

CICRA
C A M P U S

C|EH^{v13}

[Certified Ethical Hacker]^{AI}

Version 13

A New Era in Cybersecurity



***Certified Ethical Hacker Training
for Tomorrow's Cyber Guardians.***



*Experience a **World Class** training by
Award Winning **International Trainer**
exclusively @ CICRA Campus*

Powered by AI Capabilities

LEARN | CERTIFY | ENGAGE | COMPETE

EC-Council **C|EH**^{v13}

Certified Ethical Hacker

Build Your Career with the **Most** **In-Demand** Ethical Hacking Certification

Ranked 1st in Ethical Hacking
Certifications by ZDNet

Ranked in the List of **Top 10**
Cybersecurity Certifications

Ranked 4th Among
the Top 50 Leading
Cybersecurity Certifications

01 The **World's #1** Ethical Hacking
Certification for 20+ years

01 EC-Council Introduces the **Industry's**
First AI Cybersecurity Courses

12 C|EH Ranks 12th among the
Top 75 Highest-Paying IT
Certifications in the US and Globally

97% Stated That the Skills They
Acquired in CEH Helped
Safeguard Their Organizations

95% Chose C|EH for
Career Growth

92% of **Hiring Managers Prefer**
Candidates with the C|EH for
Jobs That Require Ethical Hacking Skills

45+ Cybersecurity Job Roles Are
Mapped to the C|EH Certification in
2024, Compared to 20+ Roles in 2022

1 in every 2 Professionals Received
Promotions After Completing the C|EH

C|EH is the only Globally In-Demand
Ethical Hacking Certification that covers
Core Domains of Cybersecurity and has
Global Recognition and Accreditations
while offering a Higher Employability Rate

Future Proof Your Cybersecurity Career with AI

The Demand for
Cybersecurity Professionals
with AI Skills is on the Rise

AI Skills No Longer Optional;
They Are Essential

42% of large enterprises actively use AI, and 59% of early adopters plan to increase investment and accelerate AI integration (IBM, 2024)

40% surge in demand for specialists in Artificial Intelligence and Machine Learning (World Economic Forum, 2023)

96% of security leaders deem AI solutions essential for countering AI-powered threats due to their speed and effectiveness (Darktrace, 2024)

87% of business leaders expect at least a quarter of their workforce will need to upskill in AI (IBM, 2024)

*McAfee Report. †Darktrace. ‡Forbes. *Projected by Future of Jobs Report 2023.
~2023 Emerging Jobs Report, LinkedIn.

AI in Cybersecurity

Threats

83% note tangible alterations in attack methodologies amidst the AI revolution (EC-Council, 2024)

66% admit Being Unprepared for AI Cyber Onslaughts (EC-Council, 2024)

Countermeasures

Up to **90%** of fraud costs can be reduced by AI models in specific scenarios where behavioral data analysis is effectively applied (IBM, 2024)

AI and automation slashed breach impact by 30%, saving businesses USD 850,000 and reducing breach lifecycles by 108 days (IBM, 2023)

Gain Cybersecurity Mastery for Real-world Success with **Certified Ethical Hacker v13**

Why Should You Join the AI Revolution with the Certified Ethical Hacker Program?

By joining the AI Revolution as a Certified Ethical Hacker, you'll gain the expertise to navigate the cutting-edge world of cybersecurity.

Certified Ethical Hackers, trained in the latest version of CEH v13, are equipped with AI-powered tools and techniques to identify, exploit, and secure vulnerabilities in systems and networks. You'll learn to leverage AI for automating threat detection, predicting security breaches, and responding swiftly to cyber incidents. Moreover, you'll also gain the skills needed to secure AI-driven technologies against potential threats. This combination of ethical hacking and AI capabilities will place you at the forefront of cybersecurity, ready to defend organizations across industries from advanced threats and adapt to evolving challenges.

Amplify Your Edge as a Certified Ethical Hacker Powered by AI Capabilities:

Advanced Knowledge: As an AI-powered Certified Ethical Hacker, you'll possess in-depth knowledge of ethical hacking methodologies, enhanced with cutting-edge AI techniques.

AI Integration: You'll effectively integrate AI across every phase of ethical hacking, from reconnaissance and scanning to gaining access, maintaining access, and covering your tracks.

