EC-Council

Building A Culture Of Security

D|SE

DevSecOps | Essentials

DevSecOps Essentials

Begin Your Cybersecurity Journey with Hands-On, Technical Foundational Skills in DevSecOps

No IT / Cybersecurity Experience Required

Video Lessons • Hands-on Labs • Capstone Project • Proctored Exam

EC-COUNCIL ESSENTIALS SERIES

Cybersecurity is a multifaceted industry with several specialized domains, each demanding unique skills. Choosing the right domain to start your cybersecurity career can get challenging.

That is why EC-Council brings the Essentials Series to help you develop the foundational skills that are right for you. This Essentials series is a hands-on, immersive program to help you learn solid technical foundational skills in various cybersecurity fields, ensuring that it is highly affordable. Specially designed for high school students, fresh graduates, career switchers, starters, and IT or technology teams with little or no experience in IT/cybersecurity, this series aims to help you start your career in cybersecurity. These courses will help you learn about several aspects of cybersecurity, allowing you to discover your areas of interest and develop foundational job-ready cybersecurity skills. The final module of lab capstone project test your skills to solve real-world challenges as a hacker or defender.

EC-Council DevSecOps Essentials

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. Put your newly acquired abilities to the test in an exhilarating Capstone project to develop the hands-on proficiencies essential for success in your cyber professional role. After completing this program, you will be prepared to move toward a career in secure application development.

DevSecOps Essentials Program Information

Course Outline

Module 1: Introduction to Application Development

Topics covered:
- History of Application Development
- Evolution of Application Development Methodologies
- Introduction to Application Architectures
- Introduction to the Application Development Lifecycle

Module 2: Application Development Concepts

Topics covered:
- Role of Risk Management in Secure Development
- Project Management Role in Application Development
- Application Testing and Quality Assurance
- Application Monitoring, Maintenance, and Support

Module 3: Application Security Fundamentals

Topics covered:
- What is Secure Application Development
- Need for Application Security
- Common Application Security Risks and Threats
- OWASP Top 10
- Application Security Techniques
- Secure Design Principles

Module 4: Introduction to Application Security Testing and Configuration

Topics covered:
- Threat Modeling
- Secure Coding
- Secure Code Review
- SAST and DAST Testing
- Secure Configurations
- Educating Developers

Module 5: Introduction to DevOps

Topics covered:

- Introduction to DevOps
- DevOps Principles
- DevOps Pipelines
- DevOps and Project Management

Module 6: Introduction to DevSecOps

Topics covered:

- Understanding DevSecOps
- DevOps vs. DevSecOps
- DevSecOps Principles
- DevSecOps Culture
- Shift-Left Security
- DevSecOps Pipelines
- Pillars of DevSecOps
- DevSecOps Benefits and Challenges

Module 7: Introduction to DevSecOps Management Tools

Topics covered:

- Project Management Tools
- Integrated Development Environment (IDE) Tools
- Source-Code Management Tools
- Build Tools
- Continuous Testing Tools

Module 8: Introduction to DevSecOps Code and CI/CD Tools

Topics covered:

- Continuous Integration Tools
- Infrastructure as Code Tools
- Configuration Management Tools
- Continuous Monitoring Tools

Module 9: Introduction to DevSecOps Pipelines

Topics covered:

- Role of DevSecOps in the CI/CD Pipeline
- DevSecOps Tools
- Embracing the DevSecOps Lifecycle
- DevSecOps Ecosystem
- Key Elements of the DevSecOps Pipeline
- Integrating Security into the DevOps Pipeline

Module 10: Introduction to DevSecOps CI/CD Testing and Assessments

Topics covered:

- Implementing Security into the CI/CD Pipeline and Security Controls
- Continuous Security in DevSecOps with Security as Code
- Continuous Application Testing for CI/CD Pipeline Security
- Application Assessments and Penetration Testing

Module 11: Implementing DevSecOps Testing & Threat Modeling

Topics covered:

- Integrating Security Threat Modeling in Plan Stage
- Integrating Secure Coding in the Code Stage
- Integrating SAST, DAST, and IAST in the Build and Test Stage
- Integrating RASP and VAPT in the Release and Deploy Stage

Module 12: Implementing DevSecOps Monitoring and Feedback

Topics covered:

- Integrating Infrastructure as Code (IaC)
- Integrating Configuration Orchestration
- Integrating security in the Operate and Monitor Stage
- Integrating Compliance as Code (CaC)
- Integrating Logging, Monitoring, and Alerting
- Integrating Continuous Feedback Loop

What Skills Will You Learn

- Learn the fundamentals of application development.
- Gain knowledge of application security.
- Understand DevOps and DevSecOps.
- Explore the DevSecOps toolchain.
- Gain insights into DevSecOps and CI/CD pipelines.
- Learn about implementing and using tools for DevSecOps in CI/CD pipelines.

