INFORMATION SECURITY AND CYBERSECURITY ACADEMY

EC-Council

Hackers are here. Where are you?

SCORPIONSHIELD

ACADEMY

EC-Council Accredited Training Center

TRAINING EC-Council PARTNER

C|HFI TRAINED

C|CISO TRAINED

C|EH TRAINED

C|HFI CERTIFIED

C|CISO CERTIFIED

C|EH CERTIFIED

C|EH MASTER CERTIFIED

2020

INFORMATION SECURITY & CYBERSECURITY ACADEMY
FULL EC-COUNCIL CERTIFICATION BOARD (C|CISO + C|EH + C|HFI)

ABOUT EC-COUNCIL AND SCORPIONSHIELD

With years of experience, EC-COUNCIL is today the most reputed Cybersecurity training Organization in the World. It has the capabilities and expertise to take your cybersecurity training to the next level.

At SCORPIONSHIELD, we combine EC-COUNCIL insights and skills to transform your processes and strategies, but also your security staff training, and in turn, your company. We're proud to help shape and improve how our client's structure and manage their information security. SCORPIONSHIELD is striving on a close partnership with the EC-COUNCIL, to provide a local academy in information security, for its own customers and consultants, for all of them to be constantly upgraded in the necessary skills needed, to excel on our customer's projects. Also, the Academy is opened for the market. We are working towards to be an EC-COUNCIL Accredited Training Center, and our trainers are certified instructors from the EC-COUNCIL.

SCORPIONSHIELD Cybersecurity is an EC-COUNCIL Accredited Training Center, and an On-Demand Service for Cybersecurity professionals: Certified Chief Information Security Officers, Certified Ethical Hackers, Certified Hacking Forensic Investigators, and Data Protection Officers.

EC-Council
Accredited
Training Center
EC-Council C|HFI TRAINED
EC-Council C|CISO TRAINED
EC-Council C|EH TRAINED
EC-Council C|HFI CERTIFIED
EC-Council C|CISO CERTIFIED
EC-Council C|EH CERTIFIED
EC-Council C|EH MASTER CERTIFIED

Accredited Training Center

Cert ID EATC14110

Scorpionshield

EC-Council recognizes this organization as an Accredited Training Center meeting strict standards of excellence for delivering instructor-led training. The EC-Council ATC network is the premier channel for delivering high-quality EC-Council information security related training to businesses and industry professionals.

Issue Date: **October 15, 2019** Expiry Date: **October 30, 2020**

EC-Council

Sanjay Bavisi, President

TIMELINE

The SCORPIONSHIELD Academy Program comprises 6 months in part-time, 4 weeks per month, 2 sessions per week, post-working hours, from 19h30 to 22h30, 3 hours per session. Hence, equivalents to 144 hours, which represents 40 hours per specific type of training to grants along with the 3 vouchers included, for attaining the 3 certifications - CEH, CHFI and CCISO. Albeit, there are extra 24 hours for the CEH Practical, which enables the additional desired certificate of CEH MASTER.

EC-Council Certified Chief Information Security Officer v3

DESCRIPTION

EC-Council's CCISO Program has certified leading information security professionals around the world. The CCISO Advisory Board contributed by forming the foundation of the program and outlining the content that would be covered by the exam, body of knowledge and training. Some members of the Board contributed as authors, others as exam writers, others as quality assurance checks and still others as trainers. Each segment of the program was developed with the aspiring CISO in mind and looks to transfer the knowledge of seasoned professionals to the next generation in the areas that are most critical in the development and maintenance of a successful information security program. The Certified CISO (CCISO) program is the first of its kind training and certification program aimed at producing top-level information security executives. The CCISO does not focus solely on technical knowledge but on the application of information security management principles from an executive management point of view. The program was developed by sitting CISOs for current and aspiring CISOs. In order to sit for the CCISO exam and earn the certification, candidates must meet the basic CCISO requirements. Candidates who do not yet meet the CCISO requirements but are interested in information security management can pursue the EC-Council Information Security Management (EISM) certification

C|CISO
Certified Chief Information Security Officer
Join the Next Generation of Information Security Leaders

