



OVER 1,200
Highly Qualified
Certified Instructors

195+
Countries

700+
Locations

OVER 4,200
Classes Annually
in Cyber Security

CYBER SECURITY PROGRAMS

EC-Council
Building A Culture Of Security

Table of Content

Who We Are	04
Security Wall	05
EC-Council at a Glance	06
Accrediations	07
Your Learning Options	11

Tracks

Foundation Track	17
Vulnerability Assessment and Penetration Testing	18
Cyber Forensics	19
Network Defense and Operations	
Software Security	20
Governance	21

Certifications

Certified Secure Computer User (C SCU)	22
Digital Forensics Essentials (D FE)	23
Network Defense Essentials (N HE)	24
Ethical Hacking Essentials (E HE)	25
Cloud Security Essentials (C SE)	26
DevSecOps Essentials (D SE)	27
IoT Security Essentials (I SE)	28
SOC Essentials (S CE)	29

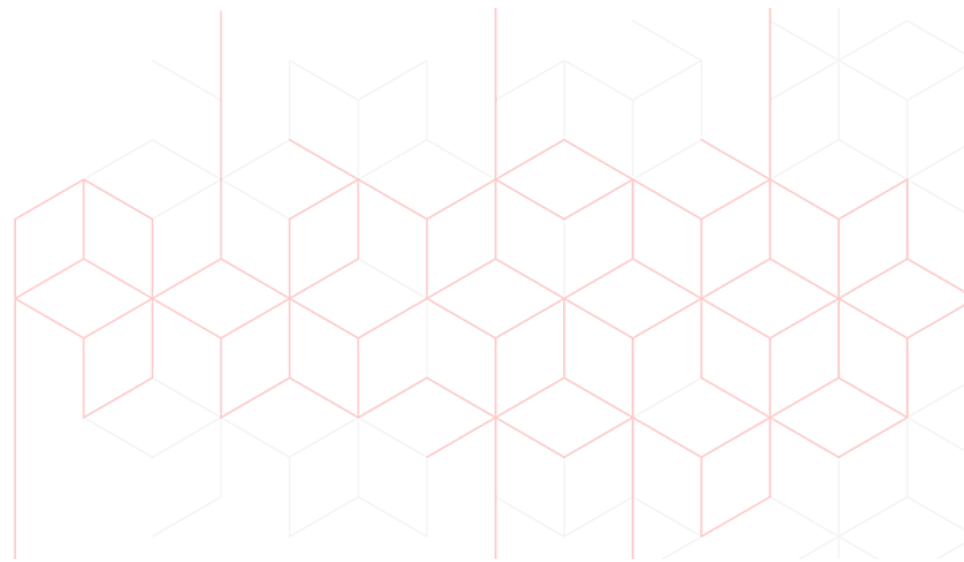
Threat Intelligence Essentials (T IE)	30
Web Application Hacking and Security (W AHS)	31
Certified Cybersecurity Technician (C CT)	32
Certified DevSecOps Engineer (E CDE)	33
Certified Cloud Security Engineer (C CSE)	34
ICS/SCADA	35
EC-Council Certified Security Specialist (E CSS)	36
EC-Council Certified Encryption Specialist (E CES)	37
Certified Network Defender (C ND)	38
Certified Threat Intelligence Analyst (C TIA)	39
Certified SOC Analyst (C SA)	40
Certified Penetration Testing Professional (C PENT)	41
EC-Council Certified Incident Handler (E CIH)	42
Computer Hacking Forensic Investigator (C HFI)	43
Certified Application Security Engineer (CASE) Java	44
Certified Application Security Engineer (CASE).Net	45
Advanced Penetration Testing (APT)	46
The Licensed Penetration Tester (Master) Credential - LPT (Master)	47
Center for Advanced Security Training	48
Certified Chief Information Security Officer (C CISO)	49
EC-Council Disaster Recovery Professional (E DRP)	50
Blockchain Developer Certification (B DC)	51

Table of Content

Business Leader Certification (B BLC)	52
Blockchain Fintech Certification (B FC)	53
Cyber Security Learning Track	54
Aware	55
EC-Council Learning	56
EC-Council Learning Plans	57

Academic Programs

Bachelor of Science in Cyber Security (BSCS)	58
Graduate Certificate Programs	59
Master of Science in Cyber Security (MSCS)	60
EC-Council Masterclass	61



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 the 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), and Licensed 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), 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 220,000 professionals in various e-business and cybersecurity skills.

iClass is EC-Council's 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 sessions, 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.

EC-Council University is accredited by the Distance Education Accrediting Commission. The university offers programs such as a Bachelor of Science in

Cyber Security, a Master of Science in Cyber Security, and a Graduate Certificate Program.

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

EC-Council's 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 a "capture the flag" type competition with approximately 1,000 global participants. EC-Council brings 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.



Jay Bavisi
President & CEO
EC-Council

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

Pentagon trains workers to hack Defense computers

By Larry Shaughnessy, CNN Pentagon Producer
March 15, 2010 -- Updated 1414 GMT (2214 HKT)

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 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 Uni-Aid - Don't stop learning



EC-Council Uni Aid is an EC-Council scholarship that provides information technology students at public universities globally, access to EC-Council's industry-recognized information security education and certification and related technical disciplines.



Universities and student recipients will be part of a global community of scholarship recipients from the United States, Europe, Middle East, Africa and Asia-Pacific, all of whom share similar passion for information security and academic excellence.

EC-Council has pledged \$1,000,000 worth of information security scholarships for the 2011-2012 academic year to universities globally.

EC-Council

EC-Council Featured in CNN | The Wolf Blitzer Show



Aug 4, 2011 | Albuquerque, NM - Jay Bavisi, president of EC-Council, was earlier interviewed by CNN, to comment on the massive cyber spying incident which targeted agencies and groups in 14 countries, including U.S. government agencies, the United Nations, defence contractors and Olympic bodies.



As reported by CNN McAfee said the attacks, which it calls Operation Shady RAT, have allowed hackers potentially to gain access to military and industrial secrets from 72 targets, most of them in the United States, over a five-year period.

EC-Council

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

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

Division of Conferences,
Forums, Summits, Workshops
& Industry Awards

ECF

EC-Council Foundation
Non-Profit Organization
for Cyber Security

3,80,000+ certified members

20+
years
experience

40+
training &
certification
programs

195+
countries

1000+
subject matter
experts

2823+
training
partners
worldwide

3000+
tools &
technologies

Accreditations



American National Standards Institute (ANSI)

EC-Council has achieved accreditation for its Certified Ethical Hacker (C|EH), C|EH Practical Exam, Certified Chief Information Security Officer (C|CISO), Certified Network Defender (C|ND), and Computer Hacking Forensic Investigator (C|HFI) and EC-Council Certified Incident Handler (E|CIH) to meet the ANAB 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 these EC-Council certifications will also have that extra credential meeting the respective ANAB Certification Training Standards requirements.



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 (C|EH), Computer Hacking Forensics Investigator (C|HFI), Disaster Recovery Professional (EDRP), 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 provides procedures and guidance for the protection of national security systems.



Candidates who complete the EC-Council Certified Ethical Hacker (C|EH), Computer Hacking Forensics Investigator (C|HFI), Disaster Recovery Professional (EDRP), certification will also have that extra credential meeting the requirements of the respective CNSS 4011-4016 Federal Security Certification Training Standards.

Accreditations



Department of Defense (DoD)

EC-Council's Certified Ethical Hacker (C|EH), CEH Practical Exam, Computer Hacking Forensic Investigator (C|HFI), Certified Chief Information Security Officer (C|CISO), and EC-Council Certified Incident Handler (E|CIH) programs are formally integrated as baseline skill certification options for the U.S. Department of Defense (DoD) cyber workforce in several categories. This recognition helps strengthen national security in 28 important cybersecurity roles within the DoD Cyberspace Workforce Framework. These certifications provide tailored training to enhance job performance and contribute to national cybersecurity preparedness, including ethical hacking, network defense, incident response, digital forensics, and cybersecurity leadership. [Click here for more detailed information.](#)



GCHQ Certified Training (GCT)

EC-Council has achieved accreditation for its Certified Ethical Hacker (C|EH), 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-Council's 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.



National Infocomm Competency Framework (NICF)

EC-Council Certified Ethical Hacker (C|EH) and Computer Hacking Forensic Investigator (C|HFI) 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.

Accreditations



Department of Veterans Affairs

The Department of Veterans Affairs has included EC-Council Certified Ethical Hacker (C|EH), Computer Hacking Forensic Investigator (C|HFI), under its GI Bil[®] 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

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

Building A Culture Of Security



EC-Council Certification

Certified Ethical Hacker (C|EH)

CERTIFIED ETHICAL HACKER
PRACTICAL (C|EH PRACTICAL)

CERTIFIED CHIEF INFORMA-
TION SECURITY OFFICER
(C|CISO)

COMPUTER HACKING FORENSIC
INVESTIGATOR (C|HFI)

CERTIFIED NETWORK
DEFENDER (C|ND)

EC-COUNCIL CERTIFIED
INCIDENT HANDLER (E|CIH)

DoD 8140 Approved Work Roles

111 - All-Source Analyst
141 - Warning Analyst
511 - Cyber Defense Analyst
531 - Cyber Defense Incident Responder
541 - Vulnerability Assessment Analyst
661 - Research & Development Specialist

111 - All-Source Analyst
141 - Warning Analyst
511 - Cyber Defense Analyst
531 - Cyber Defense Incident Responder
541 - Vulnerability Assessment Analyst
661 - Research & Development Specialist

611 - Authorizing Official/Designating Representative
722 - Information Systems Security Manager
723 - COMSEC Manager
731 - Cyber Legal Advisor
801 - Program Manager
802 - IT Project Manager
803 - Product Support Manager
804 - IT Investment/Portfolio Manager
805 - IT Program Auditor

211 - Forensics Analyst
212 - Cyber Defense Forensics Analyst
221 - Cyber Crime Investigator

511 - Cyber Defense Analyst
521 - Cyber Defense Infrastructure Support Specialist
531 - Cyber Defense Incident Responder

531 - Cyber Defense Incident Responder

Your Learning Options



Instructor-led Training

EC-Council has a large network of Accredited Training Centers (ATC) spread across 145 countries. Each center has a certified trainer to deliver the entire EC-Council program from a training facility in your city.



Online Training

iLearn online training is a distance learning program designed for those who cannot attend a live course. The program is for the people who have a very busy schedule and want to learn at their own pace through self-study. This modality is also available from our enterprise teams.



Mobile Learning

Our world class content is also available on a mobile device, allowing our students to learn on the go. This program is designed for those who cannot attend a live course, but are keen to improve their cyber security skills. This modality is also available from our enterprise teams.



Computer-based Training

EC-Council iLabs allows students to dynamically access a host of virtual machines preconfigured with vulnerabilities, exploits, tools, and scripts from anywhere. Our simplistic web portal enables the student to launch an entire range of target machines and access them remotely with one simple click. It is the most cost-effective, easy to use, live range lab solution available. Most of our courses are equipped with iLabs, but iLabs can be purchased independently as well.



Hands-on Experience with the EC-Council Cyber Range (iLabs)

EC-Council iLabs allows students to dynamically access a host of virtual machines preconfigured with vulnerabilities, exploits, tools, and scripts from anywhere. Our simplistic web portal enables the student to launch an entire range of target machines and access them remotely with one simple click. It is the most cost-effective, easy to use, live range lab solution available. Most of our courses are equipped with iLabs, but iLabs can be purchased independently as well.