Who Is It For

- School students, graduates, professionals, career starters and changers, IT / Technology / Cybersecurity teams with little or no work experience.
- Anyone who wants to start a career in cybersecurity, application security, and development and is interested in cloud technology.
- Any professional involved in developing, testing, and deploying applications to production environments, including on-premises, public cloud, and hybrid environments.
- This program is also beneficial for application developers, risk managers, project managers, application administrators, administrators, engineers, and architects.

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.

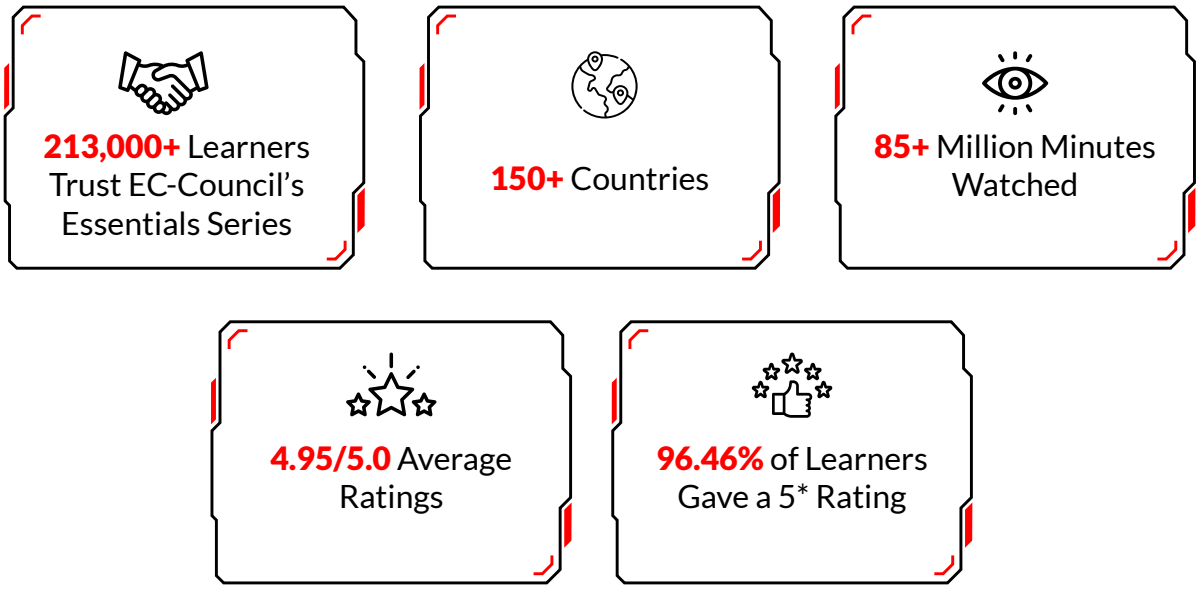
Exam Details:

- Exam Code: 112-55
- Number of Questions: 75
- Duration: 2 hours
- Test Format: Multiple Choice

Key Features

- Engage in 7 practical lab exercises to develop the required skills to manage and monitor security throughout the application development lifecycle.
- Access to 7+ hours of premium self-paced video training.
- 900+ pages of ecourseware.
- Capstone Projects with Real-World Challenges
- Get year-long access to courseware and labs.
- Receive a proctored exam voucher with one-year validity.
- Learn about secure application development with easy-to-follow modules.
- Increase your value in the job market to advance your career.
- Earn a globally recognized EC-Council certification.

Why EC-Council's Essentials Series is the Most Popular and Fastest Growing Beginner Level Training Program for Career Starters and Career Changers



Why Do Professionals, Students, Career Starters and Changers Worldwide Choose the EC-Council's Essentials Certification?

Gene (USA)
Strong Cybersecurity Foundation
★★★★★

It has given me a solid foundation in the basics of cybersecurity. I now have a better understanding of the different types of cyberattacks, the tools and techniques that attackers use, and the ways to protect myself and my organization from these attacks.

Taylor Cooper (USA)
Career Advancement through Ethical Hacking
★★★★★

This has helped me enhance my knowledge and skills in tech. I will be able to showcase my knowledge by certifying myself as an ethical hacker and adding it to my resume, which will allow me to advance my career and opt for higher-paying roles.

Deeptankshu (USA)
Top Notched Cyber Investigation Skills
★★★★★

It helped by teaching me how to collect data and evidence to solve crimes and prevent wrongdoers in the Cyber realm. As a Security and Intelligence major, I want to be well-versed in cyber and other realms.

Samuel Tetteh (USA)
Strong Foundation for Digital Forensics
★★★★★

After completing this course, I had the foundation I needed. It assisted me in completing my MS Cybersecurity course in digital forensics, which actually expanded my knowledge even further. This foundational course is perfect for a start in Digital Forensics.

