



EC-Council

Building A Culture Of Security



SOC Essentials

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

No IT / Cybersecurity Experience Required

Video Lessons • Hands-on Labs • CTF Challenges • Proctored Exam



EC-COUNCIL ESSENTIALS SERIES

With the growing demand for security measures in every industry, companies need skilled cybersecurity professionals. EC-Council's Essentials Series aims to create a secure digital landscape for every industry by providing candidates with hands-on, immersive programs. By helping the students acquire solid technical foundational skills and preparing them for entry-level roles in several cybersecurity areas at an affordable range, EC-Council aims to meet the industries' demand for cybersecurity professionals. Gain skills for your first CTF competition with this Essentials Series Course. The final module of lab capstone project features a simulated CTF to test your skills in a controlled environment. Use live virtual machines, real software, and networks to solve real-world challenges as a hacker or defender.

The EC-Councils Essentials Series is designed to cater to high school students, fresh graduates, career switchers, starters, and IT/technology teams who have little or no experience in IT/cybersecurity. Candidates can choose to enroll in any of the eight courses offered by the Essentials Series - Ethical Hacking, Network Defense, Digital Forensics, Cloud Security, IoT Security, SOC, Threat Intelligence, and DevSecOps. Upon completion of courseware and proctored exams, candidates will get globally recognized certification and a chance to start their careers in cybersecurity.

EC-Council SOC Essentials (S|CE)

The SOC Essentials (S|CE) Series is designed for security professionals and freshers to enhance their skills and knowledge about essential security technologies. Focused on honing candidates with in-demand skills, the S|CE course will provide insights into security operations frameworks and related technologies that are required to master the foundational concepts of SOC.

In this program students will learn the basics of computer networks, TCP/IP model, OSI model, Windows/Linux/Unix security concepts, threats, vulnerabilities, and attack concepts in terms of cyber threats. Further, students will go through the complete SOC architecture: its importance, workflow, and processes of SOC. Students will learn more advanced architectural concepts like SIEM architecture and deployment models, and data sources that are commonly used. Learn everything about Log Management like; dashboards, reports, and incident escalation in terms of dealing with real positive and false alerts. This course will also teach you sources, types, and lifecycle of threat intelligence and give an introduction to threat hunting as well while diving deep into incident response lifecycle processes. Put your newly acquired abilities to the test with an exhilarating Capture the Flag (CTF) Exercise seamlessly integrated



in our Capstone project. This CTF is seamlessly integrated by live virtual machines, genuine software, and real networks, all delivered within a secure and regulated sandbox environment. With these exclusive hands-on, human-versus-machine CTF challenges you will develop the hands-on proficiencies essential for success in your cyber professional role. If you are looking to learn advanced SOC certification, click here: [Certified SOC Analyst \(C|SA\)](#)



SOC Essentials Program Information

Course Outline



Module 1: Computer Network and Security Fundamentals

Topics covered:

- TCP/IP Model
- OSI Model
- Types of a Network
- Network Topologies
- Network Hardware Components
- TCP/IP Protocol Suite
- Network Security Controls
- Network Security Devices
- Windows Security
- Unix/Linux Security
- Web Application Fundamentals
- Information Security Standards, Laws, and Acts



Module 2: Fundamentals of Cyber Threats

Topics covered:

- Cyber Threats
 - Intent-Motive-Goal
 - Tactics-Techniques-Procedures
 - Opportunity-Vulnerability-Weakness
 - Vulnerability
 - Threats & Attacks
 - Example of Attacks
 - Network-Based Attacks
 - Application-Based Attacks
 - Host-Based Attacks
 - Insider Attacks
 - Malware
 - Phishing and Social Engineering
-



Module 3: Introduction to Security Operations Center

Topics covered:

- What is a Security Operations Center (SOC)
 - Importance of SOC
 - SOC Team Roles and Responsibilities
 - SOC KPI
 - SOC Metrics
 - SOC Maturity Models
 - SOC Workflow and Processes
 - Challenges in Operating a SOC
-



