EC-Council E|CIH

OUR LEARNING EXCLUSIVE

- Custom exam prep software and materials
- Exam delivery in the classroom, with a **98% success rate**
- Course-specific thinQtank® Learning publications to keep the learning engaging
- Extended hours of training, including immersive hands-on exercises
- **We do not teach the test.** We always deliver valuable hands-on experience
- All reading material and study guides sent to you when you register
- Every course taught by certified instructors

TRAINING CAMP FORMAT

thinQtank® Learning delivers this course as an **instructor-led training camp**, with the exam sat in the classroom as part of the camp. Camps are scheduled by cohort rather than to a fixed calendar, and the balance of lecture and lab work is set to suit the group and the delivery method. Contact us for the schedule covering your dates.

PREREQUISITES

- **At least one year working in cybersecurity.** EC-Council states this plainly, and it is the honest bar — this course assumes you have seen a live environment
- Working knowledge of networks, operating systems and common attacks
- No certification is required first, but Security+ or CND is a comfortable place to be standing

TARGET AUDIENCE

- SOC analysts who are already handling incidents and want the method behind it
- Incident response team members and team leads
- Cyber forensic investigators, consultants and analysts
- Penetration testers who need to understand the other side of the callout
- Security administrators and engineers on the escalation path

EXAM

212-89 — EC-Council Certified Incident Handler

One hundred multiple-choice questions, three hours, through the EC-Council Exam Portal. ANAB accredited and approved by the US Department of Defense under directive 8140.

The passing mark moves. EC-Council uses several forms of this exam and sets a cut score for each one, ranging from 60% to 78%. There is no single published passing number, so prepare for the top of that range rather than the bottom — you do not find out which form you have until you sit it.

Built on **ECIH v3**, the current version of the program — ten modules, one more than v2.

COURSE OVERVIEW

thinQtank® Learning offers an industry-unique training camp in which students earn the **EC-Council Certified Incident Handler (E|CIH)** certification. As with all our EC-Council training experiences, the exam is delivered in the classroom.

E|CIH is the method course. Not how an attack works — what you do about it, in order, under pressure, and how you write it up afterward. Malware, email, network, web application, cloud, endpoint and insider incidents, each with its own handling and response track, plus the forensic readiness and first response that decides whether the evidence survives.

It is a specialist, hands-on program and EC-Council expects a year in the field before you take it. Exam **212-89**, and the **voucher is available** at $450 USD.

COURSE OBJECTIVES

Primary course objectives:

- Explain incident handling and response, and where it sits in a security program
- Understand the signs of an incident, and the cost of missing them
- Apply the incident handling and response process end to end
- Build incident handling and response policies, plans and playbooks
- Establish forensic readiness before an incident, not during one
- Carry out a first response that preserves evidence rather than destroying it
- Handle and respond to malware incidents
- Handle and respond to email security incidents
- Handle and respond to network security incidents
- Handle and respond to web application security incidents
- Handle and respond to cloud security incidents
- Handle and respond to insider threats
- Handle and respond to endpoint security incidents
- Apply the laws, regulations and standards that constrain an investigation
- Report and document an incident so the record stands up later
- Contribute to recovery, and to the post-incident review that prevents a repeat

DELIVERY METHODS

- Instructor-led training
- Immersive live-online training
- On-site and custom delivery

EC-Council E|CIH

WHAT YOU WILL BE ABLE TO DO

- Run an incident through a defined process instead of improvising
- Preserve evidence from the first minute, so an investigation stays possible
- Handle each incident type on its own terms, not with one generic runbook
- Write an incident report that survives review

EXCLUSIVE LEARNING PACKAGE

- Hands-on labs across every incident type in the course
- Live incident simulations run end to end, with a real clock
- Forensic readiness and first-response drills
- E|CIH video course
- E|CIH reading plan and review guide
- E|CIH certification practice exam