Customized Learning

Love a course we offer, but want it customized? No problem! EC-Council has a dedicated team to cater to your needs. We have access to the largest pool of EC-Council certified instructors via our ATC channel. Let us know where and when you want the training delivered, and we will arrange for an instructor and all that's required for a course to be taught at a location of your choice. Contact our accredited training partners for a custom solution. EC-Council client-site training includes official courseware, certification exam (ECC-Exam or VUE), iLabs, online labs (wherever available), and our test-pass guarantee.



Live Online Training

If self-study or self-paced learning does not fit into your personal learning style, we offer you our live online model, iWeek. With iWeek, an instructor will teach you live online while you are seated in the comfort of your home. This training method gives you the freedom to get trained from a location of your choice. Individuals who choose this delivery method consistently attribute their choice to the preference of having a live instructor available for whom questions can be asked and answered. We offer early-bird rates, group rates, and even private courses delivered anytime.

Discover Why C|EH® Is Trusted by Organizations Around the World!

For 20 years, EC-Council's cybersecurity programs have empowered cybersecurity professionals around the world to exercise their training and expertise to combat cyberattacks. The C|EH Hall of Fame celebrates those individuals who have excelled, achieved, and fostered a spirit of leadership among their colleagues and peers within the cyber community.

Below Key Findings Reported by Thousands of Cybersecurity Professionals from C|EH Hall of Fame Report:

Over
1 In Every 2

Of Professionals Received Promotions After C|EH

97%

Stated That the Skills They Acquired In C|EH Helped Safeguard Their Organizations.

97%

Found That C|EH Labs Accurately Mimic Real-World Cyber Threats.

95%

Chose C|EH For Career Growth.

93%

Said That C|EH Skills Improved Their Organizational Security.

92%

Of Hiring Managers Prefer Candidates With C|EH For Jobs That Require Ethical Hacking Skills.

92%

Reported That C|EH Boosted Their Self-Confidence.

88%

Considered C|EH Is the Most Comprehensive Ethical Hacking Program In The Industry.

85%

Credited C|EH With Helping Them Give Back to The Cybersecurity Community.

80%

Started Their Cybersecurity Careers with C|EH.

[Download C|EH Hall of Fame Report](#)



Certified Ethical Hacker v13

Ethical hacking now with the AI edge

What's new for version 13



From the creators of Certified Ethical Hacker (CEH) comes the new and evolved version 13 with added AI capabilities. Structured across 20 learning modules covering over 550 attack techniques, CEH provides cybersecurity professionals with the core knowledge they need to detect and defend against emerging threats.

CEH v13 will equip individuals and teams with:



- In-depth knowledge of ethical hacking methodologies and practices, augmented with AI techniques
- The skills to integrate AI across ethical hacking phases: reconnaissance, scanning, gaining access, maintaining access, and covering tracks
- AI techniques to automate tasks, boost efficiency, and detect sophisticated threats beyond traditional methods
- Tools that will utilize AI for proactive threat hunting, anomaly detection, and predictive analysis to prevent cyber-attacks

Course summary



CEH offers a balanced blend of knowledge-based training and hands-on labs. This all takes place in a virtual environment with live targets as well as the latest in AI tools, techniques and systems.

- 100% visualization with full access to pre-configured targets, networks, and attack tools
- Pre-configured vulnerable websites
- Vulnerable, unpatched operating systems
- Fully networked environments
- 4000+ hacking tools
- 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

AI-powered framework

CEH follows a one-of-a-kind 4-step framework



Learn



Certify



Engage



Compete

<https://www.eccouncil.org/ceh>

For More Information on Certification: <https://cert.eccouncil.org/ethical-hacking-essentials.html>



Certified Ethical Hacker v13

Ethical hacking now with the AI edge

Who CEH v13 is for



Cybersecurity professionals

Those looking to drive their cybersecurity career forward with the power of AI.

Teams and organizations

Teams looking to turbocharge their AI knowledge in order to stay one step ahead of malicious actors.

Government and military

Government departments and defense bodies looking for a trusted and highly valued global certification partner.

What's new for version 13



AI-powered

The world's first ethical hacking program to harness the power of AI.

Hands-on experience

Cybersecurity professionals can hone their skills in real-world scenarios through hands-on labs. Here, they'll practice attack vectors and master advanced hacking tools.

40% more efficient

Learn AI-driven techniques to boost 40% more efficiency in cyber defense while streamlining workflows.

Power-packed, updated curriculum

Master the latest advanced attack techniques, trends and countermeasures.

2x productivity gains

Advanced threat detection, enhanced decision making, adaptive learning, enhanced reporting and automation of repetitive tasks.

Real-world skills, proven mastery

Participate in monthly global hacking competitions, compete with peers, and make it onto the leaderboard.

AI-powered framework



CEH's exclusive learning framework, Learn | Certify | Engage | Compete, prepares learners for certification and provides in-depth, practical exercises that make it the most comprehensive cybersecurity program available.

Learn

Develop skills in core domains of cybersecurity with over 20 modules. Learners will experience 220+ hands-on labs, 550 attack techniques and over 4,000 hacking and security tools.

Engage

Take part in a mock ethical hacking engagement. This 4-part security engagement gives learners the opportunity to engage in a real ethical hacking engagement experience from start to finish against an emulated organization.

Certify

Take a 4-hour exam with 125 multiple-choice questions and a 6-hour practical exam with 20 real-life challenges to earn the CEH Master certification in CEH v13.

Compete

Compete with peers globally with year-long access to 12 CTF challenges of 4 hours each. This helps learners level up their skills and stay current on latest trends.

<https://www.eccouncil.org/ceh>

For More Information on Certification: <https://cert.eccouncil.org/ethical-hacking-essentials.html>



Certified Ethical Hacker v13

Ethical hacking now with the AI edge

Course outline



From the creators of Certified Ethical Hacker (CEH) comes the new and evolved version 13 with added AI capabilities. Structured across 20 learning modules covering over 550 attack techniques, CEH provides the core knowledge needed to thrive as a cybersecurity professional.

Course Outline			
Module 01	Introduction to Ethical Hacking	Module 11	Session Hijacking
Module 02	Footprinting and Reconnaissance	Module 12	Evading IDS, Firewalls, and Honeypots
Module 03	Scanning Networks	Module 13	Hacking Web Servers
Module 04	Enumeration	Module 14	Hacking Web Applications
Module 05	Vulnerability Analysis	Module 15	SQL Injection
Module 06	System Hacking	Module 16	Hacking Wireless Networks
Module 07	Malware Threats	Module 17	Hacking Mobile Platforms
Module 08	Sniffing	Module 18	IoT Hacking
Module 09	Social Engineering	Module 19	Cloud Computing
Module 10	Denial-of-Service	Module 20	Cryptography

<https://www.eccouncil.org/ceh>

For More Information on Certification: <https://cert.eccouncil.org/ethical-hacking-essentials.html>



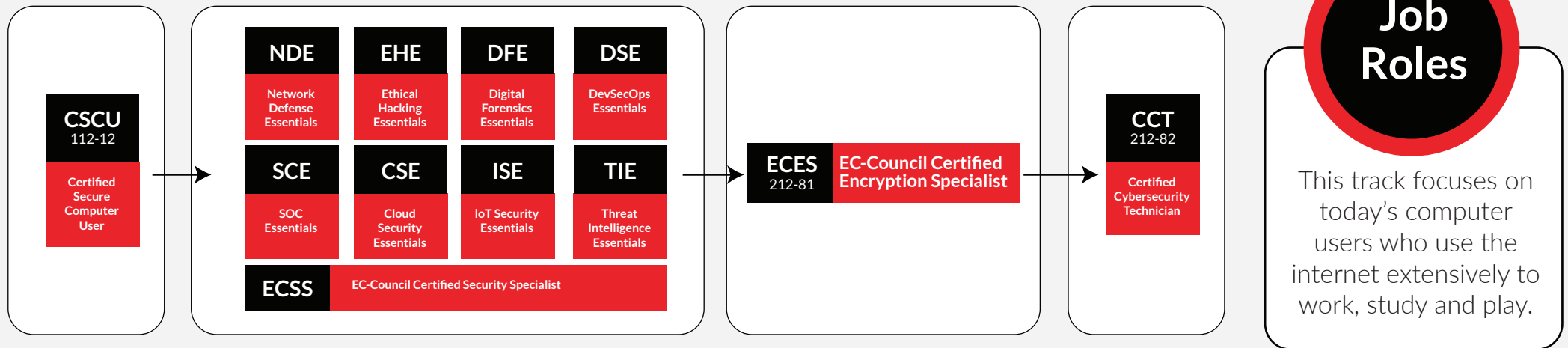
Certified Ethical Hacker (Practical)

Course Description ➔		C EH (Practical) Credential Holders Can ➔
<p>CEH 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.</p>		<ul style="list-style-type: none">• 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 organization's network, communication Infrastructure, and end systems etc.
Key Outcomes ➔	Exam Information ➔	
<p>CEH 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.</p>	<ul style="list-style-type: none">• Number of Practical Challenges: 20• Duration: 6 hours• Availability: Aspen - iLabs• Test Format Ilabs Cyber Range• Passing Score: 70%	

<https://www.eccouncil.org/ceh>

For More Information on Certification: <https://cert.eccouncil.org/ethical-hacking-essentials.html>

Foundation Track



What will You Learn

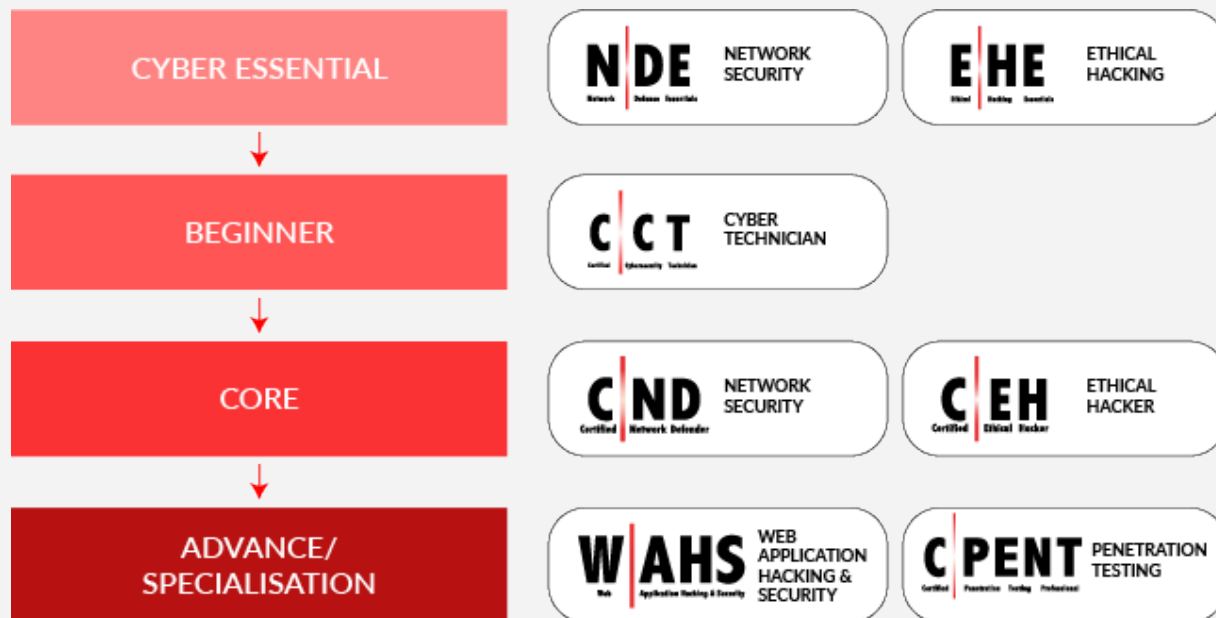


Our Certified Foundation Professionals are Employed at:



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

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

Academic Track

Bachelor of Science in Cyber Security

Graduate Certificate in Incident management and Business Continuity

Master of Science in Cyber Security

*Additional University courses/pre-requisites maybe required.