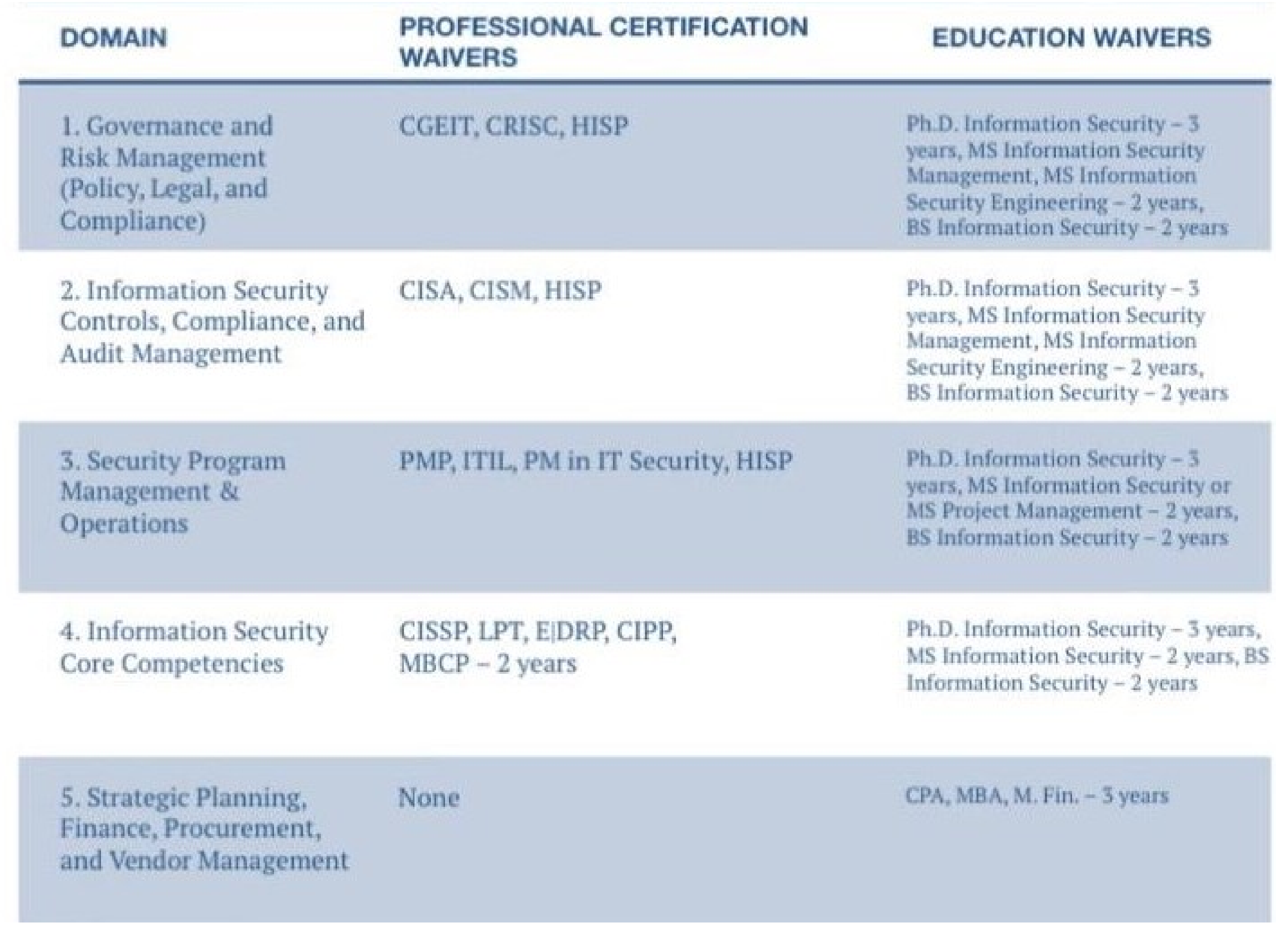
TOPICS

- Governance
- Is Risk, Controls & Auditing Management
- Information Security Leadership – Projects & Operations
- ISCoreCompetencies
- Strategic Planning & Finance

TARGET AUDIENCE AND PRE-REQUISITES

5 years' experience on 3 out of 5 Domains, or equivalent Cert Waivers / Post Grads (MS / PhD)

