Address - # 215, 1st Floor, Shashi Arcade,
New BEL Road, Sanjay Nagar,
Bangalore 560054 (India),

info@ehackacademy.com
https://www.ehackacademy.com

+91-98860 35330
Landline 080 - 4131 4190
080 - 4218 5443

EC-Council

eHACK ACADEMY

Your Future Starts Here...

Rise in Digitization leads to increase in number of Cyber Attacks..
As Data Keeps Increasing, Concern about its Security…

SOLUTION???? CYBERSECURITY

EC-Council

eHACK ACADEMY

WHO ARE WE...

eHack Academy is One of the foremost Training Centers in Bangalore for providing Cyber Security Courses. We began our academy in the year 2015 and started providing Cyber Security and networking training along with International Certifications.

eHack Academy provides you a good high-end Infrastructure with latest Technology and certified Instructors for the students to have effective and quality education. We help our students to enhance their Knowledge and skills related to Cyber Security, enhancing their carrier opportunities in this field.

We have organized 50+ workshops throughout India and have provided different kinds of learning Techniques for the betterment of the students. Through our innovative Analysis we help our students bring a change in the cyber World. We prepare our students to Protect Data and crimes in the Cyber World, which will be priceless experience to enhance one's Resume.

We have launched customized program to create awareness and risk factors involved when data is breached. We have created these courses to enable all our students, working Professionals, and other individuals become aware of cyber security.

eHack Academy Accredition with EC Council

EC-Council Accredited Training Center

EHACK Academy is a Cybersecurity Training & Consultancy Company, Having foot prints in 50 Cities in India through its Business Satellite Centres. EHACK ACADEMY is a largest Accredited Training Partner of EC-Council. Ehack Flagship Programs like Advanced Diploma, Graduate and Master's Program with Global Certifications on VAPT, Digital Forensics, Network Defence and Cloud Security Engineering gives students expertise on each cybersecurity Vertical and that makes them land in their dream Career.

Why eHack Academy?

Passion for Excellence in Information Security

Real Time Labs

Since we are associated with EC-council and CISCO, we ensure that our candidates get exposed of real time labs, of how the vulnerabilities are found and exploited? How the pen testing is done for a network? We render our students to perform activities with tools provided by the EC-Council during the course.

World Class Infrastructure

Our lab infrastructure is built according to EC-council and Cisco standards, enabling our students understand the subject with ease. Complemented with Dedicated high-speed broadband connectivity. Our Students can utilize the well stacked library resources.

Certified Faculties

eHack academy provides the latest internationally practiced technological knowledge for enriching student's carrier. Our experienced instructors are duly certified by EC-Council and CISCO.

EC-Council

eHACK ACADEMY

Four Major Reasons to opt for Cyber Security Career

1. High employer demand, fabulous salaries, great promotion prospects
2. Thanks to the pace of technology, the field of cyber security is changing at very high speed.
3. New Emerging Technologies, New kind of Attacks and New challenges every day.
4. The Job has a real Impact.

Consultancy Services:

All Type of Customers: Including Private Companies, Corporates, Private Individuals etc. as following:

- **Providing Workforce of Cyber Forensic and Cyber Security Analysts to our customers.**
- **Vulnerability Assessment to check and hardening the security of the PC's and Network for bugs and Security issues.**
- **VAPT audit for organizations.**
- **Hard Disk Cloning Services for Single and Bulk Hard Drives. To copy/replicate One Hard Drive to another or many at High Speed as well as Hard Disk Data Analysis.**
- **Data Recovery from Hard Drives, Pen drives, Memory Cards, etc. for recovery of Lost or Deleted or accidentally Formatted Drives as well as RAID Data Recovery.**
- **Password Breaking of Encrypted Files likes Word/Excel/PDF, etc.**
- **Awareness Workshops and training Programs on Forensic Investigation.**
- **Information Security Compliance/Auditing for protection of Valuable Data and IPs.**

EC-Council

iHACK ACADEMY

CYBER SECURITY PROGRAMS

Over 1,200
Highly Qualified
Certified Instructors

145+
Countries

700+
Locations

Over 4,200
Classes Annually
in Cyber Security

www.eccouncil.org

Table of Contents

Tracks

Certifications

Academic Programs

Who We Are

The EC-Council group is made up of several entities that all help serve the same goal which is to create a better, safer cyber world through awareness and education. Our entities include International Council of eCommerce Consultants (EC-Council), iClass, EC-Council University, EC-Council Global Services (EGS), and EC-Council Conferences and Events.

EC-Council creates content (course materials and exams) and certification delivered through our channel of authorized training centers which consists of over 700 partners representing over 2,000 physical locations in more than 145 countries across the globe. We are the owner and developer of the world-famous Certified Ethical Hacker (CEH), Computer Hacking Forensics Investigator (CHFI), EC-Council Certified Security Analyst (ECSA), and License Penetration Tester (LPT)(Master) programs.

Our certification programs are recognized worldwide and have received endorsements from various government agencies, including the United States Federal Government (via the Montgomery GI Bill), the National Security Agency (NSA), and the Committee on National Security Systems (CNSS). All these reputed organizations have certified Certified Ethical Hacking (CEH), Computer Hacking Forensics Investigator (CHFI), EC-Council Disaster Recovery Professional (EDRP), EC-Council Certified Security Analyst (ECSA) and The Advanced Penetration Testing Program and The Licensed Penetration Tester (LPT) (Master) programs for meeting the 4011, 4012, 4013A, 4014, 4015 and 4016 training standards for information security professionals. EC-Council has received accreditation from the American National Standards Institute (ANSI) for our coveted CEH, CCISO, CHFI, and CND programs. We have so far certified over 2,20,000 professionals in various e-business and cybersecurity skills.

iClass is EC-Councils direct certification training program. iClass delivers EC-Council certification courses through various training methodologies: instructor-led at client facilities, synchronous delivery through live, online instructor-led, and asynchronously through our streaming video platform. iClass course videos can also be loaded onto a mobile device, such as an iPad, and shipped to a client location.

"Our lives are dedicated to the mitigation and remediation of the cyber plague that is menacing the world today"

Jay Bavisi
President & CEO
EC-Council

EC-Council University is accredited by the Distance Education Accrediting Commission. The university offering programs such as Bachelor of Science in Cyber Security, Master of Science in Cyber Security, and Graduate Certificate Program.

EC-Council Global Services (EGS) is dedicated to helping organizations understand and manage their cyber-security risk posture effectively. EGS specializes in helping clients make informed business decisions to protect their organizations. EGS has over 20 dedicated cyber security practice areas informed by the best cyber security practitioners, each of whom have dedicated their lives to defending organizations from cyber-attacks.

EC-Councils Conference and Events Group is responsible for planning, organizing, and running conferences throughout the globe. TakeDownCon and Hacker Halted are IT security conferences that bring world renowned speakers together for keynotes, panels, debates, and breakout sessions. Conferences have been run in Dallas, Las Vegas, St. Louis, Huntsville, Maryland, Connecticut, Myrtle Beach, Miami, Atlanta, Iceland, Hong Kong, Egypt, Singapore, Mumbai, Dubai, Bahrain, London, Abu Dhabi and Kuala Lumpur.

Other events include CISO Summits, Global CISO Forums, and Executive Cocktail Receptions where EC-Council brings speakers and content to executive level IT Security Professionals.

The Global Cyberlympics competition is acapture the flag type competition with approximately 1,000 global participants. EC-Council brings the hackers together online for preliminary elimination rounds and then brings the top two teams (6-8 players per team) from each region to compete in the final head-to-head competition.

Pentagon trains workers to hack Defense computers

March 10, 2010 | By Larry Shaughnessy, CNN Pentagon Producer

CNN

The Pentagon is training people to hack into its own computer networks.

"To beat a hacker, you need to think like one," said Jay Bavisi, co-founder and president of the International Council of Electronic Commerce Consultants, or EC-Council. His company was chosen by the Pentagon to oversee training of Department of Defense employees who work in computer security-related jobs and certify them when the training is complete.

The idea behind the Pentagon's training is that thinking like a hacker can beat a hacker.

The Department of Defense does not consider this hacking.

"DoD personnel are not learning to hack. They are learning to defend the network against hackers," said spokesman Lt. Col. Eric Butterbaugh.

"EC-Council - Trusted worldwide for its end-to-end enterprise cyber security solutions for human capital development"

EC-Council

eHACK ACADEMY

EC-Council at a Glance

EC-Council Group is a multidisciplinary institution of global Information Security professional services.

EC-Council Group is a dedicated Information Security organization that aims at creating knowledge, facilitating innovation, executing research, implementing development, and nurturing subject matter experts in order to provide their unique skills and niche expertise in cybersecurity.

Some of the finest organizations around the world such as the US Army, US Navy, DoD, the FBI, Microsoft, IBM, and the United Nations have trusted EC-Council to develop and advance their security infrastructure.

ICECC
International Council of E-Commerce Consultants
EC-Council Group

ECC
EC-Council Training & Certification
Division of Professional Workforce Development

EGS
EC-Council Global Services
Division of Corporate Consulting & Advisory Services

ECCU
EC-Council University
Division of Academic Education

EGE
EC-Council Global Events
Division of Conferences, Forums, Summits, Workshops & Industry Awards

ECF
EC-Council Foundation
Non-Profit Organization for Cyber Security Awareness Increase.

