



SCORPIONSHIELD ACADEMY



SCORPIONSHIELD
FOR A CYBER SECURED WORLD

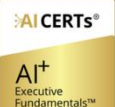
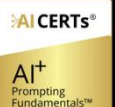
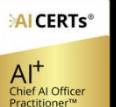
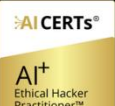
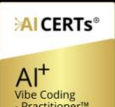


EC-Council



Authorized Training Partner



INFORMATION SECURITY, CYBERSECURITY AND AI

ABOUT SCORPIONSHIELD

SCORPIONSHIELD is a Portuguese Cybersecurity Institution, with a clear mission on fostering first class training in cybersecurity and information security, towards a cyber secured world.

ABOUT EC-COUNCIL



With years of experience, **EC-COUNCIL** is today one of the most reputed Cybersecurity training Organization in the World, and one of the few accredited institutions globally that specializes in Information Security. Is accredited by: CNSS (Committee on National Security Systems), NSA (National Security Agency), DoD (Department of Defense), ANSI (American National Standards Institute) - ANSI 17024 Personnel Certification, DEAC (Distance Education Accrediting Commission), CHEA (Council for Higher Education Accreditation), O*NET (U.S. Department of Labor's Occupational Information Network).

ABOUT SCORPIONSHIELD AND EC-COUNCIL



SCORPIONSHIELD is **EC-COUNCIL Accredited Training Center (ATC)**, holding a close partnership to provide a specialized academy of Information and Cybersecurity, through its body of Certified EC-COUNCIL Instructors **CEI**. Currently provides 12 courses.

ABOUT AI CERTS



AI CERTS® is a New York-based certification body (a DBA of Sarder Inc.), founded in 2023 to close the gap between the AI skills organisations need and what the market can certify. It offers more than eighty role-based, continuously updated certifications in areas including business, leadership,

security, cloud, development, data, healthcare and blockchain, delivered through a global network of authorised training, academic and association partners.

ABOUT SCORPIONSHIELD AND AI CERTS



SCORPIONSHIELD is an **AI CERTS® Authorized Training Partner (ATP)** in Portugal. The partnership lets ScorpionShield offer role-based AI certifications to Portuguese organisations and professionals, with a focus on AI security, AI leadership and governance, and AI development. These complement ScorpionShield's portfolio of AI projects and services, forming a single learning path from core cybersecurity to the secure, responsible adoption of AI.

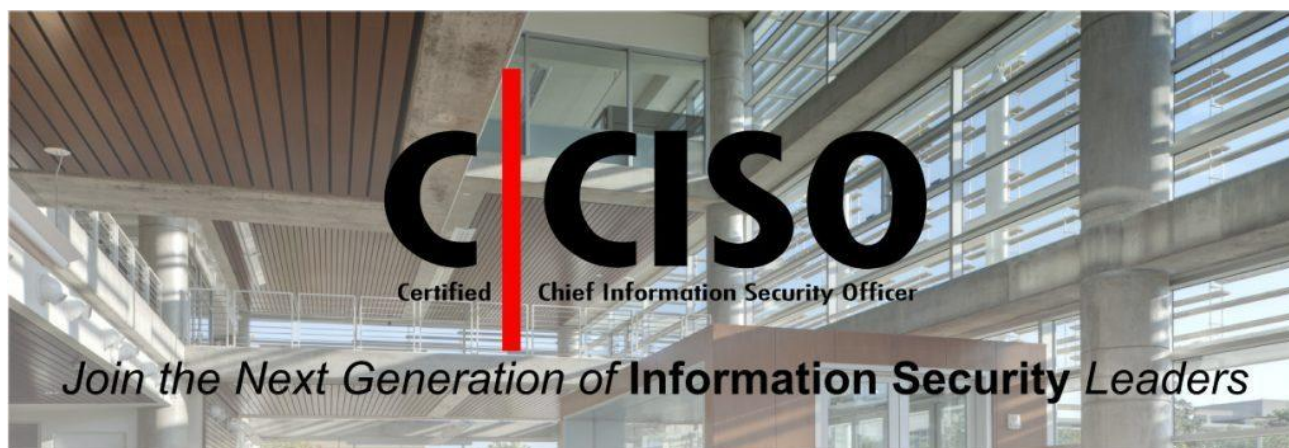
EC-Council

EC-Council Certified Chief Information Security Officer (C|CISO) v4

DESCRIPTION

C|CISO v4 is EC-Council's AI-enhanced executive certification for current and aspiring CISOs. 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 C|CISO does not focus solely on technical knowledge but on the application of information security management principles from an executive point of view. Version 4 integrates AI across the curriculum — AI-driven GRC and auditing, generative AI and LLM security, AI-powered threat intelligence, predictive risk modelling and AI in vendor governance — preparing security leaders to govern AI-enabled organisations. The program was developed by sitting CISOs for current and aspiring CISOs.



