NEW ARRIVAL

CERTIFIED

Certified Ethical Hacker and Network Defense Program

As Cyber threats continue to evolve, the demand for skilled cybersecurity professionals has reached an all-time high. Digitalearn Ethical Hacking and Network Defense (EHND) program is designed to equip aspiring and seasoned IT professionals with the expertise required to safeguard systems, networks, and data from malicious attacks.

Join the CEH + C|ND combo program and become a dual-skilled cybersecurity professional, ready to tackle challenges on both ends of the security spectrum. Equip yourself with cutting-edge skills and certifications that open doors to exciting opportunities in the ever-evolving field of cybersecurity.

- **Ethical Hacking:** Learn to identify vulnerabilities, simulate attacks, and secure systems effectively.
- **Network Defense:** Master strategies to protect networks from cyber threats, prevent data breaches, and ensure robust security.

Key **Feature** to Determine **Success**

- Live Projects
- Exam Simulation
- Access to Recorded Sessions
- 40-Hour LIVE Instructor-led Training
- Updated Content (Market Trends)
- Class Feedback with Assigned Advisor
- Micro Batches (10 Students per Class)
- Individual Doubt Sessions
- Career Guidance and Mentorship
- Practical Sessions (Online)

Digitalearn
TO INSPIRE

How this program works differently with highlighted **Key Solutions** ?

Career Preparation

- Mock Interview Prep (Technical + Behavioral)
- Resume Building (Ready-to-use Templates)
- Job Application Guide (Tips for Finding the Right Job)
- Internship Benefits (Hands-on Experience with Tools)

Practical Learning

- Live Projects (5+ Real-World Projects)
- Practical Sessions (Interactive Online Learning)
- Updated Tools and Techniques (Stay Ahead with the Latest in Cybersecurity)

Learning Support

- Personality Development Classes (Enhance Soft Skills)
- Class Recordings (Access Anytime for Review)
- E-books (Comprehensive Learning Materials)

Certification and Exams

- Exam Simulation (Prepare Effectively)
- Exam vouchers (Subject to Availability)

Ongoing Mentorship

- Lifetime Career Mentorship (Guidance Throughout Your Career)

Continuous Learning

- Updated Content (Stay Current with Market Trends)
- Demos (Optional Hands-on Demonstrations)

Cybersecurity Mastery Program: Certified Ethical Hacker (CEH v13) + Certified Network Defender (C|ND)

Step into the forefront of cybersecurity with the Digitalearn CEH v13 and C|ND training combo. This dual program equips you with advanced offensive and defensive cybersecurity skills, preparing you to secure critical systems, networks, and applications while responding to modern-day threats with precision. Designed for aspiring ethical hackers and network defenders, this program ensures a well-rounded cybersecurity education that combines cutting-edge technologies, hands-on labs, and globally recognized certifications.

Certified Ethical Hacker (CEH v13)

The CEH v13 is the latest version of the globally renowned ethical hacking certification, enhanced with AI capabilities to tackle modern challenges. This program teaches the tools, techniques, and methodologies used by hackers, empowering you to think and act like one to proactively safeguard systems.

Key Highlights:

- **AI Integration:** Learn to leverage artificial intelligence in cybersecurity.
- **Comprehensive Modules:** Covers over 550 attack techniques across 20 modules.
- **Hands-On Practice:** Simulated environments for real-world hacking scenarios.
- **Global Certification:** Prepare for the CEH certification exam and elevate your career.

Digitalearn
TO INSPIRE

Benefits of Having CEH and C|ND Certifications

Professional Benefits:

- Comprehensive Cybersecurity Expertise:
  - CEH equips you with offensive skills to think like a hacker and identify vulnerabilities.
  - C|ND focuses on defensive techniques, teaching you how to secure and protect networks and systems.
- Enhanced Employability:
  - With dual certifications, you qualify for diverse roles such as Ethical Hacker, Network Security Engineer, Cybersecurity Analyst, or SOC Specialist.
- Globally Recognized Certifications:
  - Both certifications are recognized worldwide, making you a standout candidate in the competitive job market.
- Broader Skill Set:
  - Gain mastery over threat detection, mitigation, log analysis, network monitoring, and incident response.
- Higher Salary Potential:
  - Certified professionals often command higher salaries due to their specialized skill sets.

