EC-Council iLearn Courses

1. Self-Paced Online Courses

Each course package includes:

- Instructor-led, streaming video training modules – 1-year access
- Official EC-Council e-courseware – 1-year access
- iLabs, EC-Council's virtual lab platform – 6 months access
- Certification Exam Voucher – 1-year access
- Certificate of Attendance

	Course Name	Course Description	Course Pre-requisite
1	Certified Ethical Hacker (CEH)	The Certified Ethical Hacker (C|EH v10) program is a trusted and respected ethical hacking training program that any information security professional will need. This course will immerse you into a "Hacker Mindset" in order to teach you how to think like a hacker and better defend against future attacks. It puts you in the driver's seat with a hands-on training environment employing a systematic ethical hacking process.	Basic knowledge of OS, Scripting languages, Networking, Computer Architecture

2	Certified Chief Information Security Officer (CCISO)	The Certified CISO (CCISO) program is aimed at producing top-level information security executives. The CCISO does not focus solely on technical knowledge but on the application of information security management principles from an executive management point of view.	Must show 5 years of experience in 3 of the 5 CCISO domains in order to take the CCISO exam
3	Certified Application Security Engineer (CASE JAVA/CASE .NET)	Focuses on secure application software development processes. It is a, hands-on, comprehensive application security course that will help you create a secure application software. This course encompasses security activities involved in all phases of the Secure Software Development Lifecycle (SDLC): Planning, creating, testing, and deploying an application.	Minimum 2 years of development experience
4	Certified Incident Handler V2 (ECIH V2)	Designed to provide the fundamental skills to handle and respond to computer security incidents in an information system.	Minimum 1 year of work experience in the domain that would like to apply to take the exam

		Provides incident response training by addressing various underlying principles and techniques for detecting and responding to current and emerging computer security threats. After attending the course, you will be able to create incident handling and response policies and deal with various types of computer security incidents.	
5	Certified Secure Computer User (CSCU)	This course is specifically designed for todays' computer users who use the internet extensively. The purpose of the CSCU training program is to provide individuals with the necessary knowledge and skills to protect their information assets.	None
6	Certified Encryption Specialist (ECES)	The program introduces professionals to the field of cryptography. Participants will learn the foundations of modern symmetric and key cryptography including the details of algorithms such as Feistel Networks, DES, and AES. Anyone	Basic Computer/Internet Skills; Basic IP addressing knowledge; No mathematical skills beyond algebra

		involved in the selection and implementation of VPN's or digital certificates should attend this course.	
7	Advanced Penetration Tester (APT)	This course prepares you for the LPT (Master) certification exam and covers the testing of modern infrastructures, operating systems and application environments. It also covers the process to document and prepare a professional penetration testing report. ***not a certification; This is course preparation for LPT***	Attendees must be ECSA-certified and in good standing, as well as possess a minimum of 2 years experience in penetration testing.
8	Certified Threat Intelligence Analyst (CTIA)	This is a combination of cyber security and threat intelligence to help identify and mitigate business risks by converting unknown internal and external threats into known threats. It is a comprehensive, specialist-level program that teaches a structured approach for building effective threat intelligence.	Basic knowledge of programming language C and PHP

9	Computer Hacking Forensic Investigator (CHFI)	This course covers knowledge of digital forensic techniques and standard forensic tools to collect the intruder's footprints necessary for his investigation. It delivers on methodological ways to deal with digital forensics, including seizing, chain of custody, acquisition preservation, analysis and presentation of digital evidence.	Basic knowledge on IT and cyber security, computer forensics and incident response. Prior completion of CEH training would be an advantage.
10	Certified Security Analyst/Licensed Pentester (ECSA)	The ECSA course is a fully hands-on program with labs and exercises that cover real world scenarios. By practicing the skills that are provided to you in the ECSA class, we are able to bring you up to speed with the skills to uncover the security threats that organizations are vulnerable to.	Certified Ethical Hacker (CEH) certification is not required but strongly recommended as a prerequisite to attending this course
11	Certified Network Defender (CND)	This course prepares Network Administrators on network security technologies and operations to attain Defence-in-Depth network security skills. It contains hands-on labs,	Fundamental knowledge of Networking Concepts