CORE

ADVANCED

EXPERT

This track maps to NICE's Specialty Areas:

1. Protect and Defend(PR)

- Cybersecurity Defense Analysis(DA)
- Cybersecurity Defense Infrastructure Support (INF)

Incident Response(IR)

- Vulnerability Assessment and Management (VA)

2. Securely Provision(SP)

- Test and Evaluation

3. Analyze(AN)

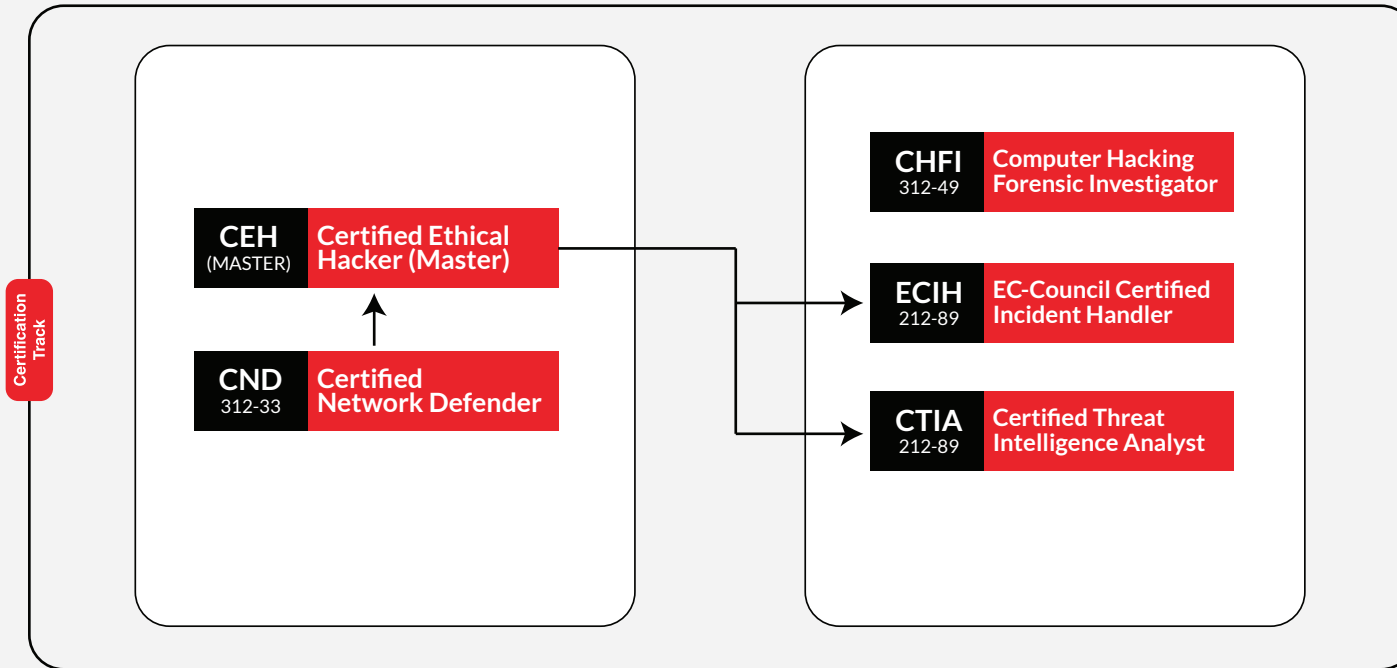
- Threat Analysis (TA)
- Exploitation Analysis(XA)

Our Certified VAPT Professionals are Employed at:



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

Cyber Forensics



*Additional University courses/pre-requisites maybe required.

CORE

ADVANCED

This Track Maps to NIC's to Specialty Areas:

- | | | |
|-------------------------------------|--|--|
| 1. Securely Provision (SP) | • Systems Analysis (AN) | • Cybersecurity Defense Infrastructure Support (INF) |
| • Risk Management (RM) | | • Incident Response (IR) |
| • Test and Evaluation | | • Vulnerability Assessment and Management (VA) |
| 2. Operate and Maintain (OM) | 3. Oversee and Govern (OV) | |
| • Network Services (NET) | • Cybersecurity Management (MG) | |
| • Systems Administration (SA) | 4. Protect and Defend (PR) | 5. Analyze (AN) |
| | • Cybersecurity Defense Analysis (DA) | • Threat Analysis (TA) |
| | • Cybersecurity Defense Infrastructure Support (INF) | • Exploitation Analysis (XA) |

Job Roles

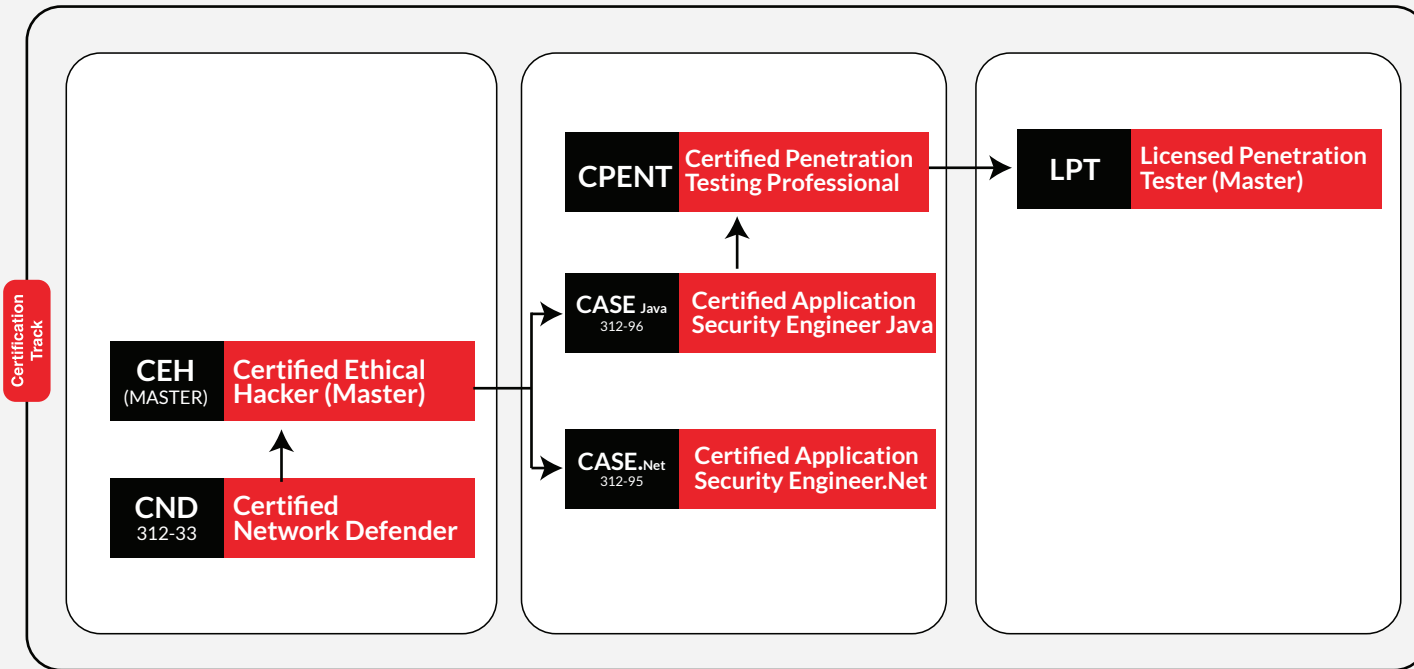
- Computer Forensic Analyst
- Computer Network Defense (CND)
- Forensic Analyst
- Digital Forensic Examiner

Our Certified VAPT Professionals are Employed at:



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

Software Security



CORE

ADVANCED

EXPERT

This Track Maps to NICE's to Specialty Areas:

- | | | |
|--|--|---|
| <ol style="list-style-type: none"> Securely Provision (SP) <ul style="list-style-type: none"> Software Development (DEV) Technology (RD) Operate and Maintain (OM) <ul style="list-style-type: none"> Data Administration (DA) Systems Analysis (AN) | <ol style="list-style-type: none"> Oversee and Govern (OV) <ul style="list-style-type: none"> Cybersecurity Management (MG) Protect and Defend (PR) <ul style="list-style-type: none"> Cybersecurity Defense Analysis (DA) Vulnerability Assessment and Management (VA) | <ol style="list-style-type: none"> Analyze (AN) <ul style="list-style-type: none"> Analyzes collected information to identify vulnerabilities and potential for exploitation. |
|--|--|---|

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:



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

Governance



This Track Maps to NICE's to Specialty Areas:

- | | | |
|---|--|--|
| 1. Securely Provision (SP) <ul style="list-style-type: none"> • Risk Management (RM) • Technology R&D (RD) • Systems Requirements Planning (RP) | <ul style="list-style-type: none"> • Training, Education, and Awareness (ED) • Cybersecurity Management (MG) • Strategic Planning and Policy (PL) | <ul style="list-style-type: none"> • Executive Cybersecurity Leadership (EX) • Acquisition and Program/Project Management (PM) |
| 2. Oversee and Govern (OV) <ul style="list-style-type: none"> • Legal Advice and Advocacy (LG) | | 5. Collect and Operate (CO) <ul style="list-style-type: none"> • Cyber Operational Planning (PL) |

Job Roles

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

Our Certified CCISO Professional are Employed at:



WHAT IS THE C|SCU?

The C|SCU curriculum is designed to educate computer users on the more practical aspects of networking and security, allowing them to expand their computer skills. Students will develop a foundational understanding of a variety of computer and network security concerns, including identity theft, credit card fraud, online banking phishing scams, malware, loss of sensitive information, and social engineering. This certification is an excellent complement to educational offerings in the domain of security and networking.

ABOUT THE EXAM:

EXAM TITLE

**Certified Secure
Computer
User (C|SCU)**

NUMBER OF QUESTIONS

50

TEST DURATION

2 hours

PASSING SCORE

70%

TEST FORMAT

**Multiple
Choice**

EXAM CODE

112-12

AVAILABILITY

**EC-Council
Exam Portal**

COURSE OUTLINE

Module 1: Introduction to Data Security
Module 2: Securing Operating Systems
Module 3: Malware and Antivirus
Module 4: Internet Security
Module 5: Security on Social Networking Sites
Module 6: Securing Email Communications
Module 7: Securing Mobile Devices
Module 8: Securing the Cloud
Module 9: Securing Network Connections
Module 10: Data Backup and Disaster Recovery
Module 11: Securing IoT Devices and Gaming Consoles
Module 12: Secure Remote Work

KEY OUTCOMES

- Learn 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
- Learn To Safeguard Your IoT Devices and Gaming Consoles
- Secure Their Cloud Accounts & Network Connections

WHO IS IT FOR?

C|SCU goes well beyond traditional security awareness courses providing the training to become an individual power user. Securing your own computer, mobile device, gaming system, home network, Smart Home devices is critical to avoiding low level scams and attacks that many consumers fall victim to every day. This program was designed for any individual who uses computers and/or devices with internet services, including the web, social media, email, messaging apps, etc. that is interested in securing their devices and communication channels.

D|FE Program Overview

This course will introduce learners to Computer Forensics Fundamentals and the Computer Forensics Investigation process. They will learn about the Dark Web, Windows, Linux, Malware Forensics, and much more. The interactive labs component of this course ensure that learners receive the hands-on, practical experience required to succeed in digital forensics.