TOPICS

- Domain 1. Governance, Risk, Compliance and Audit Management
- Domain 2. Organizational Executive Leadership
- Domain 3. Information Security Controls, Security Program Management & Operations
- Domain 4. Information Security Core Competencies
- Domain 5. Strategic Planning, Finance, Procurement and Third-Party Management

TARGET AUDIENCE AND PRE-REQUISITES

Full certification: 5+ years of experience in at least 3 of the 5 C|CISO domains (with official training).

Associate C|CISO: 2+ years in one domain, or holding CISSP®, CISM® or CISA®. Target audience:

CISOs, CIOs, CTOs, Chief AI Officers, security directors, GRC leaders, and security managers, auditors and architects moving into executive roles.

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



Exam Title: Certified Chief Information Security Officer (ANSI)

Number of Questions: 150

Duration: 2,5 hours

Test Format: Multiple Choice

Exam Prefix: 712-50

Passing Score: cutting score 70-80% depending on form (ANSI)

OUTLINE

Domain 1. Governance, Risk, Compliance and Audit Management
Information security governance and strategy
Risk management, compliance and GRC
Regulatory and legal compliance
AI-driven GRC and auditing
Domain 2. Organizational Executive Leadership
Leadership, ethics and executive presence
Board and stakeholder communication
Participation in AI ethics and governance boards
Privacy, awareness and security culture
Domain 3. Information Security Controls, Security Program Management & Operations
Design, deployment and assurance of security controls
Security program and project management
Security operations, SOC and incident management
Integrating AI into SIEM/SOAR
Domain 4. Information Security Core Competencies
Technical and architecture foundations
Secure architecture for AI/ML pipelines
Generative AI and LLM security
AI-powered threat intelligence
Identity, network, application and data security
Domain 5. Strategic Planning, Finance, Procurement and Third-Party Management
Security strategic planning aligned with business goals
Financial management, budgeting and predictive modelling
Procurement, vendor governance and third-party risk
AI-based contract analysis and vendor scoring

EC-Council

EC-Council Computer Hacking Forensics Investigator (CHFI) v11

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

WHAT IS CHFI

The Computer Hacking Forensic Investigator (CHFI) credential is an ANSI 17024 accredited certification.

The CHFI v11 program has been redesigned and updated after a thorough investigation into current market requirements, job tasks analysis, and the recent industry focus on forensic skills.

It is designed and developed by experienced subject matter experts and digital forensics practitioners.

CHFI v11 program includes extensive coverage of Malware Forensics processes, along with new modules such as Dark Web Forensics and IoT Forensics.

It also covers detailed forensic methodologies for public cloud infrastructure, including Amazon AWS and Azure.

The program is developed with an in-depth focus on Volatile data acquisition and examination processes (RAM Forensics, Tor Forensics, etc.).

CHFI v11 is a complete vendor-neutral course covering all major forensics investigation technologies and solutions.

CHFI has detailed labs for a hands-on learning experience. On average, 50% of training time is dedicated to labs, loaded on EC-Council's CyberQ (Cyber Ranges).

It covers all the relevant knowledge bases and skills to meet regulatory compliance standards such as ISO 27001, PCI DSS, SOX, HIPPA, etc.

It comes with an extensive number of white papers for additional reading.

The program presents a repeatable forensics investigation methodology from a versatile digital forensic professional, increasing employability.

The courseware is packed with forensics investigation templates for evidence collection, the chain of custody, final investigation reports, etc.

The program comes with cloud-based virtual labs, loaded on advanced Cyber Ranges, enabling students to practice various investigation techniques in real-time and realistically simulated environments.



