



Cloud Security Essentials

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

No IT / Cybersecurity Experience Required

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

EC-COUNCIL ESSENTIALS SERIES

The complexity of cyberthreats is expanding in breadth and scope. Every industry needs cybersecurity professionals to protect their systems and organizations from evolving cyber threats but the industry faces a massive skills gap. To address this talent shortage, EC-Council developed the Essentials Series, designed for individuals to find their cybersecurity niche, develop the required job-ready skills, and meet the growing demand for skilled professionals. The Essentials Series courses offer an immersive, hands-on learning experience at an affordable cost. They equip candidates with solid technical foundational skills across diverse cybersecurity fields, preparing them for entry-level roles. The final module of lab capstone project test your skills to solve real-world challenges as a hacker or defender.

Start Your Cybersecurity Journey with the Essentials Series!

EC-Council's Cloud Security Essentials

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. Put your newly acquired abilities to the test in our exhilarating Capstone project to develop the hands-on proficiencies essential for success in your cyber professional role. 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.





Cloud Security Essentials Program Information

Course Outline



Module 1: Cloud Computing and Security Fundamentals

This module will introduce you to the course and provide foundational information about cloud infrastructure and security.

Student Objectives:

1. Students will learn the cloud principles and terminology essential for talking to customers and cloud engineers.
2. Students will be introduced to key cloud security concepts and threats and attacks that are common in cloud environments.
3. After completing this module, students will have these foundational cloud and cloud security principles, as well as the key understanding of design and architecture necessary for the rest of the course.

Topics covered:

- Cloud Computing Types and Service Models
 - Cloud Security Challenges and Concerns
 - Cloud and Security Shared Responsibility
 - Cloud Service Models (IaaS, PaaS, and SaaS)
 - Evaluating Cloud Service Providers
 - Cloud Security Benefits
 - Threats and Attacks in Cloud Environments
 - Cloud Security Design Principles
 - Cloud Security Architecture
-



Module 2: Identity and Access Management (IAM) in the Cloud

This module will focus on the protection of identity and access management. This will include how to protect users and assign proper permissions.

Labs: Assign roles and enforce MFA in AWS, and implement roles and enforce MFA with conditional access policies in Azure.

Modules Objectives:

1. Students will learn identity and access principles and concepts to protect the perimeter of the cloud.
2. Students will understand the key concepts for protecting identity and access.
3. After completing this module, students will be able to comprehend the importance of identity and access management, as well as the concepts for monitoring and managing users and identities.



Topics covered:

- IAM Fundamentals
 - Principal Roles of IAM in the Cloud
 - Role-Based Access Control (RBAC)
 - Identity Federation
 - Single Sign-on (SSO) and Self-Service Password Reset (SSPR)
 - Multi-Factor Authentication (MFA)
 - Principle of Least Privilege
 - IAM Auditing and Monitoring
-



Module 3: Data Protection and Encryption in the Cloud

This module will focus on the protection of identity and access management. This will include how to protect users and assign proper permissions.

Labs: Set up KMS in AWS, set up Key Vault in Azure, and create DLP policies in M365.

Module Objectives:

1. Students will learn the key concepts for protecting data in the cloud.
2. Students will grasp the importance of understanding the data the company stores and avoiding exposure to sensitive data.
3. After completing this module, students will be able to explore the concepts and techniques for encrypting and protecting data within a cloud environment.

Topics covered:

- Data Classification and Lifecycle
 - Encryption Techniques (at rest, in trANABt)
 - Customer vs. Cloud Provider Managed Keys
 - Key Management in the Cloud
 - Data Loss Prevention (DLP)
 - Backup and Disaster Recovery Strategies
-



Module 4: Network Security in Cloud Environments

This module will teach you how to securely architect your network to protect against unauthorized access and detect potential network attacks.

Labs: Create a VPC and configure NACL and NSG in AWS, as well as create a VNET and configure an NSG in Azure.

Module Objectives:

1. Students will learn the concepts of networking in the cloud and how to architect public and private network communication.
2. Students will be introduced to cloud connections within cloud, hybrid, and multi-cloud networks.
3. After completing this module, students will have a foundational understanding of network connectivity and communications within a cloud and hybrid architecture and how to secure these connections.



Topics covered:

- Cloud Network Fundamentals
 - Virtual Private Clouds (VPCs)
 - Network Isolation and Segmentation
 - Network Access Control Lists (NACLs)
 - Security Groups
 - Firewalls and Intrusion Detection
-



Module 5: Application Security in Cloud Environments

This module will show you how to secure applications, web access, and databases in cloud environments.