D|FE-certified learners have an assured means of formal recognition to add to their resumes and demonstrate their expertise and skills to prospective employers.

Who Is it For?

School students, fresh graduates, Professionals, Career starters and switchers, IT / Technology / Cybersecurity teams with little or no work experience.

D|FE Key Features

- 11+ hours of premium self-paced video training.
- 11 lab activities in a simulated lab environment.
- 750+ pages of ecourseware.
- Capstone Projects with Real-World CTF Challenges.
- Proctored exam.

D|FE Course Outline

Module 01: Computer Forensics Fundamentals

Module 02: Computer Forensics Investigation Process

Module 03: Understanding Hard Disks and File Systems

Module 04: Data Acquisition and Duplication

Module 05: Defeating Anti-forensics Techniques

Module 06: Windows Forensics

Module 07: Linux and Mac Forensics

Module 08: Network Forensics

Module 09: Investigating Web Attacks

Module 10: Dark Web Forensics

Module 11: Investigating Email Crimes

Module 12: Malware Forensics

Training & Exam

Training Details: Self-paced, in-demand lecture videos led by world-class instructors and hands-on labs.

Pre-requisite: No prior cybersecurity knowledge or IT work experience required.

Exam Details:

Exam Code: 112-53

Number of Questions: 75

Duration: 2 hours

Test Format: Multiple Choice

N|DE Program Overview

Network Defense Essentials covers the fundamental concepts of information security and network defense. This introductory cybersecurity course is designed for today's entry-level information security or cybersecurity career professionals and is ideal for learners aspiring to pursue a career in cybersecurity.

The course gives a holistic overview of the key components of information security, which include identification, authentication, and authorization, virtualization and cloud computing, wireless networks, mobile and IoT devices, and data security. The interactive labs component ensures that learners receive the hands-on, practical experience required for a future in cybersecurity.

N|DE Course Outline

Module 01: Network Security Fundamentals

Module 02: Identification, Authentication and Authorization

Module 03: Network Security Controls - Administrative Controls

Module 04: Network Security Controls - Physical Controls

Module 05: Network Security Controls - Technical Controls

Module 06: Virtualization and Cloud Computing

Module 07: Wireless Network Security

Module 08: Mobile Device Security

Module 09: IoT Device Security

Module 10: Cryptography and PKI

Module 11: Data Security

Module 12: Network Traffic Monitoring

Who Is it For?

School students, fresh graduates, Professionals, Career starters and switchers, IT / Technology / Cybersecurity teams with little or no work experience.

N|DE Key Features

- 14+ hours of premium self-paced video training.
- 11 lab activities in a simulated lab environment.
- 750+ pages of ecourseware.
- Capstone Projects with Real-World CTF Challenges.
- Proctored exam.

Training & Exam

Training Details: Self-paced, in-demand lecture videos led by world-class instructors and hands-on labs.

Pre-requisite: No prior cybersecurity knowledge or IT work experience required.

Exam Details:

Exam Code: 112-51

Number of Questions: 75

Duration: 2 hours

Test Format: Multiple Choice

E|HE Program Overview

The Ethical Hacking Essentials (E|HE) program is an introductory cybersecurity course that covers ethical hacking and penetration testing fundamentals and prepares learners for a career in cybersecurity. This ethical hacking course will introduce learners to computer and network security concepts such as threats and vulnerabilities, password cracking, web application attacks, IoT and OT attacks, cloud computing, pen testing fundamentals, and more. EC-Council's Ethical Hacking Essentials courses provide hands-on, practical experience to learners, thus giving them the skills necessary for a future in cybersecurity.

Who Is it For?

School students, fresh graduates, Professionals, Career starters and switchers, IT / Technology / Cybersecurity teams with little or no work experience.

E|HE Key Features

- 15+ hours of premium self-paced video training.
- 11 lab activities in a simulated lab environment.
- 750+ pages of ecourseware.
- Capstone Projects with Real-World CTF Challenges.
- Proctored exam.

E|HE Course Outline

Module 01: Information Security Fundamentals
Module 02: Ethical Hacking Fundamentals
Module 03: Information Security Threats and Vulnerability Assessment
Module 04: Password Cracking Techniques and Countermeasures
Module 05: Social Engineering Techniques and Countermeasures
Module 06: Network Level Attacks and Countermeasures
Module 07: Web Application Attacks and Countermeasures
Module 08: Wireless Attacks and Countermeasures
Module 09: Mobile Attacks and Countermeasures
Module 10: IoT and OT Attacks and Countermeasures
Module 11: Cloud Computing Threats and Countermeasures
Module 12: Penetration Testing Fundamentals

Training & Exam

Training Details: Self-paced, in-demand lecture videos led by world-class instructors and hands-on labs.

Pre-requisite: No prior cybersecurity knowledge or IT work experience required.

Exam Details:

Exam Code: 112-52
Number of Questions: 75

Duration: 2 hours
Test Format: Multiple Choice

C|SE Program Overview

This course will provide you with the skills that you need to understand the foundational and essential aspects of Cloud Security. You will learn the fundamentals of cloud computing and the essential aspects of securing identities, data, and applications within cloud providers and hybrid infrastructures. After completing this course, you will be prepared to move toward a career in cloud security and take the next steps in cloud security certifications.

Who Is it For?

School students, fresh graduates, professionals, career starters and switchers, and IT / Technology / Cybersecurity teams with little or no work experience.

C|SE Key Features

- 6 lab practical exercises.
- 10+ Hours of premium self-paced video training.
- 900+ Pages of ecourseware.
- Capstone Projects with Real-World Challenges.
- Proctored exam.

C|SE Course Outline

Module 1: Cloud Computing and Security Fundamentals
Module 2: Identity and Access Management (IAM) in the Cloud
Module 3: Data Protection and Encryption in the Cloud
Module 4: Network Security in Cloud Environments
Module 5: Application Security in Cloud Environments
Module 6: Cloud Security Monitoring and Incident Response
Module 7: Cloud Security Risk Assessment and Management
Module 8: Cloud Compliance and Governance

Training & Exam

Training Details: Self-paced, in-demand lecture videos led by world-class instructors and hands-on labs.

Pre-requisite: No prior cybersecurity knowledge or IT work experience required.

Exam Details:

Exam Code: 112-54
Number of Questions: 75

Duration: 2 hours
Test Format: Multiple Choice

D|SE Program Overview

The DevSecOps Essentials program will provide you with the foundation knowledge and essential aspects of secure application development, or DevSecOps. In this course, you will gather key insights into identifying application development risk and securing and testing applications within on-premises, cloud providers, and hybrid infrastructures. After completing this program, you will be prepared to move toward a career in secure application development.

Who Is it For?

High school students, fresh graduates, professionals, career starters and switchers, and IT / Technology / Cybersecurity teams with little or no work experience.

D|SE Key Features

- 7 practical lab exercises.
- 7+ Hours of premium self-paced video training.
- 900+ pages of ecourseware.
- Capstone Projects with Real-World Challenges.
- Proctored exam.

D|SE Course Outline

Module 01: Introduction to Application Development
Module 02: Application Development Concepts
Module 03: Application Security Fundamentals
Module 04: Introduction to Application Security Testing and Configuration
Module 05: Introduction to DevOps
Module 06: Introduction to DevSecOps
Module 07: Introduction to DevSecOps Management Tools
Module 08: Introduction to DevSecOps Code and CI/CD Tools
Module 09: Introduction to DevSecOps Pipelines
Module 10: Introduction to DevSecOps CI/CD Testing and Assessments
Module 11: Implementing DevSecOps Testing & Threat Modeling
Module 12: Implementing DevSecOps Monitoring and Feedback

Training & Exam

Training Details: Self-paced, in-demand lecture videos led by world-class instructors and hands-on labs.

Pre-requisite: No prior cybersecurity knowledge or IT work experience required.

Exam Details:

Exam Code: 112-55

Number of Questions: 75

Duration: 2 hours

Test Format: Multiple Choice

I|SE Program Overview

EC-Council's IoT Security Essentials program provides comprehensive coverage of essential topics in securing Internet of Things (IoT) systems. From understanding the fundamental concepts of IoT to addressing advanced security threats, students will gain the knowledge and skills necessary to design, deploy, and maintain secure IoT solutions. Through a combination of theoretical learning and hands-on exercises, participants will explore IoT fundamentals, networking and communication protocols, cloud integration, threat intelligence, incident response, and security engineering principles. Ultimately, students will be equipped with the expertise needed to effectively identify, assess, and mitigate security risks in IoT environments, ensuring the integrity, confidentiality, and availability of IoT systems and data.

I|SE Course Outline

Module 01: IoT Fundamentals

Module 02: IoT Networking and Communication

Module 03: IoT Processors and Operating Systems

Module 04: Cloud and IoT

Module 05: IoT Advanced Topics

Module 06: IoT Threats

Module 07: Basic Security

Module 08: Cloud Security

Module 09: Threat Intelligence

Module 10: IoT Incident Response

Module 11: IoT Security Engineering

Who Is it For?

School students, fresh graduates, professionals, career starters and switchers, and IT / Technology / Cybersecurity teams with little or no work experience.

I|SE Key Features

- 5 lab practical exercises.
- 8+ Hours of premium self-paced video training.
- 900+ pages of ecourseware.
- Capstone Projects with Real-World CTF Challenges.
- Proctored exam.

Training & Exam

Training Details: Self-paced, in-demand lecture videos led by world-class instructors and hands-on labs.

Pre-requisite: No prior cybersecurity knowledge or IT work experience required.

Exam Details:

Exam Code: 112-58

Number of Questions: 75

Duration: 2 hours

Test Format: Multiple Choice

S|CE Program Overview

The SOC Essentials (S|OCE) series is tailored to help security professionals and newcomers build essential security technology skills and knowledge. It focuses on the skills needed in Security Operations Centers (SOCs) to prepare individuals for a career in cybersecurity.

This course begins with basic computer networking and security concepts and then moves on to cyber threats, vulnerabilities, and attack types. Provides an overview of Security Operations Center (SOC) architecture and discusses advanced SOC topics such as SIEM architecture and data sources. Additionally, learn about log management with a focus on events, logs, incidents, and centralization. The course covers incident detection and analysis including dashboards, reports, and alarm handling. Additionally, threat intelligence and hunting is explored, leading to incident response and lifecycle processes.

S|CE Course Outline

Module 1: Computer Network and Security Fundamentals

Module 2: Fundamentals of Cyber Threats

Module 3: Introduction to Security Operations Center

Module 4: SOC Components and Architecture

Module 5: Introduction to Log Management

Module 6: Incident Detection and Analysis

Module 7: Threat Intelligence and Hunting

Module 8: Incident Response and Handling

Who Is it For?

High school students, fresh graduates, professionals, career starters and switchers, IT / Technology / Cybersecurity teams with little or no work experience.

S|CE Key Features

- 6 lab practical exercises.
- 10+ Hours of premium self-paced video training.
- 900+ pages of ecourseware.
- Capstone Projects with Real-World CTF Challenges.
- Proctored exam.

Training & Exam

Training Details: Self-paced, in-demand lecture videos led by world-class instructors and hands-on labs.

Pre-requisite: No prior cybersecurity knowledge or IT work experience required.

Exam Details:

Exam Code: 112-56

Number of Questions: 75

Duration: 2 hours

Test Format: Multiple Choice

T|IE Program Overview

This program is designed to deepen your understanding of basic threat intelligence concepts, highlight the differences between intelligence, data, and information, and emphasize their critical role in cybersecurity. Explore the threat intelligence lifecycle and explore its implications for team roles, ethical and legal issues, and the importance of measuring effectiveness.

