EC-Council

Essentials Series

EC-Council's MOOC Certification Course Series

Network Defense

N|DE
Network Defense Essentials

Ethical Hacking

E|HE
Ethical HackingE ssentials

Digital Forensics

D|FE
Digital Forensics Essentials

Essential Skills for Tomorrow's Entry-Level Cybersecurity Careers

A cybersecurity workforce development initiative by EC-Council.

Copyright EC-Council. All Rights Reserved.

Why Join the Cybersecurity Industry?

Given that the threat landscape has increased in scope and remote workers are soft targets for hackers, organizations across the globe are looking to hire qualified information and cybersecurity specialists. The need for qualified ethical hackers, network defenders, cybersecurity analysts, system administrators, SOC analysts, information security analysts, and digital forensics analysts, among others, is only going to increase in the future.

According to Monster, the unemployment rate in the cybersecurity field is close to 0%

Cybersecurity Professionals Are in Demand in These Industries

The demand for cybersecurity professionals has only continued to grow, and extends across a spectrum of industries, including banking and financial services, information technology and management, government agencies, and consulting services.

Scope and Career Growth

Cybersecurity is a fast-growing sector globally and this offers tremendous job opportunities for IT professionals and aspiring cybersecurity enthusiasts.

One can specialize in any domain of their choice, including ethical hacking, endpoint security, digital forensics, security analysis, mobile forensics, incident handling, and more.

Copyright EC-Council. All Rights Reserved.

What is the Essentials Series?

The Essentials Series' Massive Open Online Courses (MOOCs) contain eCourseware and video instruction, which is being offered free, with optional paid upgrades to course labs, exam prep, course assessments, and exam vouchers leading to certifications across each of the three Essentials Series courses.

ESSENTIALS SERIES

N|DE Network Defense Essentials

E|HE Ethical Hacking Essentials

D|FE Digital Forensics Essentials

EC-Council's Essentials Series is the first MOOC certification course series covering essential skills in network defense, ethical hacking, and digital forensics. The Network Defense Essentials (N|DE), Ethical Hacking Essentials (E|HE), and Digital Forensics Essentials (D|FE) are foundational programs that help students and early career professionals choose their area of competency or select a specific interest in cybersecurity.

The Essentials Series was designed to give students the foundation on which to build and develop the essential skills for tomorrow's careers in cybersecurity. These programs educate learners in a range of techniques across industry verticals, such as securing networks, mitigating cyber risks, conducting forensic investigations, and more.

Designed by the Experts

The Essentials Series was designed by industry experts to provide an unbiased approach to learning and exploring **industry best practices**. It empowers individuals to:

- **Gain foundational knowledge in cybersecurity**
- **Practice essentials skills such as how to defend networks and investigate them**
- **Challenge industry recognized exams and earn cybersecurity credentials to build and further your career**

Copyright EC-Council. All Rights Reserved.

Course Material & Benefits

Included In MOOCs:

- eBook
- Video lectures & lab lectures

Optional (Paid) Upgrades:

- Lab Range
- Post Course Assessment & Certificate of Completion
- Certification Exam (On-site Testing or Remote Proctor Services - RPS)

Free Courseware: The Essentials series comes with free learning resources such as eCourseware, lab tutorials, and video lectures that are easy to download and read on any device.

Lab Range (Paid): Practical hands-on learning in a simulated environment gives candidates a competitive edge to hone their skills. Each course in the Essentials Series includes 12 modules with learning exercises and lab ranges that provide a basic to intermediate knowledge of network defense, ethical hacking, and digital forensics.

Certification (Paid): Each Essentials course comes with an onsite or remote certification exam. Following a successful exam attempt, the course-specific certification credential will have a validity period of three years from the date of the successful exam attempt.

Unlock paid add-ons, such as lab exercises within the modules, a certification of completion, and certification exams at a fraction of the cost.

Who Should Attend These Courses?

EC-Council's Essentials Series programs and certifications build and validate candidates' skills for their cybersecurity future. It is ideal for IT professionals who are seeking to **foray** into the exciting world of cybersecurity. Cybersecurity enthusiasts and students will readily find the program interesting, challenging, and useful.

Copyright EC-Council. All Rights Reserved.

