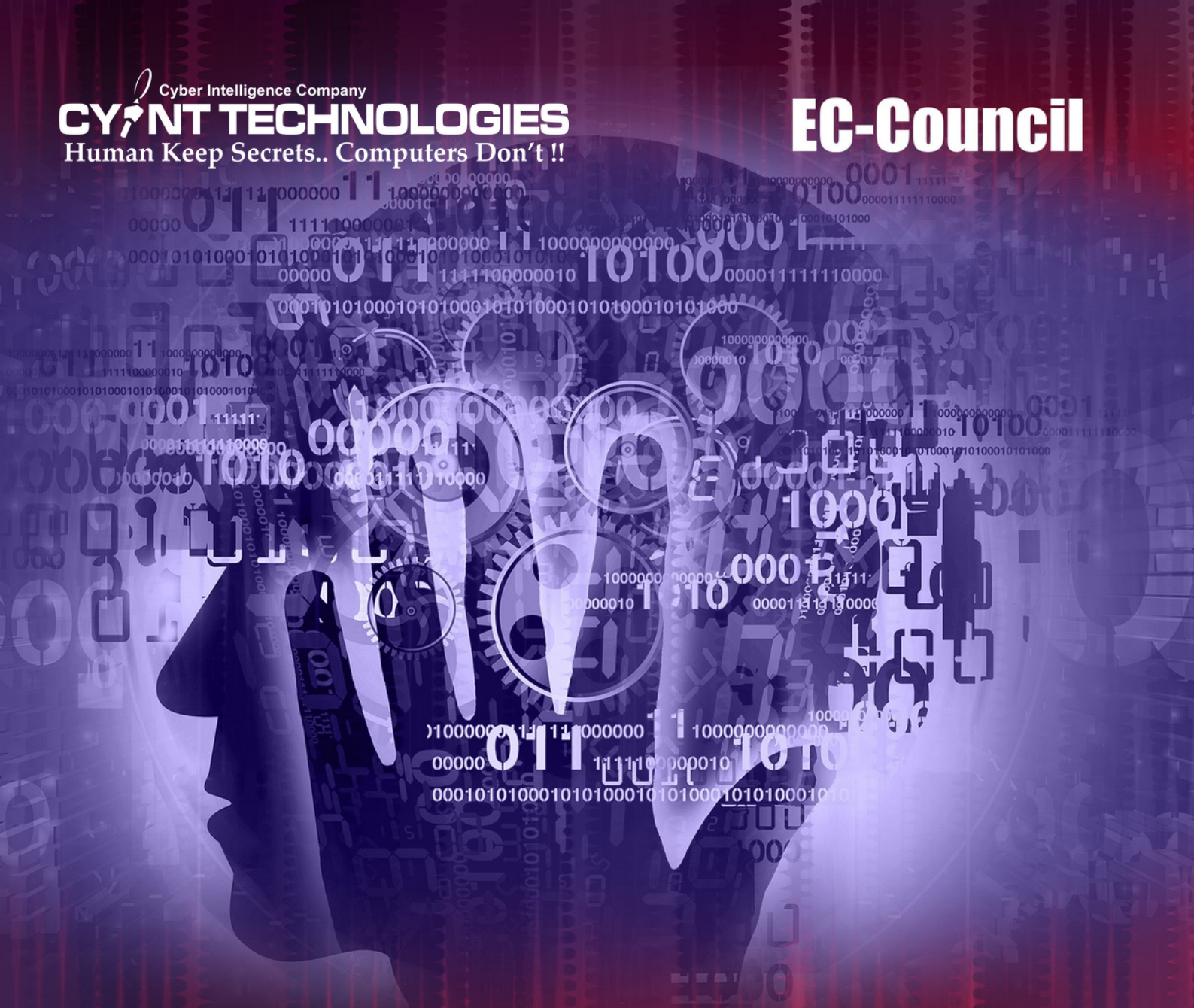
Cyber Intelligence Company

CYNT TECHNOLOGIES

Human Keep Secrets.. Computers Don't !!

EC-Council



The All-New

C|EH® v12

Certified Ethical Hacker

1 LEARN

2 CERTIFY

3 ENGAGE

4 COMPETE

Attain the World's No.1 Credential in Ethical Hacking

Cyber Intelligence Company
CYINT TECHNOLOGIES
Human Keep Secrets... Computers Don't !!