Throughout the program, you will master different types of threat intelligence - strategic, operational, tactical and technical - and learn how each contributes to compliance and risk management. Participate in hands-on activities including data collection, analysis, and use of Threat Intelligence Platforms (TIPs) for threat hunting and detection. The course concludes with a focus on continuous learning and staying ahead of cybersecurity trends.

Who Is it For?

School students, fresh graduates, professionals, career starters and switchers, IT / Technology / Cybersecurity teams with little or no work experience.

T|IE Key Features

- 5 practical lab exercises.
- 18+ Hours of premium self-paced video training.
- 900+ pages of ecourseware.
- Capstone Projects with Real-World CTF Challenges.
- Proctored exam.

T|IE Course Outline

- Module 1:** Introduction to Threat Intelligence
- Module 2:** Types of Threat Intelligence
- Module 3:** Cyber Threat Landscape
- Module 4:** Data Collection and Sources of Threat Intelligence
- Module 5:** Threat Intelligence Platforms
- Module 6:** Threat Intelligence Analysis
- Module 7:** Threat Hunting and Detection
- Module 8:** Threat Intelligence Sharing and Collaboration
- Module 9:** Threat Intelligence in Incident Response
- Module 10:** Future Trends and Continuous Learning

Training & Exam

Training Details: Self-paced, in-demand lecture videos led by world-class instructors and hands-on labs.

Pre-requisite: No prior cybersecurity knowledge or IT work experience required.

Exam Details:

Exam Code: 112-57

Number of Questions: 75

Duration: 2 hours

Test Format: Multiple Choice

Web Application Hacking and Security

What is WAHS? ➔	Course Content ➔	Who is it for ➔
EC-Council's Web Application Hacking and Security is a specialization certification that enables you to play, learn, hack, test, and secure web applications from existing and emerging security threats in the industry verticals.	100% hands-on lab-based learning about application vulnerabilities and web application hacking. The course provided the challenger with the ability to follow an instructor as they make their way through the challenges.	<ul style="list-style-type: none"> • Penetration Tester • Ethical Hacker • Web Application Penetration • Tester/Security Engineer/Auditor • Red Team Engineer • Information Security Engineer • Risk/Vulnerability Analyst • Vulnerability Manager • Incident responder
Key Outcomes ➔	Related Courses ➔	Exam Information ➔
<ol style="list-style-type: none"> 1. Learn Application Vulnerabilities 2. Hack and Defend web applications 3. Advanced Web Application Penetration Testing 4. Advanced SQL Injection 5. Security Misconfigurations 6. Reflected, Stored and DOM-based Cross Site Scripting (XSS) 7. Cross Site Request Forgery (CSRF) - GET and POST Methods 8. Server-Side Request Forgery (SSRF) 9. CMS Vulnerability Scannin 10. 25+ More 	<ul style="list-style-type: none"> • CND • CEH • CEH (Practical) • CPENT • LPT (Master) • CASE 	<p>EXAM TITLE : WAHS DURATION : 6 Hours AVAILABILITY : ECC Exam Portal</p>

<https://www.eccouncil.org/ceh>

For More Information on Certification: <https://cert.eccouncil.org/ethical-hacking-essentials.html>

Certified Cybersecurity Technician

What is C|CT?



The C|CT is an entry-level cybersecurity program engineered by EC-Council, the creator of the Certified Ethical Hacker (CEH) certification, to address the global need and demand for cybersecurity technicians with strong foundational skills. C|CT is focused on hands-on practice, with more than 50% of training time dedicated to labs.

Course Content



- The C|CT training is accompanied by critical thinking tasks and immersive lab exercises that allow candidates to apply their knowledge and move into the skill development phase in the class itself.
- The C|CT develops participants. Fundamental cybersecurity skills across the fields of network defense, ethical hacking, digital forensics, and security operations giving learners the foundation they need to kickstart a career in cybersecurity.

Who is it for



The C|CT is ideal for anyone looking to start their career in cybersecurity or add a strong foundational understanding of the cybersecurity concepts and techniques required to be effective on the job. The course is especially well suited to:

- Early-career IT professionals, IT managers, career changer, and career advancers
- Students and recent graduates

Key Outcomes



1. Key concepts in cybersecurity, including information security and network Security
2. Information security threats, vulnerabilities, and attacks
3. The different types of malware
4. Identification, authentication, and authorization
5. Network security controls
6. Network security assessment techniques and tools (threat hunting, threat intelligence, vulnerability assessment, ethical hacking, penetration testing, configuration and asset management)
7. Application security design and testing techniques
8. Fundamentals of virtualization, cloud computing, and cloud security
9. Wireless network fundamentals, wireless encryption, and related security measures
10. Fundamentals of mobile, IoT, and OT devices and related security measures
11. Cryptography and public-key infrastructure
12. Data security controls, data backup and retention methods, and data loss prevention techniques
13. Network troubleshooting, traffic and log monitoring, and analysis of suspicious traffic
14. The incident handling and response process
15. Computer forensics and digital evidence fundamentals, including the phase of a forensic investigation
16. investigation
17. Concepts in business continuity and disaster recovery
18. Risk management concepts, phases and frameworks

Exam Information



- EXAM TITLE : Certified Cloud Security Engineer
- EXAM CODE : 212-82
- # OF QUESTIONS : 60
- DURATION : 3 Hours
- AVAILABILITY : ECC Exam Portal
- TEST FORMAT : Multiple choice and Real Life
- hands-on Practical Exam
- EXAM MODE : Remote Proctoring Services

<https://www.eccouncil.org/ceh>

For More Information on Certification: <https://cert.eccouncil.org/ethical-hacking-essentials.html>

Certified DevSecOps Engineer

Solution Overview: ➔

The E|CDE is a hands-on, instructor-led comprehensive DevSecOps certification program that helps professionals build the essential skills needed to design, develop, and maintain secure applications and infrastructure both On-premises and on Cloud Platforms.

Requirements to Meet: ➔

Anyone with prior knowledge of Application Security who wants to build a career in DevSecOps.

Key Target Audience: ➔

- EC-Council's C|ASE-certified professionals
- Application security professionals
- DevOps engineers
- Software engineers and testers
- IT security professionals
- Cybersecurity engineers and analysts

Competitive Differentiators: ➔

- 80+ guided Hands-on Labs
- 32 On-premises-focused labs, 32 AWS – focused labs, and 29 Azure-focused labs
- On-premises and Cloud native DevSecOps
- Application and Infrastructure DevSecOps
- Security in all 8 stages (Plan, Code, Build, Test, Release, Deploy, Operate and Monitor) of DevOps

Customer Pain points ➔

- Lack of DevSecOps discipline results in longer development timelines and insecure code opening applications up to Cyber threats.
- General lack of qualified DevSecOps Professionals.
- Failing to shift left shifts delivery timelines right.

Customer Gains ➔

- Understand DevOps security bottlenecks and discover how the culture, philosophy, practices, and tools of DevSecOps can enhance collaboration and communication across development and operations teams.
- Understand the DevSecOps toolchain and how to include security controls in automated DevOps pipelines.

FAQs: ➔

1. What is the eligibility criteria to apply for the E|CDE exam?
 - a. Applicants must be aware of application security concepts.
2. What is the format of the E|CDE exam?
 - a. The E|CDE exam is an MCQ (Multiple-Choice Question) + Practical exam and is only available at the ECC Exam Centre.
3. How many questions are there in the E|CDE exam?
 - a. The E|CDE exam contains 100 multiple-choice questions.
4. What is the duration of the exam?
 - a. The duration of the E|CDE exam is four hours.
5. What is the passing percentage of the exam?
 - a. The candidate must score 70% to pass the E|CDE exam.

What is the C|CSE - V2?



Certified Cloud Security Engineer (C|CSE) is a hands-on course designed and developed by cloud security professionals in association with subject matter experts across the globe. The C|CSE combines vendor-neutral and vendor-specific cloud security concepts and strengthens foundational knowledge and practical skills for working with popular cloud platforms like AWS, AZURE, and GCP. The C|CSE stands out among other cloud security certifications, empowering professionals to plan, implement, and maintain secure cloud environments. It validates their abilities to protect against and respond to threats in cloud network infrastructures.

Modules



- Introduction to Cloud Security
- Platform and Infrastructure Security in the Cloud
- Application Security in the Cloud
- Data Security in the Cloud
- Security Operations in the Cloud
- Penetration Testing in the Cloud
- Incident Response in the Cloud
- Forensic Investigation in the Cloud
- Business Continuity and Disaster Recovery in the Cloud
- Governance, Risk Management, and Compliance in the Cloud
- Standards, Policies, and Legal Issues in the Cloud

Who is it for?



Network Security: Administrator/Engineer/Analyst
Cyber Security: Engineer/Analyst
Cloud: Administrator/Engineer/Analyst
CND: Certified Professionals
Info: Security Professionals
Any other role that involves: Network/Cloud Administration, Management, and Operations

C|CSE USPs



- A comprehensive cloud security program that covers both generic and cloud service provider (CSP) specific security
- Focus on fundamental vendor-neutral cloud security concepts
- Covers both technical and operational aspects of cloud security
- Deep focus and demonstration on widely used vendor-specific environment like the AWS, AZURE, and GCP cloud security practices, tools, and technologies
- Dedicated focus on penetration testing, forensics investigation, incident response, BC/DR, GRC related security practices in cloud
- Intensive hands-on program with more than 80 labs
- Mapped with real-time job roles and responsibilities of cloud security professionals

Exam Details



Title of the Course: Certified Cloud Security Engineer
Exam Code: 312-40
Number of Questions: 125
Training Duration: 4 hours
Passing Score: 70%
Availability: EC-Council Exam Portal
Test Format: Multiple Choice

What's New in the C|CSE - V2



- New security labs have been added around AWS, Azure, and GCP cloud platforms.
Total number of labs in the C|CSEv2 = 88 labs (up from 54 labs in v1)
- Existing vendor-neutral and vendor-specific cloud security best practices and labs have been updated to match recent cloud technology advancements.
- The complete course curriculum is updated to match exactly with the latest security tools, and techniques for AWS, Azure, and GCP platforms.
- All the tools are updated with the latest tools.
- 33 latest concepts | 44 latest technologies | 15 new best practices added around AWS, Azure, and GCP

What Is Ethical Hacking Essentials? ➔	Course Content ➔	Course Outline
<p>Industrial automation processes use industrial control systems (ICS) and supervisory control and data acquisition (SCADA) systems to control industrial processes locally or remotely and to monitor, gather, and process real-time data.</p>	<p>The ICS/SCADA Cybersecurity course is a hands-on training module that teaches the foundations of security and defending network architectures from attacks. Students will learn to think like a malicious hacker to defend their organizations.</p> <p>ICS/SCADA teaches powerful methods to analyze risks possessed by network infrastructure in IT and corporate spaces. Once your foundation or basic concepts are clear, you will learn a systematic process of intrusion and malware analysis. After this, you will learn about digital forensic process and incident response techniques upon detecting a breach.</p>	<ol style="list-style-type: none">1. Introduction to ICS/SCADA Network Defense2. TCP/IP 101 03. Introduction to Hacking4. Vulnerability Management5. Standards and Regulations for Cybersecurity6. Securing the ICS network7. Bridging the Air Gap8. Introduction to Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS)
Who is it for? ➔	Exam Information	
<p>This course is designed for IT professionals who manage or direct their organization's IT infrastructure and are responsible for establishing and maintaining information security policies, practices, and procedures.</p>	<ul style="list-style-type: none">• EXAM TITLE: ICS / SCADA• EXAM LENGTH: 2 Hours• PLATFORM: ECC Exam Center• # OF QUESTIONS: 75• PASSING SCORE: 70%	

EC-Council Certified Security Specialist (ECSS)

Course Description



EC-Council Certified Security Specialist (ECSS) is an entry level security program covering the fundamental concepts of information security, computer forensics, and network security. It enables students to identify information security threats which reflect on the security posture of the organization and implement general security controls.

