Certified Incident Handler (ECIH) Training Course

Professional Development Training Course Outline

Category	Defense and Security	**Duration**	10 Days
Base Fee	$3,000 USD	**Delivery Mode**	Online / On-site Hybrid

Course Introduction

The increasing complexity of cyber threats, ransomware attacks, network breaches, and digital vulnerabilities has made incident handling a mission-critical capability for organizations across all sectors. As enterprises shift to cloud-based systems, hybrid infrastructure, and interconnected digital ecosystems, the need for skilled incident handlers who can rapidly detect, contain, and mitigate security incidents has never been more urgent. Certified Incident Handler (ECIH) Training Course equips participants with advanced cybersecurity incident response skills, practical tools, and globally recognized methodologies aligned with best-practice frameworks such as NIST, ISO 27035, and industry-standard digital forensics procedures.

Through a comprehensive and highly practical learning approach, participants will gain expertise in threat identification, triage, response coordination, malware containment, recovery strategies, and reporting techniques. The training emphasizes real-world operational readiness, empowering learners to respond to cyberattacks with confidence, precision, and timely decision-making. By the end of the course, participants will be prepared to support organizational resilience, ensure cyber defense continuity, and enhance enterprise-wide security posture.

Programme Curriculum

Certified Incident Handler (ECIH) Training Course

Introduction

The increasing complexity of cyber threats, ransomware attacks, network breaches, and digital vulnerabilities has made incident handling a mission-critical capability for organizations across all sectors. As enterprises shift to cloud-based systems, hybrid infrastructure, and interconnected digital ecosystems, the need for skilled incident handlers who can rapidly detect, contain, and mitigate security incidents has never been more urgent. Certified Incident Handler (ECIH) Training Course equips participants with advanced cybersecurity incident

response skills, practical tools, and globally recognized methodologies aligned with best-practice frameworks such as NIST, ISO 27035, and industry-standard digital forensics procedures.

Through a comprehensive and highly practical learning approach, participants will gain expertise in threat identification, triage, response coordination, malware containment, recovery strategies, and reporting techniques. The training emphasizes real-world operational readiness, empowering learners to respond to cyberattacks with confidence, precision, and timely decision-making. By the end of the course, participants will be prepared to support organizational resilience, ensure cyber defense continuity, and enhance enterprise-wide security posture.

Course Objectives

1. Understand core concepts, principles, and frameworks of incident handling and response.
2. Identify and classify cybersecurity threats, vulnerabilities, and attack vectors.
3. Apply trending incident response methodologies aligned with global standards.
4. Develop effective incident detection, triage, and escalation mechanisms.
5. Implement containment, eradication, and system recovery procedures.
6. Analyze malware behavior and digital forensic evidence for incident resolution.
7. Coordinate response across technical and non-technical teams during cyber incidents.
8. Develop communication protocols for internal stakeholders and regulators.
9. Manage incident documentation, reporting, and lessons-learned processes.
10. Mitigate risks associated with ransomware, phishing, insider threats, and advanced attacks.
11. Conduct post-incident evaluation and strengthen cyber resilience strategies.
12. Utilize security tools, automation platforms, and monitoring technologies.
13. Build organizational readiness through incident response planning and simulations.

Organizational Benefits

- Stronger enterprise-wide cybersecurity resilience
- Faster detection and containment of cyber incidents
- Reduced financial and reputational damage from breaches
- Improved compliance with cybersecurity regulations
- Enhanced preparedness through structured IR plans
- Greater staff awareness and cyber hygiene culture
- Optimized use of security tools and monitoring systems
- Strengthened business continuity and disaster recovery
- Reduced downtime and operational disruptions
- Better communication and coordination during incidents

Target Audiences

- Cybersecurity analysts and security operations personnel
- IT security managers and incident response team members
- Network administrators and systems engineers
- Cyber defense and threat monitoring professionals
- Digital forensics and malware analysis teams
- Risk management officers and IT audit staff
- Security compliance and governance personnel
- Technical staff preparing for ECIH certification

Course Duration: 10 days

Course Modules

Module 1: Introduction to Incident Handling & Response

- Understand incident response fundamentals and terminology
- Review global IR frameworks and industry standards
- Classify incident types and threat categories
- Map incident lifecycle stages and responsibilities
- Identify enterprise-wide IR requirements
- Case Study: Delayed incident handling causing extended downtime

Module 2: Cyber Threat Landscape & Attack Vectors

- Examine current cyber threat trends and evolving risks
- Analyze threat actors, motivations and operational tactics
- Identify common attack vectors affecting organizations
- Assess digital assets vulnerable to compromise
- Build threat intelligence awareness
- Case Study: Multi-vector phishing attack on a financial institution