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



Exam Title: Certified Computer Hacking Forensics Investigator (ANSI)

Number of Questions: 150

Duration: 4 hours

Test Format: Multiple Choice

Exam Prefix: 312-49

Passing Score: 70%

OUTLINE

1 - Computer Forensics in Today's World	9 - Malware Forensics
2 - Computer Forensics Investigation Process	10 - Investigating Web Attacks
3 - Understanding Hard Disks and File Systems	11 - Dark Web Forensics
4 - Data Acquisition and Duplication	12 - Cloud Forensics
5 - Defeating Anti-forensics Techniques	13 - Email and Social Media Forensics
6 - Windows Forensics	14 - Mobile Forensics
7 - Linux and Mac Forensics	15 - IoT Forensics
8 - Network Forensics	

ACCREDITATION



Recommendations / Accreditations / Mapping



Testimonials



The National Initiative
for Cybersecurity
Education (NICE)



American National
Standards Institute
(ANSI)



Committee on National
Security Systems (CNSS)



United States Department
of Defense (DoD)



National Infocomm
Competency Framework
(NICF)



Department of Veterans
Affairs



KOMLEK



MSC



American Council on
Education (ACE)

It is my pleasure to take the time to praise the EC-Council for having such a magnificent class, specifically THE Computer Hacking Forensic Investigator course. The course had an abundance of information, utilities, programs, and hands on experience. I am a consultant at Dell and we do have a lot of technical training, but I must comment that this one is one of the best trainings I have seen in several years. I will definitely recommend this course to all my colleagues.

- Hector Alvarez, CHFI, Enterprise & Storage Consultant,
Dell Corporation, Austin, Texas

All the treatment has been excellent, the material and the content of the course overcomes my expectations. Thanks to the instructor and to Itera for their professionalism.

- Sergio Lopez Martin, CHFI, Security Sales, IBM, Spain

CHFI is a certification that gives an complete overview of the process that a forensic investigator must follow when is investigating a cybercrime. It includes not only the right treatment of the digital evidence in order to be accepted in the Courts but also useful tools and techniques that can be applied to investigate an incident.

- Virginia Aguilar, CHFI, KPMG, Madrid

The Computer Hacking Forensic Investigator (CHFI) certification has been instrumental in assuring both my company and our clients that my skillset is among the elite in the cyber security and response profession. The CHFI allows my company to readily identify to our DoD clients that our team is trained to perform the rigorous functions required of cyber threat response team. Our company can now better brand our capability to investigate cyber security incidents, perform computer/malware forensic analysis, identify active threats, and report our findings.

- Brad W. Beatty, Cyber Security Analyst, Booz Allen Hamilton, USA

EC-COUNCIL PENTESTER PATH

To attain a level of EXPERT, from CORE and through ADVANCED, EC-COUNCIL sets the standards through 5 levels of training and certification. Scorpionshield follow this Track through a specific Academy, with the objective of develop guided Licensed Penetration Testers.



Course	Training	Exam
C EH CERTIFIED ETHICAL HACKER V12	40 h	4 h
C EH MASTER (PRACTICAL)	24 h	6 h
CPENT CERTIFIED PENETRATION TESTER PROFESSIONAL	40 h	12 h
L PT LICENSED PENETRATION TESTER MASTER (PRACTICAL)	24 h	18 h

EC-Council

EC-Council C|EH - Certified Ethical Hacker v12

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 519 attack techniques, commonly used by hackers.

THE CERTIFIED ETHICAL HACKER

The World's No. 1
Ethical Hacking
Certification for 20 Years



Ranked #1
In Ethical Hacking
Certifications by ZDNet



Ranked as a Top 10
Cybersecurity Certification



C|EH® Ranks 4th
Among Top 50 Leading
Cybersecurity Certifications

Our security experts have designed over 220 labs which mimic real time scenarios in the course to help “live” through an attack as if it were real and provide with access to over 3500 commonly used hacking tools to immerse into the hacker world:

The goal of this course is to help 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

Exam Title: Certified Ethical Hacker V12 (ANSI)