This program will give a holistic overview of the key components of information security, computer forensics, and network security. This program provides a solid fundamental knowledge required for a career in information security.

Course Outline



1. Information Security Fundamentals
2. Networking Fundamentals
3. Secure Network Protocols
4. Information Security Threats and Attacks
5. Social Engineering
6. Hacking Cycle
7. Identification, Authentication, and Authorization
8. Cryptography
9. Firewalls
10. Intrusion Detection System
11. Data Backup
12. Virtual Private Network
13. Wireless Network Security
14. Web Security
15. Ethical Hacking and Pen Testing
16. Incident Response
17. Computer Forensics Fundamentals
18. Digital Evidence
19. Understanding File Systems
20. Windows Forensics
21. Network Forensics and Investigating
22. Network Traffic
23. Steganography
24. Analyzing Logs
25. E-mail Crime and Computer Forensics
26. Writing Investigative Report

Key Outcomes



- It facilitates your entry into the world of Information Security
- It provides professional understanding about the concepts of Information Security, Network Security, and Computer Forensics
- It provides best practices to improve organizational security posture
- It enhances your skills as a Security Specialist and increases your employability

Key Outcomes



- Exam Title: EC-Council Certified Security Specialist
- Exam Code: ECSS
- Number of Questions: 50
- Duration: 2 hours
- Availability: ECC Exam Portal
- Test Format: Multiple Choice
- Passing Score: 70%

What is E|CES?

EC-Council's Certified Encryption Specialist (E|CES) program is designed to introduce professionals and students to the intricate field of cryptography.

E|CES is the credential that empowers individuals to make informed decisions in selecting suitable encryption standards for their organizations.

Course Information

- 6 comprehensive modules
- 20 hours advance training
- Practical application and hands-on experience
- In-depth understanding of cryptographic principles
- Best practices when implementing encryption technologies
- Explore steganography, cryptographic algorithms, and quantum computing

Course Content

1. Introduction and History of Cryptography
2. Symmetric Cryptography and Hashes
3. Number Theory and Asymmetric Cryptography
4. Applications of Cryptography
5. Cryptanalysis
6. Quantum Computing and Cryptography

Who is it for?

- Penetration Testers and Computer Forensics Specialists
- Cloud security architects, designers, and developers
- Anyone involved in selecting and implementing VPNs, digital certificates, and information security operations.
- Anyone involved in developing operating systems, cryptography systems, blockchain-based solutions, etc

Exam Information

Exam Title: **EC-Council Certified Encryption Specialist**
Exam Code: **212-81**
Number of Questions: **50**
Exam Duration: **2-Hours**
Exam Availability Locations: **EC-Council Exam Portal**
Exam Format: **Multiple Choice**
Passing Score: **70%**

The Credential that Sets the Global Benchmark for Network Security Skills And Builds Careers in Network Security & Blue Team



C|ND Program Overview



In C|ND students will learn the critical skills required to defend their networks and operating environments across local networks, endpoints, cloud infrastructure, applications, OT, and mobile. They will also acquire knowledge of effective proper log analysis, network traffic monitoring, basic investigation and response, as well as business continuity and disaster recovery. Additionally, they will dive into threats, analyzing the attack surface, and studying threat prediction and threat intelligence as it relates to their administration and defense responsibilities. C|ND's can apply defense and countermeasure strategies in their organizations, playing a critical role in attack prevention, detection, response, and remediation as they configure networks and systems to operate securely. The C|ND program will cover the concepts and fortify skills through hands-on practice across over 110 labs delivered on live target machines.

Learn Latest Concepts



- Asset Management
- System Integrity Monitoring
- Endpoint Detection and Response (EDR)
- Extended detection and response (XDR)
- User and Entity Behavior Analytics (UEBA)
- Privacy Impact Assessment (PIA)
- Threat Hunting
- Security Orchestration Automation and Response (SOAR)

C|ND Key Features



- World's first network security program with continual/adaptive security strategy: **1. Protect 2. Detect 3. Respond 4. Predict**
- Covers defense-in-depth security strategy: **1. Policies, Procedures, and Awareness 2. Physical 3. Perimeter 4. Internal Network 5. Host 6. Application 7. Data**
- Covers four critical security approaches: **1. Preventive Approach 2. Reactive Approach 3. Retrospective Approach 4. Proactive Approach**
- Covers all five functions of the NIST Cybersecurity Framework (CSF): **1. Identify 2. Protect 3. Detect 4. Respond 5. Recover**
- 100+ hands-on labs—the highest number of labs compared to any globally recognized network security certification.
- Accredited by the ANAB (ANSI) ISO/IEC 17024 National Accreditation Board
- Approved by the US Department of Defense (DoD) under Directive 8570/8140
- Recognized by the National Cyber Security Centre NCSC – part of GCHQ (UK's intelligence, security, and cyber agency)

Learn Modern Technologies:



- Cloud, IoT, and Virtualization
- Remote Worker Threats
- Attack Surface Analysis
- Threat Intelligence
- Software Defined Networks (SDN)
- Network Function Virtualization (NFV)
- Docker
- Kubernetes
- Container security

Exam Details:

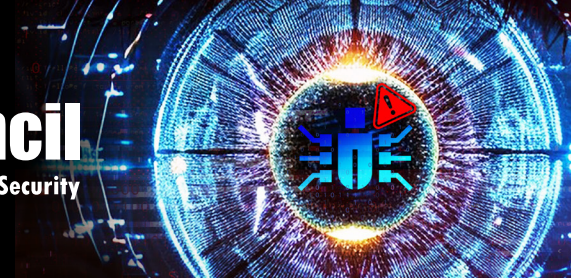


Exam Code: 312-38
Number of Questions: 100
Duration: 4 hours
Availability: EC-Council Exam Portal
Test Format: Multiple Choice

C|ND Course Outline:



- Network Attacks and Defense Strategies
- Administrative Network Security
- Technical Network Security
- Network Perimeter Security
- Endpoint Security-Windows Systems
- Endpoint Security-Linux Systems
- Endpoint Security- Mobile Devices
- Endpoint Security-IoT Devices
- Administrative Application Security
- Data Security
- Enterprise Virtual Network Security
- Enterprise Cloud Network Security
- Enterprise Wireless Network Security
- Network Traffic Monitoring and Analysis
- Network Logs Monitoring and Analysis
- Incident Response and Forensic Investigation
- Business Continuity and Disaster Recovery
- Risk Anticipation with Risk Management
- Threat Assessment with Attack Surface Analysis
- Threat Prediction with Cyber Threat Intelligence



C|TIA Program Overview

EC-Council's Certified Threat Intelligence Analyst (CTIA) program is a comprehensive specialist-level certification designed for individuals involved in collecting, analyzing, and disseminating threat intelligence information. C|TIA covers various topics, including the fundamentals of threat intelligence, the use of threat intelligence tools and techniques, and the development of a threat intelligence program. This course focuses on refining data and information into actionable intelligence that can be used to prevent, detect, and mitigate cyber attacks. The program provides credible professional knowledge required for a successful career in the domain and enhances your overall skills, thus increasing your employability. It addresses all the stages involved in the "Threat Intelligence Life Cycle," and this realistic as well as futuristic approach makes it one of the most comprehensive threat intelligence certifications in the market today.

Key Features of C|TIA

- 800+ pages of the comprehensive student manual
- 350+ pages of lab manual covering detailed lab scenarios and instructions
- 200+ threat intelligence tools
- 27 hands-on labs with real-life networks and platforms to emphasize the learning objectives
- 100% compliance with NICE and CREST Certified Threat Intelligence Manager (CCTIM) frameworks

Exam Details:

Training Duration: 3 Days
Exam Code: 312-38
Number of Questions: 50

Duration: 2 hours
Availability: EC-Council Exam Portal
Test Format: Multiple Choice

What Do You Learn from the C|TIA

1. Master the Cyber Threat Intelligence (CTI) Lifecycle

- Planning and Direction
- Analysis and Production
- Collection
- Dissemination and Integration

2. 4 Types of Threat Intelligence

- Strategic
- Tactical
- Operational
- Technical

3. Threat Hunting and Detection

4. Data Collection Techniques from Multiple Sources and Feeds

5. Threat Analysis and Threat Intelligence Evaluation, Report and Dissemination

6. Latest Threat Intelligence Tools/Platforms and Frameworks

7. Performing Threat Intelligence through Python Scripting

8. Intelligence In SOC Operations, Incident Response, and Risk Management

9. Threat Intelligence in the Cloud Environment

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 entry level 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

1. Module 1: Security Operations and Management
2. Module 2: Understanding Cyber Threats, IoCs, and Attack Methodology
3. Module 3: Incidents, Events, and Logging
4. Module 4: Incident Detection with Security
5. Information and Event Management (SIEM)
6. Module 5: Enhanced Incident Detection with Threat Intelligence
7. Module 6: Incident Response

Certified Penetration Tester

What is C|PENT?



Introducing the most extensive and advanced penetration testing program on the planet. The dynamic pen testing course culminates in a brand new 24-hr practical exam, hosted on the new EC-Council Cyber Range platform, CyberQ. C|PENT provides the capability to assess a pen tester's skills across a broad spectrum of "network zones," with each zone representing a distinct type of testing. The pen testing challenges shall truly test a candidate's ability to think-on-their-feet and perform real world maneuvers. Candidates challenging the C|PENT Program must overcome their assessment challenges which are created in various zones, which is unlike any other Penetration Testing program available in the market today.

Course Content



Students will receive their study kit consisting of physical and digital course materials, including their iLabs code. iLabs will be used to complete classroom training sessions. Students will work with the instructor to review the tools and learn how to apply them to the iLabs Cyber Range.

Who is it for?



- Penetration Testers
- Ethical Hackers
- Information Security Consultants/ Testers/Analysts/Engineers
- Network Server Administrators
- Firewall & System Administrators
- Risk Assessment Professionals

What is new in C|PENT?



- C|PENT is an all new program that is a vital element of the EC-Council VAPT learning track, which also includes C|ND and C|EH.
- Instead of one or two specialties in existing programs, the C|PENT focuses on multiple disciplines, presented through an enterprise network environment that must be attacked, exploited, evaded and defended.
- C|PENT includes advanced Windows attacks with PowerShell (or other bypass techniques), as well as advanced methods to score points within zones.
- Students attack IOT systems by locating and gaining access to the network and identifying the firmware of the IOT device.
- Students also bypass a filtered network and leverage it to gain access to web applications that must be compromised.
- The C|PENT program exposes the learners to advanced environments and techniques such as penetration testing operational technology, double pivoting, evading defence mechanism, report writing, and professional dynamic reporting.

Course Mapping



- CND
- CEH
- CEH (Practical)
- CPENT
- LPT (Master)

Key Outcomes



EXAM TITLE: Certified Penetration Tester
OF QUESTIONS: 10 + Report Writing
DURATION: 24 Hours or 12-Hour Sessions
PASSING SCORE: 70% for CPENT and 90% for LPT (Master)

EC-Council Certified Incident Handler

Gain the Ultimate Skills to Respond and Handle Any Cyber Incidents

E|CIH Advanced Labs

95 Labs environment simulates a real-time environment (Covered in 22 Scenario-based Labs)



Real-Time Environment Simulation



Complex and Advanced Labs:

Every Learning Objective Is Demonstrated Through Complex and Advanced Labs.