Technical Benefits:

- Proactive Defense:
  - CEH enables you to anticipate and counteract cyberattacks before they occur.
  - C|ND prepares you to defend against real-world threats, ensuring network and system security.
- Threat Intelligence:
  - Learn to gather, analyze, and utilize threat intelligence to predict and prevent attacks effectively.
- Hands-On Expertise:
  - Both programs emphasize practical skills through live labs, projects, and simulated environments.
- Business Continuity & Disaster Recovery:
  - With C|ND, develop skills to maintain operations during crises and minimize downtime.
- AI Integration (CEH v13):
  - Stay ahead by leveraging artificial intelligence to tackle modern cybersecurity challenges.

Benefits of Having CEH and CND Certifications

- Red Team Specialist: Use CEH skills to simulate attacks and test system vulnerabilities.
- Blue Team Specialist: Leverage C|ND expertise to defend and secure organizational networks.
- SOC Analyst: Monitor and respond to security incidents in real time.
- Threat Intelligence Analyst: Analyze and predict emerging threats.
- Penetration Tester: Conduct ethical hacking to strengthen system defenses.

Digitalearn
TO INSPIRE

Who Should Pursue **CEH and CND** Certifications?

1. IT Professionals Transitioning to Cybersecurity
2. Entry-Level Cyber security Enthusiasts
3. Network Administrators and Engineers
4. Security Operations Center (SOC) Analysts
5. System Administrators
6. IT Managers and Consultants
7. Cybersecurity Professionals Looking to Upskill
8. Red and Blue Team Members
9. Students and Fresh Graduates
10. Organizations Training In-House Teams

Digitalearn
TO INSPIRE

Curriculum

Certified Ethical Hacker (CEH v13)

Offensive techniques (Red Team focus)

Module 1: Introduction to Ethical Hacking
- Overview of Cybersecurity
- Key concepts in ethical hacking
- Legal and ethical considerations

Module 2: Footprinting and Reconnaissance
- Passive and active reconnaissance techniques
- Tools for information gathering
- Identifying potential vulnerabilities

Module 3: Scanning Networks
- Network scanning and enumeration techniques
- Vulnerability scanning tools
- Analyzing network scans

Module 4: Gaining Access
- Exploitation techniques for various platforms
- Password cracking and privilege escalation
- Real-world hacking scenarios

Module 5: Enumeration and Vulnerability Analysis
- Techniques for system and network enumeration

Certified Network Defender (CND)

Defensive strategies (Blue Team focus)

Module 1: Network Fundamentals
- Understanding network components and architecture
- OSI and TCP/IP models

Module 2: Network Security Threats, Vulnerabilities, and Attacks
- Types of network threats and vulnerabilities
- Common attack vectors and techniques

Module 3: Network Security Controls
- Firewalls, IDS/IPS, VPNs, and proxies
- Endpoint protection and hardening

Module 4: Network Traffic Monitoring and Analysis
- Packet analysis using tools like Wireshark
- Understanding logs and identifying anomalies

Module 5: Risk Assessment and Management
- Threat modeling and risk analysis
- Risk mitigation strategies

Module 6: Secure Network Design and Implementation

- Identifying and analyzing vulnerabilities
- Using vulnerability scanning tools

Module 6: Malware Threats
- Types of malware and propagation methods
- Detecting and mitigating malware threats
- Analyzing malicious code`

Module 7: Social Engineering
- Understanding psychological manipulation
- Phishing and baiting techniques
- Preventing social engineering attacks

Module 8: Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS) Attacks
- DoS/DDoS attack mechanisms
- Detection and mitigation strategies

Module 9: Session Hijacking
- Understanding session hijacking techniques
- Tools used in hijacking
- Countermeasures for session security

Module 10: Evading IDS, Firewalls, and Honeypots
- Techniques to bypass security systems
- Configuring and deploying countermeasures

Module 11: Hacking Web Applications
- Web app vulnerabilities: SQL injection, XSS, etc.