19+ YEARS EXPERIENCE

40+ TRAINING & CERTIFICATION PROGRAMS

145+ COUNTRIES

1000+ SUBJECT MATTER EXPERTS

2830+ TRAINING PARTNERS WORLDWIDE

3000+ TOOLS & TECHNOLOGIES

237,580+

CERTIFIED MEMBERS

Accreditations

American National Standards Institute (ANSI)

EC-Council has achieved accreditation for its Certified Ethical Hacker (C|EH), Certified Chief Information Security Officer (C|CISO), Certified Network Defender (C|ND), and Computer Hacking Forensic Investigator (C|HFI), to meet the ANSI/ISO/IEC 17024 Personnel Certification Accreditation standard. EC-Council is one of a handful of certification bodies, whose primary specialization is information security, to be awarded this much sought-after quality standard.

Candidates who complete the EC-Council Certified Ethical Hacker (C|EH), Computer Hacking Forensics Investigator (C|HFI), Certified Network Defender (C|ND), and Certified Chief Information Security Officer (C|CISO) certification will also have that extra credential meeting the requirements of the respective ANSI Certification Training Standards.

Accreditation Certificate

Committee on National Security Systems (CNSS) & National Security Agency (NSA)

EC-Council was honored at the 13th Colloquium for Information Systems Security Education (CISSE) by the United States National Security Agency (NSA) and the Committee on National Security Systems (CNSS) when its Certified Ethical Hacker (CEH), Computer Hacking Forensics Investigator (CHFI), Disaster Recovery Professional (EDRP), Certified Security Analyst (ECSA) and Licensed Penetration Tester (LPT) courseware was certified to have met the 4012 (Senior System Managers), 4013A (System Administrators), 4014 (Information Systems Security Officers), 4015 (Systems Certifiers) and 4016 (Information Security Risk Analyst) training standards for information security professionals in the federal government. The CNSS is a federal government entity under the U.S. Department of Defense that providesprocedures and guidance for the protection of national security systems.

Candidates who complete the EC-Council Certified Ethical Hacker (CEH), Computer Hacking Forensics Investigator (CHFI), Disaster Recovery Professional (EDRP), Certified Security Analyst (ECSA) or Licensed Penetration Tester (LPT) certification will also have that extra credential meeting the requirements of the respective CNSS 4011-4016 Federal Security Certification Training Standards.

Department of Defense (DoD)

EC-Council Certified Ethical Hacker (CEH), Computer Hacking Forensic Investigator (C|HFI), and Certified Chief Information Security Officer programs are formally integrated as baseline skill certification options for the U.S. Department of Defense (DoD) cyber workforce in several categories. Specifically, the C|CISO program is a recognized certification for the DoD IAM Level II, IAM Level III, and CSSP Manager, all specialized cyber management personnel classifications within the DoDs information assurance workforce. C|HFI is now recognized as a baseline certification for CSSP Incident Responder and C|EH is now required for the DoDs computer network defenders (CNDs) CND Analyst, CND Infrastructure Support, CND Incident Responder, and CND Auditor.

NCSC Certified Training

EC-Council has achieved accreditation for its Certified Ethical Hacker (C|EH), Certified Security Analyst (ECSA), and Chief Information Security Officer (C|CISO), to meet the GCHQ Certified Training standard. This recognition is a feather in the cap for EC-Council s much sought-after credentials, which are among the most comprehensive programs in the field of Vulnerability Assessment and Penetration Testing, and Information Security Leadership.

This affirms EC-Councils commitment to offering high-quality certification programs that are developed to help arm information security professionals with the right skills to safeguard the cyber world and achieve successful professional roles.

CREST Equivalency

Leading cyber security certification bodies CREST and EC-Council have announced mutual equivalency for their professional entry-point technical qualifications. The direct equivalency relates to the EC-Council Security Analyst (ECSA v10) qualification with the CREST Practitioner Security Analyst (CPSA) qualification. In addition, equivalency can also be granted for the for ECSA (Practical) with the CREST Registered Tester (CRT) certification, provided that the candidate already holds a valid CREST CPSA qualification.

National Infocomm Competency Framework (NICF)

EC-Council Certified Ethical Hacker (CEH) and Computer Hacking Forensic Investigator (CHFI) programs have been accepted into National Infocomm Competency Framework (NICF) Infocomm professionals competency requirement list. In addition to the inclusion, Infocomm professionals training to be certified for the EC-Council programs at NICF accredited training centers, will be entitled to receive partial funding from Critical Infocomm Technology Resource Program (CITREP) upon certification completion.

NICF determines the skills and competencies; and develops training strategies for Infocomm professionals to build a niche Infocomm workforce in Singapore. CITREP is a training incentive program that assists Infocomm professionals with funding to gain recognized and specialized skills.

Department of Veterans Affairs

The Department of Veterans Affairs has included EC-Council Certified Ethical Hacker (CEH), Computer Hacking Forensic Investigator (CHFI), and EC-Council Certified Security Analyst (ECSA) under its GI Bill® for the reimbursement of test fees for veterans and other eligible persons in accordance with the provisions of PL 106-4

Distance Education Accrediting Commission (DEAC)

EC-Council University is accredited by the Distance Education Accrediting Commission. The Distance Education Accrediting Commission is listed by the U.S. Department of Education as a recognized accrediting agency. The Distance Education Accrediting Commission is recognized by the Council for Higher Education Accreditation (CHEA).

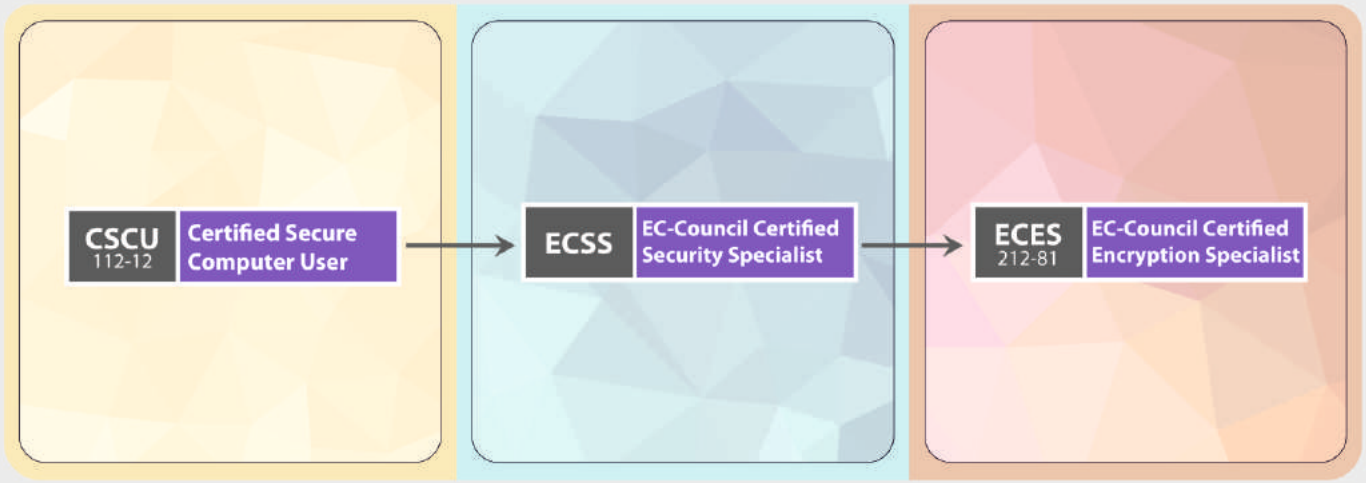
CHEA
Accredited by a CHEA-recognized accrediting organization

A national advocate and institutional voice for promoting academic quality through accreditation, CHEA is an association of 3,000 degree-granting colleges and universities and recognizes approximately 60 institutional and programmatic accrediting organizations.
EC-Council University as well as our accreditor are acknowledged members of The Council for Higher Accreditation (CHEA).

EC-Council

eHACK ACADEMY

Foundation Track



Target Audience

This track focuses on todays computer users who use the internet extensively to work, study and play.

What will You Learn

- Cloud Security
- Password Security
- Social Engineering Countermeasures
- Mitigating Identity Theft
- Email Security
- Safe Browsing
- Data Protection
- Physical Security
- Mobile Device Security
- Encryption
- Social Network Security
- Antiviruses Protection
- Disaster Recovery
- Internet Security
- Credit Card Security
- Monitoring Kids Online
- Wireless & Home Network Security
- OS Security

Our Certified Foundation Professionals are Employed at:

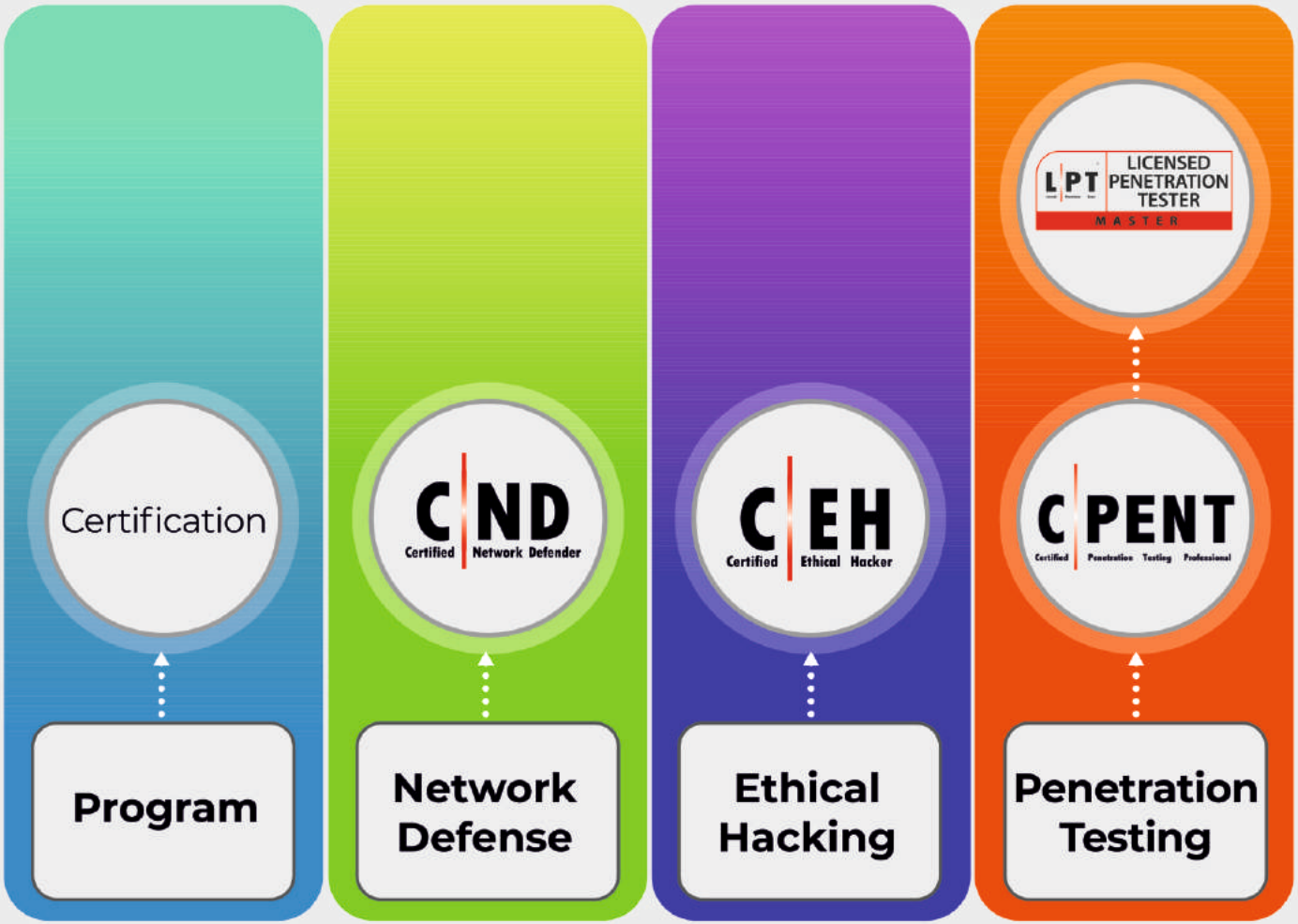
Caritas · Grant Thornton · IBM · PALADION · Poly technique · Unique Academy · NTT DATA · happiest minds · ingenia · icddr,b · Bank · vodafone · UNP · RELIANCE · core4 factory · Nestlé · • • •

*All credentials can be attained individually. Please refer to cert.eccouncil.org for the eligibility criteria.

EC-Council

eHACK ACADEMY

Vulnerability Assessment & Penetration Testing (VAPT)



Job Roles

- Information Assurance (IA) Security Officer
- Information Security Analyst/Administrator
- Information Security Manager/Specialist
- Information Systems Security Engineer/Manager
- Security Analyst
- Information Security Officers
- Information Security Auditors
- Risk/Vulnerability Analyst

Our Certified VAPT Professionals are Employed at:

cisco, EY, Microsoft, accenture, Infosys, amazon, AIG, hp, Bank of America, Booz | Allen | Hamilton, Capgemini, Deloitte., NEC, bugcrowd, TATA, lastline, axiata, U.S. ARMY, Marriott, Hero

This track maps to NICEs Specialty Areas:

1. Protect and Defend (PR)
- a. Cybersecurity Defense Analysis (DA)
- b. Cybersecurity Defense Infrastructure Support (INF)
- c. Incident Response (IR)
- d. Vulnerability Assessment and Management (VA)

2. Securely Provision (SP)
- a. Test and Evaluation

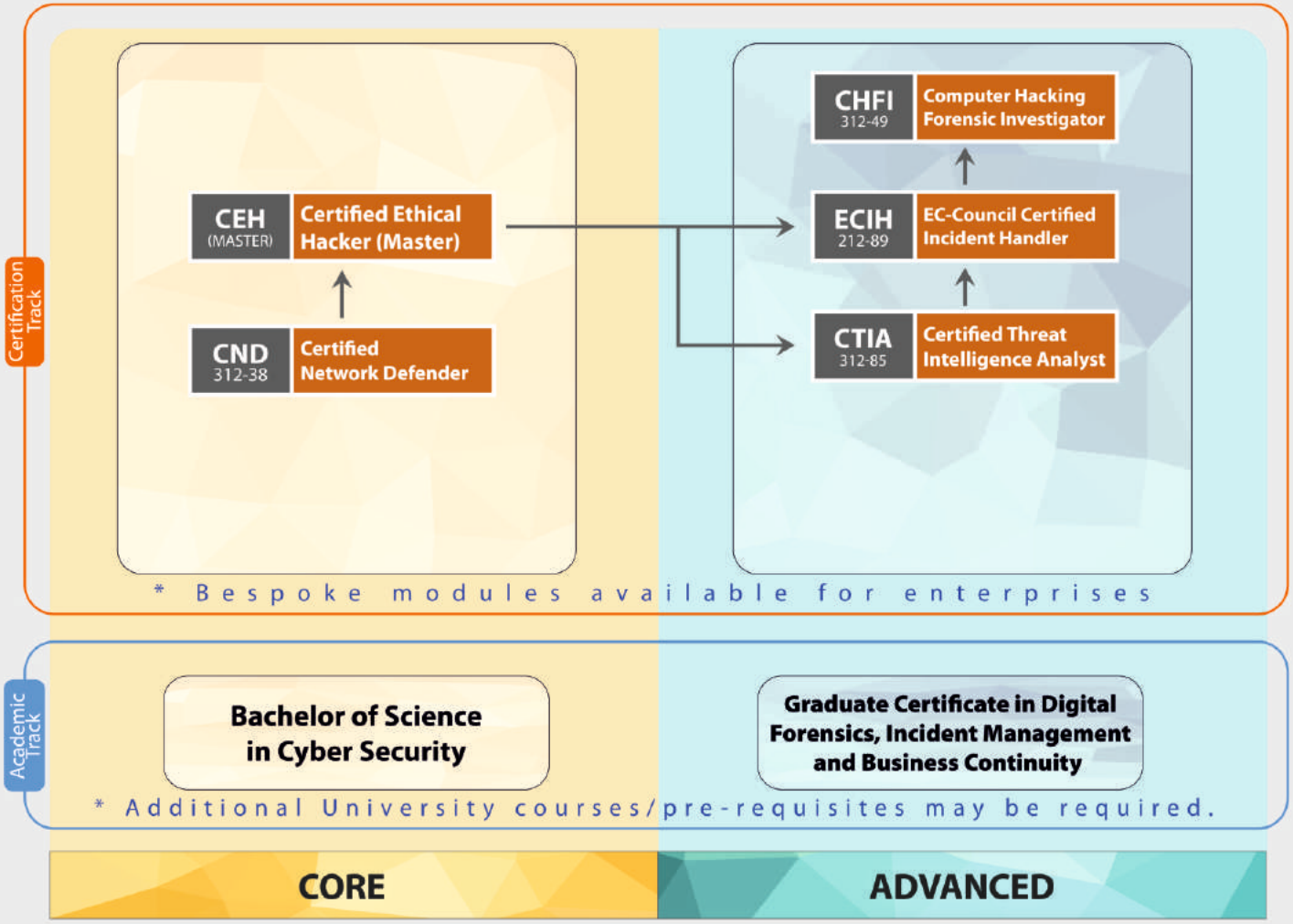
3. Analyze (AN)
- a. Threat Analysis (TA)
- b. Exploitation Analysis (XA)

**All credentials can be attained individually. Please refer to cert.eccouncil.org for the eligibility criteria.*

EC-Council

eHACK ACADEMY

Cyber Forensics



Job Roles

- Computer Forensic Analyst
- Computer Network Defense (CND)
- Forensic Analyst
- Digital Forensic Examiner

This Track Maps to NICE's Specialty Areas:

1. Securely Provision (SP)
a. Risk Management (RM)
b. Test and Evaluation

2. Operate and Maintain (OM)
a. Network Services (NET)
b. Systems Administration (SA)
c. Systems Analysis (AN)

3. Oversee and Govern (OV)
a. Cybersecurity Management (MG)

4. Protect and Defend (PR)
a. Cybersecurity Defense Analysis (DA)
b. Cybersecurity Defense Infrastructure Support (INF)
c. Incident Response (IR)
d. Vulnerability Assessment and Management (VA)

5. Analyze (AN)
a. Threat Analysis (TA)
b. Exploitation Analysis (XA)

Our Certified Cyber Forensic Professionals are Employed at:

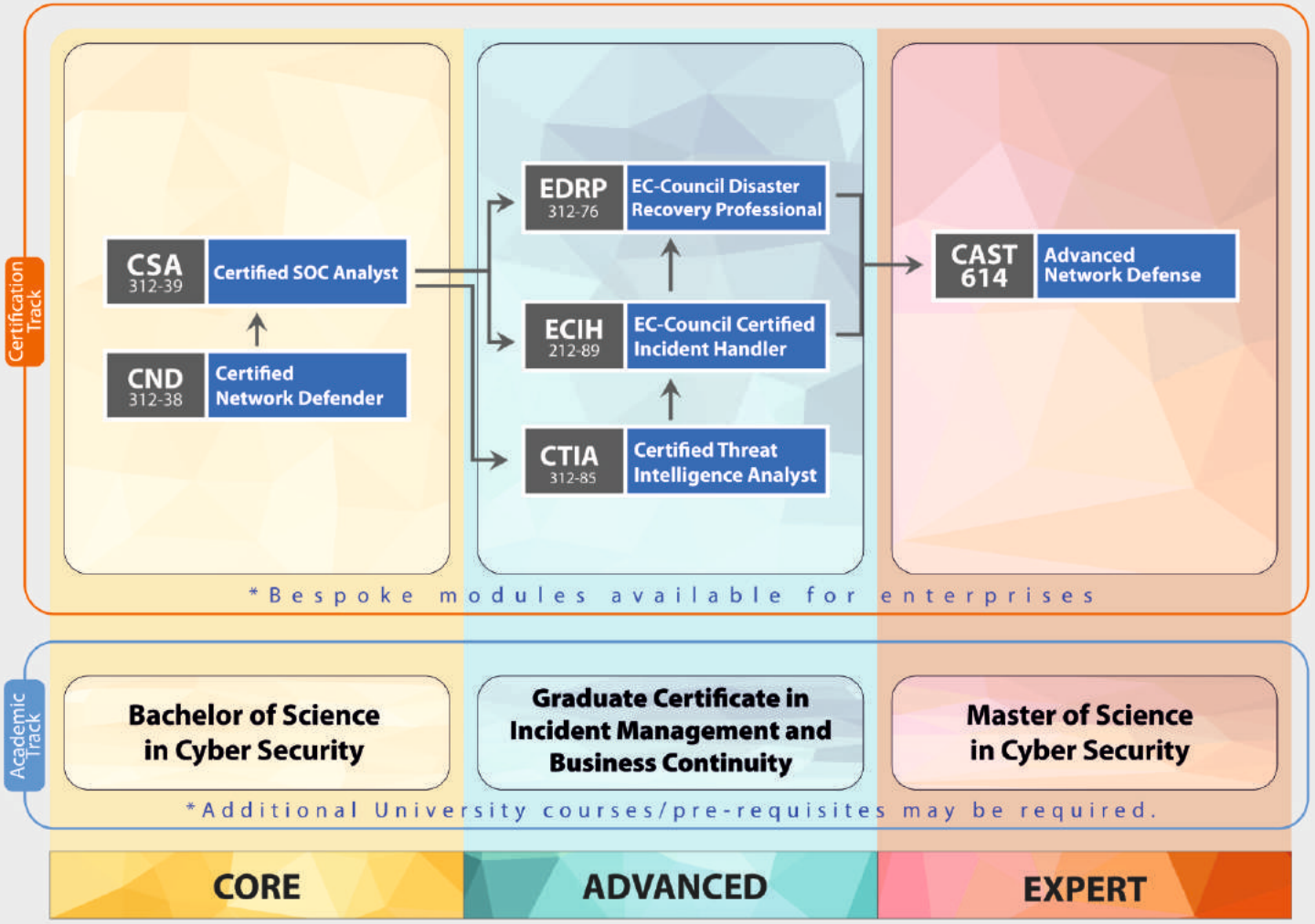
BARCLAYS, AIG, accenture, Infosys, U.S. ARMY, ICICI Bank, Bank of America, HDFC BANK, h+k, BMC SWITZERLAND, Telkom Indonesia, LEXINGTON MEDICAL CENTER, pwc, du, HSBC, WIPRO, ...

*All credentials can be attained individually. Please refer to cert.eccouncil.org for the eligibility criteria.

EC-Council

eHACK ACADEMY

Network Defense and Operations



Job Roles

- Network Security Administrators
- Network Security Engineer/Specialist
- Network Defense Technicians
- Security Analyst
- Security Operator
- Computer Network Defense(CND) Analyst
- Cybersecurity Intelligence Analyst
- Enterprise Network Defense(END) Analyst

Our Certified Network Defense Professionals are Employed at:

FGB, IBM, KPMG, DISA, mitra solusi telematika, Ameriprise Financial, COMCAST, NCB الأهلي, IPDC Finance, Johnson Controls, sopra steria Consulting, Rockwell Automation, MAPFRE, • • •

This Track Maps to NICE's Specialty Areas:

1. Securely Provision (SP)
a. Risk Management (RM)
b. Test and Evaluation (TE)

2. Operate and Maintain (OM)
a. Network Services (NET)
b. Systems Administration (SA)
c. Systems Analysis (AN)

3. Oversee and Govern (OV)
a. Cybersecurity Management (MG)

4. Protect and Defend (PR)
a. Cybersecurity Defense Analysis (DA)
b. Cybersecurity Defense Infrastructure Support (INF)
c. Incident Response (IR)
d. Vulnerability Assessment and Management (VA)

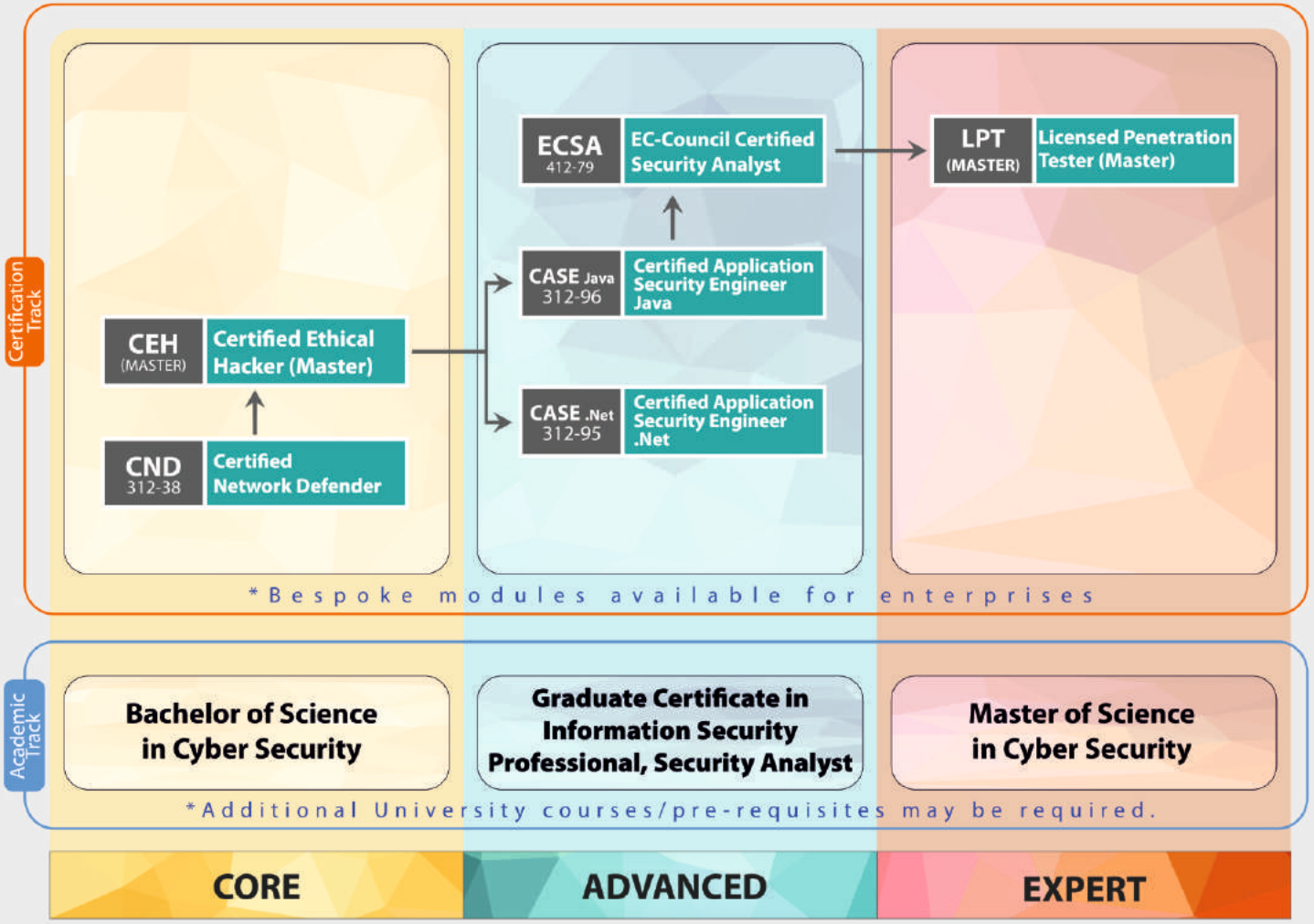
5. Analyze (AN)
a. Threat Analysis (TA)

*All credentials can be attained individually. Please refer to cert.eccouncil.org for the eligibility criteria.

EC-Council

iHACK ACADEMY

Software Security



Job Roles

- Secure Software Engineer
- Security Engineer
- Software Developer
- Software Engineer/Architect
- Systems Analyst
- Web Application Developer
- Application Security Tester

Our Certified Software Security Professionals are Employed at:

WELLS FARGO, ITU, AIRBUS, TATA, axiata, BlueCross BlueShield, bol.com, alBaraka, Cognizant, Deloitte., EY Building a better, ecovadis, Infoblox CONTROL YOUR NETWORK, KASPERSKY, . . .