Automation and Efficiency: You'll leverage AI to automate tasks, boost efficiency, and detect sophisticated threats that traditional methods might overlook.

Proactive Defense: With AI at your disposal, you'll be equipped for proactive threat hunting, anomaly detection, and predictive analysis to prevent cyber-attacks before they happen.

How C|EH v13 Powered by AI Redefines Your Cybersecurity Career

- | Experience the world's first ethical hacking program powered by AI
- | Master the five phases of ethical hacking integrated with AI
- | Achieve 40% efficiency and double your productivity with AI-driven skills
- | Learn how to hack AI systems
- | Become an AI expert with hands-on labs for practicing AI skills
- | Master the latest advanced attack techniques, trends, and countermeasures
- | Gain practical experience with 221 labs, attack vectors, and hacking tools
- | Experience with over 550 attack techniques
- | Explore 4,000+ commercial-grade hacking and security tools
- | Follow a unique four-phase learning framework: Learn, Certify, Engage, Compete
- | Practice hacking a real organization in a live cyber range
- | Validate your skills in a 6-hour practical exam or 4-hour knowledge-based exam
- | Compete with hackers in global CTF competitions on the latest issues
- | Earn the globally recognized No.1 Ethical Hacking Certification
- | Gain a certification that is approved and accredited by U.S. DoD 8140, ANAB 17024, and NCSC
- | Meet the rigorous standards of NICE 2.0 and the NIST Framework
- | Get the opportunity to be employed by top organizations including Fortune 500 companies, government, and private sector firms

What's New in The CEH v13

The C|EH v13 not only provides extensive hands-on coverage but also integrates AI into all five phases of ethical hacking:



Get C|EH Trained from Anywhere with our World-Class Instructors

1. Live-Online
2. Self-Paced Video Lectures
3. In-Person training
4. Masterclass

Master AI to **Automate Ethical Hacking** Tasks, to hack and defend against **AI systems**,

and boost your task **efficiency by 40%** in your job role.

Develop a Hacker's Mindset: Master the 5 Phases of Ethical Hacking and Gain AI Skills to Automate Them

1. Reconnaissance

| Learn to gather essential information about your target

2. Vulnerability Scanning

| Gain the ability to identify weaknesses in the target system

3. Gaining Access

| Learn how to actively exploit identified vulnerabilities

4. Maintaining Access

| Develop skills to maintain continued access to the target systems

5. Clearing Tracks

| Master the art of erasing any trace of your activities

Learn AI Tools:

- ShellGPT
- ChatGPT
- FraudGPT
- WormGPT
- DeepExploit
- Nebula
- Veed.io

And many more!

Learn to Hack AI Systems Based on OWASP's Top 10 AI Attack Vulnerabilities and Threats

In C|EH v13, you will not only master AI-driven cybersecurity but also learn to hack AI systems. This comprehensive training equips you with cutting-edge AI-driven skills, enhancing your ability to execute cybersecurity tasks with up to 40% greater efficiency, while significantly boosting your productivity.

Prompt Injection
Insecure Output Handling
Training Data Poisoning
Model Denial of Service
Supply Chain Vulnerabilities
Sensitive Information Disclosure
Insecure Plugin Design
Excessive Agency
Overreliance
Model Theft

C|EH v13 Gain Skills to Battle AI Against AI Your Ultimate Training Ground for Mastering AI-driven Cybersecurity Skills

C|EH v13 equips professionals with advanced skills to enhance their hacking techniques and leverage AI. Gain the expertise to:

Drive 40% efficiency in
cybersecurity tasks

Double your productivity
with AI-driven methods

Master the application of
AI in cybersecurity

Learn to hack AI systems

Explore multiple AI and GPT tools

Automate repetitive tasks

Detect advanced threats

Make informed decisions using
AI-enhanced analysis

Adapt to evolving threats
through AI-driven learning

Improve reporting with
AI-powered insights

CEH v13: **The World's First** Ethical Hacking Certification with a 4-Phase AI-Powered Learning Framework

The CEH v13 is a specialized, one-of-a-kind training program that helps you gain expertise in ethical hacking, AI, and machine learning. With hands-on training labs, knowledge-based and practical exams, a mock ethical hacking engagement on live networks, and a global hacking competition, this program ensures you master the most in-demand skills needed to excel and stand out in the cybersecurity industry.