Exam & Certification

There are no eligibility criteria for the Essentials Series. The certification is valid for three years from the date the certificate is issued. The recertification window is at the end of 3-years, and EC-Council members may recertify by passing the exam again. There are no annual fees or EC-Council Continuing Education Credits (ECE's) required to maintain the certification credential during the three-year term.

Exam Length : 2 Hours

Exam Format : MCQ

Exam Platform : ECC Exam Centre

No. of Questions : 75

Certification : Course Specific (NDE, EHE, DFE)

Get Certified

Job Roles That Benefit from These Essentials Programs

Professionals in the following roles who are looking to enhance their knowledge or transition from an IT role into cybersecurity would benefit from the Essentials Courses.

N|DE™ Network Defense Essentials	E|HE™ Ethical Hacking Essentials	D|FE™ Digital Forensics Essentials
Local Area Network Specialist	Help Desk Technician	Cybersecurity Technician
Network Security Analyst	Technical Support Specialist	Cyber Forensic Specialist
Network Technician	Systems Specialist	Cyber Operations Technician
Network Administrator	Computer Support Specialist	Intelligence Operations Specialist
Network Coordinator	Cybersecurity Specialist	IT Security Specialist

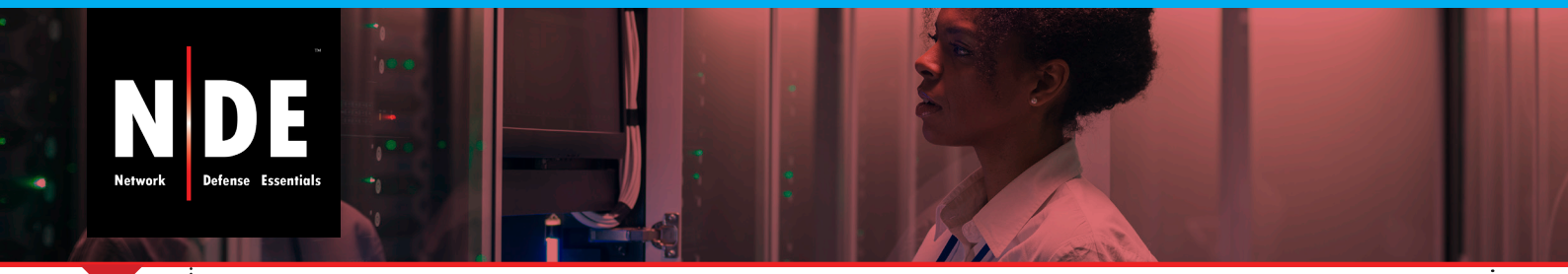
Copyright EC-Council. All Rights Reserved.

Network Defense Essentials is a first-of-its-kind MOOC certification that provides foundational knowledge and skills in network security with add-on labs for hands-on experience. The course includes 12 modules and optional upgrades to lab ranges covering fundamental network security concepts, including IoT, cryptography, and PKI.

Modules: What You Will Learn

01	**Network Security Fundamentals**	• Fundamentals of network security • Network security protocols that govern the flow of data
02	**Identification, Authentication, and Authorization**	• Access control principles, terminologies, and models • Identity and access management (IAM)
03	**Network Security Controls: Administrative Controls**	• Regulatory frameworks, laws, and acts • Security policies, and how to conduct security and awareness training
04	**Network Security Controls: Physical Controls**	• Importance of physical security and physical security controls • Physical security policies and procedures • Best practices to strengthen workplace security • Environmental controls
05	**Network Security Controls: Technical Controls**	• Types of bastion hosts and their role in network security • IDS/IPS types and their role in network defense • Types of honeypots and virtual private networks (VPNs) • Security incident and event management (SIEM)
06	**Virtualization and Cloud Computing**	• Key concepts of virtualization and OS virtualization security • Cloud computing fundamentals and cloud deployment models • Cloud security best practices
07	**Wireless Network Security**	• Fundamentals of wireless networks and encryption mechanisms • Wireless network authentication methods • Implementing wireless network security measures

Copyright EC-Council. All Rights Reserved.



