Certified Incident Handler Training Course

Professional Development Training Course Outline

Category	Data Security	**Duration**	5 Days
Base Fee	$1,500 USD	**Delivery Mode**	Online / On-site Hybrid

Course Introduction

Certified Incident Handler Training Course is engineered to equip modern cybersecurity professionals with the critical skills to effectively manage the full Incident Response Lifecycle. In an era defined by advanced persistent threats (APTs), pervasive ransomware-as-a-service (RaaS), and escalating cloud security challenges, proactive defense is no longer sufficient; rapid, systematic response is the key to minimizing financial and reputational damage. Our curriculum integrates the latest Threat Intelligence and MITRE ATT&CK Framework methodologies, moving beyond foundational concepts to embrace advanced techniques like digital forensics, malware analysis, and Security Orchestration, Automation, and Response (SOAR) integration. Participants will gain the practical expertise to build, lead, and execute a high-performance Computer Security Incident Response Team (CSIRT) program that aligns with global best practices like NIST and ISO 27001.

The program emphasizes hands-on labs and real-world case studies to validate mastery of detection, containment, eradication, and recovery procedures across complex hybrid and multi-cloud environments. Graduates will be proficient in using industry-leading DFIR tools to conduct deep-dive investigations, ensuring legal and ethical evidence handling for potential litigation. By focusing on cyber resilience and post-incident root cause analysis, this certification prepares practitioners to transform security breaches from crises into opportunities for continuous improvement and a stronger Zero Trust Architecture. This training is essential for IT and security teams committed to maintaining business continuity against the sophisticated threats of 2025 and beyond.

Programme Curriculum

Certified Incident Handler Training Course

Introduction

Certified Incident Handler Training Course is engineered to equip modern cybersecurity professionals with the critical skills to effectively manage the full Incident Response Lifecycle. In an era defined by advanced persistent threats (APTs), pervasive ransomware-as-a-service (RaaS), and escalating cloud security challenges, proactive defense is no longer sufficient; rapid, systematic response is the key to minimizing financial and reputational damage. Our curriculum integrates the latest Threat Intelligence and MITRE ATT&CK Framework methodologies, moving beyond foundational concepts to embrace advanced techniques like digital forensics, malware analysis, and Security Orchestration, Automation, and Response (SOAR) integration. Participants will gain the practical expertise to build, lead, and execute a high-performance Computer Security Incident Response Team (CSIRT) program that aligns with global best practices like NIST and ISO 27001.

The program emphasizes hands-on labs and real-world case studies to validate mastery of detection, containment, eradication, and recovery procedures across complex hybrid and multi-cloud environments. Graduates will be proficient in using industry-leading DFIR tools to conduct deep-dive investigations, ensuring legal and ethical evidence handling for potential litigation. By focusing on cyber resilience and post-incident root cause analysis, this certification prepares practitioners to transform security breaches from crises into opportunities for continuous improvement and a stronger Zero Trust Architecture. This training is essential for IT and security teams committed to maintaining business continuity against the sophisticated threats of 2025 and beyond.

Course Duration

5 days

Course Objectives

Upon completion, participants will be able to:

1. Master the NIST Incident Response (IR) Lifecycle and its application in modern enterprises.
2. Execute advanced Threat Hunting techniques using cutting-edge Cyber Threat Intelligence (CTI).
3. Implement Containment Strategies for diverse threats, including ransomware and APT attacks.
4. Perform volatile and non-volatile Digital Forensics and Incident Response (DFIR) analysis on endpoints.
5. Analyze and reverse-engineer Malware Threats to identify indicators of compromise
6. Apply the MITRE ATT&CK Framework for effective adversary tracking and defensive gap analysis.
7. Handle complex security incidents within Cloud Environments
8. Develop and customize SOAR Playbooks for efficient, automated incident triage and response.
9. Investigate and mitigate threats originating from Insider Attacks and compromised credentials.
10. Ensure adherence to Legal and Regulatory Compliance during evidence gathering.
11. Conduct thorough Root Cause Analysis (RCA) and implement robust Cyber Resilience plans.
12. Build and lead an effective CSIRT/SOC team, focusing on communication and coordination.
13. Utilize AI/ML driven security tools for Automated Threat Detection and real-time anomaly analysis.

Target Audience

1. Incident Handlers / Incident Responders (Primary Audience)
2. SOC (Security Operations Center) Analysts / Engineers
3. Cyber Threat Intelligence (CTI) Analysts
4. Digital Forensics Specialists
5. Security Engineers / Administrators
6. IT/Security Managers and Team Leads
7. Vulnerability Management Professionals
8. Internal/External Security Auditors and Risk Assessors

Course Modules

Module 1: Incident Response Program Planning and Preparation

- Defining the Incident Response Policy and establishing the CSIRT/SOC structure.
- Implementing Zero Trust Architecture principles in IR planning and preventative controls.
- Integrating Cyber Threat Intelligence for proactive threat actor tracking and early warning.
- Developing and maintaining comprehensive IR Playbooks and runbooks.
- Legal, regulatory, and ethical considerations for incident handling and data breach notification.
- Case Study: The SolarWinds Supply Chain Attack.