Module 4: SOC Components and Architecture

Topics covered:

- | | |
|---|-------------------------|
| • Key Components of a SOC | • Data Sources in SIEM |
| • People in SOC | • SIEM Logs |
| • Process in SOC | • Network in SIEM |
| • Technologies in SOC | • Endpoint Data in SIEM |
| • SOC Architecture and Infrastructure | |
| • Different Types of SOC's and Their Purposes | |
| • Introduction to SIEM | |
| • SIEM Architecture | |
| • SIEM Deployment Models | |



Module 5: Introduction to Log Management

Topics covered:

- Incident
 - Event
 - Log
 - Typical Log Sources
 - Need of Log
 - Typical Log Format
 - Local Log Management
 - Centralized Log Management
 - Logging Best Practices
 - Logging/Log Management Tools
-



Module 6: Incident Detection and Analysis

Topics covered:

- SIEM Use Case Development
 - Security Monitoring and Analysis
 - Correlation Rules
 - Dashboards
 - Reports
 - Alerting
 - Triaging Alerts
 - Dealing with False Positives Alerts
 - Incident Escalation
 - Communication Paths
 - Ticketing Systems
-



Module 7: Threat Intelligence and Hunting

Topics covered:

- | | |
|---|--|
| • Introduction to Threat Intelligence | • Introduction to Threat Hunting |
| • Threat Intelligence Sources | • Threat Hunting Techniques |
| • Threat Intelligence Types | • Threat Hunting Methodologies |
| • Threat Intelligence Lifecycle | • Role of Threat Hunting in SOC Operations |
| • Role of Threat Intelligence in SOC Operations | • Leveraging Threat Intelligence for Hunting |
| • Threat Intelligence Feeds | • Threat Hunting Tools |
| • Threat Intelligence Sharing and Collaboration | |
| • Threat Intelligence Tools/Platforms | |



Module 8: Incident Response and Handling

Topics covered:

- Incident Handling Process
 - Incident Classification and Prioritization
 - Incident Response Lifecycle
 - Preparation
 - Identification
 - Containment
 - Eradication
 - Recovery
 - Post-incident Analysis and Reporting
-

What You'll Learn

- Learn the basics of computer networks
 - Dive deep into the cyber threat concepts like threats, vulnerabilities, and attacks.
 - Gain insights into the Security Operations Center (SOC) architecture and learn the importance, workflow, and processes of SOC.
 - Understand advanced architectural concepts like SIEM architecture and deployment models.
 - Learn what log management is and its key parts, like events, logs, and incidents.
 - Learn how you can perform centralized management of logs.
 - Gain knowledge on dashboards, reports, and incident escalation in terms of dealing with real positive and false alerts.
 - Discover the sources, types, and lifecycle of threat intelligence and get introduced to threat hunting.
 - Deep dive into the Incident response lifecycle.
-

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 and is interested in SOC.
- This course is also helpful for IT professionals, SOC analysts, system security professionals, security engineers, threat management professionals, incident response teams, security administrators, vulnerability management professionals, and any cybersecurity professional.

Training and 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:

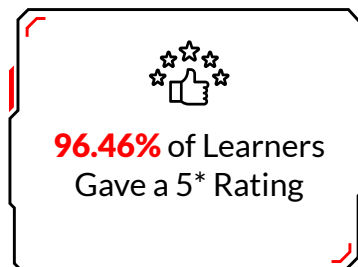
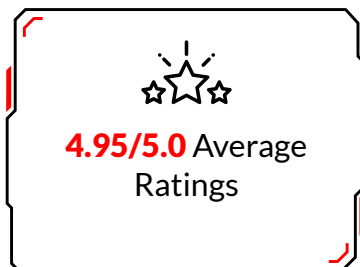
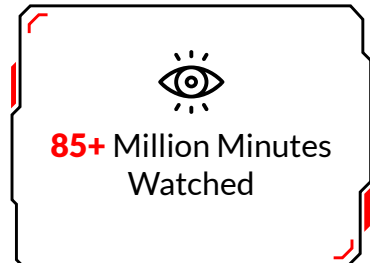
- Exam Code: 112-56
 - Number of Questions: 75
 - Duration: 2 hours
 - Test Format: Multiple Choice
-