WAIVERS PER DOMAIN



DOMAIN	PROFESSIONAL CERTIFICATION WAIVERS	EDUCATION WAIVERS
1. Governance and Risk Management (Policy, Legal, and Compliance)	CGEIT, CRISC, HISP	Ph.D. Information Security – 3 years, MS Information Security Management, MS Information Security Engineering – 2 years, BS Information Security – 2 years
2. Information Security Controls, Compliance, and Audit Management	CISA, CISM, HISP	Ph.D. Information Security – 3 years, MS Information Security Management, MS Information Security Engineering – 2 years, BS Information Security – 2 years
3. Security Program Management & Operations	PMP, ITIL, PM in IT Security, HISP	Ph.D. Information Security – 3 years, MS Information Security or MS Project Management – 2 years, BS Information Security – 2 years
4. Information Security Core Competencies	CISSP, LPT, E|DRP, CIPP, MBCP – 2 years	Ph.D. Information Security – 3 years, MS Information Security – 2 years, BS Information Security – 2 years
5. Strategic Planning, Finance, Procurement, and Vendor Management	None	CPA, MBA, M. Fin. – 3 years

DURATION

40 hours

EXAM

Certified Chief Information Security Officer (ANSI)

Number of Questions: 150

Duration: 2,5 hours

Test Format: Multiple Choice

Exam Prefix: 712-50

OUTLINE

I. Governance

A. Information program security management
B. Information security governance program
C. Regulatory and legal compliance
D. Risk management

II. Is Risk, Controls & Auditing Management

A. Design, Deploy and Manage Security Controls
B. Security Control Types and Objectives
C. Implement Control Assurance Frameworks Audit Management

III. Information Security Leadership – Projects & Operations

A. The role of the CISO
B. Information security projects
C. Integration of security requirements into other operational processes (change management, version control, disaster recovery, etc.)

IV. ISCoreCompetencies

A. Access controls
B. Physical security
C. Disaster recovery and business continuity planning
D. Network security
E. Threat and vulnerability management
F. Application security
G. Encryption
H. Vulnerability assessments and penetration testing
I. Computer forensics and incident response

V. Strategic Planning & Finance

A. Security Strategic Planning
B. Alignment with Business Goals and Risk Tolerance
C. Security emerging trends
D. Key Performance Indicators (KPI)
E. Financial Planning
F. Development of business cases for security
G. Analyzing, forecasting, and developing a capital expense budget
H. Analyzing, forecasting, and developing an operating expense budget
I. Return on investment (ROI) and cost-benefit analysis
J. Vendor management
K. Integrating security requirements into the contractual agreement and procurement process
L. Taken together, these five domains translate to a thoroughly knowledgeable, competent executive information security practitioner

EC-Council Certified Ethical Hacker v10

DESCRIPTION

The world's most advanced ethical hacking course with 20 of the most current security domains an ethical hacker will want to know when planning to beef up the information security posture of their organization. In 20 comprehensive modules, the course covers over 270 attack technologies, commonly used by hackers. Our security experts have designed over 140 labs which mimic real time scenarios in the course to help you "live" through an attack as if it were real and provide you with access to over 2200 commonly used hacking tools to immerse you into the hacker world. The goal of this course is to help you master an ethical hacking methodology that can be used in a penetration testing or ethical hacking situation.

TARGET AUDIENCE

Ethical hackers, System and Network Administrators, Engineers, Web-managers, Auditors, Security Professionals.

DURATION

40 hours

EXAM

Certified Ethical Hacker (ANSI)

Number of Questions: 125

Duration: 4 hours

Test Format: Multiple Choice

Exam Prefix: 312-50

OUTLINE

Module 01: Introduction to Ethical Hacking	**Module 12: Evading IDS, Firewalls, and Honeypots**
Module 02: Footprinting and Reconnaissance	**Module 13: Hacking Web Servers**
Module 03: Scanning Networks	**Module 14: Hacking Web Applications**
Module 04: Enumeration	**Module 15: SQL Injection**
Module 05: Vulnerability Analysis	**Module 16: Hacking Wireless Networks**
Module 06: System Hacking	**Module 17: Hacking Mobile Platforms**
Module 07: Malware Threats	**Module 18: IoT Hacking**
Module 08: Sniffing	**Module 19: Cloud Computing**
Module 09: Social Engineering	**Module 20: Cryptography**
Module 10: Denial-of-Service	
Module 11: Session Hijacking	

EC-Council Certified Ethical Hacker Practical (CEH MASTER)