This learning framework offers 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.

Master Ethical Hacking and AI Skills That Go Beyond Certification

Learn

Courseware
Cyber Range
Gain Skills

1

Certify

Knowledge-Based
Practical Exam
Gain Recognition

2

Engage

Live Cyber Range
Gain Experience

3

Compete

Global Ethical
Hacking Competition
Gain Respect

4

Beat Hackers in their Own Game with CEH v13! A Revolutionary Way to Learn Ethical Hacking

1. Learn

- 20 modules
- 2500+ pages of student manual
- 2000 pages of lab manual
- Over 221 hands-on labs to practice attack vectors and hacking tools
- AI integrated skills in the 5 phases of the ethical hacking framework
- Hacking AI system, based on the Top 10 OWASP vulnerabilities
- Over 4000 hacking and security tools
- Learn how to hack multiple operating systems (Windows 11, Windows servers, Linux, Ubuntu, Android)
- More than 50% of training time is dedicated to labs

2. Certify

Knowledge-Based Exam
(ANAB ISO 17024 and US DoD 8140)

- 4 hours
- 125 multiple-choice questions

Practical Exam
(ANAB ISO 17024 and US DoD 8140)

- 6 hours
- 20 real scenario based questions

3. Engage

- 4000 hacking tools
- 550 attack techniques
- Conduct a real-world ethical hacking assignment
- Apply the 5 phases
 1. Reconnaissance
 2. Scanning
 3. Gaining access
 4. Maintaining access
 5. Covering your tracks

4. Compete

- New challenges every month
- 4-hour CTF competition
- Compete with your peers worldwide
- Hack your way to the top of the leaderboard
- Focus on new attack vectors
- Exploit emerging vulnerabilities
- Challenges include:
 - Ransomware
 - Web app hacking and pen testing
 - Web app hardening
 - Reverse engineering
 - Unpatched software
 - Cryptography
 - System hacking
 - Encryption
 - Service exploitation
 - Hacking cloud networks
 - Incident response
 - ICS/SCADA
 - Forensic analysis

Learn

Learn ethical hacking with the revolutionary C|EH v13—a game-changer for aspiring ethical hackers.

With 20 cutting-edge modules, you'll gain the core skills needed to dominate the cybersecurity landscape. C|EH isn't just keeping pace—it's leading the charge, evolving with the latest operating systems, exploits, tools, and hacking techniques to ensure you're always ahead of the curve.

Dive deep into the future of cybersecurity with training that integrates AI into all five phases of ethical hacking, reconnaissance and scanning to gaining access, maintaining access, and covering tracks. You'll harness the power of AI to supercharge your hacking techniques and disrupt AI systems—giving you 10x efficiency in your cybersecurity role.

CEH v13 isn't just a certification; it's a fully immersive experience. CEH combines comprehensive knowledge-based training with immersive hands-on labs to ensure a well-rounded learning experience. You'll engage with live targets, tools, and vulnerable systems in a controlled environment, building real-world skills that empower you to confidently apply your expertise in any scenario. Get ready to transform the way you hack and protect the digital world!

Course Outline

Get the AI edge with
20 Power-packed
Modules of the CEH v13



Learn	Course Outline
Module 01 Introduction to Ethical Hacking	Learn the fundamentals and key issues in information security, including the basics of ethical hacking, information security controls, relevant laws, and standard procedures.
Module 02 Footprinting and Reconnaissance	Learn how to use the latest techniques and tools for footprinting and reconnaissance, a critical pre-attack phase of ethical hacking
Module 03 Scanning Networks	Learn different network scanning techniques and countermeasures.
Module 04 Enumeration	Learn various enumeration techniques, including 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 are also included.
Module 06 System Hacking	Learn about the various system hacking methodologies used to discover system and network vulnerabilities, including steganography, steganalysis attacks, and how to cover tracks.
Module 07 Malware Threats	Learn about different types of malware (Trojan, viruses, worms, etc.), APT and fileless malware, malware analysis procedures, and malware countermeasures.
Module 08 Sniffing	Learn about packet sniffing techniques and their uses for discovering network vulnerabilities, plus 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, plus the tools used to audit a target and devise DoS and DDoS countermeasures and protections.