Module 7: Network Incident Response and Management
- Developing an incident response plan
- Techniques for threat containment and remediation

Module 8: Log Analysis and Threat Intelligence
- Analyzing system and network logs
- Using threat intelligence for proactive defense

Module 9: Business Continuity and Disaster Recovery
- Developing disaster recovery plans
- Ensuring business continuity during attacks

Module 10: Network Security Policies and Procedures
- Creating and enforcing security policies
- Compliance and regulatory considerations

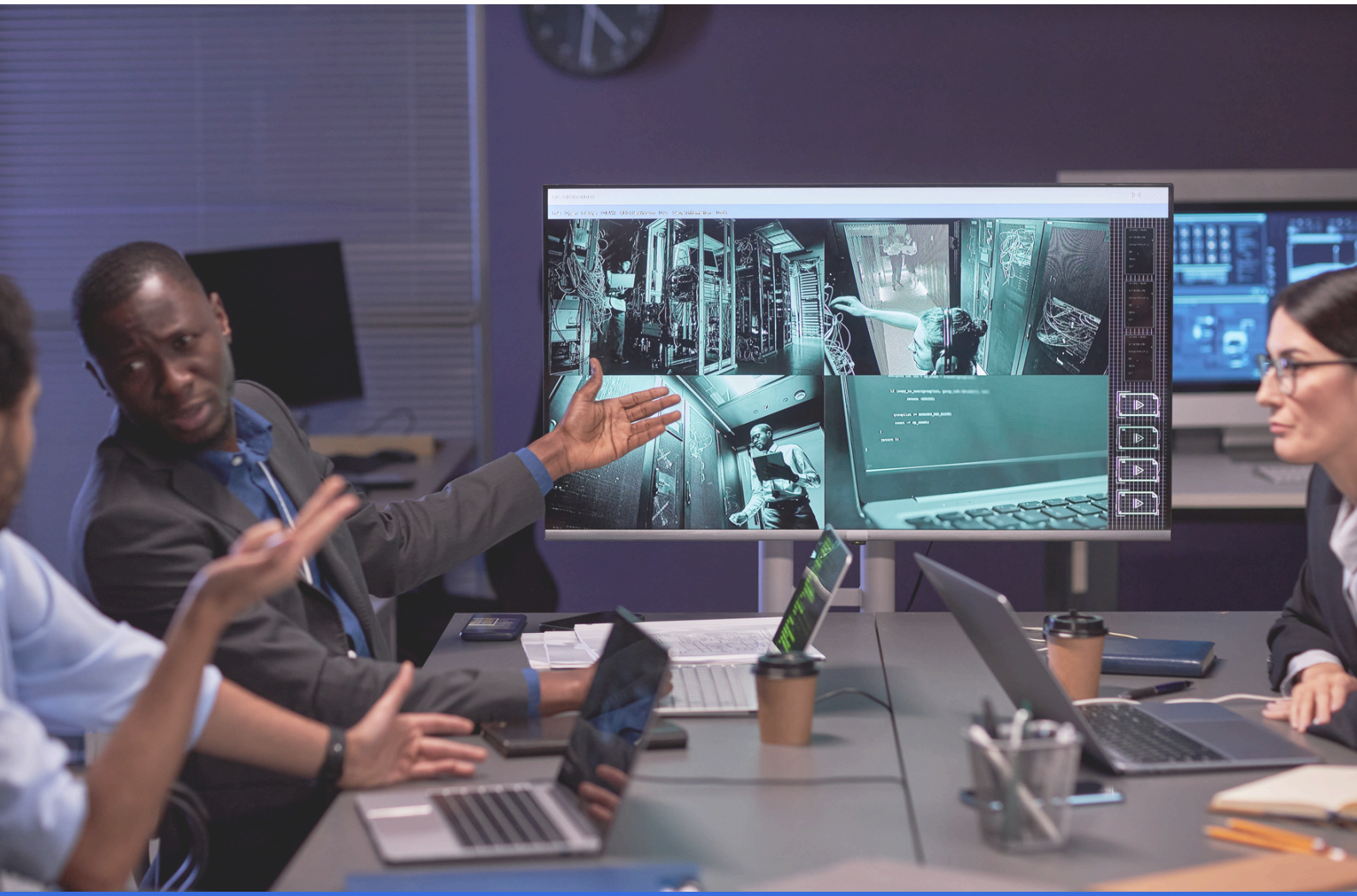
Module 11: Hands-On Labs
- Over 100+ live labs for real-world simulation
- Working with tools like Kali Linux, Metasploit, Snort, and more