This Track Maps to NICEs Specialty Areas:

1. Securely Provision
a. Software Development (DEV)
b. Technology (RD)

2. Operate and Maintain (0M)
a. Data Administration (DA)
b. Systems Analysis (AN)

3. Oversee and Govern (OV)
a. Cybersecurity Management (MG)

4. Protect and Defend (PR)
a. Cybersecurity Defense Analysis (DA)
b. Vulnerability Assessment and Management (VA)

5. 5. Analyze (AN)
a. Analyzes collected information to identify vulnerabilities and potential for exploitation.

*All credentials can be attained individually. Please refer to cert.eccouncil.org for the eligibility criteria.

EC-Council

eHACK ACADEMY

Governance

Master of Science in Cyber Security

Graduate Certificate in:

- **Information Security Professional**
- **Executive Leadership in Information Assurance**

Job Roles

- Chief Information Security Officer (CISO)
- Chief Security Officer (CSO)
- Information Security (IS) Director
- Information Assurance (IA) Program Manager

Our Certified CCISO Professionals are Employed at:

marta, U.S. Army, Akamai, MUFG, Santander, BOFI Federal Bank, Chase, Chemical Bank, Generali, Government of South Australia, KPMG, Malwarebytes, Police Department, Polycom, Rockwell Collins, Tadawul, The Bancorp, GE, HSBC, ICF, Juniper Networks, L'Oréal, Rabobank, vodafone, TELSTRA, ...

This Track Maps to NICEs Specialty Areas:

1. Securely Provision (SP)
a. Risk Management (RM)
b. Technology R&D (RD)
c. Systems Requirements Planning (RP)

2. Oversee and Govern (OV)
a. Legal Advice and Advocacy (LG)
b. Training, Education, and Awareness (ED)
c. Cybersecurity Management (MG)
d. Strategic Planning and Policy (PL)
e. Executive Cybersecurity Leadership (EX)
f. Acquisition and Program/Project Management (PM)

3. Collect and Operate (CO)
a. Cyber Operational Planning (PL)

*All credentials can be attained individually. Please refer to cert.eccouncil.org for the eligibility criteria.

EC-Council

eHACK ACADEMY

CSCU
Certified Secure Computer User

Certified Secure Computer User (CSCU)

Course Description

CSCU provides individuals with the necessary knowledge and skills to protect their information assets.

This course covers fundamentals of various computer and network security threats such as identity theft, credit card fraud, phishing, virus and backdoors, emails hoaxes, loss of confidential information, hacking attacks, and social engineering.

OhPhish: OhPhish covers phishing, smishing, and vishing solutions in a single revolutionary platform to help organizations strengthen their most vulnerable asset, their people. Learn more about OhPhish

READ MORE

Key Outcomes

- Fundamentals of various computer and network security threats
- Understanding of identity theft, phishing scams, malware, social engineering, and financial frauds
- Learn to safeguard mobile, media and protect data
- Protecting computers, accounts, and social networking profiles as a user
- Understand security incidents and reporting

Exam Information

- Exam Title: Certified Secure Computer User
- Exam Code: 112-12
- Number of Questions: 50
- Duration: 2 Hours
- Availability: ECC Exam Portal
- Test Format: Multiple Choice
- Passing Score: 70%

Course Outline

- Introduction to Security
- Securing Operating Systems
- Malware and Antivirus
- Internet Security
- Security on Social Networking Sites
- Securing Email Communications
- Securing Mobile Devices
- Securing Cloud
- Securing Network Connections
- Data Backup and Disaster Recovery

EC-Council

eHACK ACADEMY

Certified Network Defender (CND)

Course Description

The CND certification program focuses on training Network Administrators to protect, detect, respond to, and predict threats on the network. This builds upon the typical knowledge and skills of Network Administrators in network components, traffic, performance and utilization, network topology, system locations, and security policies.

Key Outcomes

Adaptive Security Strategy - Protect, Detect, Respond, and Predict.

IoT Security - challenges and measures to mitigate.

Implementing and managing the security of virtualization technologies.

Mobile security measures and enterprise mobile device security.

Cloud security with enterprise cloud security.

Threat intelligence concepts

Exam Information

Exam Title: Certified Network Defender

Exam Code: 312-38

Number of Questions: 100

Duration: 4 hours

Availability: ECC Exam Portal

Test Format: Multiple Choice

Passing Score: Please refer to

Passing Score: Please refer to https://cert.eccouncil.org/faq.html

Course Outline

Module 01: Network Attacks and Defense Strategies
Module 02: Administrative Network Security
Module 03: Technical Network Security
Module 04: Network Perimeter Security
Module 05: Endpoint Security-Windows Systems
Module 06: Endpoint Security-Linux Systems
Module 07: Endpoint Security- Mobile Devices
Module 08: Endpoint Security-IoT Devices
Module 09: Administrative Application Security
Module 10: Data Security
Module 11: Enterprise Virtual Network Security
Module 12: Enterprise Cloud Network Security
Module 13: Enterprise Wireless Network Security
Module 14: Network Traffic Monitoring and Analysis
Module 15: Network Logs Monitoring and Analysis
Module 16: Incident Response and Forensic Investigation
Module 17: Business Continuity and Disaster Recovery
Module 18: Risk Anticipation with Risk Management
Module 19: Threat Assessment with Attack Surface Analysis
Module 20: Threat Prediction with Cyber Threat Intelligence

EC-Council

eHACK ACADEMY

Certified Ethical Hacker (C|EH)

Course Description

CEH is the leading ethical hacking training and certification program in cybersecurity. Students audit a system for weaknesses and vulnerabilities using the same tools and exploits as malicious hackers, but under proper legal circumstances and in the best interest of assessing the security posture of a target system and organization. It teaches how hackers think and act maliciously so you can learn to better position your organization's security infrastructure and defend against future attacks.

Key Outcomes

- Thorough introduction to ethical hacking
- Exposure to threat vectors and countermeasures
- Addresses emerging areas of IoT, cloud and mobile hacking
- Prepares you to combat Trojans, malware, backdoors, and more
- Enables you to hack using mobile

Exam Information

- Exam Title: Certified Ethical Hacker (ANSI)
- Exam Code: 312-50 (ECC EXAM), 312-50 (VUE)
- Number of Questions: 125
- Duration: 4 hours
- Availability: ECC Exam Portal, VUE
- Test Format: Multiple Choice
- Passing Score: Please refer to https://cert.eccouncil.org/faq.html

Course Outline

- Introduction to Ethical Hacking
- Footprinting and Reconnaissance
- Scanning Networks
- Enumeration
- Vulnerability Analysis
- System Hacking
- Malware Threats
- Sniffing
- Social Engineering
- Denial-of-Service
- Session Hijacking
- Evading IDS, Firewalls, and Honeypots
- Hacking Web Servers
- Hacking Web Applications
- SQL Injection
- Hacking Wireless Networks
- Hacking Mobile Platforms
- IoT Hacking
- Cloud Computing
- Cryptography

EC-Council

eHACK ACADEMY

C|EH ETHICAL HACKER PRACTICAL

Certified Ethical Hacker (Practical)

Course Description

C|EH Practical is a six-hour, rigorous exam that requires you to demonstrate the application of ethical hacking techniques such as threat vector identification, network scanning, OS detection, vulnerability analysis, system hacking, web app hacking, etc. to solve a security audit challenge.

This is the next step after you have attained the highly acclaimed Certified Ethical Hacker certification.

Key Outcomes

Mastery of Ethical Hacking skills.

Demonstrate the application of the knowledge to find solutions to real-life challenges.

Commitment to code of ethics.

Validate essential skills required in the ethical hacking domains.

Exam Information

Exam Title: Certified Ethical Hacker (Practical)

Number of Practical Challenges: 20

Duration: 6 hours

Availability: Aspen - iLabs

Test Format: iLabs Cyber Range

Passing Score: 70%

C|EH (Practical) Credential Holders Can

Demonstrate the understanding of attack vectors

Perform network scanning to identify live and vulnerable machines in a network.

Perform OS banner grabbing, service, and user enumeration.

Perform system hacking, steganography, steganalysis attacks, and cover tracks.

Identify and use viruses, computer worms, and malware to exploit systems.

Perform packet sniffing.

Conduct a variety of web server and web application attacks including directory traversal, parameter tampering, XSS, etc.

Perform SQL injection attacks.

Perform different types of cryptography attacks.

Perform vulnerability analysis to identify security loopholes in the target organizations network, communication infrastructure, and end systems etc.

EC-Council

eHACK ACADEMY

CPENT

Certified Penetration Testing Professional

Certified Penetration Testing Professional (CPENT)

Course Description

Rewriting the standards of penetration testing skill development with the Certified Penetration Testing Professional or the CPENT certification program, for short. What makes this program unique is our approach that provides you a chance to attain 2 certifications with just one exam. The key philosophy behind the CPENT is simple a penetration tester is as good as their skills, thats why we urge you to go beyond kali, and go beyond tools. Not that we dont believe in the OS or tools. Candidates with an over-reliance on Kali tools, will find it incredibly difficult to adapt to the multi-disciplinary approach of the real-world penetration testing engagements. We urge you to still go beyond and explore the vast horizons of penetration testing that differentiate the great from the good.

Key Outcomes

100% mapped with the NICE framework.
Comes Blended with both manual and automated penetration testing approach
Maps to the job role of a penetration tester and security analyst, based on major job portals.
Gives a real-world experience through an Advanced Penetration Testing Range.
100% methodology-based penetration testing program.
Is designed based on the most common penetration testing services offered by the best service providers in the market.
Provides strong reporting writing guidance.
Offers standard templates that can help during a penetration test.