Module 2: Detection and Analysis of Security Incidents

- Advanced techniques for log aggregation and analysis using SIEM/XDR platforms.
- Identifying Indicators of Compromise and Indicators of Attack from network and endpoint data.
- Threat Hunting methodologies to proactively search for hidden and evasive adversaries.
- Triage and prioritization using MITRE ATT&CK and risk-scoring frameworks.
- Leveraging Endpoint Detection and Response tools for deep-dive host analysis.
- Case Study: Target Data Breach.

Module 3: Containment, Eradication, and Recovery

- Implementing strategic Containment techniques
- Forensic collection of volatile and non-volatile evidence while maintaining the Chain of Custody.
- In-depth Root Cause Analysis to identify the initial vulnerability and attack path.
- Developing and executing the Eradication plan to fully remove the threat and backdoors.
- System Recovery and hardening procedures, including patch management and configuration baselines to restore Business Continuity.
- Case Study: WannaCry Ransomware Outbreak.

Module 4: Digital Forensics for Incident Handlers (DFIR)

- Introduction to Digital Forensics principles and essential DFIR toolkits
- Collecting and analyzing Disk and File System artifacts on Windows, Linux, and macOS.
- Conducting Memory Forensics to analyze live processes, hidden malware, and credential theft.
- Investigating Network Forensics using packet analysis tools like Wireshark and network telemetry.
- Cloud Forensics.
- Case Study: Colonial Pipeline Attack

Module 5: Malware Analysis and Insider Threats

- Static and Dynamic Malware Analysis techniques to understand payload and command-and-control
- Analyzing common Malware Families and their TTPs.
- Techniques for detecting and responding to sophisticated Insider Threats
- Monitoring User and Entity Behavior Analytics to flag anomalous activity and data exfiltration.
- Handling incidents involving Phishing and Business Email Compromise
- Case Study: Twitter's Internal Breach.

Module 6: Cloud and Application Security Incidents

- Understanding the Shared Responsibility Model and its impact on Cloud IR scope.
- Incident handling for SaaS and IaaS environments.

- Investigating incidents stemming from Web Application attacks
- Security best practices for securing Containerization and microservices.
- Leveraging Cloud Security Posture Management tools for continuous monitoring and IR automation.
- Case Study: Capital One Breach.

Module 7: Automation, Orchestration, and Post-Incident Activities

- Introduction to Security Orchestration, Automation, and Response platforms and their role in accelerating IR.
- Designing and implementing automated Playbooks for common alerts.
- Developing effective Post-Incident Reporting and documentation for legal and executive audiences.
- Conducting "Lessons Learned" sessions and implementing a formal Continuous Improvement plan.
- Measuring IR effectiveness using key metrics and reporting on Cyber Risk.
- Case Study: Maersk NotPetya Attack.

Module 8: Hands-On Incident Simulation and Certification Review

- Full-scale, timed Simulated Attack Scenario
- Team-based execution of the full PICERL/NIST IR process from detection to recovery.
- Practical use of command-line and GUI DFIR Tools for evidence collection and analysis.
- Role-playing and practicing executive-level Communication and Crisis Management.
- Review of core concepts, exam preparation strategies, and industry certification paths
- Case Study: Your Final Capstone Exercise.

Training Methodology

This course employs a participatory and hands-on approach to ensure practical learning, including:

- Interactive lectures and presentations.
- Group discussions and brainstorming sessions.
- Hands-on exercises using real-world datasets.
- Role-playing and scenario-based simulations.
- Analysis of case studies to bridge theory and practice.
- Peer-to-peer learning and networking.
- Expert-led Q&A sessions.
- Continuous feedback and personalized guidance.

Register as a group from 3 participants for a Discount

Send us an email: info@fineskilltrainingcenter.org or call +254769199797

Certification

Upon successful completion of this training, participants will be issued with a globally- recognized certificate.

Tailor-Made Course

We also offer tailor-made courses based on your needs.

Key Notes

a. The participant must be conversant with English.

b. Upon completion of training the participant will be issued with an Authorized Training Certificate

c. Course duration is flexible and the contents can be modified to fit any number of days.

d. The course fee includes facilitation training materials, 2 coffee breaks, buffet lunch and A Certificate upon successful completion of Training.

e. One-year post-training support Consultation and Coaching provided after the course.

f. Payment should be done at least a week before commence of the training, to Fineskill Training Center account, as indicated in the invoice so as to enable us prepare better for you.

Upcoming Scheduled Sessions

Start Date	End Date	Location	Price
23 Nov 2026	27 Nov 2026	Online	$1,000
23 Nov 2026	27 Nov 2026	Physical	$1,500
23 Nov 2026	27 Nov 2026	Physical	$3,000
23 Nov 2026	27 Nov 2026	Physical	$3,000
23 Nov 2026	27 Nov 2026	Physical	$6,000
23 Nov 2026	27 Nov 2026	Physical	$4,500
23 Nov 2026	27 Nov 2026	Physical	$6,000
23 Nov 2026	27 Nov 2026	Physical	$6,000

Ready to enroll or request a customized program? Book online or contact us:

Register Online Now

Email: info@fineskilltrainingcenter.com | Website: www.fineskilltrainingcenter.com