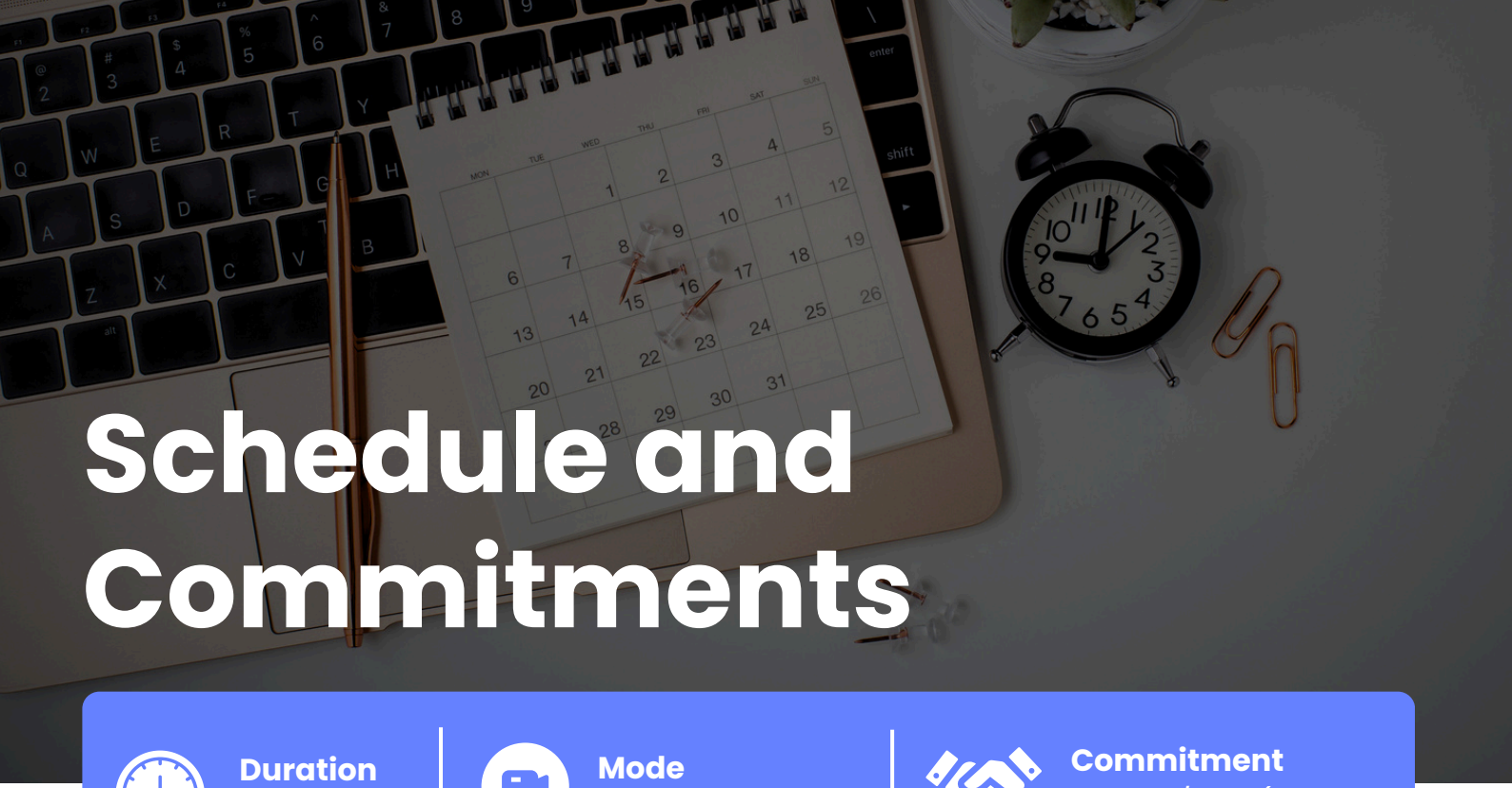
- Penetration testing for web apps

Module 12: Hacking Wireless Networks
- Wireless encryption protocols and vulnerabilities
- Wireless network penetration testing

Module 13: IoT Hacking
- Securing IoT devices
- Exploiting IoT vulnerabilities

Module 14: Cloud Computing Security
- Cloud service models and risks
- Penetration testing in cloud environments





Schedule and Commitments

Duration
2 months
(8 weeks)

Mode
100% online (Live sessions, coding tasks, and self-paced study)

Commitment
2 hours/day (Mon-Wed-Thur-Sat) for a total of 70 hours

What are **Practical Tasks** in the training Program?

Network Monitoring and Threat Detection
Use Wireshark to analyse network traffic and detect anomalies.

Vulnerability Assessment
Conduct vulnerability scans and assess risk impact on simulated environments.

Incident Response Simulation