08	**Mobile Device Security**	• Mobile device connection methods and management • Mobile use approaches in enterprises • Security risks and guidelines associated with enterprise mobile usage policies • Implement various enterprise-level mobile security management solutions • Best practices on mobile platforms
09	**IoT Device Security**	• IoT devices, application areas, and communication models • How security works in IoT-enabled environments
10	**Cryptography and PKI**	• Cryptographic tools, security techniques, and algorithms • Public key infrastructure (PKI) to authenticate users and devices in the digital world
11	**Data Security**	• Data security and its importance • Security controls for data encryption • Perform data backup and retention • Implement data loss prevention concepts
12	**Network Traffic Monitoring**	• Network traffic monitoring concepts. • Traffic signatures for normal and suspicious network traffic. • Perform network monitoring to detect suspicious traffic.

Tools You Will Learn and Use

Docker Bench for security, AWS, Miradore MDM, HashCalc, MD5 calculator, HashMyFiles, VeraCrypt, Data Recovery Wizard, and Wireshark

» e-Learning resources including eBook and videos are available to all learners, free of charge.
» Unlock powerful add-ons, including cloud labs that provide intensive skills training and practice, official EC-Council certification exams, exam preps and certification of completion.

Exam Information

Certification : Network Defence Essentials
Exam Length : 2 Hours
Exam Format : MCQ
No. of Questions: 75

Get Certified

Copyright EC-Council. All Rights Reserved.

Ethical Hacking Essentials is a first-of-its-kind MOOC certification that provides foundational knowledge and skills in ethical hacking with add-on labs for hands-on experience. The course contains 12 modules and add-on labs covering fundamental ethical hacking concepts, including emerging technologies like IoT and OT, cloud computing, etc.

Modules: What You Will Learn

01	**Information Security Fundamentals**	• Information security fundamentals • Information security laws and regulations
02	**Ethical Hacking Fundamentals**	• Cyber Kill Chain methodology • Hacking concepts, hacking cycle, and different hacker classes • Ethical hacking concepts, scope, and limitations
03	**Information Security Threats and Vulnerabilities**	• Detect various threat sources and vulnerabilities in a network or system • Different types of malwares
04	**Password Cracking Techniques and Countermeasures**	• Types of password cracking techniques
05	**Social Engineering Techniques and Countermeasures**	• Social engineering concepts and techniques • Insider threats and identity theft concepts
06	**Network-Level Attacks and Countermeasures**	• Packet sniffing concepts and types • Sniffing techniques and countermeasures • DoS and DDoS attacks under sniffing attacks
07	**Web Application Attacks and Countermeasures**	• Web Server Attacks • Web Application Attacks • Web Application Architecture and Vulnerability Stack • Web Application Threats and Attacks • SQL Injection Attacks • Types of SQL Injection Attacks

Copyright EC-Council. All Rights Reserved.

08	**Wireless Attacks and Countermeasures**	• Wireless Terminology • Types of Wireless Encryption • Wireless Network-specific Attack Techniques • Bluetooth Attacks • Wireless Attack Countermeasures
09	**Mobile Attacks and Countermeasures**	• Mobile Attack Anatomy • Mobile Attack Vectors and Mobile Platform Vulnerabilities
10	**IoT and OT Attacks and Countermeasures**	IoT Attacks • IoT Devices, their need and Application Areas • IoT Threats and Attacks OT Attacks • Understand OT Concepts • OT Challenges and Attacks • OT Attacks Countermeasures
11	**Cloud Computing Threats and Countermeasures**	• Cloud Computing Concepts • Container Technology • Cloud Computing Threats • Cloud Computing Countermeasures
12	**Penetration Testing Fundamentals**	• Fundamentals of Penetration Testing and its Benefits • Various Types and Phases of Penetration Testing • Guidelines and Recommendations for Penetration Testing

Tools You Will Learn and Use

LOphtCrack, Netcraft, SQL Injection Detection Tool, Web Application Security Scanner, ARP Spoofing Detection Tools

» e-Learning resources including eBook and videos are available to all learners, free of charge.
» Unlock powerful add-ons, including cloud labs that provide intensive skills training and practice, official EC-Council certification exams, exam preps, and certification of completion.

Exam Information

Certification : Ethical Hacking Essentials
Exam Length : 2 Hours
Exam Format : MCQ
No. of Questions: 75

Get Certified

Copyright EC-Council. All Rights Reserved.

Digital Forensics Essentials is a first-of-its-kind MOOC certification that offers foundational knowledge and skills on digital forensics with add-on labs for hands-on experience. Twelve modules cover the fundamental concepts of digital forensics, such as dark web forensics, investigating web application attacks, and more.