Learn	Course Outline
Module 11 Session Hijacking	Learn 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	Learn about firewalls, intrusion detection systems (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 hacking methodology for auditing vulnerabilities in web applications and countermeasures.
Module 15 SQL Injection	Learn about SQL injection attack techniques, evasion techniques, and SQL injection countermeasures.
Module 16 Hacking Wireless Networks	Learn about different types of encryption, threats, hacking methodologies, hacking tools, security tools, and countermeasures for wireless networks.
Module 17 Hacking Mobile Platforms	Learn mobile platform attack vectors, Android and iOS hacking, mobile device management, mobile security guidelines, and security tools.
Module 18 IoT Hacking	Learn different types of Internet of Things (IoT) and operational technology (OT) attacks, hacking methodologies, hacking tools, and countermeasures.
Module 19 Cloud Computing	Learn different cloud computing concepts, such as container technologies and serverless computing, various cloud computing threats, attacks, hacking methodologies, 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.

Hands-On Learning Labs

With 221 hands-on labs in our cutting-edge cyber range, you'll practice every skill on live machines and real-world vulnerabilities. Armed with over 4,000 powerful hacking tools and a range of operating systems, you'll gain unrivaled, practical expertise with the most widely used security tools, current vulnerabilities, and industry-standard operating systems.

This revolutionary environment brings the industry's top security tools and the latest vulnerabilities to your fingertips, all in a web-accessible platform. No matter where you are, you can dive into the real-world experience and emerge as a force to be reckoned with in cybersecurity.

Lab Environment

Cloud-Based Cyber Range

What's Covered

100% virtualization for a complete learning experience

Full access to pre-configured targets, networks, and the attack tools necessary to exploit them:

Pre-configured vulnerable websites

Vulnerable, unpatched operating systems

Fully networked environments

4000+ hacking tools and so much more!

Wide range of target platforms to hone your skills

550 attack techniques covered

Objective-oriented flags for critical thinking and applied knowledge assessment

Cloud-based cyber range

Certify

Prove Your Skills and Abilities with Online, Practical Examinations

CEH Exams: 4-hour Knowledge-Based Exam and 6-hour Practical Exam.

In the C|EH v13, a student has the option to attempt both the exams: a knowledge-based exam and a practical exam for the C|EH Master certification. Both these exams are approved by the U.S. DoD 8140 and accredited by ANAB ISO/IEC 17024.

Industry practitioners meticulously vet certification domains to align with current industry demands. Each exam undergoes rigorous psychometric evaluation, ensuring a fair and accurate assessment of your ethical hacking expertise.

Achieving the C|EH certification and passing both the knowledge-based and practical exams earns you the prestigious C|EH Master certification. This advanced recognition demonstrates not only your theoretical understanding but also your mastery of real-world ethical hacking skills, proving you're ready to excel in any cybersecurity role.

Certification Outline

Knowledge Exam
4 Hours
Multiple-Choice Exam

Skills Exam
6 Hours
20 Practical Challenges



Engage

The C|EH v13 program immerses you in real-world ethical hacking through the dynamic C|EH practice environment. With C|EH Engage, you'll sharpen your skills and prove you have what it takes to thrive as an ethical hacker.

New to C|EH v13, learners will embark on their first emulated ethical hacking engagement. This four-phase engagement requires students to think critically and test the knowledge and skills gained by capturing a series of flags in each phase. It demonstrates the live application of skills and abilities in a consequence-free environment through EC-Council's new "Cyber Range."

As you complete your training and labs, C|EH Engage empowers you to put theory into practice through a mock hacking engagement. You'll navigate a real-world, four-part engagement, targeting an emulated organization. Using a capture-the-flag format, you'll progress by answering critical "flag" questions, gaining hands-on experience in a full-scale ethical hacking operation.

Your Mission:

Whether this is your first engagement or you're honing your skills, get ready to test your ethical hacking knowledge like never before! Once you've practiced through the hands-on guided labs, it's time to apply your knowledge, take on the hacker's persona, and find the vulnerabilities and weaknesses in the ABCD organization (fictitious organization, but with real live networks)—all built within our C|EH Engage (practice range).