Key Features

- Engage in 6 lab practical exercises in every module to develop skills and understand how to secure cloud solutions.
- Get access to 10+ hours of premium self-paced video training.
- 900+ pages of ecourseware.
- Capstone Projects with Real-World CTF Challenges
- Gain year-long access to courseware and 6-month access to labs.
- Receive a proctored exam voucher with one-year validity.
- Increase your value in the job market to advance your career.
- Earn a globally recognized EC-Council certification.
- Learn about network fundamentals, Windows and Unix/Linux Security, exploits, SOC architecture, SIEM development, and threat hunting.
- Understand how to deal with alerts.



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 give me an opportunity to advance in 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 the Cyber realm as well as 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 expanded my knowledge even further. This foundation 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)

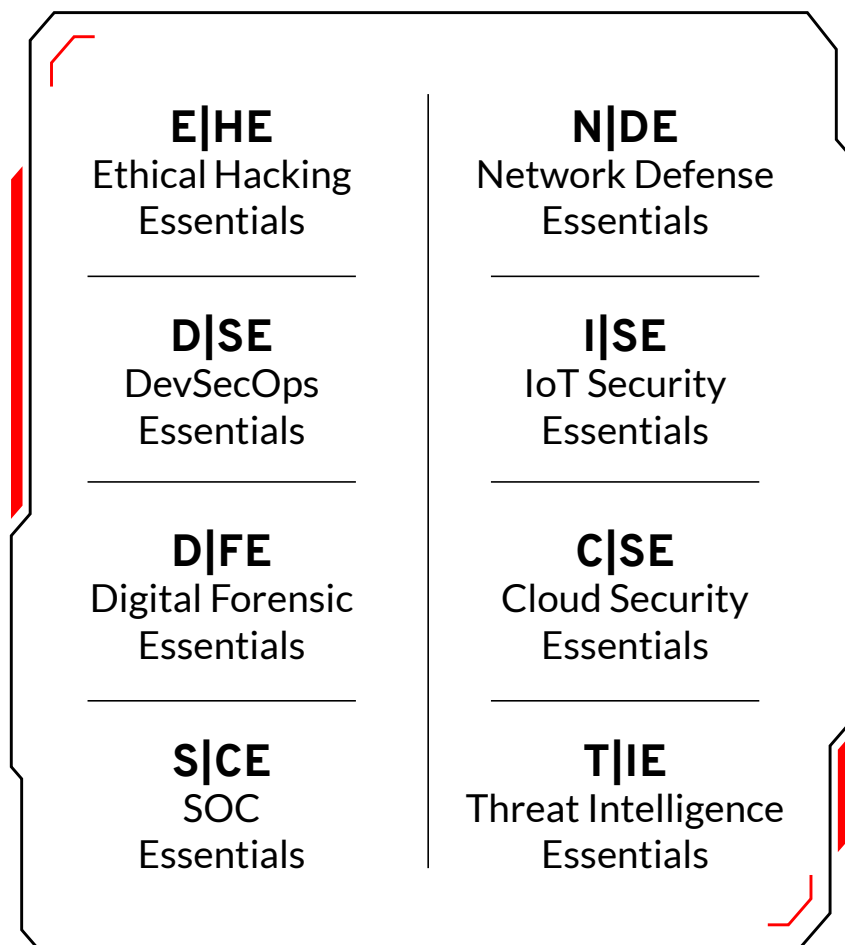
Practical Learning for Career Growth.

★★★★★

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



SOC Essentials

www.eccouncil.org