Build your career with the most in-demand cybersecurity certification in the world:

THE CERTIFIED ETHICAL HACKER

The World's No. 1 Ethical Hacking Certification for 20 Years

Ranked #1 In Ethical Hacking Certifications by ZDNet

Ranked as a Top 10 Cybersecurity Certification

C|EH® Ranks 4th Among Top 50 Leading Cybersecurity Certifications

Who is a Certified Ethical Hacker?

A Certified Ethical Hacker is a specialist typically working in a red team environment, focused on attacking computer systems and gaining access to networks, applications, databases, and other critical data on secured systems. A C|EH® understands attack strategies, the use of creative attack vectors, and mimics the skills and creativity of malicious hackers. Unlike malicious hackers and actors, Certified Ethical Hackers operate with permission from the system owners and take all precautions to ensure the outcomes remain confidential. Bug bounty researchers are expert ethical hackers who use their attack skills to uncover vulnerabilities in the systems.

What is C|EH® v12?

The Certified Ethical Hacker has been battle-hardened over the last 20 years, creating hundreds of thousands of Certified Ethical Hackers employed by top companies, militaries, and governments worldwide.

In its 12th version, the Certified Ethical Hacker provides comprehensive training, hands-on learning labs, practice cyber ranges for engagement, certification assessments, cyber competitions, and opportunities for continuous learning into one comprehensive program curated through our new learning framework: 1. Learn 2. Certify 3. Engage 4. Compete.

The C|EH v12 also equips aspiring cybersecurity professionals with the tactics, techniques, and procedures (TTPs) to build ethical hackers who can uncover weaknesses in nearly any type of target system before cybercriminals do.

What's New in the C|EH® v12

LEARN | CERTIFY | ENGAGE | COMPETE

The C|EH® v12 is a specialized and one-of-a-kind training program to teach you everything you need to know about ethical hacking with hands-on training, labs, assessment, a mock engagement (practice), and global hacking competition. Stay on top of the game with the most in-demand skills required to succeed in the field of cybersecurity.

Master ethical hacking skills that go beyond the certification.

Gain Skills

Gain Recognition

Gain Experience

Gain Respect

The new learning framework covers not only a comprehensive training program to prepare you for the certification exam but also the industry's most robust, in-depth, hands-on lab and practice range experience.

1 LEARN

The C|EH® v12 training program includes 20 modules covering various technologies, tactics, and procedures, providing prospective ethical hackers with the core knowledge needed to thrive in cybersecurity. Delivered through a carefully curated training plan that typically spans five days, the 12th version of the C|EH® continues to evolve to keep up with the latest OS, exploits, tools, and techniques. The concepts covered in the training program are split 50/50 between knowledge-based training and hands-on application through our cyber range.Every tactic discussed in training is backed by step-by-step labs conducted in a virtualized environment with live targets, live tools, and vulnerable systems. Through our lab technology, every participant will have comprehensive hands-on practice to learn and apply their knowledge."

20 REFRESHED MODULES

3000+ PAGES OF STUDENT MANUAL

Course Outline

20 Modules That Help You Master the Foundations of Ethical Hacking and Prepare to Take the C|EH Certification Exam

Module 01

Introduction to Ethical Hacking

Cover the fundamentals of key issues in the information security world, including the basics of ethical hacking, information security controls, relevant laws, and standard procedures.

Module 02

Foot Printing and Reconnaissance

Learn how to use the latest techniques and tools to perform foot printing and reconnaissance, a critical pre-attack phase of the ethical hacking process.

Module 03

Scanning Networks

Learn different network scanning techniques and countermeasures.

Module 04

Enumeration

Learn various enumeration techniques, such as Border Gateway Protocol (BGP) and Network File Sharing (NFS) exploits, and associated countermeasures.

Module 05

Vulnerability Analysis

Learn how to identify security loopholes in a target organization's network, communication infrastructure, and end systems. Different types of vulnerability assessment and vulnerability assessment tools.

Module 06

System Hacking

Learn about the various system hacking methodologies—including steganography, steganalysis attacks, and covering tracks—used to discover system and network vulnerabilities.

Module 07

Malware Threats

Learn different types of malware (Trojan, virus, worms, etc.), APT and fileless malware, malware analysis procedure, and malware countermeasures.

Module 08

Sniffing

Learn about packet-sniffing techniques and how to use them to discover network vulnerabilities, as well as countermeasures to defend against sniffing attacks.