COURSE MODULES

01 Introduction to Incident Handling and Response
- Topic A: What incident handling and response is, and is not
- Topic B: Signs of an incident, and classification
- Topic C: Information security threats and attack vectors
- Topic D: Incident response teams and their roles
- Topic E: Laws, regulations and standards that apply

02 Incident Handling and Response Process
- Topic A: Preparation
- Topic B: Detection and analysis
- Topic C: Containment, eradication and recovery
- Topic D: Post-incident activity and lessons learned
- Topic E: Policies, plans, playbooks and escalation

03 First Response
- Topic A: Forensic readiness, established before you need it
- Topic B: Securing and documenting the scene
- Topic C: Collecting and preserving evidence
- Topic D: Chain of custody, and what breaks it
- Topic E: Handing over to a forensic investigator

04 Malware Incidents
- Topic A: Types of malware, and what each one leaves behind
- Topic B: Detection and triage
- Topic C: Containment and eradication
- Topic D: Recovery and verification
- Topic E: Preventing the repeat

05 Email Security Incidents
- Topic A: Email-borne threats and their delivery
- Topic B: Phishing, spear phishing and business email compromise
- Topic C: Investigating a suspicious message
- Topic D: Containment and user communication
- Topic E: Hardening the mail path afterward

06 Network Security Incidents
- Topic A: Unauthorized access and reconnaissance
- Topic B: Denial-of-service and distributed attacks
- Topic C: Wireless network incidents
- Topic D: Detection, containment and eradication
- Topic E: Network evidence and what it can prove

07 Web Application Security Incidents
- Topic A: Common web application attacks
- Topic B: Detecting an application-layer incident
- Topic C: Investigating logs and application evidence
- Topic D: Containment without destroying the site
- Topic E: Remediation and re-testing

08 Cloud Security Incidents
- Topic A: What changes when the incident is in the cloud
- Topic B: Shared responsibility, and where your authority ends
- Topic C: Cloud-specific detection and evidence sources
- Topic D: Containment and eradication in a tenant you do not own
- Topic E: Working with a provider during an incident

09 Insider Threats
- Topic A: Types of insider threat, malicious and accidental
- Topic B: Indicators, and why they are missed
- Topic C: Investigating without tipping off
- Topic D: Legal, HR and privacy constraints
- Topic E: Controls that reduce the exposure

10 Endpoint Security Incidents
- Topic A: Endpoint attack surface and detection
- Topic B: Triage and isolation of a compromised endpoint
- Topic C: Mobile and removable-media incidents
- Topic D: Eradication, reimaging and restoration
- Topic E: Endpoint hardening after the fact

TERMS

© 2026 thinQtank® Global, Inc. All rights reserved. The product or learning materials are protected by U.S. and intellectual property laws. thinQtank Global, thinQtank Learning and the Q-Man logo are registered trademarks of thinQtank Global, Inc. in the United States and/or other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies.

thinQtank Global, Inc. warrants that it will perform these training services in a reasonable manner using generally accepted industry standards and practices. THE EXPRESS WARRANTY SET FORTH IS IN LIEU OF ALL OTHER WARRANTIES, EXPRESS, IMPLIED, STATUTORY OR OTHERWISE INCLUDING IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE WITH RESPECT TO THE SERVICES AND DELIVERABLES PROVIDED BY THINQTANK GLOBAL, INC., OR AS TO THE RESULTS WHICH MAY BE OBTAINED THEREFROM. THINQTANK GLOBAL, INC. WILL NOT BE LIABLE FOR ANY THIRD-PARTY SERVICES OR PRODUCTS IDENTIFIED OR REFERRED TO CUSTOMER. All materials provided in this training are copyrighted by thinQtank Global, Inc. ("Learning Materials"). thinQtank Global, Inc. grants the customer of this learning a license to use Learning Materials strictly for the purpose of facilitating such company's internal understanding, utilization and operation of the technology covered herein. Except as set forth expressly in the sentence above, there is no transfer of any intellectual property rights or any other license granted under the terms of this training.