Lab-Intensive and Hands-On Approach



Diverse Lab Environment:

Windows, Ubuntu, Parrot Security, Pfsense Firewall, OSSIM Server, and Android



Comprehensive Tools and Platforms:

Forensic Software, Threat Intelligence Platforms, Network Monitoring Solutions, IH&R Tools, SIEM Tools & Solutions

E|CIH Program Overview

EC-Council's Certified Incident Handler program equips students with the knowledge, skills, and abilities to effectively handle and neutralize threats and threat actors in real-time incidents. It covers the entire process of incident handling and response, including hands-on labs that teach tactical procedures and techniques for planning, recording, triage, notification, and containment. Students gain expertise in managing diverse incidents, conducting risk assessments, and understanding relevant laws and policies. By the end of the course, students can create comprehensive IH&R policies and confidently address security incidents like malware, email, network and web application security, cloud security, and insider threats.

E|CIH Key Features:

1600+

Pages of the comprehensive student manual

800+

Incident handling and response tools

10+

Incident handling playbooks and runbooks

780+

Illustrated instructor slides

125

Incident handling templates, checklists, and toolkits

100%

Compliance to NICE 2.0 Framework

100%

Compliance with CREST CCIM

Covers Latest & Largest Collections of IH&R: Templates, Playbooks and Runbooks, Tools/Platforms, Frameworks, Checklists & Toolkits, Cheat Sheets, Real-Time Case studies, Standards, Laws, and Legal Compliance

E|CIH Examination

Exam Title: EC-Council Certified Incident Handler	Exam Availability: ECC Exam Portal	Test Format: Multiple Choice
Duration: 3 hours	Exam Code: 212-89	Number of Questions: 212-89

Course Outline:

• Introduction to Incident Handling and Response	• Handling and Responding to Web Application Security Incidents
• Incident Handling and Response Process	• Handling and Responding to Cloud Security Incidents
• First Response	• Handling and Responding to Insider Threats
• Handling and Responding to Malware Incidents	• Handling and Responding to Endpoint Security Incidents
• Handling and Responding to Email Security Incidents	• Handling and Responding to Network Security

The Credential That Sets the Global Benchmark for Job-Ready Forensic Skills with the Latest Advanced Strategies.



C|HFI Program Overview

EC-Council's C|HFI program prepares cybersecurity professionals with the knowledge and skills to perform effective digital forensics investigations and bring their organization into a state of forensic readiness. This includes establishing the forensics process, lab, evidence handling procedures, as well as the investigation procedures required to validate/triage incidents and point the incident response teams in the right direction. Forensic readiness could be the difference between a minor incident and a major cyber-attack that brings a company to its knees.

C|HFI Course Modules:

- Computer Forensics in Today's World
- Computer Forensics Investigation Process
- Understanding Hard Disks and File Systems
- Data Acquisition and Duplication
- Defeating Anti-forensics Techniques
- Windows Forensics
- Linux and Mac Forensics
- Network Forensics
- Malware Forensics
- Investigating Web Attacks
- Dark Web Forensics
- Cloud Forensics
- Email and Social Media Forensics
- Mobile Forensics
- IoT Forensics

Key Features and Critical Components

- 2100+ pages of the comprehensive student manual
- 1550+ pages of lab manual
- 600+ digital forensics tools
- 68 hands-on labs
- 70+ GB of crafted evidence files for investigation purposes
- Approved and Accredited by US Department of Defense (DoD) 8570/8140 and ANAB (ANSI) ISO/IEC 17024
- Understand regulatory compliance standards such as ISO 27001, PCI DSS, SOX, HIPPA, etc.
- EC-Council C|HFI is mapped to 30+ job roles.

Exam Title: Computer Hacking Forensic Investigator

Exam Code: 312-49

Number of Questions: 150

Duration: 4 hours

Availability: ECC EXAM Portal

Training: 5 Days

What Will You Learn from the C|HFI:

1. Master a methodological forensics framework:

- Documenting the Crime Scene
- Search and Seizure
- Evidence Preservation
- Data Acquisition
- Data Examination
- Reporting

3. Learn diverse types of digital forensic investigation and investigation through Python Scripting.

And more...

2. Gain in-depth skills in

- Social Media Forensics
- Mobile Forensics Analysis
- Wireless Network Forensics
- RAM forensics and Tor forensics
- Electron Application and Web Browser Forensics
- Malware Forensics Process and Malware Analysis
- Forensic Methodologies for Cloud Infrastructure (AWS, Azure, and GCP)
- Dark Web and IoT Forensics

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 today's insecure operating environment.

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

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%

<https://www.eccouncil.org/ceh>

For More Information on Certification: <https://cert.eccouncil.org/ethical-hacking-essentials.html>

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. It's 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

Advanced Penetration Testing

Course Description



In the Advanced Penetration Testing Course, you are presented with minimal network information along with a Scope of Work (SOW). The course was created to provide you with advanced concepts that will help when it comes to attempting the LPT (Master) Certification exam.

The last module of the course includes an SOW for each of the various networks we have created for the course. This, combined with the composition of various ranges, mimics a professional penetration test. Time is limited and you will be required to identify the attack surface followed by the weaknesses of the machines that are on the network.

Key Outcomes



- Prepare you for the LPT (master) exam.
- Learn professional security and penetration testing skills.
- Show advanced concepts like scanning against defenses, pivoting between networks, deploying proxy chains, and using web shells.

Course Outline



- Introduction to Vulnerability Assessment and Penetration Testing
- Information Gathering Methodology
- Scanning and Enumeration
- Identify Vulnerabilities
- Exploitation
- Post Exploitation
- Advanced Tips and Techniques
- Preparing a Report
- Practice Ranges



The Licensed Penetration Tester (Master) Credential- LPT(Master)

Course Description



The LPT (Master) credential is developed in collaboration with SMEs and practitioners around the world after a thorough job role, job task, and skills-gap analysis.

The LPT (Master) practical exam is the capstone to EC-Council's entire information security track, right from the CEH to the ECSA Program. The LPT (Master) exam covers the skill-sets, technical analysis and report writing, required to be a true professional penetration tester.

Key Outcomes



- Mastery of penetration testing skills
- Ability to perform repeatable methodology
- Commitment to code of ethics
- Ability to present analysed results through structured reports

Exam Information



- 3 Levels
- 9 Challenges
- Fully Proctored
- Live Online
- 18 Hours

Testimonial



"Converting fear into confidence with LPT_(Master)"

by Adithya Naresh



"Proud to attain the LPT_(Master) credential"

by Ali Isikli



"LPT_(Master) : Extremely challenging and one of the toughest exams"

by Mark Horvat



"Real-life penetration testing with LPT_(Master)"

by Moustafa Mohamed Mohsen

<https://www.eccouncil.org/ceh>

For More Information on Certification: <https://cert.eccouncil.org/ethical-hacking-essentials.html>

CAST 614 – Advanced Network Defense

Course Description



CAST 614 is an advanced course offering you the opportunity to deep dive into the crucial practical aspects of enterprise network security.

It covers fundamental areas of fortifying your defenses by discovering methods of developing a secure baseline and how to harden your enterprise architecture from the most advanced attacks. Once a strategy for a fortified perimeter is denied, the course moves on to defending against the sophisticated malware that is on the rise today, and the importance of live memory analysis and real time monitoring.

Course Outline



- Firewalls
- Advanced Filtering
- Firewall Configuration
- Hardening: Establishing a Secure Baseline
- Intrusion Detection and Prevention
- Protecting Web Applications
- Memory Analysis
- Endpoint Protection
- Securing an Enterprise

Key Outcomes



- Stage a strong defense against popular security threats
- Fortify your organization with a good foundation of risk protection methods
- Apply latest references and guidance on best practices in the field of cybersecurity
- Secure your enterprise architecture from a medium threat level and build towards more sophisticated threats

Exam Information



Exam Title: CAST 614 - Advanced Network Defense
Number of Questions: 50 (Written) and 10 (Practical)
Duration: 90 minutes (Written) and 60 minutes (Practical)
Availability: ECC Exam Portal
Passing Score: Written Exam (60%) and Practical Exam (70%)

EC-Council Disaster Recovery Professional (E|DRP)

Course Description



The EDRP course identifies vulnerabilities and takes appropriate countermeasures to prevent and mitigate failure risks for an organization. It also provides the networking professional a foundation in disaster recovery course principles, including preparation of a disaster recovery plan, assessment of risks in the enterprise, development of policies and procedures, an understanding of the roles and relationships of various members of an organization, implementation of a plan, and recovering from a disaster.

Course Outline



- Introduction to Disaster Recovery and Business Continuity
- Business Continuity Management (BCM)
- Risk Assessment
- Business Impact Analysis (BIA)
- Business Continuity Planning (BCP)
- Data Backup Strategies
- Data Recovery Strategies
- Virtualization-Based Disaster Recovery
- System Recovery
- Centralized and Decentralized System Recovery
- Disaster Recovery Planning Process
- BCP Testing, Maintenance, and Training

Key Outcomes



- Introduction to business continuity, risk management, and disaster recovery
- Disasters and emergency management, and applicable regulations
- DR planning process, preparation, recovery of systems and facilities
- Incident response and liaison with public services and regulatory bodies
- Exposure to various services from government and other entities

Exam Information



Exam Title: EC-Council Disaster Recovery Professional
Exam Code: 312-76
Number of Questions: 150
Duration: 4 hours
Availability: ECC Exam Portal
Test Format: Multiple Choice
Passing Score: 70%

<https://www.eccouncil.org/ceh>

For More Information on Certification: <https://cert.eccouncil.org/ethical-hacking-essentials.html>

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.

Course Outline



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

Exam Information



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

Blockchain Developer Certification (B|DC)

Course Description



The course aims to provide developers with a comprehensive understanding of blockchain technology, including its impact and applications in business and finance. Students will learn about cryptography, cryptomining, quantum computing, blockchain project implementation, Ethereum, and more.

Key Outcomes



- Blockchain network structure and decentralization: Understand the structure and working of blockchain networks, with a focus on decentralization.
- Hashing, consensus algorithms, and their role in blockchain: Learn about the importance of hashing and consensus algorithms like PoW and PoS in blockchain networks.
- Benefits and suitability of blockchain technology: Discover the advantages of blockchain and how to assess its applicability for your business needs.
- Blockchain scalability and resolution: Explore the scalability challenges faced by blockchain networks and potential solutions.
- Digital currencies and leading cryptocurrencies: Gain knowledge about different types of cryptocurrencies, tokenization, and the functioning of popular cryptocurrencies such as Bitcoin, Altcoin, Litecoin, and Zcash.
- Other key learnings include the structure and components of the Bitcoin network, Bitcoin's limitations, cryptomining and its relation to PoW consensus, development in Python, JavaScript, and Java, Ethereum ecosystem and Solidity, secure smart contract development, permissioned and permission less blockchains, Hyperledger Fabric framework, privacy in blockchains, decentralized autonomous organizations (DAOs), blockchain-based identity solutions, machine learning and blockchain, convergence of blockchain and AI, IoT and blockchain convergence, blockchain use cases in healthcare, fintech, and supply chain, Blockchain as a Service, impact of quantum computing on blockchains, and the future of blockchain technology and research.

Prerequisites



- General awareness of business management processes
- Basic knowledge of computers
- Access to a Linux machine that can be configured as a virtual machine

Who Is It For?