Exam Information

A Hands-On Exam Like No Other.

The 24 hours that will define your career

CPENT is a fully online, remotely proctored practical exam, which challenges candidates through a gruelling 24-hour performance-based, hands-on exam, categorized into 2 practical exams of 12-hours each, which will test your perseverance and focus by forcing you to outdo yourself with each new challenge. Candidates have the option to choose either 2 12-hour exams or one 24-hour exam depending on how straining they would want the exam to be.

Candidates who score more than 90%, will establish themselves as Penetration Testing Masters and will therefore win a chance to attain the prestigious LPT (Master) credential!

Course Outline

Module 01: Introduction to Penetration Testing

Module 02: Penetration Testing Scoping and Engagement

Module 03: Open Source Intelligence (OSINT)

Module 04: Social Engineering Penetration Testing

Module 05: Network Penetration Testing External

Module 06: Network Penetration Testing Internal

Module 07: Network Penetration Testing Perimeter Devices

Module 08: Web Application Penetration Testing

Module 09: Wireless Penetration Testing

Module 10: IoT Penetration Testing

Module 11: OT/SCADA Penetration Testing

Module 12: Cloud Penetration Testing

Module 13: Binary Analysis and Exploitation

Module 14: Report Writing and Post Testing Actions

EC-Council

eHACK ACADEMY

C|TIA
Certified | Threat Intelligence Analyst

Certified Threat Intelligence Analyst (CTIA)

Course Description

C|TIA is a method-driven program that uses a holistic approach, covering concepts from planning the threat intelligence project to building a report to disseminating threat intelligence. These concepts are highly essential while building effective threat intelligence and, when used properly, can secure organizations from future threats or attacks.

This program addresses all the stages involved in the Threat Intelligence Life Cycle. This attention to a realistic and futuristic approach makes C|TIA one of the most comprehensive threat intelligence certifications on the market today.

Key Outcomes

- Enable individuals and organizations with the ability to prepare and run a threat intelligence program that allows evidence-based knowledge and provides actionable advice about existing and unknown threats
- Ensure that organizations have predictive capabilities rather than just proactive measures beyond active defense mechanism
- Empower information security professionals with the skills to develop a professional, systematic, and repeatable real-life threat intelligence program
- Differentiate threat intelligence professionals from other information security professionals
- Provide an invaluable ability of structured threat intelligence to enhance skills and boost their employability

Exam Information

Exam Title: Certified Threat Intelligence Analyst

Exam Code: 312-85

Number of Questions: 50

Duration: 2 hours

Availability: EC-Council Exam Portal

Test Format: Multiple Choice

Passing Score: 70%

Course Outline

Introduction to Threat Intelligence

Cyber Threats and Kill Chain Methodology

Requirements, Planning, Direction, and Review

Data Collection and Processing

Data Analysis

Intelligence Reporting and Dissemination

EC-Council

eHACK ACADEMY

Certified SOC Analyst (CSA)

Course Description

The Certified SOC Analyst (CSA) program is the first step to joining a security operations center (SOC). It is engineered for current and aspiring Tier I and Tier II SOC analysts to achieve proficiency in performing entrylevel and intermediate-level operations. CSA is a training and credentialing program that helps the candidate acquire trending and in-demand technical skills through instruction by some of the most experienced trainers in the industry. The program focuses on creating new career opportunities through extensive, meticulous knowledge with enhanced level capabilities for dynamically contributing to a SOC team. Being an intense 3-day program, it thoroughly covers the fundamentals of SOC operations, before relaying the knowledge of log management and correlation, SIEM deployment, advanced incident detection, and incident response. Additionally, the candidate will learn to manage various SOC processes and collaborate with CSIRT at the time of need.

Key Outcomes

- Gain Knowledge of SOC processes, procedures, technologies, and workflows.
- Able to recognize attacker tools, tactics, and procedures to identify indicators of compromise (IOCs) that can be utilized during active and future investigations.
- Gain experience and extensive knowledge of Security Information and Event Management.
- Able to develop threat cases (correlation rules), create reports, etc.
- Plan, organize, and perform threat monitoring and analysis in the enterprise.
- Able to prepare briefings and reports of analysis methodology and results.
- Gain understating of SOC and IRT collaboration for better incident response.

Exam Information

Exam Title: Certified SOC Analyst

Exam Code: 312-39

Number of Questions: 100

Duration: 3 hours

Availability: EC-Council Exam Portal (please visit https://www. eccexam.com)

Test Format: Multiple Choice

Passing Score: 70%

Course Outline

Module 1: Security Operations and Management

Module 2: Understanding Cyber Threats, IoCs, and Attack Methodology

Module 3: Incidents, Events, and Logging

Module 4: Incident Detection with Security Information and Event Management (SIEM)

Module 5: Enhanced Incident Detection with Threat Intelligence

Module 6: Incident Response

EC-Council

eHACK ACADEMY

ECSA

EC-Council Certified Security Analyst

EC-Council Certified Security Analyst (ECSA)

Course Description

ECSA is a globally accepted hacking and penetration testing program that covers the testing of modern infrastructures, operating systems, and application environments while teaching the students how to document and write a penetration testing report.

This program takes the tools and techniques covered in C|EH to next level by utilizing EC-Councils published penetration testing methodology.

Key Outcomes

- Introduction to security analysis and penetration testing methodologies
- In-depth vulnerability analysis, network penetration testing from external and internal evading firewalls and IDS
- Learn to own web applications and databases, and take over cloud services
- Analyze security of mobile devices and wireless networks
- Present findings in a structured actionable report

Exam Information

Exam Title: EC-Council Certified Security Analyst

Exam Code: 412-79

Number of Questions: 150

Duration: 4 hours

Availability: ECC Exam Portal

Test Format: Multiple Choice

Passing Score: 70%

Course Outline

- Penetration Testing Essential Concepts (Student Introduction)
- Introduction to Penetration Testing and Methodologies
- Penetration Testing Scoping and Engagement Methodology
- Open-Source Intelligence (OSINT) Methodology
- Social Engineering Penetration Testing Methodology
- Network Penetration Testing Methodology External
- Network Penetration Testing Methodology Internal
- Network Penetration Testing Methodology Perimeter Devices
- Web Application Penetration Testing Methodology
- Database Penetration Testing Methodology
- Wireless Penetration Testing Methodology
- Cloud Penetration Testing Methodology
- Report Writing and Post Testing Actions

EC-Council

eHACK ACADEMY

ECSA SECURITY ANALYST PRACTICAL

EC-Council Certified Security Analyst (Practical)

Course Description

ECSA (Practical) is a 12-hour, rigorous practical exam built to test your penetration testing skills.

The candidates are required to demonstrate the application of the penetration testing methodology that is presented in the ECSA program, and are required to perform a comprehensive security audit of an organization, just like in the real world. You will start with challenges requiring you to perform advanced network scans beyond perimeter defenses, leading to automated and manual vulnerability analysis, exploit selection, customization, launch, and post exploitation maneuvers.

Key Outcomes

Test your ability to perform threat and exploit research, understand exploits in the wild, write your own exploits, customize payloads, and make critical decisions

Create a professional pen testing report with essential elements

Exam Information

Exam Title: EC-Council Certified Security Analyst (Practical)

Number of challenges: 8

Duration: 12 hours

Availability: Aspen- iLabs

Test Format: iLabs cyber range

Passing Score: 5 out of 8 challenges and submission of an acceptable penetration testing report

ECSA (Practical) Credential Holders Can

Perform advanced network scans beyond perimeter defenses, leading to automated and manual vulnerability analysis, exploit selection, customization, launch and post exploitation maneuvers.

Customize payloads

Make critical decisions at different phases of a pen-testing engagement

Perform advanced network scans beyond perimeter defenses

Perform automated and manual vulnerability analysis

Customization, launch, and post exploitation maneuvers

Perform a full fledged Penetration Testing engagement

Create a professional pen-testing report

Demonstrate the application of penetration testing methodology presented in the ECSA program

EC-Council

eHACK ACADEMY

EC-Council Certified Incident Handler (ECIH)

Course Description

The ECIH program is designed to provide the fundamental skills to handle and respond to the computer security incidents in an information system. The course addresses various underlying principles and techniques for detecting and responding to current and emerging computer security threats.

The comprehensive training program will make students proficient in handling as well as responding to various security incidents such as network security incidents, malicious code incidents, and insider attack threats.

Key Outcomes

- Principals, processes and techniques for detecting and responding to security threats/ breaches
- Liaison with legal and regulatory bodies
- Learn to handle incidents and conduct assessments
- Cover various incidents like malicious code, network attacks, and insider attacks

Exam Information

- Exam Title: EC-Council Certified Incident Handler
- Exam Code: 212-89
- Number of Questions: 50
- Duration: 2 hours
- Availability: ECC Exam Portal
- Test Format: Multiple Choice
- Passing Score: 70%

Course Outline

- Introduction to Incident Response and Handling
- Risk Assessment
- Incident Response and Handling Steps
- CSIRT
- Handling Network Security Incidents
- Handling Malicious Code Incidents
- Handling Insider Threats
- Forensic Analysis and Incident Response
- Incident Reporting
- Incident Recovery
- Security Policies and Laws

EC-Council

eHACK ACADEMY

Computer Hacking and Forensic Investigator (CHFI)

Course Description

CHFI is a comprehensive course covering major forensic investigation scenarios, enabling students to acquire hands-on experience.

