth Amendment's "Reasonable Expectation of Privacy" in Cases Involving
3. Computers: General Principles
4. § A.4: Private Searches
5. The Privacy Protection Act
6. Federal Information Security Management Act (FISMA)
7. Mexico
8. Brazilian Laws
9. Canadian Laws
10. United Kingdom's Laws
11. Belgium Laws
12. German Laws
13. Italian Laws
14. Cybercrime Act 2001
15. Information Technology Act
16. Singapore Laws
17. Sarbanes-Oxley Act
18. Social Security Act
19. Gramm-Leach-Bliley Act
20. Health Insurance Portability and Accountability Act (HIPAA)
V. Intellectual Property Laws
1. Intellectual Property
2. US Laws for Trademarks and Copyright
3. Australia Laws For Trademarks and Copyright
4. UK Laws for Trademarks and Copyright
5. China Laws for Trademarks and Copyright
6. Indian Laws for Trademarks and Copyright

# EC-Council Certified Incident Handler

## Course Outline (con't)

7. Japanese Laws for Trademarks and Copyright
8. Canada Laws for Trademarks and Copyright
9. South African Laws for Trademarks and Copyright
10. South Korean Laws for Trademarks and Copyright
11. Belgium Laws for Trademarks and Copyright
12. Hong Kong Laws for Intellectual Property