Number of Questions: 125

Duration: 4 hours

Test Format: Multiple Choice

Exam Prefix: 312-50

Passing Score: 70%



OUTLINE CJEH

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



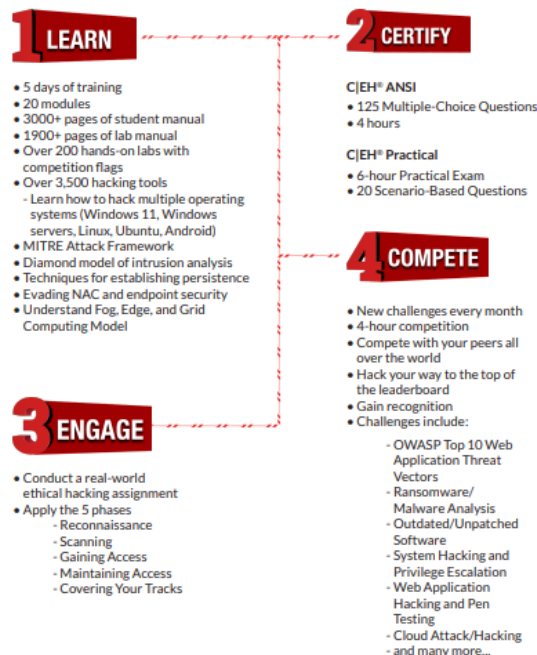
In its 12th version, the Certified Ethical Hacker provides comprehensive training, hands-on learning labs, practice cyber ranges for engagement, certification assessments, cyber competitions, and opportunities for continuous learning into one comprehensive program curated through our new learning framework: 1. Learn 2. Certify 3. Engage 4. Compete.

Master ethical hacking skills that go beyond the certification.



The new learning framework covers not only a comprehensive training program to prepare you for the certification exam but also the industry's most robust, in-depth, hands-on lab and practice range experience.

Enter the Hackerverse™ With the C|EH® v12
Enhance Your Ethical Hacking Career



The C|EH® v12 training program includes 20 modules covering various technologies, tactics, and procedures, providing prospective ethical hackers with the core knowledge needed to thrive in cybersecurity.

Delivered through a carefully curated training plan that typically spans five days, the 12th version of the C|EH® continues to evolve to keep up with the latest OS, exploits, tools, and techniques.

The concepts covered in the training program are split 50/50 between knowledge-based training and hands-on application through our cyber range. Every tactic discussed in training is backed by step-by-step labs conducted in a virtualized environment with live targets, live tools, and vulnerable systems.

Through our lab technology, every participant will have comprehensive hands-on practice to learn and apply their knowledge."

EC-Council



EC-Council Certified Ethical Hacker Practical (CEH MASTER)

DESCRIPTION

To be placed at the tip of organization's cyber spear, must be confident, proficient in job, and be at the top of game. Must be able to think, act quickly, appropriately, and proportionally. Make a mistake and bad things can happen. CEH Master gives the opportunity to prove to employer, peers, and most importantly to oneself that can in fact take on and overcome challenges found in everyday life as an Ethical Hacker. To prove this, though, we don't give exam simulations.

We test abilities with real-world challenges in a real-world environment, and with a time limit.



WHAT IS CEH 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 a way of saying, "I learned it, I know it, I proved it." To earn the CEH Master designation one must successfully demonstrate one knowledge of Ethical Hacking through two distinctly different proving grounds.

First, one must attempt and successfully pass the ANSI Accredited Certified Ethical Hacker (CEH) multiple choice exam. Once one complete this first step, one can move on to the second part of earning the CEH Master designation, the CEH Practical Exam.

TARGET AUDIENCE AND PRE-REQUISITES

It's the hands-on Exam of CEH Practical Certification, so pre-requisite is 312-50 CEHv11 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

EC-Council Certified Penetration Tester Professional (CPENT)

DESCRIPTION

The heart of the CPENT program is all about helping one master one pen testing skills by putting them to use on our live cyber ranges. The CPENT ranges were designed to be dynamic in order to give one a real-world training program, so just as targets and technology continue to change in live networks, both the CPENT practice and exam ranges will mimic this reality as our team of engineers continue to add targets and defenses throughout the CPENT course's lifetime.

WHAT IS CPENT

EC-Council's Certified Penetration Tester (CPENT) program teaches one how to perform an effective penetration test in an enterprise network environment that must be attacked, exploited, evaded, and defended. If one have only been working in flat networks, CPENT's live practice range will teach one to take one skills to the next level by teaching one how to pen test IoT systems, OT systems, how to write one own exploits, build one own tools, conduct advanced binaries exploitation, double pivot to access hidden networks, and also customize scripts/exploits to get into the innermost segments of the network.