The program provides a strong baseline knowledge of key concepts and practices in the digital forensic domains relevant to todays organizations. Moreover, CHFI provides firm grasp on the domains of digital forensics.

Key Outcomes

- Comprehensive forensics investigation process
- Forensics of file systems, operating systems, network and database, websites, and email systems
- Techniques for investigating on cloud, malware, and mobile
- Data acquisition and analysis as well as anti-forensic techniques
- Thorough understanding of chain of custody, forensic report, and presentation

Exam Information

- Exam Title: Computer Hacking Forensic Investigator
- Exam Code: 312-49 exam
- Number of Questions: 150
- Duration: 4 hours
- Availability: ECC Exam Portal
- Test Format: Multiple Choice
- Passing Score: Please refer to https://cert.eccouncil.org/faq.html

Course Outline

- Computer Forensics in Todays World
- Computer Forensics Investigation Process
- Understanding Hard Disks and File Systems
- Data Acquisition and Duplication
- Defeating Anti-Forensics Techniques
- Operating System Forensics
- Network Forensics
- Investigating Web Attacks
- Database Forensics
- Cloud Forensics
- Malware Forensics
- Investigating Email Crimes
- Mobile Forensics
- Forensics Report Writing and Presentation

EC-Council

eHACK ACADEMY

Certified Application Security Engineer (CASE) Java

Course Description

The **CASE Java** program is designed to be a hands-on, comprehensive application security training course that will help software professionals create secure applications. It trains software developers on the critical security skills and knowledge required throughout a typical software development life cycle (SDLC), focusing on the importance of the implementation of secure methodologies and practices required in todays insecure operating environment.

Key Outcomes

- Security Beyond Secure Coding - Challenging the traditional mindset where secure application means secure coding
- Testing and credentialing secure application development across all phases of the SDLC
- CASE Program maps to many Specialty Areas under Securely Provision category in the NICE 2.0 Framework
- Covers techniques such as Input Validation techniques, Defense Coding Practices, Authentications and Authorizations, Cryptographic Attacks, Error Handling techniques, and Session Management techniques, among many others

Exam Information

- Exam Title: Certified Application Security Engineer (Java)
- Exam Code: 312-96
- Number of Questions: 50
- Duration: 2 hours
- Availability: ECC Exam Portal
- Test Format: Multiple Choice
- Passing Score: 70%

Course Outline

- Understanding Application Security, Threats, and Attacks
- Security Requirements Gathering
- Secure Application Design and Architecture
- Secure Coding Practices for Input Validation
- Secure Coding Practices for Authentication and Authorization
- Secure Coding Practices for Cryptography
- Secure Coding Practices for Session Management
- Secure Coding Practices for Error Handling
- Static and Dynamic Application Security Testing (SAST & DAST)
- Secure Deployment and Maintenance

EC-Council

eHACK ACADEMY

Certified Application Security Engineer (CASE) .Net

Course Description

CASE goes beyond just the guidelines on secure coding practices but include secure requirement gathering, robust application design, and handling security issues in post development phases of application development.

This makes CASE one of the most comprehensive certifications for secure software development in the market today. Its desired by software application engineers, analysts, testers globally, and respected by hiring authorities.

The hands-on training program encompasses security activities involved in all phases of the Secure Software Development Life Cycle (SDLC): planning, creating, testing, and deploying an application.

Key Outcomes

Ensure that application security is no longer an afterthought but a foremost one.

It lays the foundation required by all application developers and development organizations, to produce secure applications with greater stability and fewer security risks to the consumer.

Ensure that organizations mitigate the risk of losing millions due to security compromises that may arise with every step of application development process.

Helps individuals develop the habit of giving importance to security sacrosanct of their job role in the SDLC, therefore opening security as the main domain for testers, developers, network administrator etc.

Exam Information

Exam Title: Certified Application Security Engineer (.NET)

Exam Code: 312-95

Number of Questions: 50

Duration: 2 hours

Availability: ECC Exam Portal

Test Format: Multiple Choice

Passing Score: 70%

Course Outline

Understanding Application Security, Threats, and Attacks

Security Requirements Gathering

Secure Application Design and Architecture

Secure Coding Practices for Input Validation

Secure Coding Practices for Authentication and Authorization

Secure Coding Practices for Cryptography

Secure Coding Practices for Session Management

Secure Coding Practices for Error Handling

Static and Dynamic Application Security Testing (SAST & DAST)

Secure Deployment and Maintenance

EC-Council

eHACK ACADEMY

Certified Chief Information Security Officer (C|CISO)

Course Description

The C|CISO certification is an industry-leading program that recognizes the real-world experience necessary to succeed at the highest executive levels of information security. Bringing together all the components required for a C-Level positions, the C|CISO program combines audit management, governance, IS controls, human capital management, strategic program development, and the financial expertise vital for leading a highly successful IS program.

The C|CISO Training Program can be the key to a successful transition to the highest ranks of information security management.

Key Outcomes

- Establishes the role of CISO and models for governance
- Core concepts of information security controls, risk management, and compliance
- Builds foundation for leadership through strategic planning, program management, and vendor management

Exam Information

- Number of Questions: 150
- Duration: 2.5 hours
- Test Format: Multiple Choice

Domains

- Governance
- Security Risk Management, Controls, & Audit Management
- Security Program Management & Operations
- Information Security Core Competencies
- Strategic Planning, Finance, & Vendor Management

OhPhish

Warning System For Cyber Canopy

OhPhish

Course Description

OhPhish portal imitates real-world phishing scenarios. The platform equips employees with the most efficient solutions and products to combat phishing attacks and prevent data breaches. It caters to the need for businesses by creating a safe working environment from Phishing, Smishing, and Vishing attacks. OhPhish integrates e-Learning and gamification modules in a Learning Management System (LMS), helping employees to stay aware of phishing attacks.

Key Outcomes

- Builds a user-friendly cybersecurity awareness training solution
- Maintains Active Directory to launch comprehensively laid out phishing templates
- Generates extensive reports in PDF and Excel formats
- Tracks real-time updates with snapshots (availability on Mobile Applications)
- Identifies trends based on user, department, and other critical demographic

OhPhish Solutions

- Email Phishing
- Vishing
- Smishing
- Spear Phishing

EC-Council

CODERED

Empowering Cyber Professionals

Code Red Subscription/ EC-Council Micro-degrees:

CodeRed is a continuous learning platform designed for Busy Cyber professionals - offering them content rich courses created by worlds' leading cybersecurity certification provide

eHACK ACADEMY

Why CodeRed:

- Unlimited access to a library of 100s of courses
- Courses built by world-class experts and cybersecurity influencers
- Courses are aligned to current job hiring trends
- More than 40% of the courses are hands-on

EC-Council Microdegrees

Python Security Microdegree	Cloud Security Microdegree	PHP Security Microsecurity

Master advanced cybersecurity skills with the modern flexibility of self-paced learning and practical hands-on labs. EC-Council's Microdegree offers a unique form of learning experience that encourages a learner to acquire specialized skill sets in a relatively short amount of time. The MicroDegree engages the learner in over 200 hours of comprehensive deep-dive, hands-on learning experience, enabling them to excel in their career.

What's Included:

Official Course Manual	Practical Video Learning Content	Cyber Range
Lab Manuals	Assessments/Quiz	Proctored Exam

EC-COUNCIL UNIVERSITY
ACCREDITED. FLEXIBLE. ONLINE.

Bachelor of Science in Cyber Security (BSCS)

Program Description

The **Bachelor of Science in Cyber Security (BSCS)** prepares students the knowledge for careers in cyber security and assurance. The program consists of topical areas dealing with computer security management, incident response, and security threat assessment, etc.

Key Outcomes

Application of technical strategies, tools and techniques to provide security for information systems.

Adherence to a high standard of ethical behavior.

Use of research in both established venues and innovative applications to better provide risk assessment, policy updates and security for established enterprise systems.

Understanding the importance of critical thinking to creatively and systematically solve the problems within the parameters of existing information systems.

Achieve the competency skills needed to fulfill position requirements in the cyber security field.

Exam Information

Completion of 60 credit hours of 300/400 level courses in which the candidate earned a cumulative GPA of 2.0 or better.

Completion of 120 + total semester credit hours including all transfer credit awarded.

Satisfactory completion of the summative capstone course.

All degree requirements must be completed within one and a half times the program length as measured by maintaining a cumulative course completion rate of 67% of course work from the first term the student enrolls in the University and begins the program to graduation.

Courses

CIS 300 Fundamentals of Information Systems Security
CIS 301 Legal Issues in Cyber Security
CIS 302 Managing Risk in Information Systems
CIS 303 Security Policies and Implementation Issues
CIS 304 Auditing IT Infrastructures for Compliance
CIS 308 Access Control
CIS 401 Security Strategies in Windows Platforms and Applications
CIS 402 Security Strategies in Linux Platforms and Applications
CIS 403 Network Security, Firewalls, and VPNs
CIS 404 Hacker Techniques, Tools, and Incident Handling
CIS 405 Internet Security: How to Defend Against Online Attackers
CIS 406 System Forensics, Investigation, and Response
CIS 407 Cyberwarfare
CIS 408 Wireless and Mobile Device Security
CIS 410 Capstone Course
COM 340 Communication and Technical Writing
MTH 350 Introduction to Statistics
PSY 360 Social Psychology
BIS 430 Ethics for the Business Professional
ECN 440 Principles of Microeconomics
MGT 450 Introduction to Project Management

EC-COUNCIL UNIVERSITY

ACCREDITED. FLEXIBLE. ONLINE.