Module 3: Incident Detection & Monitoring

- Implement monitoring tools for proactive detection
- Establish alerting thresholds and triage procedures
- Analyze security logs from multiple data sources
- Identify anomalies using SIEM technologies
- Collaborate across teams for real-time response
- Case Study: Detection failure due to misconfigured SIEM alerts

Module 4: Evidence Collection & Digital Forensics

- Apply forensic principles for preserving digital evidence
- Capture volatile and non-volatile system data
- Follow chain-of-custody procedures
- Utilize forensic tools for incident analysis
- Document findings for legal or regulatory needs
- Case Study: Evidence contamination during investigation

Module 5: Incident Prioritization & Classification

- Categorize incidents based on severity and impact
- Prioritize response actions using structured criteria
- Allocate resources to critical incidents
- Establish escalation pathways and response timelines
- Coordinate communication with relevant teams
- Case Study: Misclassified incident leading to delayed response

Module 6: Containment Strategies

- Apply short-term and long-term containment actions
- Isolate compromised systems and network segments
- Prevent lateral movement of threats

- Reduce operational disruption during containment
- Implement quarantine procedures
- Case Study: Containment failure during ransomware outbreak

Module 7: Eradication & Recovery

- Remove malicious code and unauthorized access points
- Restore system integrity and verify normal operations
- Perform clean-up steps and vulnerability remediation
- Validate patching, configuration, and hardened systems
- Reintegrate recovered assets into production
- Case Study: Reinfection due to incomplete eradication

Module 8: Malware Analysis Fundamentals

- Understand malware types and common behaviors
- Analyze malicious patterns and indicators
- Use automated and manual malware analysis techniques
- Identify persistence mechanisms and payloads
- Share findings with response teams for mitigation
- Case Study: Malware variant bypassing traditional antivirus tools

Module 9: Network Security Incident Handling

- Investigate network intrusions and anomalous traffic
- Respond to DDoS, man-in-the-middle, and port-scanning attacks
- Implement network-level containment and filtering
- Monitor packets and analyze network logs
- Secure communication channels and protocols
- Case Study: Large-scale DDoS attack reducing service availability

Module 10: Web Application Incident Handling

- Identify vulnerabilities within web applications
- Respond to SQL injection, XSS and session hijacking
- Secure APIs, authentication, and web-based systems
- Monitor application logs for suspicious activity
- Implement secure coding and patching practices
- Case Study: Web app breach exposing sensitive user data

Module 11: Email & Social Engineering Incident Handling

- Recognize phishing, spear phishing and CEO fraud
- Establish secure email filtering and verification controls
- Respond to compromised email accounts
- Train staff to detect social engineering attempts
- Implement standardized reporting procedures
- Case Study: Social engineering attack compromising credentials

Module 12: Insider Threat Incident Handling

- Identify behaviors associated with internal malicious activity

- Monitor access privileges and sensitive data handling
- Respond to data exfiltration and policy violations
- Conduct user behavior analytics and monitoring
- Implement role-based access governance
- Case Study: Insider theft of customer data

Module 13: Cloud Incident Handling

- Address cloud-specific threat vectors and vulnerabilities
- Investigate unauthorized access in cloud environments
- Implement cloud-native monitoring and detection tools
- Apply shared responsibility principles for cloud security
- Respond to misconfigured cloud resources
- Case Study: Cloud storage misconfiguration exposing data

Module 14: Incident Documentation & Reporting

- Prepare structured incident reports for leadership
- Record timelines, actions, and recovery processes
- Maintain regulatory and audit-ready documentation
- Use templates for consistent reporting
- Ensure records support legal and compliance needs
- Case Study: Incomplete documentation causing audit challenges

Module 15: Post-Incident Analysis & Continuous Improvement

- Conduct lessons-learned workshops and root-cause analysis
- Strengthen internal controls and cyber readiness programs
- Update response plans based on incident findings
- Enhance security awareness training for staff
- Improve detection, prevention, and response capabilities
- Case Study: Organization-wide improvements after major breach

Training Methodology

- Instructor-led sessions with practical demonstrations
- Hands-on lab simulations and technical scenarios
- Case study analysis from real-world cyber incidents
- Collaborative group problem-solving activities
- Role-based exercises for incident escalation and coordination
- Use of standardized templates, checklists, and reporting tools

Register as a group from 3 participants for a Discount

Send us an email: info@fineskilltrainingcenter.com 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
07 Sep 2026	18 Sep 2026	Physical	$3,000
14 Sep 2026	25 Sep 2026	Physical	$3,000
21 Sep 2026	02 Oct 2026	Physical	$3,000
28 Sep 2026	09 Oct 2026	Physical	$3,000
05 Oct 2026	16 Oct 2026	Physical	$3,000
12 Oct 2026	23 Oct 2026	Physical	$3,000
19 Oct 2026	30 Oct 2026	Physical	$3,000
26 Oct 2026	06 Nov 2026	Physical	$3,000

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

Register Online Now

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