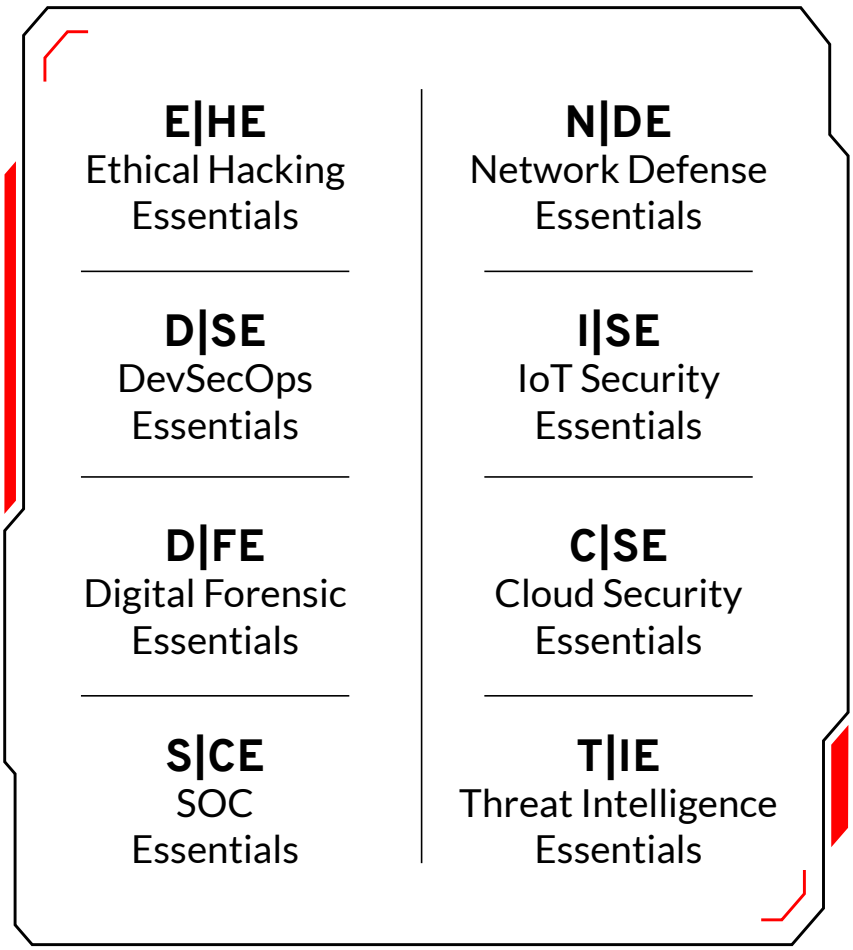
Brian (USA)
Rebuilding Network Defense Knowledge
★★★★★

This course helped rebuild my baseline knowledge of network defense, which I required before progressing toward more advanced studies in the field.

Nicolas Ntibaziyaremye (USA)
Practical Learning for Career Growth
★★★★★

The course is project-based. This allows me to apply what I learn in the lectures to real-world problems. I have learned a lot from this course, and I am confident that it will help me in my career.

Learn Foundational Cybersecurity Skills with EC-Council's 8 Essential Series



About EC-Council

EC-Council's sole purpose is to build and refine the cybersecurity profession globally. We help individuals, organizations, educators, and governments address global workforce problems by developing and curating world-class cybersecurity education programs and their corresponding certifications. We also provide cybersecurity services to some of the largest businesses globally. Trusted by 7 of the Fortune 10, 47 of the Fortune 100, the Department of Defence, Intelligence Community, NATO, and over 2,000 of the best Universities, Colleges, and Training Companies, our programs have proliferated through over 140 countries. They have set the bar in cybersecurity education. Best known for the Certified Ethical Hacker programs, we are dedicated to equipping over 2,30,000 information age soldiers with the knowledge, skills, and abilities required to fight and win against the black hat adversaries. EC-Council builds individual and team/organization cyber capabilities through the Certified Ethical Hacker Program, followed by a variety of other cyber programs, including Certified Secure Computer User, Computer Hacking Forensic Investigator, Certified Security Analyst, Certified Network Defender, Certified SOC Analyst, Certified Threat Intelligence Analyst, Certified Incident Handler, as well as the Certified Chief Information Security Officer.

We are an ANAB 17024 accredited organization and have earned recognition by the DoD under Directive 8140/8570 in the UK by the GCHQ, CREST, and various other authoritative bodies that influence the entire profession.

Founded in 2001, EC-Council employs over 400 individuals worldwide with ten global offices in the USA, UK, Malaysia, Singapore, India, and Indonesia. Its US offices are in Albuquerque, NM, and Tampa, FL.

Learn more at www.eccouncil.org

DevSecOps Essentials

www.eccouncil.org