		based on major network security tools and techniques which will provide Network Administrators real world expertise on current network security technologies and operations.	
12	EC-Council Disaster Recovery Program (EDRP)	EDRP provides the professionals with a strong understanding of business continuity and disaster recovery principles, including conducting business impact analysis, assessing of risks, developing policies and procedures, and implementing a plan. It also teaches professionals how to secure data by putting policies and procedures in place, and how to recover and restore their organization’s critical data in the aftermath of a disaster.	Basic experience in the IT BC/DR domain
13	Ethical Hacking Core Skills (EHCS)	This course is the first step on the EC Council Pen testing career track. In this course you will learn the core skills to build a solid security foundation.	None

14	Licensed Penetration Tester (LPT)	The LPT (Master) standardizes the knowledge base for penetration testing professionals by incorporating best practices followed by experienced experts in the field. The objective is to ensure that each licensed professional follows a strict code of ethics, is exposed to the best practices in the domain of penetration testing and aware of all the compliance requirements required by the industry.	There is no predefined eligibility criteria for those interested in attempting the LPT (Master) exam
15	Certified Ethical Hacker (CEH) (Practical)	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. _*Exam only_	There is no predefined eligibility criteria for those interested in attempting the CEH(Practical) exam.

16	Certified Security Analyst/Licensed Pentester (ECSA) (Practical)	ECSA Practical is a 12-hour, rigorous practical exam built to test your penetration testing skills. **Exam only*	There is no predefined eligibility criteria for those interested in attempting the ECSA (Practical) exam.
17	Certified Blockchain Professional (CBP)	CBP is fully vendor-agnostic and practical, focusing on the current state of blockchain technology as well as its future potential. The Certified Blockchain Professional course digs deep into the main characteristics and features of the distributed ledger technology (DLT) as well as introduces Blockchain's new 3S (Secure-Scalable-Sustainable) proprietary framework. Students will also get a deep understanding of blockchain technology and mining of cryptocurrency.	Program is specifically tailored to full-stack developers
18	Certified Threat Intelligence Analyst (CTIA)	CTIA is designed and developed in collaboration with cybersecurity and threat intelligence experts across the globe to help organizations identify and	Minimum of 2 years working experience in information security

		mitigate business risks by converting unknown internal and external threats into known threats. It is a comprehensive, specialist-level program that teaches a structured approach for building effective threat intelligence.	
19	Certified SOC Analyst (SOC)	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.	Minimum one year of work experience in the Network Admin/Security domain

2. Self-Paced Online Workshops

	Course Name	Workshop Description	Course Details
1	Risk Management Approach & Practices	This risk management course is specifically designed to guide a CISO in defining and implementing a risk management approach within an IS program. The course introduces the student to the most common approaches and practices used by	This is a 2-day course that includes e-courseware and videos. Participants will receive a certificate of participation at the end of this workshop.

		organizations worldwide. It is not intended to cover risk outside of the IS enterprise (including financial and business risks).	
2	Dark Web Forensics Deep Dive Workshop	This is an in-depth workshop on Dark Web Forensics investigations including technical details of how the dark web/TOR works, a tour of actual dark web markets; and specific investigative techniques or tools for dark web investigations.	This is a 2-day course that includes videos. Participants will receive a certificate of participation at the end of this workshop.
3	Malware & Memory Deep Dive Workshop	This course assumes basic understanding of PC's, networks, and basic forensics. The purpose is to teach students essential memory forensics.	This is a 2-day course that includes videos. Participants will receive a certificate of participation at the end of this workshop.
4	Mobile Forensics Deep Dive Workshop	This is a two-day course designed to immerse the person in phone forensics.	This is a 2-day course that includes videos. Participants will receive a certificate of participation at the end of this workshop.