Target Organization Characteristics

- ABCDorg is a nationwide IT/ITES organization
- Realistic segmented networks
- Demilitarized zones (DMZs) and private subnets stretch across the infrastructure to support various business units
- Various application servers and services support ABCDorg Operations
- Real networks, real operating systems, and real applications
- Private, dedicated access — no shared resources
- Fully automated network deployment with EC-Council's Cyber Range
- 24x7 browser-based access

Objectives

Armed with your attack platform (Parrot OS) and a plethora of tools used by ethical hackers, you will embark on a 4-part engagement to assess ABCDorg's security posture. Follow the process, practice your TTP, and experience the real thing in a controlled environment with no consequences. It's the ultimate learning experience to support your career as an ethical hacker! Each phase builds on the last as you progress through your ABCDorg engagement.

Phase 1

Vulnerability assessment:

- Footprinting & Reconnaissance
- Scanning
- Enumeration
- Vulnerability Analysis

Phase 2

Gaining access:

- System Hacking
- Malware Threats
- Sniffing
- Social Engineering
- Denial-of-Service

Phase 4

Mobile, IoT, OT Exploitation:

- Hacking Wireless Networks
- Hacking Mobile Platforms
- IoT Hacking
- OT Hacking
- Cloud Computing
- Cryptography

Phase 3

Perimeter and Web App Exploitation:

- Session Hijacking
- Evading IDS
- Firewalls
- Honeypots
- Hacking Web Servers
- Hacking Web Applications
- SQL Injection

Stay Ahead of Emerging Threats:

New Focus Areas and Trends in C|EH v13

Trained to think outside the box with a hacker's mindset, individuals who pursue the Certified Ethical Hacker (C|EH) v13 thoroughly explore top OWASP attacks, active directory breaches, the vulnerability of traditional encryption to quantum computing, the growing ransomware threat, and other emerging risks, equipping learners with strategies to implement zero trust architecture and other cybersecurity measures. C|EH v13 is comprehensive with the latest knowledge, providing cybersecurity professionals with the skills, tools, techniques, and strategies to defend against trending, modern, and complex cyber threats effectively and efficiently.

Active Directory Attacks

Ransomware Attacks and Mitigation

AI and Machine Learning in Cybersecurity

Critical Infrastructure Vulnerabilities

Extended Detection and Response (XDR)

Quantum Computing Risks and Attacks

Post-Quantum Cryptography

Deepfake Threats

Zero Trust Architecture

Cloud Security

IoT Security Challenges

Critical Infrastructure Vulnerabilities

CEH Skills Mapped To 49 Cybersecurity Job Roles

1. Mid-Level Information Security Auditor
2. Cybersecurity Auditor
3. Security Administrator
4. IT Security Administrator
5. Information Security Analyst 1
6. Infosec Security Administrator
7. Cybersecurity Analyst (Level 1, Level 2, & Level 3)
8. Network Security Engineer
9. SOC Security Analyst
10. Network Engineer
11. Senior Security Consultant
12. Information Security Manager
13. Senior SOC Analyst
14. Solution Architect
15. Cybersecurity Consultant
16. Cyber Defense Analyst
17. Vulnerability Assessment Analyst
18. Warning Analyst
19. All-Source Analyst
20. Cyber Defense Incident Responder
21. Research & Development Specialist
22. Senior Cloud Security Analyst
23. Third Party Risk Management:
24. Threat Hunting Analyst
25. Penetration Tester
26. Cyber Delivery Manager
27. Application Security Risk
28. Threat Modelling Specialist
29. Web Application Penetration Testing
30. SAP Vulnerability Management – Solution Delivery Advisor
31. Ethical Hacker
32. SIEM Threat Responder
33. Product Security Engineer / Manager
34. Endpoint Security Engineer
35. Cybersecurity Instructor
36. Red Team Specialist
37. Data Protection & Privacy Officer
38. SOAR Engineer
39. AI Security Engineer
40. Sr. IAM Engineer
41. PCI Security Advisor
42. Exploitation Analyst (EA)
43. Zero Trust Solutions Engineer / Analyst
44. Cryptographic Engineer
45. AI/ML Security Engineer
46. Machine Learning Security Specialist
47. AI Penetration Tester
48. AI/ ML Security Consultant
49. Crypto Security Consultant

