
EC-Council Certified Incident Handler (E|CIH) + Exam voucher

Duration: 3 Days **Course Code: ECIH** **Version: 2.0**

Overview:

The latest revision of EC-Council's Certified Incident Handler (E|CIH) certified program has been designed and developed in collaboration with cybersecurity and incident handling/response practitioners across the globe.

The ECIH program focuses on a structured approach to the incident handling and response (IH&R) process. This IH&R process includes stages such as; incident handling and response preparation, incident validation and prioritization, incident escalation and notification, forensic evidence gathering and analysis, incident containment, systems recovery, and incident eradication. This systematic incident handling and response process creates awareness among the incident responders in knowing how to respond to various types of security incidents happening in organisations today. The types of cybersecurity incidents covered include malware incidents, email security incidents, network security incidents, web application security incidents, cloud security incidents, and insider threat-related incidents.

It is a comprehensive specialist level program, that imparts knowledge and skills on how organisations can effectively handle post breach consequences by reducing the impact of the incident, both financially and reputationally. The learning objectives are emphasised through practical learning with 40% of this course covering hands-on experience of the latest incident handling and response tools, techniques, methodologies, frameworks, etc.

The E|CIH lab environment consists of the latest and patched operating systems including Windows 10, Windows Server 2016, Ubuntu Linux, and OSSIM for performing labs.

Students will have access to over 50 labs, 800 tools, and 4 OSs! as well as a large array of templates, check lists, and cheat sheets.

The ECIH Program is 100% Compliant with the NICE 2.0 Framework AND CREST Framework.

Please Note: An exam voucher is included with this course

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.

Objectives:

- **After completing this course you should be able to:**
 - Understand the key issues plaguing the information security world
 - Combat the different types of cybersecurity threats, attack vectors, threat actors and their motives, goals, and objectives of cybersecurity attacks
 - Explain the fundamentals of incident management (information security incidents, signs and costs of an incident, incident handling and response and their advantages, etc.)
 - Explain the fundamentals of vulnerability management, threat assessment, risk management, incident response automation and orchestration
 - Master all incident handling and response best practices, standards, cybersecurity frameworks, laws, acts, and regulations
 - Decode the various steps involved in planning incident handling and response program (Planning, Recording and Assignment, Triage, Notification, Containment, Evidence Gathering and Forensic Analysis, Eradication, Recovery, and Post-Incident Activities)
 - Have an understanding of the fundamentals of computer forensics and forensic readiness
 - Comprehend the importance of first response and first response procedure (Evidence collection, packaging, transportation, storing, data acquisition, volatile and static evidence collection, and evidence analysis)
 - Find out anti-forensics techniques used by attackers to uncover cybersecurity incident cover-ups
 - Apply the right techniques to different types of cybersecurity incidents in a systematic manner (malware incidents, email security incidents, network security incidents, web application security incidents, cloud security incidents, and insider threat-related incidents)
-

Prerequisites:

Attendees should meet the following prerequisites:

- It is recommended that you have at least 1 year of experience in the cybersecurity domain in order to maximize course outcomes.

Testing and Certification

Recommended as preparation for the following exam:

- **212-89** - EC-Council Certified Incident Handler
- To be eligible to attend the E|CIH Exam, candidates must either:**
- Attend the E|CIH training through any of EC-Council's Authorized Training Centers (ATCs) or attend EC-Council's live online training via iWeek or join our self-study program through iLearn.
 - Candidates with a minimum of 1 year work experience in the domain that would like to apply to challenge the exams directly without attending training are required to pay the USD100 Eligibility Application Fee. This fee is included in your training fee should you choose to attend training.
-

Content:

<p>Introduction to Incident Handling and Response</p> <ul style="list-style-type: none">Overview of Information Security ConceptsUnderstanding Information Security Threats and Attack VectorsUnderstanding Information Security IncidentOverview of Incident ManagementOverview of Vulnerability ManagementOverview of Threat AssessmentUnderstanding Risk ManagementUnderstanding Incident Response Automation and OrchestrationIncident Handling and Response Best PracticesOverview of StandardsOverview of Cybersecurity FrameworksImportance of Laws in Incident HandlingIncident Handling and Legal Compliance <p>Incident Handling and Response Process</p> <ul style="list-style-type: none">Overview of Incident Handling and Response (IH;R) ProcessStep 1: Preparation for Incident Handling and ResponseStep 2: Incident Recording and AssignmentStep 3: Incident TriageStep 4: NotificationStep 5: ContainmentStep 6: Evidence Gathering and Forensics AnalysisStep 7: EradicationStep 8: RecoveryStep 9: Post-Incident Activities <p>Forensic Readiness and First Response</p> <ul style="list-style-type: none">Introduction to Computer ForensicsOverview of Forensic ReadinessOverview of First ResponseOverview of Digital EvidenceUnderstanding the Principles of Digital Evidence CollectionCollecting the EvidenceSecuring the EvidenceOverview of Data AcquisitionUnderstanding the Volatile Evidence CollectionUnderstanding the Static Evidence CollectionPerforming Evidence AnalysisOverview of Anti-Forensics	<p>Handling and Response to Malware Incidents</p> <ul style="list-style-type: none">Overview of Malware Incident ResponsePreparation for Handling Malware IncidentsDetecting Malware IncidentsContainment of Malware IncidentsEradication of Malware IncidentsRecovery after Malware IncidentsGuidelines for Preventing Malware Incidents <p>Handling and Responding to Email Security Incidents</p> <ul style="list-style-type: none">Overview of Email Security IncidentsPreparation for Handling Email Security IncidentsDetection and Containment of Email Security IncidentsEradication of Email Security IncidentsRecovery after Email Security Incidents <p>Handling and Responding to Network Security Incidents</p> <ul style="list-style-type: none">Overview of Network Security IncidentsPreparation for Handling Network Security IncidentsDetection and Validation of Network Security IncidentsHandling Unauthorized Access IncidentsHandling Inappropriate Usage IncidentsHandling Denial-of-Service IncidentsHandling Wireless Network Security Incidents	<p>Handling and Responding to Web Application Security Incidents</p> <ul style="list-style-type: none">Overview of Web Application Incident HandlingWeb Application Security Threats and AttacksPreparation to Handle Web Application Security IncidentsDetecting and Analyzing Web Application Security IncidentsContainment of Web Application Security IncidentsEradication of Web Application Security IncidentsRecovery from Web Application Security IncidentsBest Practices for Securing Web Applications <p>Handling and Responding to Cloud Security Incidents</p> <ul style="list-style-type: none">Cloud Computing ConceptsOverview of Handling Cloud Security IncidentsCloud Security Threats and AttacksPreparation for Handling Cloud Security IncidentsDetecting and Analyzing Cloud Security IncidentsContainment of Cloud Security IncidentsEradication of Cloud Security IncidentsRecovering from Cloud Security IncidentsBest Practices Against Cloud-based Incidents <p>Handling and Responding to Insider Threats</p> <ul style="list-style-type: none">Introduction to Insider ThreatsPreparation for Handling Insider ThreatsDetecting and Analyzing Insider ThreatsContainment of Insider ThreatsEradication of Insider ThreatsRecovery after Insider AttacksBest Practices Against Insider Threats
-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Further Information:

For More information, or to book your course, please call us on 00 971 4 446 4987

training@globalknowledge.ae

www.globalknowledge.com/en-ae/

Global Knowledge, Dubai Knowledge Village, Block 2A, First Floor, Office F68, Dubai, UAE