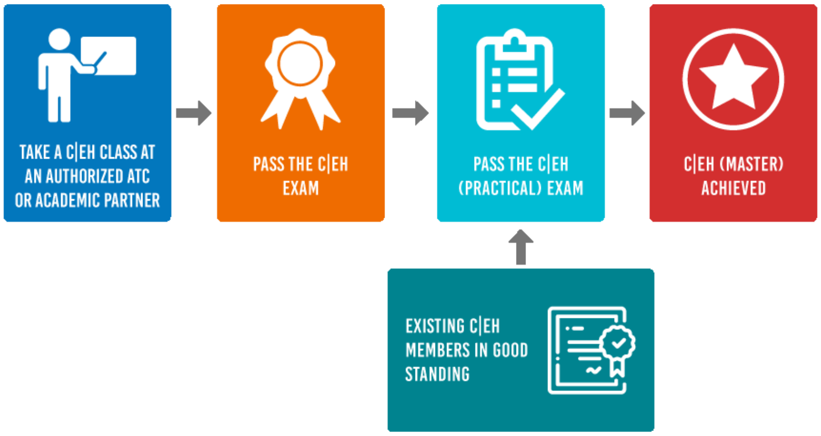
DESCRIPTION

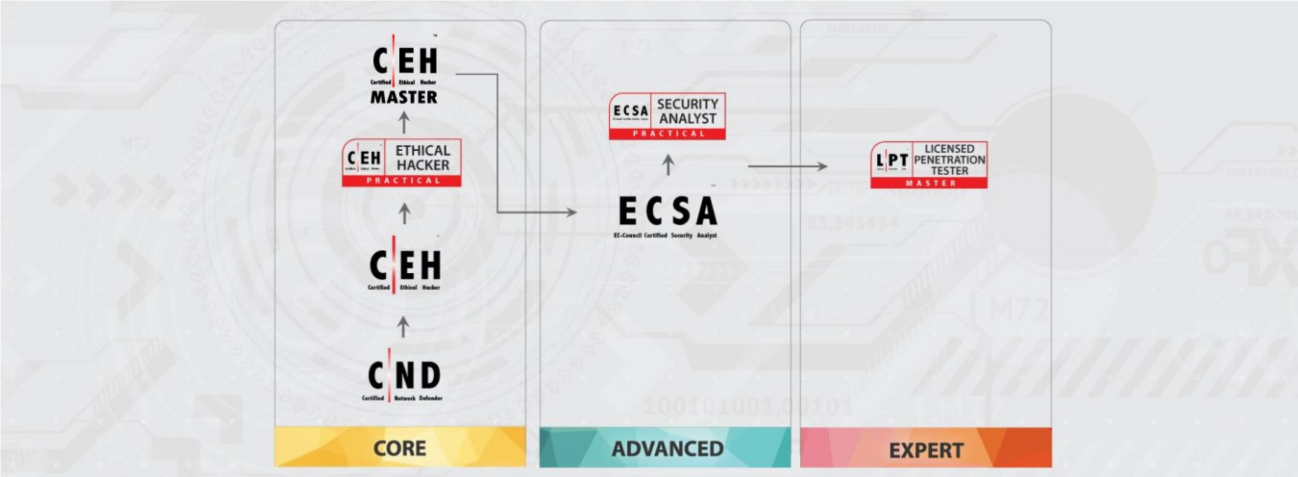
To be placed at the tip of your organization's cyber spear, you must be confident, proficient in your job, and be at the top of your game. You must be able to think on your feet, act quickly, appropriately, and proportionally. Make a mistake and bad things can happen. CEH Master gives you the opportunity to prove to your employer, your peers, and most importantly to yourself that you can in fact take on and overcome challenges found in everyday life as an Ethical Hacker. To prove this, though, we don't give you exam simulations. We test your abilities with real-world challenges in a real-world environment, and with a time limit, just as you would find in your job. Do you run towards danger? Do you take charge during unsettling and challenging times? Do you want to be the one your team can rely on to take the fight to the bad guys? If your answers are yes, prove yourself with CEH Master!

WHAT IS C|EH MASTER

CEH Master is the brainchild of our CEO, Jay Bavisi. It is the next evolution for the world-renowned Certified Ethical Hacker program, and a logical 'next step' for those holding this prestigious certification. CEH is meant to be the foundation for anyone seeking to be an Ethical Hacker. The CEH Practical Exam was developed to give Ethical Hackers the chance to prove their Ethical Hacking skills and abilities. Earning the CEH Master designation is your way of saying, "I learned it, I know it, I proved it."

To earn the CEH Master designation you must successfully demonstrate your knowledge of Ethical Hacking through two distinctly different proving grounds. First, you must attempt and successfully pass the ANSI Accredited Certified Ethical Hacker (CEH) multiple choice exam. Once you complete this first step, you can move on to the second part of earning the CEH Master designation, the CEH Practical Exam.