PROGRAM BRIEF

Certified Ethical Hacker (C|EH) v13 is a globally acclaimed course by EC-Council, USA, that provides advanced ethical hacking skills crucial for information security professionals. This certification equips professionals with critical techniques and tools to detect and safeguard against vulnerabilities in organizational network and system infrastructures. The C|EH v13 program integrates hands-on labs, assessments, a mock engagement, and real-world hacking competitions under its Learn | Certify | Engage | Compet framework, delivering the most comprehensive, practical training for mastering ethical hacking. CICRA CAMPUS, a pioneering institution in Cyber Security and Ethical Hacking education in Sri Lanka, upholds a strong legacy, having trained over 1,000 ethical hackers across 41 batches with highly qualified international trainers. Recognized for its high standards in cybersecurity education, CICRA ensures graduates gain not only certification but also industry-relevant skills to excel in their careers.

TRAINER PROFILE

- 🏆 **WORLD'S 1st Certified Penetration Tester (CPENT)**
- 🏆 **EC Council Master Trainer**
- 🏆 **Winner of EC Council Excellence Awards**



Belly Rachdianto

- ✓ **Ecourseware**
- ✓ **Exam voucher**
- ✓ **Extra 1 Exam retake vouchers 6**
- ✓ **months official iLabs**
- ✓ **CEH Practical exam voucher**
- ✓ **10 Ethical Hacking Video**
- ✓ **courses CEH Engage**
- ✓ **Global CEH Challenge**

DURATION

5 Full day trainings

DELIVERY

Weekend

O N L I N E

ENTRY

Working professionals or
undergraduates in relevant field

CICRA STUDY PATHWAYS

[Click here to view](#)

TECHNICAL REQUIREMENTS

- **PC requirements**
 - Recommended requirements - i5 Processor with 16GB ram and 150 GB free Hard Disk Space.
 - Minimum requirements - i3 Processor with 12GB ram and 150 GB free Hard Disk Space.
- **Data usage** - 70 GB
- **Required softwares** - VMware workstation 14
- **Practical Sessions** - Yes (VM, Windows are used with several hacking tools)
- **Way of sharing software** - Using google drive

ACADEMIC PARTNER

- ▶ Established in 148 countries
- ▶ World's largest cyber security technical certification awarding Institute
- ▶ Accredited by Department of Defence (DoD)
- ▶ Accredited by the Distance Education Accrediting Commission (DEAC)
- ▶ Recognised by the US Department of Labour's Occupational Information Network (O*NET)
- ▶ Recognised by the Malaysian Military Cyber Security Warfare Department (KOMLEK)

EC-Council

ABOUT CICRA

CICRA
C A M P U S

- ▶ Pioneers in cyber security education in Sri Lanka with over 12 years of excellence
- ▶ 2000+ Alumni
- ▶ 800+ Ethical Hackers
- ▶ Continued Academic excellence
- ▶ Partnered with leading universities and certifications awarding entities in UK, Australia, USA and Malaysia
- ▶ Award winning organization for system innovation
- ▶ Partnerships with leading business conglomerates in Sri Lanka for internship opportunities

AWARDS



E Swabhimani Award for Business & Commerce 2020 | Microsoft Partner of the year 2022 - Raising Azure Technology Award | National ICT award (NBQSA) 2021
EC Council Circle of Excellence award | Best Client Delivery Innovation - Regional winner - Western Province | Best Client Delivery Innovation - National winner
Best Disruptive product Innovation - Regional winner - Western Province | Best Disruptive product Innovation - National winner

HOW TO REGISTER

Step 1 : Click the link below and fill the registration form

Step 2 : Make the payment for below account details and send the payment receipt:

Account Name: CICRA CAMPUS (Pvt) Ltd.

Account Number: 0009 1000 8366

Bank: Sampath Bank PLC

Branch: Nawam Mawatha

Step 3 : Submit below documents along with the payment receipt to complete the registrations.

All documents should be English and in PDF format with proper titles. (eg- Shehan - ID copy)

1. Sign the student agreement provided by the CICRA student counselor
2. NIC/ Valid passport
3. 1 Passport size coloured photograph
4. Non Disclosure Form (NDA)

Step 4 : You will receive the payment acknowledgement from the finance team within 1 working day

Step 5 : Academic department will share the login credentials before the course commencement with training instructions

CLICK HERE TO

REGISTER

No 245, Srimath Anagarika Dharmapala Mawatha, Colombo 07

www.cicra.edu.lk | 071 060 0800