The CPENT Challenge Edition is a low-cost study resource that will provide a refresher in areas such as IoT, ICS, SCADA, and binary analysis. The CPENT Challenge Edition includes a selection of labs from each of the CPENT course modules that will introduce one to the concepts that are required to obtain the required points across the different zones.

The CPENT range consists of entire network segments that replicate an enterprise network — this is not a computer game simulation; this is an accurate representation of an enterprise network that will present the latest challenges to the pen tester. The benefit of hands on learning in a live cyber range is that candidates will encounter multiple layers of network segmentation, and the CPENT course will teach candidates how to navigate these layers, so that once access is gained in one segment, a candidate will know the latest pivoting techniques required to reach the next. However, that won't be enough on its own as the targets and segments are progressive in nature, so once one get into one machine and or segment, the next one will challenge one even more.

CPENT is a fully online, remotely proctored practical exam that challenges candidates through a grueling 24-hour performance-based, hands-on exam. The exam is broken into 2 practical exams of 12-hours each that will test one perseverance and focus by forcing one to outdo oneself with each new challenge. Candidates have the option to choose either 2 12-hour exams or one 24-hour exam. Candidates who score more than 70% will earn the CPENT certification. Candidates who score more than 90% attain the prestigious LPT (Master) credential.

TARGET AUDIENCE AND PRE-REQUISITES

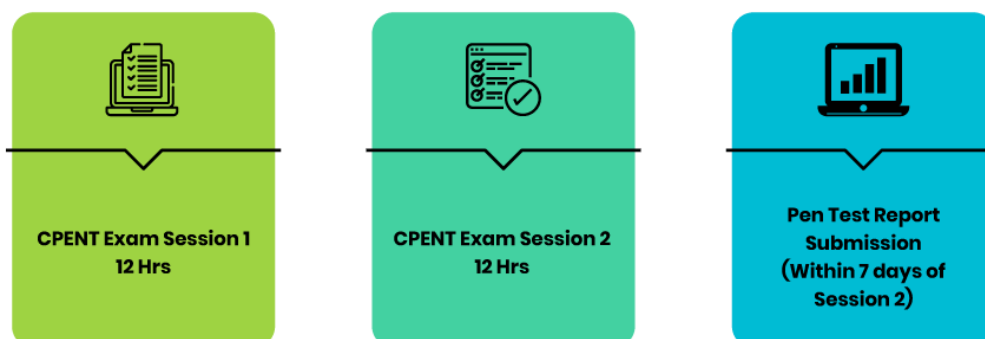
Ethical Hackers; Penetration Testers; Network server administrators; Firewall Administrators; Security Testers; System Administrators; Risk Assessment professionals;

DURATION

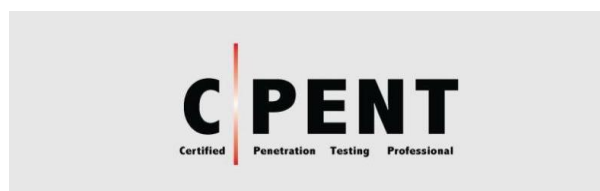
40 hours

One have the potential to earn two certifications with one exam. If one score above a 90% on the CPENT live range exam, not only will one earn the CPENT certification, but one will also earn the Licensed Penetration Tester (LPT) Master Credential. To be a LPT (Master) means that one can find chinks in the armor of defense-in-depth network security models with the help of network pivoting, making exploit codes work in one favor, or by writing Bash, Python, Perl, and Ruby scripts. The live range CPENT exam demands that one think on one feet, be creative in one approach, and not rely on the conventional techniques.

Outsmarting and out maneuvering the adversary is what sets one apart from the crowd. The CPENT's hands-on exam offers a challenge like no other by simulating a complex network in real time. This experience will test one perseverance and focus by forcing one to outdo oneself with each new challenge.