Module 09

Social Engineering

Learn social engineering concepts and techniques, including how to identify theft attempts, audit human-level vulnerabilities, and suggest social engineering countermeasures.

Module 10

Denial-of-Service

Learn about different Denial of Service (DoS) and Distributed DoS (DDoS) attack techniques, as well as the tools used to audit a target and devise DoS and DDoS countermeasures and protections.

Module 11

Session Hijacking

Understand the various session hijacking techniques used to discover network-level session management, authentication, authorization, and cryptographic weaknesses and associated countermeasures.

Module 12

Evading IDS, Firewalls, and Honeypots

Get introduced to firewall, intrusion detection system (IDS), and honeypot evasion techniques; the tools used to audit a network perimeter for weaknesses; and countermeasures.

Module 13

Hacking Web Servers

Learn about web server attacks, including a comprehensive attack methodology used to audit vulnerabilities in web server infrastructures and countermeasures.

Module 14

Hacking Web Applications

Learn about web application attacks, including a comprehensive web application hacking methodology used to audit vulnerabilities in web applications and countermeasures.

Module 15

SQL Injection

Learn about SQL injection attacks, evasion techniques, and SQL injection countermeasures.

Module 16

Hacking Wireless Networks

Understand different types of wireless technologies, including encryption, threats, hacking methodologies, hacking tools, Wi-Fi sedcurity tools, and countermeasures.

Module 17

Hacking Mobile Platforms

Learn Mobile platform attack vector, android and iOS hacking, mobile device management, mobile security guidelines, and security tools.

Module 18

IoT Hacking

Learn different types of IoT and OT attacks, hacking methodology, hacking tools, and countermeasures.

Module 19

Cloud Computing

Learn different cloud computing concepts, such as container technologies and server less computing, various cloud computing threats, attacks, hacking methodology, and cloud security techniques and tools.

Module 20

Cryptography

Learn about encryption algorithms, cryptography tools, Public Key Infrastructure (PKI), email encryption, disk encryption, cryptography attacks, and cryptanalysis tools.

About EC-Council

EC-Council's sole purpose is to build and refine the cybersecurity profession globally. We help individuals, organizations, educators, and governments address global workforce problems by developing and curating world-class cybersecurity education programs and their corresponding certifi cations. We also provide cybersecurity services to some of the largest businesses globally. Trusted by 7 of the Fortune 10, 47 of the Fortune 100, the Department of Defence, Intelligence Community, NATO, and over 2,000 of the best Universities, Colleges, and Training Companies, our programs have proliferated through over 140 countries. They have set the bar in cybersecurity education. Best known for the Certified Ethical Hacker programs, we are dedicated to equipping over 2,30,000 information age soldiers with the knowledge, skills, and abilities required to fight and win against the black hat adversaries. EC-Council builds individual and team/organization cyber capabilities through the Certified Ethical Hacker Program, followed by a variety of other cyber programs, including Certified Secure Computer User, Computer Hacking Forensic Investigator, Certified Security Analyst, Certified Network Defender, Certified SOC Analyst, Certified Threat Intelligence Analyst, Certified Incident Handler, as well as the Certified Chief Information Security Officer.

We are an ANSI 17024 accredited organization and have earned recognition by the DoD under Directive 8140/8570 in the UK by the GCHQ, CREST, and various other authoritative bodies that influence the entire profession.

Founded in 2001, EC-Council employs over 400 individuals worldwide with ten global o

Learn more at www.eccouncil.org

Cyber Intelligence Company
CYINT TECHNOLOGIES
Human Keep Secrets... Computers Don't !!

(AUTHORIZED TRAINING PARTNER OF EC-COUNCIL)

Cyint Technologies is a Cyber/ Digital Intelligence based organization that works in the field of Digital Forensics. Cyint has been working actively with EC-Council and holds the title of Authorized Training Partner of the organization.

We have been working in the field of Digital Forensics from past 14+ years and are the leading providers of Products || Services || Trainings. Provides solutions and technical support to Government & Law Enforcement Agencies, and Top Corporates all over the India. We have trained 5000+ personnel from different organizations.

In Cyint, we have highly skilled team of instructors and trainers to provide you with instructor-led training sessions. Our trainers are proficient and have expertise in the domain, they are certified to deliver trainings.

Best known for the Computer Hacking Forensic Investigator (CHFI) and Certified Ethical Hacker (CEH)programmes. We are equipped with tools and solutions to run into the practical oriented trainings and demonstrate digital forensic tools.