Practice identifying, responding to, and documenting security incidents.

Risk Assessment Project
Develop a risk management plan aligned with industry standards

Upon Completing the **Program**, You'll Receive:

- Digitalearn Certified Ethical Hacking and Network Defense (EHND) Program Certificate
- Portfolio-ready projects and access to career advancement resources

4.9 Average Rating | 3500+ Students Got Job | 4000+ Satisfied Learners | 100+ Highly Qualified Trainers

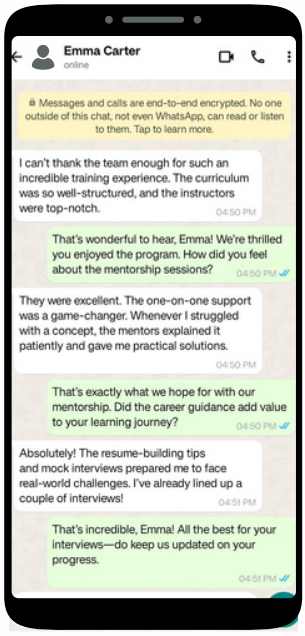
What Kind of Support Will You Receive?

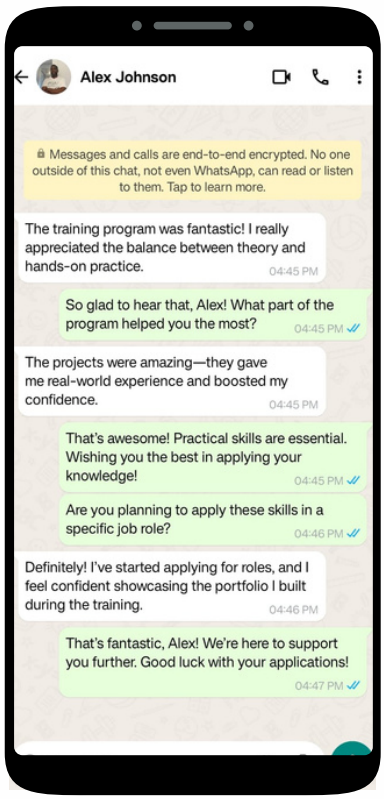
Mentorship
A dedicated mentor to guide you through the learning journey

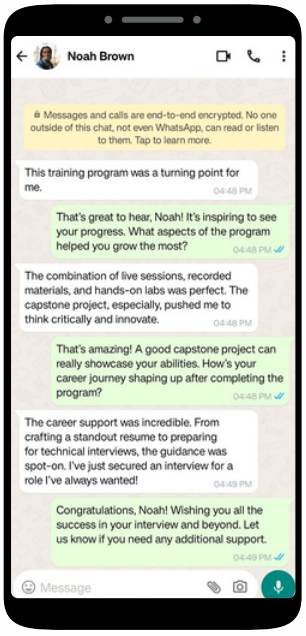
Alumni Network
Access to a supportive community of cybersecurity professionals

Career Assistance
Networking tips, job search strategies, and interview prep

What our **students** say ?