EXAM



- **Exam Title:** CPENT Exam:
- **Credit Towards Certification:** CPENT
- **Practical:** iLABS
- **Passing Score:** 70% (90% for LPT degree)
- **Test Duration:** 12 Hours or 24 Hours

Exam features:

- Choose a challenge! Either two 12-Hour sessions or a single 24-Hour exam!
- EC-Council specialists proctor the entire exam – Validity is not in question.
- Score at least 70% and become a CPENT
- Score at least 90% and earn the highly regarded LPT (Master) designation!

OUTLINE

Module 01: Introduction to Penetration Testing
Module 02: Penetration Testing Scoping and Engagement
Module 03: Open Source Intelligence (OSINT)
Module 04: Social Engineering Penetration Testing
Module 05: Network Penetration Testing – External
Module 06: Network Penetration Testing– Internal
Module 07: Network Penetration Testing – Perimeter Devices
Module 08: Web Application Penetration Testing
Module 09: Wireless Penetration Testing
Module 10: IoT Penetration Testing
Module 11: OT/SCADA Penetration Testing
Module 12: Cloud Penetration Testing
Module 13: Binary Analysis and Exploitation



EC-Council

EC-Council Licensed Penetration Tester Practical (LPT MASTER)

DESCRIPTION

This exam has one purpose: To Differentiate The Experts From The Novices In Penetration Testing!

There are good penetration testers and then there are great penetration testers.

Unless one are bent on being nothing other than the best in penetration testing, don't bother registering for this program, as one are probably not cut out for it. We know that the only way to find out what one are made of is by testing one at the brink of exhaustion — which is why the LPT (Master) exam is 18 hours long!

One pen testing skills will be challenged over three levels, each with three challenges, against a multi-layered network architecture with defense-in-depth controls. One will be required to make knowledgeable decisions under immense pressure at critical stages while selecting one approach and exploits.



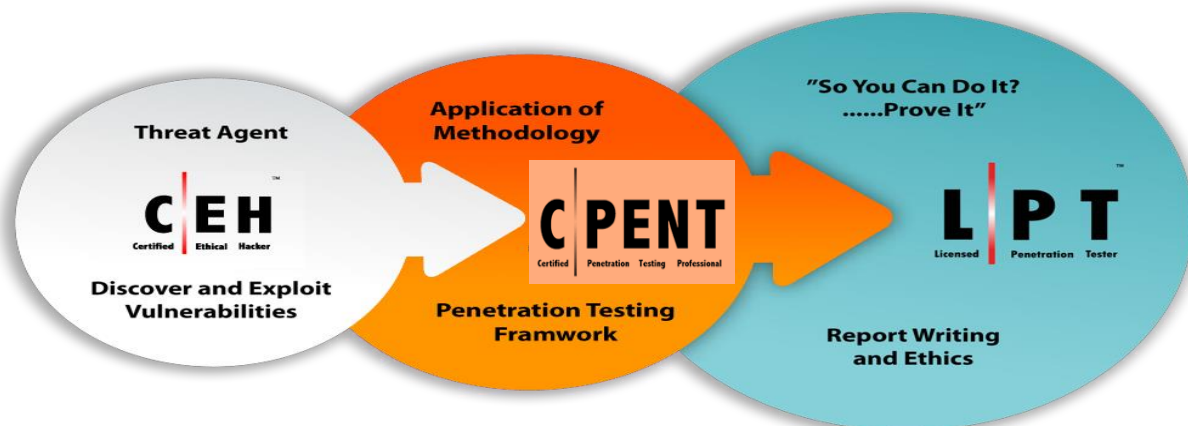
As one progress along these levels, one will need to maneuver web application, network, and host penetration testing tools and tricks in an internal and external context to ultimately pwn the hosts and exfiltrate data required for the completion of the challenges.

The exam will require one to demonstrate mastery of deploying advanced pen testing techniques and tools including multi-level pivoting, OS vulnerabilities exploits, SSH tunnelling, host-based application exploits, privilege escalation, web server and web application exploitation such as arbitrary local and remote file upload, SQL injection and parameter manipulation, etc – all in a real life scenario on hardened machines, networks, and applications.

WHAT IS EC-Council Licensed Penetration Tester Practical (LPT MASTER)

To introducing the World's Most Advanced Penetration Testing Program, One must understand the Learning Track behind EC-COUNCIL. First CEH teaches to discover and exploit vulnerabilities, then CPENT the penetration testing techniques and framework, and last LPT to learn how to be the best penetration tester.