Graduate Certificate Programs

Program Description

EC-Council Universitys Graduate Certificate Program focuses on the competencies necessary for information assurance professionals to become managers, directors, and CIOs. Students will experience not only specialized technical training in a variety of IT security areas, but will also acquire an understanding of organizational structure and behavior, the skills to work within and across that organizational structure, and the ability to analyze and navigate its hierarchy successfully. Each certificate targets skills and understandings specific to particular roles in the IT security framework of an organization. The certificates can be taken singly or as a progressive set of five, each building on the one before it to move students from IT practitioner skill levels to IT executive skill levels.

Graduate Certificates

Information Security Professional

Security Analyst

Cloud Security Architect

Incident Management and Business Continuity

Executive Leadership in Information Assurance

Exam Information

Completion of mandated credit hours of courses in which the candidate earned a cumulative GPA or 3.0 or better

All certificate requirements must be completed within one and a half times the program length as measured by maintaining a cumulative course competition rates of 67% of course work from the first term the student enrolls in the University and begins the program to the last course needed.

Courses

Information Security Professional

- Managing Secure Networks (C|ND)
- Ethical Hacking and Countermeasures (C|EH)
- Research and Writing for the IT Practitioner

Security Analyst

- Security analyst and vulnerability assessment (ECSA)
- Conducting Penetration and Security Tests (LPT-Master)
- Securing Wireless Networks

Cloud Security Architect (Any 3 of the 4 courses below)

- Secure Programming
- Advanced Network Defense
- Advanced Mobile Forensics or
- Designing and Implementing Cloud Security

Incident Management and Business Continuity

- Beyond Business Continuity
- Disaster Recovery (EDRP)
- Incident Handling and Response (ECIH)

Executive Leadership in Information Assurance

- Global Business Leadership
- Project Management
- Executive Governance and Management (CCISO)

EC-COUNCIL UNIVERSITY

ACCREDITED. FLEXIBLE. ONLINE.

Master of Science in Cyber Security (MSCS)

Program Description

The **Master of Science in Cyber Security (MSCS)** Program prepares information technology professionals for careers in cyber security and assurance. The program consists of topical areas dealing with computer security management, incident response, and cyber security threat assessment, which require students to be the creators of knowledge and inventors of cyber security processes, not merely users of information. Additionally, students will receive instruction in leadership and management in preparation for becoming cyber security leaders, managers, and directors.

Key Outcomes

Application of cyber security technical strategies, tools, and techniques to secure data and information for a customer or client
Adherence to a high standard of cyber security ethical behavior
Use of research in both established venues and innovative applications to expand the body of knowledge in cyber security
Application of principles of critical thinking to creatively and systematically solve the problems and meet the challenges of the everchanging environments of cyber security
Mastery of the skills necessary to move into cyber security leadership roles in companies, agencies, divisions, or departments

Exam Information

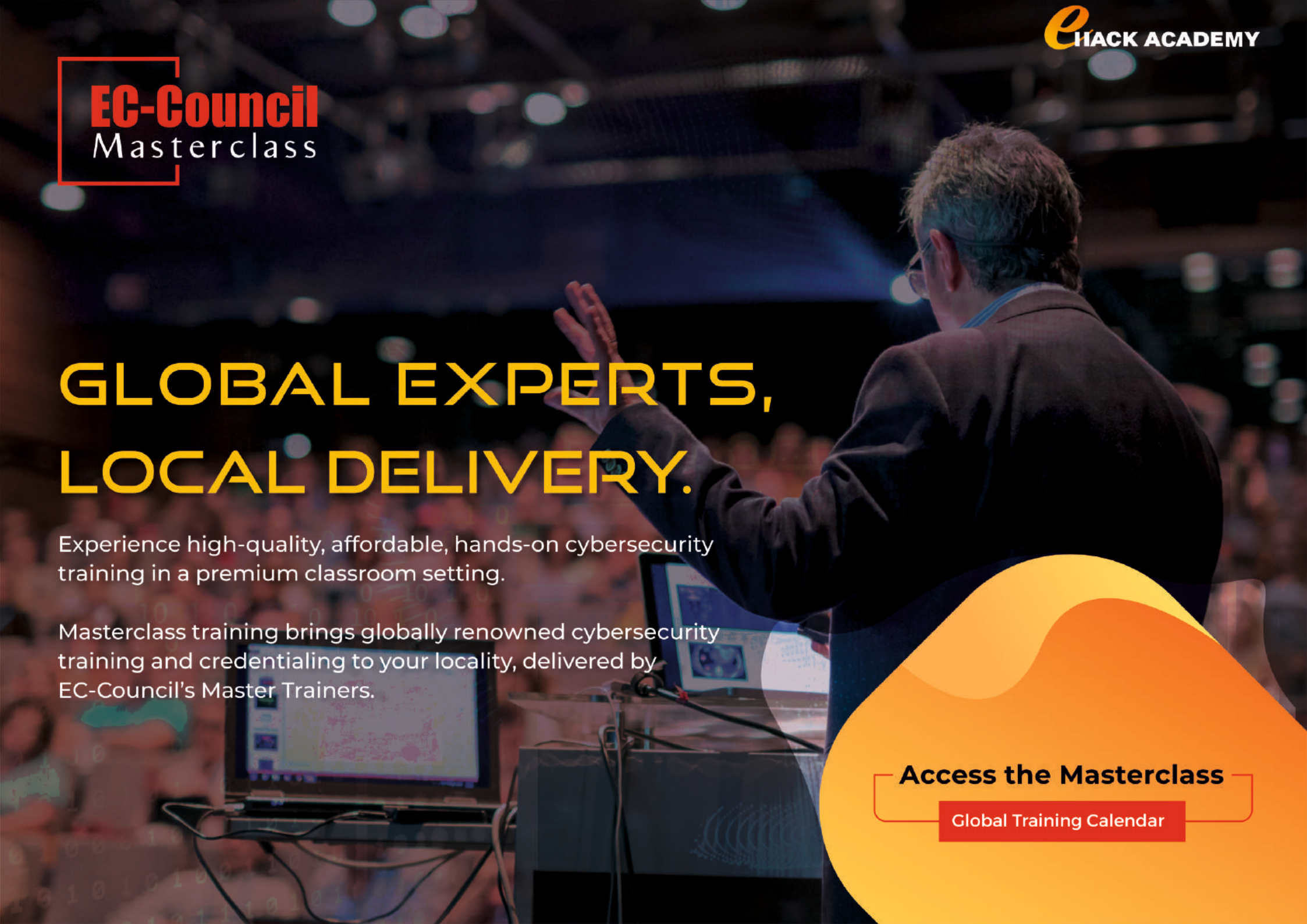
Completion of thirty-six (36) credits of 500 level courses in which the candidate earned a cumulative GPA of 3.0 or better

Satisfactory completion of the summative capstone course

All degree requirements must be completed within one and a half times the program length or have a cumulative course completion rate of 67% of coursework from the date the student enrolls in the University and begins the program.

Courses

ECCU 500 Managing Secure Network Systems
MGMT 502 Business Essentials
ECCU 501 Ethical Hacking & Countermeasures
ECCU 502 Investigating Network Intrusions and Computer Forensics
ECCU 503 Security Analysis and Vulnerability Assessment
ECCU 504 Foundations of Organizational Behavior for the IT Practitioner
ECCU 505 Introduction to Research and Writing for the IT Practitioner
ECCU 506 Conducting Penetration and Security Tests
ECCU 507 Linux Networking and Security
ECCU 509 Securing Wireless Networks
ECCU 510 Secure Programming
ECCU 511 Global Business Leadership
ECCU 512 Beyond Business Continuity: Managing Organizational Change
ECCU 513 Disaster Recovery
ECCU 514 Quantum Leadership
ECCU 515 Project Management in IT Security
ECCU 516 The Hacker Mind: Profiling the IT Criminal
ECCU 517 Cyber Law
ECCU 518 Special Topics
ECCU 519 Capstone
ECCU 520 Advanced Network Defense
ECCU 521 Advanced Mobile Forensics and Security
ECCU 522 Incident Handling and Response
ECCU 523 Executive Governance Management
ECCU 524 Designing and Implementing Cloud Security
ECCU 525 Securing Cloud Platforms


EC-Council
Masterclass
eHACK ACADEMY
GLOBAL EXPERTS,
LOCAL DELIVERY.
Experience high-quality, affordable, hands-on cybersecurity training in a premium classroom setting.
Masterclass training brings globally renowned cybersecurity training and credentialing to your locality, delivered by EC-Council's Master Trainers.
Access the Masterclass
Global Training Calendar

Name of the Influencer / Partner/ Individuals: _____

_____

LEARN & EARN

100% SCHOLARSHIP/CASH REWARDS* T&C Apply

Subject to:

1. Registration of min 10 enrollments with full fee collections
2. In case of Cash reward, it will be calculated as average of minimum 10 enrollments fee collection.

REGISTRATION FORM (To be completed in candidate's own hand writing)

Name of the candidate : Mr/ Ms : _____

Father's name / Husband Name : _____

Date of birth : _____ / _____ / _____

Address : _____

_____

Pin : _____

Email : _____

School/college : _____

Company / organisations : _____

Website : _____

Phone No (home) : _____

Mobile : _____

Please paste a recent colour photograph of size 3.5 * 4.5 cms. Photograph must not be large rthan this box

Use the photocopy of the same for referring students.

EC-Council

eHACK ACADEMY

www.eccouncil.org