Software engineers, programmers, project managers, network administrators, and other technical professionals interested in integrating blockchain applications and architectures into their organization.

Exam Information



EXAM TITLE: Blockchain Fintech Certification: 312-81
NUMBER OF QUESTIONS : 50
TEST DURATION : 1.5 Hours
TEST FORMAT: Multiple Choice
TEST DELIVERY: EC-Council Exam

<https://www.eccouncil.org/ceh>

For More Information on Certification: <https://cert.eccouncil.org/ethical-hacking-essentials.html>

Business Leader Certification (B|BLC)

Course Description



The B|BLC course aims to teach business leaders how to use blockchain technology to improve business operations by equipping them with technical knowledge and hands-on experience with blockchain technologies. The curriculum covers Ethereum and Bitcoin in detail, in addition to issues such as blockchain security and Blockchain as a Service (BaaS).

Key Outcomes



- Blockchain network structure and decentralization: Understand how blockchain networks are organized and the concept of decentralization.
- Hashing and consensus algorithms in blockchain: Learn about the role of hashing and consensus algorithms like PoW and PoS in maintaining the integrity of blockchain networks.
- Digital currencies and leading cryptocurrencies: Explore different types of digital assets, the tokenization process, and how popular cryptocurrencies like Bitcoin, Altcoin, Litecoin, and Zcash function.
- Benefits and suitability of blockchain technology: Discover the advantages of using blockchain technology and how to determine if it's the right solution for your business.
- ICOs vs. IPOs: Understand the differences between Initial Coin Offerings (ICOs) and Initial Public Offerings (IPOs) for fund raising purposes.
- Other key learnings include securitization of physical assets, resolving blockchain scalability issues, designing blockchain-based identity solutions, exploring various blockchain use cases, understanding Solidity and Ethereum, creating private blockchain networks, Bitcoin's structure and mining, secure smart contract development, privacy and confidentiality in blockchains, Blockchain as a Service (BaaS), permissioned and permissionless blockchains, Hyperledger Fabric framework, and decentralized autonomous organizations (DAOs) and more.

Prerequisites



- General awareness of business management processes
- Basic knowledge of computers
- Access to a Linux machine that can be configured as a virtual machine

Who Is It For?



Business leaders at all levels, from mid-level managers to senior executives who want to incorporate blockchain technology into their organization.

Exam Information



EXAM TITLE: Blockchain Business Leader
CERTIFICATION: 312-83
NUMBER OF QUESTIONS: 50
TEST DURATION: 1.5 Hours
TEST FORMAT: Multiple Choice
TEST DELIVERY : EC-Council Exam

Blockchain Fintech Certification (B|FC)

Course Description



The BIFC course will enable financial professionals to utilize blockchain technology to improve financial services and the insurance industry. Students learn the laws and regulations related to financial applications of blockchain and how to use PoW and PoS consensus mechanisms. In addition, the program provides in-depth insights into cryptocurrencies, including Bitcoin wallets and exchanges, among other topics.

Key Outcomes



- Blockchain network structure and decentralization: Understand the organization and decentralization of blockchain networks.
- Hashing, consensus algorithms, and their role in blockchain: Learn about the role of hashing, consensus algorithms (PoW and PoS), and their significance in blockchain networks.
- Benefits and suitability of blockchain technology: Discover the advantages of using blockchain technology and how to assess its suitability for your business.
- Digital currencies and leading cryptocurrencies: Explore different types of digital assets, tokenization, and gain insights into popular cryptocurrencies like Bitcoin, Altcoin, Litecoin, and Zcash.
- Financial applications of blockchain: Understand how blockchain works in the financial sector, including decentralized finance, apps, exchanges, insurance, and common use cases.
- Other key learnings include ICOs vs. IPOs, securitization of physical assets, Solidity and Ethereum basics, private blockchain networks using Ethereum, Bitcoin network structure, Bitcoin mining and variants, secure smart contract development, privacy in blockchains, Blockchain as a Service, permissioned and permissionless blockchains, Hyperledger Fabric framework, and decentralized autonomous organizations (DAOs) and more.

Prerequisites



- General awareness of business management processes
- Basic knowledge of computers
- Access to a Linux machine that can be configured as a virtual machine

Who Is It For?



Finance professionals, fintech professionals, and related professionals interested in integrating blockchain into their organization's financial applications and needs.

Exam Information

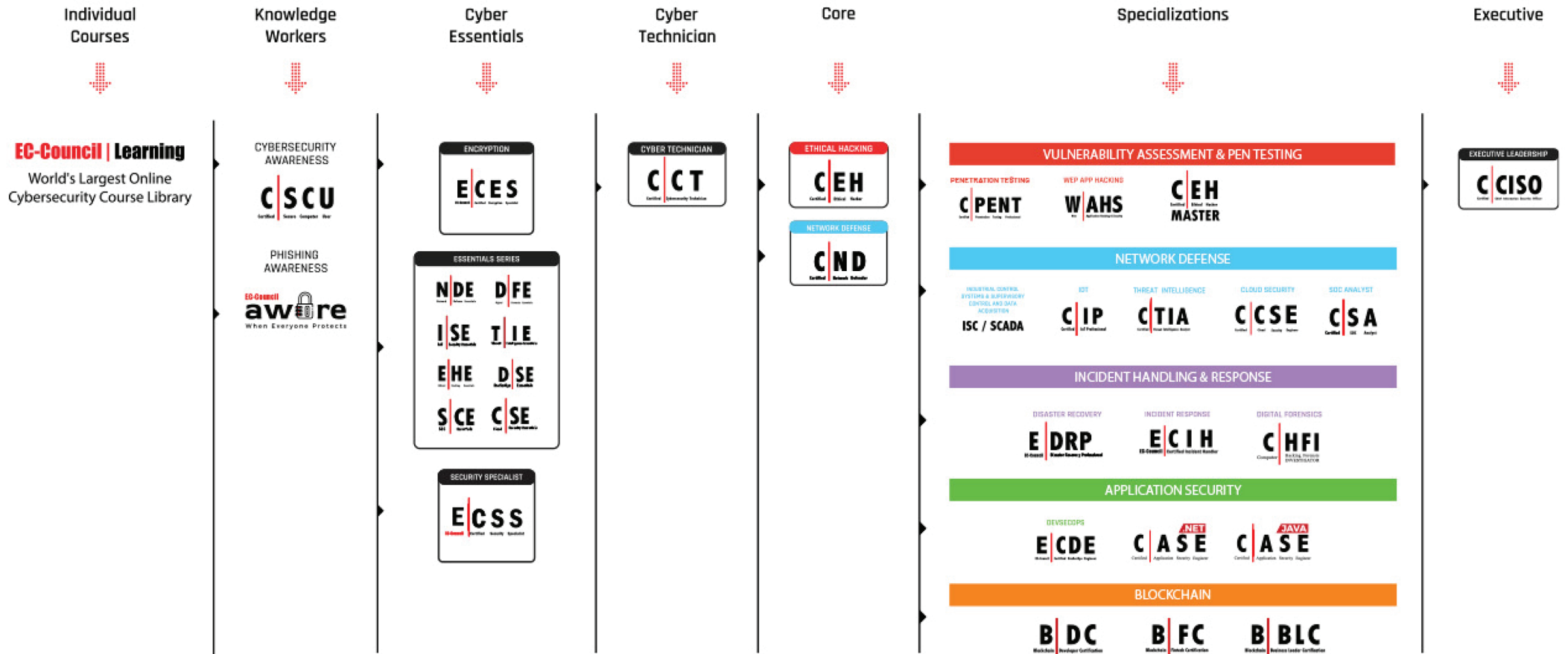


EXAM TITLE: Blockchain Fintech Certification: 312-82
NUMBER OF QUESTIONS : 50
TEST DURATION: 1.5 Hours
TEST FORMAT: Multiple Choice
TEST DELIVERY : EC-Council Exam

<https://www.eccouncil.org/ceh>

For More Information on Certification: <https://cert.eccouncil.org/ethical-hacking-essentials.html>

Cybersecurity Learning Track



Course Description



Aware 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. Aware 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

Aware Solutions



- Email Phishing
- Vishing
- Smishing
- Spear Phishing

EC-Council | Learning

EC-Council Learning / EC-Council Micro-degrees:

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

Why EC-Council Learning :

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 Learning Plans

Pro

Ideal for continuous learning, offering extensive resources with 600+ courses and diverse Learning Paths to enhance your skills.



What is included

- ✓ Access to 600+ Premium Short Courses
- ✓ 80+ Structured Learning Paths
- ✓ Certificates of Completion with all courses and learning paths
- ✓ New Courses are added every month

Pro +

Experience immersive learning with Practice Labs, CTF Challenges, and exclusive EC-Council certifications for comprehensive skill-building.

Everything in Pro and :

- ✓ 500+ Practice Lab exercises with guided instructions
- ✓ 70+ CTF Challenges with detailed walkthroughs 
- ✓ New Practice Labs and Challenges added every month 
- ✓ 3 Official Certifications from EC-Council

Exclusive Bonus with Annual





Pro+ For Teams

Maximize team performance with tailored training solutions, including custom learning paths and robust reporting capabilities.





Everything in Pro+ and:

- ✓ Detailed reporting on users and courses
- ✓ Create custom Learning Paths for your users
- ✓ Create custom Learning Paths for your user group management and reporting with sub-account Features
- ✓ Dedicated Success Manager

Bachelor of Science in Cyber Security (BSCS)

Course Description 		Course Outline 
<p>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.</p>		<ul style="list-style-type: none"> • 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
Key Outcomes 	Exam Information 	
<ul style="list-style-type: none"> • 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. 	<ul style="list-style-type: none"> • 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. 	

Graduate Certificate Programs

Course Description 		Course Outline 	
<p>EC-Council University's 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.</p>		<ul style="list-style-type: none"> • Information Security Professional <ul style="list-style-type: none"> - Managing Secure Networks (C ND) - Ethical Hacking and Countermeasures (C EH) - Research and Writing for the IT Practitioner • Security Analyst <ul style="list-style-type: none"> - 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) <ul style="list-style-type: none"> - Secure Programming - Advanced Network Defense - Advanced Mobile Forensics or - Designing and Implementing Cloud Security • Incident Management and Business Continuity <ul style="list-style-type: none"> - Beyond Business Continuity - Disaster Recovery (EDRP) - Incident Handling and Response (ECIH) • Executive Leadership in Information Assurance <ul style="list-style-type: none"> - Global Business Leadership - Project Management - Executive Governance and Management (CCISO) 	
Key Outcomes 	Exam Information 		
<ul style="list-style-type: none"> • Information Security Professional • Security Analyst • Cloud Security Architect • Incident Management and Business Continuity • Executive Leadership in Information Assurance 	<ul style="list-style-type: none"> • Completion of mandated credit hours of courses in which the candidate earned a cumulative GPA of 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 completion 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. 		

<https://www.eccouncil.org/ceh>

For More Information on Certification: <https://cert.eccouncil.org/ethical-hacking-essentials.html>

Master of Science in Cyber Security (MSCS)

Course 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.

Course Outline



- 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

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

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.

<https://www.eccouncil.org/ceh>

For More Information on Certification: <https://cert.eccouncil.org/ethical-hacking-essentials.html>



EC-Council
Masterclass

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

The logo graphic consists of a central black circle containing the text 'EC-Council' and 'Building A Culture Of Security'. This circle is surrounded by a thick red ring. A white line separates the red ring from a larger, faint grey circle in the background. A thick red horizontal bar extends from the right side of the red ring across the bottom of the image.

EC-Council

Building A Culture Of Security

www.eccouncil.org