Modules: What You Will Learn

01	**Computer Forensics Fundamentals**	• Fundamentals of computer forensics and digital evidence • Objectives of forensic readiness to reduce the cost of investigation • Roles and responsibilities of a forensic investigator. • Legal compliance in computer forensics
02	**Computer Forensics Investigation Process**	• Forensic investigation process and its importance • Forensic investigation phases
03	**Understanding Hard Disks and File Systems**	• Types of disk drives and their characteristics • Booting process of Windows, Linux, and Mac operating systems • Examine file system records during an investigation
04	**Data Acquisition and Duplication**	• Data acquisition fundamentals, methodologies, and their different types • Determine the data acquisition format
05	**Defeating Anti-forensics Techniques**	• Anti-forensics techniques and their countermeasures
06	**Windows Forensics**	• How to gather volatile and non-volatile information • Perform Windows memory and registry analysis • Analyze the cache, cookie, and history recorded in web browsers • Examine Windows files and metadata
07	**Linux and Mac Forensics**	• Volatile and non-volatile data in Linux • Analyze filesystem images using the sleuth kit • Demonstrate memory forensics • Mac forensics concepts

Copyright EC-Council. All Rights Reserved.

08	**Network Forensics**	• Network forensics fundamentals • Event correlation concepts and types • Identify indicators of compromise (IoCs) from network logs • Investigate network traffic for suspicious activity
09	**Investigating Web Attacks**	• Web application forensics and web attacks • Understand IIS and Apache web server logs • Detect and investigate various attacks on web applications
10	**Dark Web Forensics**	• Dark web forensics investigation and how it works. • Tor browser forensics
11	**Investigating Email Crime**	• Email basics and how it can be used as evidence • Techniques and steps used in email crime investigation
12	**Malware Forensics**	• Malware, its components, and distribution methods • Malware forensics fundamentals and types of malware analysis • Perform static malware analysis and dynamic malware analysis • Conduct system and network behavior analysis

Tools You Will Learn and Use

Linux, Windows, Sleuth Kit, Wireshak, Splunk, TOR browser, ESEDatabaseView

» e-Learning resources including eBook and videos are available to all learners, free of charge.
» Unlock powerful add-ons, including cloud labs that provide intensive skills training and practice, official EC-Council certification exams, exam preps, and certification of completion.