TAKE A C|EH CLASS AT AN AUTHORIZED ATC OR ACADEMIC PARTNER
PASS THE C|EH EXAM
PASS THE C|EH (PRACTICAL) EXAM
C|EH (MASTER) ACHIEVED
EXISTING C|EH MEMBERS IN GOOD STANDING


CEH Certified Ethical Hacker MASTER
CEH ETHICAL HACKER PRACTICAL
CEH Certified Ethical Hacker
CND Certified Network Defender
CORE
ECSA SECURITY ANALYST PRACTICAL
ECSA EC-Council Certified Security Analyst
ADVANCED
LPT LICENSED PENETRATION TESTER MASTER
EXPERT

TARGET AUDIENCE AND PRE-REQUISITES

It's the hands-on Exam of CEH Practical Certification, so pre-requisite is 312-50 CEHv10 passing score.

DURATION

24 hours

EXAM

Exam Title: Certified Ethical Hacker (Practical)

Number of Practical Challenges: 20

Duration: 6 hours

Availability: Aspen – iLabs

Test Format: iLabs Cyber Range

Passing Score: 70%

EC-Council Computer Hacking Forensics Investigator (CHFI) v9.0

This course will provide participants the necessary skills to identify an intruders footprints and to properly gather the necessary evidence to prosecute in the court of law.

Every crime leaves a trail of evidence
Become a Digital Forensic Investigator
Scanning
C|HFI
Computer Hacking Forensic INVESTIGATOR

COURSE OBJECTIVES

Computer forensics enables the systematic and careful identification of evidence in computer related crime and abuse cases. This may range from tracing the tracks of a hacker through a client's systems, to tracing the originator of defamatory emails, to recovering signs of fraud.

TARGET AUDIENCE

Police and other laws enforcement personnel, Defense and Military personnel, e-Business Security professionals, Systems administrators, Legal professionals, Banking, Insurance and other professionals, Government agencies, involved in the field of defense and security, familiar with the virtual world and online security issues, professionals from the world of banking and insurance, professionals with some experience in law and legal aid, government officials and IT persons with experience in dealing with cybercrimes.

PRE-REQUISITES

The work of a computer hacking forensic investigator asks for highly skilled professionals with an excellent and intimate knowledge of cyber security. Candidates must also possess excellent auditing and reporting skills. They must possess the know-how to immediately detect a security breach and take steps to recover. A great deal of patience is required in order to sift through the mountain of information on the web to find evidence of a cybercrime.

DURATION

40 hours

EXAM

Certified Computer Hacking Forensics Investigator (ANSI)

Number of Questions: 150

Duration: 4 hours

Test Format: Multiple Choice

Exam Prefix: 312-49

COURSE OUTLINE

1 - COMPUTER FORENSICS AND INVESTIGATIONS AS A PROFESSION

2 - UNDERSTANDING COMPUTER INVESTIGATIONS

3 - WORKING WITH WINDOWS AND DOS SYSTEMS

4 - MACINTOSH AND LINUX BOOT PROCESSES AND DISK STRUCTURES

5 - THE INVESTIGATORS OFFICE AND LABORATORY

6 - CURRENT COMPUTER FORENSICS TOOLS

7 - DIGITAL EVIDENCE CONTROLS

8 - PROCESSING CRIME AND INCIDENT SCENES

9 - DATA ACQUISITION

10 - COMPUTER FORENSIC ANALYSIS

11 - E-MAIL INVESTIGATIONS

12 - RECOVERING IMAGE FILES

13 - WRITING INVESTIGATION REPORTS

14 - BECOMING AN EXPERT WITNESS

15 - COMPUTER SECURITY INCIDENT RESPONSE TEAM

16 - LOGFILE ANALYSIS

17 - RECOVERING DELETED FILES

18 - APPLICATION PASSWORD CRACKERS

19 - INVESTIGATING E-MAIL CRIMES

20 - INVESTIGATING WEB ATTACKS

21 - INVESTIGATING NETWORK TRAFFIC

22 - INVESTIGATING ROUTER ATTACKS

23 - THE COMPUTER FORENSICS PROCESS

24 - DATA DUPLICATION

25 - WINDOWS FORENSICS

26 - LINUX FORENSICS

27 - INVESTIGATING PDA

28 - ENFORCEMENT LAW AND PROSECUTION

29 - INVESTIGATING TRADEMARK AND COPYRIGHT INFRINGEMENT