



CYBER SECURITY

GET HANDS-ON TRAINING

Prepare yourself for certification to skill up, confidently mitigate threats, and effectively protect your organization.



C|EH is divided into 20 modules and delivered through a carefully curated training plan that typically spans across 5 days. As you progress through your training, each module offers extensive hands-on lab components that allow you to practice the techniques and procedures taught in the program in real-time on live machines.



EC-Council's Certified Hacking Forensic Investigator (CHFI) is the only comprehensive ANSI accredited, lab-focused program in the market that gives organizations vendor-neutral training in digital forensics. CHFI provides its attendees with a firm grasp of digital forensics, presenting a detailed and methodological approach to digital forensics and evidence analysis that also pivots around Dark Web, IoT, and Cloud Forensics. The tools and techniques covered in this program will prepare the learner for conducting digital investigations using ground-breaking digital forensics technologies.



The ECSA pentest program takes the tools and techniques you learned in the Certified Ethical Hacker course (CEH) and enhances your ability into full exploitation by teaching you how to apply the skills learned in the CEH by utilizing EC-Council's published penetration testing methodology. It focuses on pentesting methodology with an emphasis on hands-on learning.



CYBER SECURITY

GET HANDS-ON TRAINING

Prepare yourself for certification to skill up, confidently mitigate threats, and effectively protect your organization.



A globally recognized standard for appraising an IT auditor's knowledge, expertise, and skill in assessing vulnerabilities and instituting IT controls in an enterprise environment.

This certification is issued by ISACA to people in charge of ensuring an organization's IT and business systems are monitored, managed, and protected. It is designed for IT auditors, audit managers, consultants, and security professionals.



The certification created by the International Information Systems Security Certification Consortium (ISC) to ensure professionals in computer security have standardized knowledge of the field. Earning a Certified Information Systems Security Professional certificate can help you have a successful career as a computer security professional. It certifies security professionals in ten different areas of access control systems and methodology, business continuity planning and disaster recovery planning, physical security, operations, security, management practices, telecommunications, and networking security.