Digitalearn
TO INSPIRE

CEH and CND Training FAQ

1. What is CEH (Certified Ethical Hacker)?

Answer:

CEH is a globally recognized certification offered by EC-Council that validates the skills of ethical hackers. This certification focuses on identifying vulnerabilities in systems, conducting penetration testing, and understanding the legal and ethical issues surrounding hacking.

2. What is CND (Certified Network Defender)?

Answer:

CND is a vendor-neutral network security certification by EC-Council that prepares IT professionals to defend their networks against cyber threats. It focuses on security operations, threat monitoring, incident response, and best practices for securing networks and systems.

3. Who should pursue CEH?

Answer:

CEH is suitable for individuals interested in pursuing a career in ethical hacking, penetration testing, or cybersecurity. It is ideal for:

- Network security professionals
- Security analysts
- Penetration testers
- IT professionals looking to expand into ethical hacking

4. Who should pursue CND?

Answer:

CND is designed for IT professionals responsible for securing their organization's network infrastructure. It is recommended for:

- Network administrators
- Security engineers
- IT system administrators
- Cybersecurity professionals

5. What are the prerequisites for CEH?

Answer:

The official prerequisite for CEH is two years of work experience in the Information Security domain or attending an EC-Council-approved training course. Alternatively, you can take the CEH training and bypass the experience requirement.

6. What are the prerequisites for CND?

Answer:

There are no formal prerequisites for CND. However, it is recommended that candidates have foundational knowledge of networking, security, and basic IT skills.

7. How long does it take to complete the CEH certification?

Answer:

The CEH certification program typically takes 5 to 6 weeks, depending on your pace of study. EC-Council offers training options with flexible schedules that fit around your availability.

8. How long does it take to complete the CND certification?

Answer:

CND can typically be completed in 4 to 6 weeks, depending on the mode of study and individual progress.

9. What is the format of the CEH exam?

Answer:

The CEH exam consists of 125 multiple-choice questions, covering topics related to ethical hacking, network defense, security analysis, and penetration testing. The exam duration is 4 hours, and the passing score is 70%.

10. What is the format of the CND exam?

Answer:

The CND exam is a multiple-choice exam with 100 questions. The exam duration is 4 hours, and candidates must score at least 70% to pass.

11. How much does the CEH certification cost?

Answer:

The cost for the CEH certification varies based on the region and training provider. On average, the exam fee is around $1,199, while additional training or resources may incur extra charges.

12. How much does the CND certification cost?

Answer:

The CND certification typically costs around $1,299 for the exam, with additional training programs available at various price points depending on the provider.

13. How can I prepare for the CEH and CND exams?

Answer:

You can prepare by attending formal EC-Council training, self-study using official study materials, taking online courses, and practicing in a lab environment. For hands-on experience, both CEH and CND programs offer practical labs to reinforce the concepts.

14. What are the benefits of holding both CEH and CND certifications?

Answer:

Holding both certifications allows you to become a well-rounded cybersecurity professional. CEH focuses on offensive security (ethical hacking), while CND specializes in defensive security (network defense). This combination gives you the ability to conduct thorough security assessments, mitigate risks, and respond to cyber threats, enhancing your career prospects.

15. Are there any renewal requirements for CEH and CND certifications?

Answer:

Yes, both CEH and CND require recertification. CEH needs to be renewed every 3 years by earning 120 Continuing Professional Education (CPE) credits and paying a renewal fee. CND also has a 3-year renewal period with the requirement of 60 CPE credits.

Social Media Handles:

@digitalearn_official

Digitalearn

Ask your queries to our experts?

+91 90124 95693
+91 9625585022

www.digitalearn.info

support@digitalearn.info

Office Hours :
09:00 AM EST to 07:00 PM EST