Labs: Create an application gateway with WAF and create a WAF in AWS.

Student Objectives:

1. Students will learn the fundamental security concepts for protecting applications within the cloud.
2. Students will be introduced to application threats and vulnerabilities and how to architect the protection of these applications within development and the network.
3. After completing this module, students will understand fundamental application development concepts and how to provide security within the development process. They will also understand the network and code security techniques that will secure applications.

Topics covered:

- Secure Software Development Lifecycle (SDLC) in the Cloud
 - Web Application Firewall (WAF) in Cloud Environments
 - Web Application Security and OWASP Top Ten
 - Security by Design Principles for Cloud Applications
 - Secure Coding Practices
 - API Security and Integration Best Practices
 - Serverless Security Considerations
 - Container Security (Docker, Kubernetes)
-



Module 6: Cloud Security Monitoring and Incident Response

This module will introduce you to the foundations of security operations, including logging activity and events, identifying threats and intrusions, and responding to incidents.

Labs: Configure Azure Sentinel, configure workload protection for Microsoft Defender for the Cloud, configure Guard Duty on AWS, and configure Security Hub on AWS.

Module Objectives:

1. Students will learn the importance of logging and monitoring activity within the cloud environment as a proactive security strategy.
2. Students will be introduced to logging and monitoring solutions and how automation can be used to identify and respond to threats.
3. After completing this module, students will understand the foundational concepts and techniques for security operations.



Topics covered:

- Cloud Logging
 - Cloud Security Monitoring
 - Intrusion Detection and Prevention Systems (IDS/IPS) in the Cloud
 - SIEM and SOAR
 - Real-time Monitoring and Alerting
 - Log Management and Analysis in the Cloud
 - Cloud-native Monitoring Solutions
 - Continuous Security Monitoring Strategies
 - Cloud Security Monitoring Best Practices
 - Incident Response in the Cloud
 - Forensics and Investigation in the Cloud
-



Module 7: Cloud Security Risk Assessment and Management

This module will discuss the process of risk analysis, assessment, and management.

Module Objectives:

1. Students will learn about risk management frameworks and strategies for risk assessments.
2. Students will be introduced to how to assess risk and techniques for risk analysis.
3. After completing this module, students will understand the importance of a risk management framework and determining a company's risk and risk tolerance through risk analysis techniques.

Topics covered:

- Identifying Cloud Security Risks
 - Risk Assessment Frameworks for Cloud Environments
 - Cloud Security Controls and Countermeasures
 - Threat Modeling and Vulnerability Assessment in Cloud Environments
 - Quantitative vs. Qualitative Risk Assessment Approaches
 - Cloud Risk Treatment, Response, and Mitigation
-



Module 8: Cloud Compliance and Governance

This module will discuss the various regulatory and legal standards that you may need to adhere to within your company jurisdiction and how to maintain compliance within the cloud infrastructure.

Labs: Configure regulatory compliance in Azure and configure AWS Config for CIS standards.

Module Objectives:

1. Students will learn about the primary industry, regulatory, and national standards that govern compliance for companies.
2. Students will be introduced to cloud capabilities and solutions for monitoring and managing compliance within cloud and hybrid environments.
3. After completing this module, students will understand the role of regulations and standards on compliance within cloud and hybrid architectures.



Topics covered:

- Regulatory and Industry Compliance (e.g., GDPR, and HIPAA)
- Cloud Security Standards (e.g., ISO 27001, and NIST)
- Cloud Security Governance and Risk Management
- Auditing and Monitoring Cloud Resources
- Cloud Security Assessment and Penetration Testing

What Skills Will You Learn

- Learn the fundamentals of cloud computing and security.
 - Explore identity and access management in the cloud.
 - Learn about data protection and encryption in the cloud.
 - Gain knowledge of network security in cloud environments.
 - Dive deep into application security in cloud environments.
 - Gain insights on cloud security monitoring and incident response.
 - Explore cloud security risk assessment and management.
 - Understand the basics of cloud compliance and governance.
-

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, cloud security, or network security and is interested in cloud technology.
- Professionals securing public, private, and hybrid cloud infrastructures, identities, data, and applications.
- IT professionals, system administrators, cloud administrators, cybersecurity operations and 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:

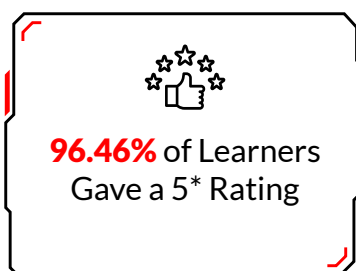
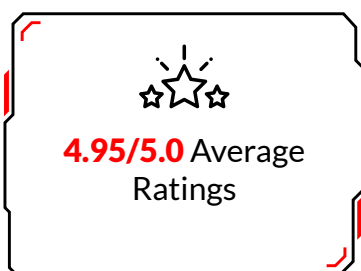
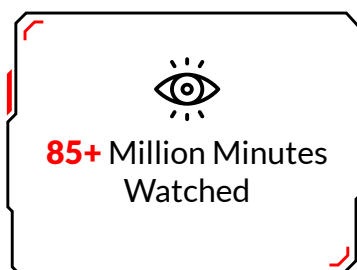
- Exam Code: 112-54
- Number of Questions: 75
- Duration: 2 hours
- Test Format: Multiple Choice

Key Features

- Engage in 6 lab practical exercises in every module to develop skills and gain an understanding of securing cloud solutions.
- Get access to 10+ hours of premium self-paced video training.
- 900+ pages of ecourseware
- Capstone Projects with Real-World Challenges
- Gain a year-long access to courseware and 6-month access to labs.
- Acquire a proctored exam voucher with one-year validity.
- Learn about cloud adoption to cloud security with easy-to-follow modules.
- Enhance your value in the job market to advance your career.
- Get globally recognized EC-Council's 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 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)

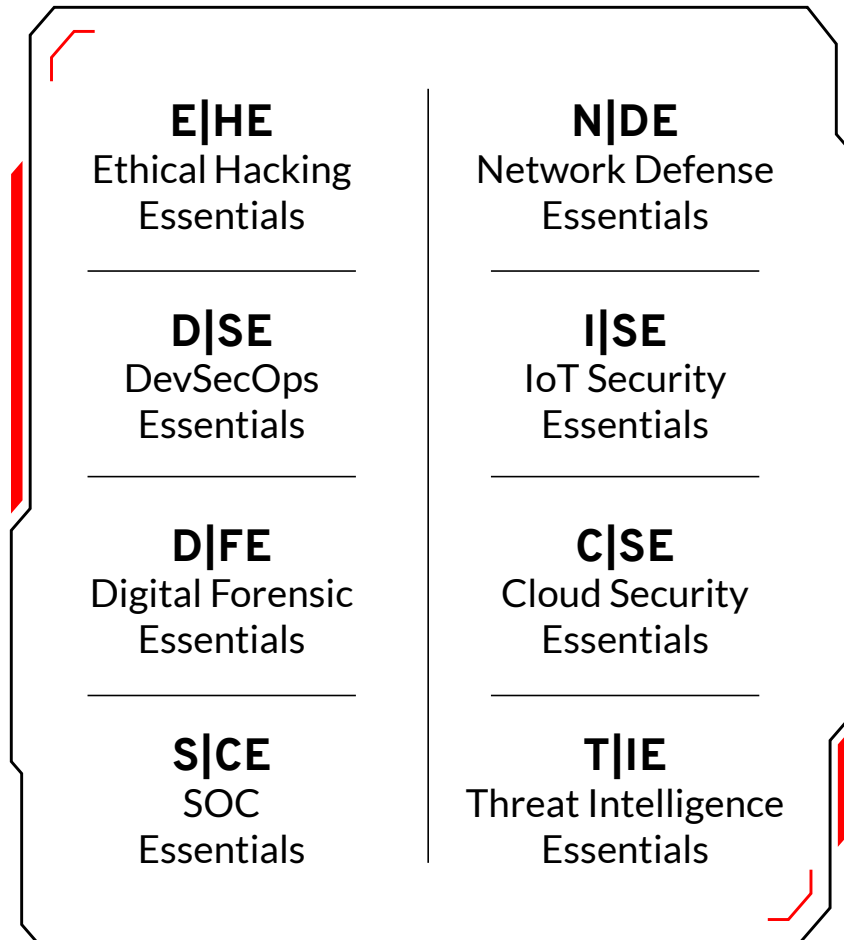
Practical Learning for Career Growth.

★★★★★

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



Cloud Security Essentials

www.eccouncil.org