Exam Information

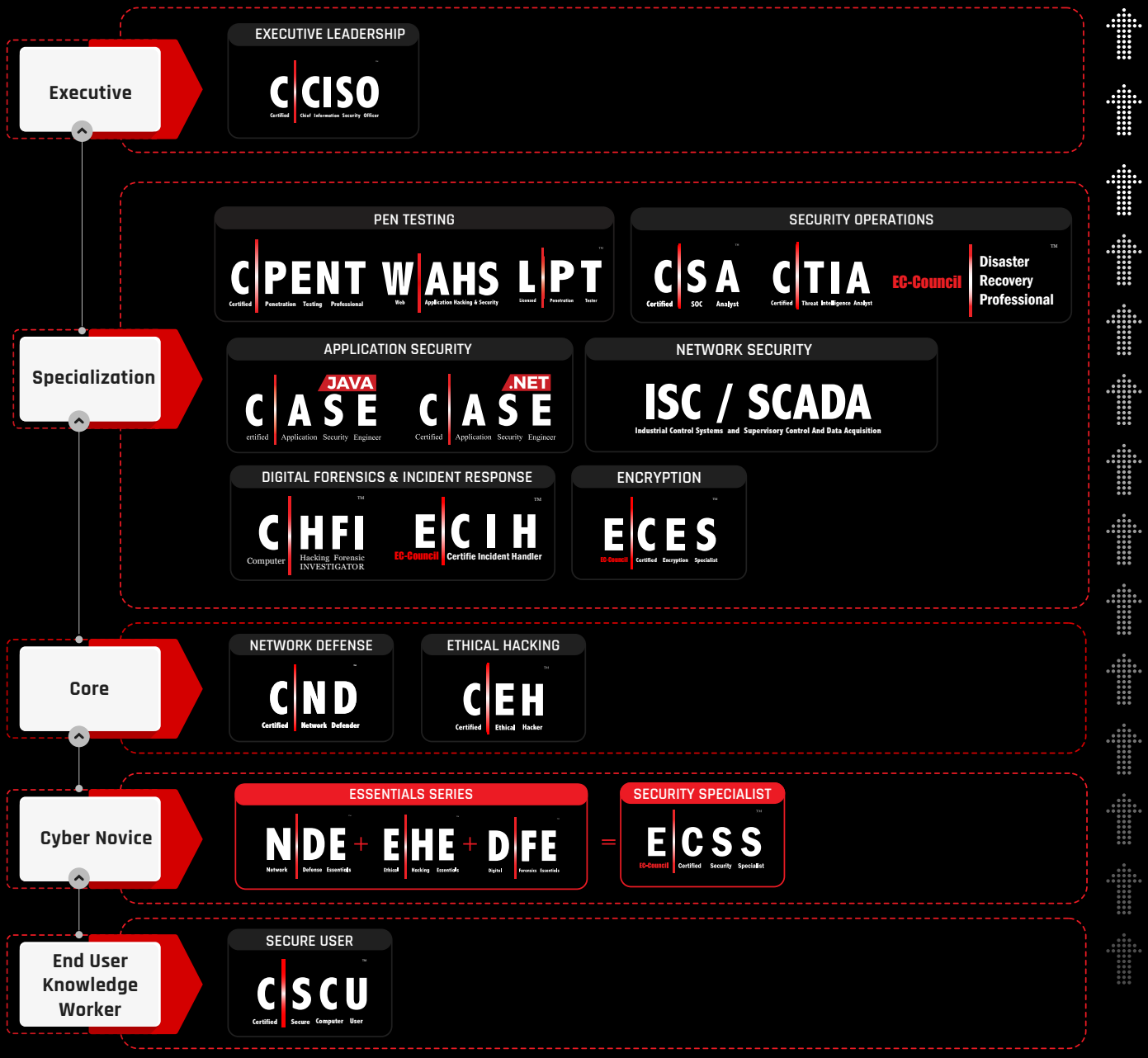
Certification : Digital Forensics Essentials
Exam Length : 2 Hours
Exam Format : MCQ
No. of Questions: 75

Get Certified

Copyright EC-Council. All Rights Reserved.

Your Pathway to a Promising Career in Cybersecurity

EC-Council certifications help professionals secure their careers in cybersecurity. These certifications have helped thousands of professionals further their careers in Fortune 500 companies. Students can choose between following the certification path or learning in-demand skills of their choice to become future cybersecurity professionals.



This is a suggested learning pathway only. Programs can be taken independently in any order depending on job role requirements and existing skill sets.

Copyright EC-Council. All Rights Reserved.

Kickstart a Career in Cybersecurity with EC-Council's

ESSENTIALS SERIES

Network Defense	Ethical Hacking	Digital Forensics
N|DE Network Defense Essentials	E|HE Ethical HackingEssentials	D|FE Digital Forensics Essentials

Register Now

About EC-Council

We Defined the Standards

EC-Council's sole purpose is to build and refine the cybersecurity profession globally. The organization helps individuals, organizations, educators, and governments address global workforce problems through the development and curation of world-class cybersecurity education programs and their corresponding certifications. EC-Council provides cybersecurity services to some of the largest businesses around the world. Trusted by 7 of the Fortune 10, 47 of the Fortune 100, the Department of Defense, the global intelligence community, NATO, and more than 2,000 of the best universities, colleges, and training companies, EC-Council's programs have proliferated through 140 countries and have set the bar in cybersecurity education. EC-Council is an ANSI 17024-accredited organization and has earned recognition from the DoD under Directive 8140/8570, in the UK by the GCHQ, CREST, and a variety of other authoritative bodies that influence the entire profession. Best known for the Certified Ethical Hacker program, we are dedicated to equipping more than 230,000 information-age soldiers with the knowledge, skills, and abilities required to fight and win against black hat adversaries.

EC-Council Accreditations & Recognition:

DoD
Department of Defense Directive 8570

ACE
American Council on Education

CNSS
Committee on National Security Systems

ANSI 17024
American National Standards Institute

US Army
US Army Credentialing Assistance

NCSC
National Cyber Security Centre

NICE Mapped
National Initiative for Cybersecurity Education

Copyright EC-Council. All Rights Reserved.

EC-Council

www.eccouncil.org

Copyright EC-Council. All Rights Reserved.