THE LEARNING TRACK



Knowledge

Skill

Ability

The Advanced Penetration Testing Course by EC-Council was created as the progression after the CPENT (Practical) to prepare those that want to challenge the Licensed Penetration Tester (Master) certification and be recognized as elite penetration testing professionals. Our training has been designed by the best in the industry and meant to push one to develop the kind of skill that you've been waiting to acquire.

LPT (Master) training is not comfortable (and the exam is even worse!) but filled with intense stress meant to illicit the best from you. Those who prevail will have developed an instinctual and intellectual response to real world penetration testing challenges. Our aim is to push one to one limit while making one solve complex problems that actual penetration testers solve daily in the real world. For four punishing and long days, one will have to perform various tasks until it becomes second nature.

This program is radically different from the CPENT. In the CPENT course, one are provided guidance on what machines to attack and an initial starting point. In the Advanced Penetration Testing Course, one are presented with minimal network information along with a Scope of Work (SOW). The course was created to provide one with advanced concepts that will help when it comes to attempting the LPT (Master) Certification exam.

Demonstrate the Mastery of Advanced Pen Testing Concepts and Techniques Including:

■ Multi-level Pivoting

■ OS Vulnerabilities Exploitation

■ SQL Injection

■ Host-Based Application Exploitation

■ Privilege Escalation

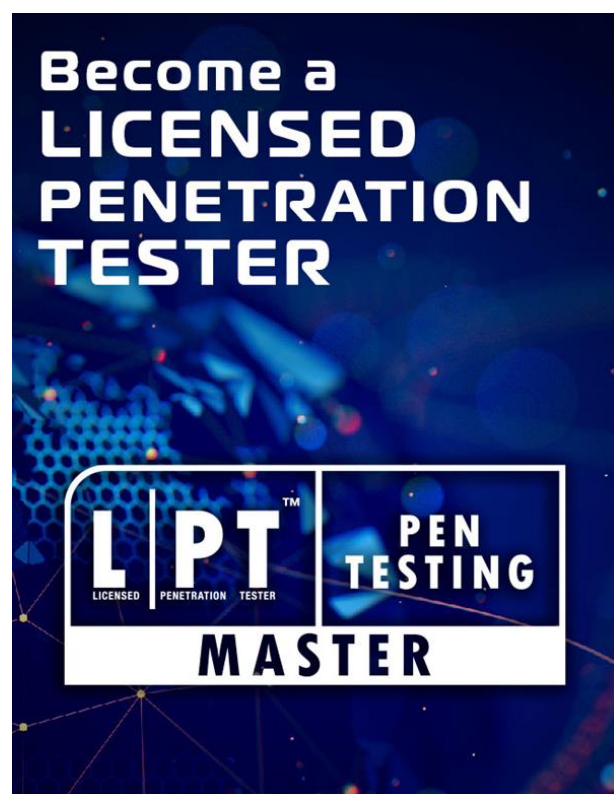
■ RFI/LFI

■ Exploit and Payload Customization

■ SSH Tunnelling

In this course one will learn professional security and penetration testing skills. The course is designed to show advanced concepts like scanning against defenses, pivoting between networks, deploying proxy chains, and using web shells. The last module of the course includes a SOW for each of the various networks we have created for the course. This, combined with the composition of various ranges, mimics a professional penetration test. Time is limited and one will be required to identify the attack surface followed by the weaknesses of the machines that are on the network.

WHAT IS EC-Council Advanced Penetration Testing Cyber Range (ECCAPT)



The Advanced Penetration Testing course from EC-Council is built on the backbone of the Advanced Penetration Testing Cyber Range (ECCAPT) and this was designed by experts who each have more than 25 years of professional security testing across the globe.

The program comes with multiple ranges designed to hone a specific set of real-life pen testing skills. The ECCAPT contains more than 180 machines with more than 250 GB RAM and more than 4000 GB of storage segregated in complex network ranges with multiple militarized and demilitarized zones. It facilitates learning and demonstration of current attack vectors, penetration testing methodology, and tools. A typical range consists of 5 to 8 subnets where each subnet represents a different business unit and comprises semi-hardened and hardened machines with more than 15 Windows and Linux OS flavors.

The range is designed to provide challenges across every level of the attack spectrum. Additionally, the range contains multiple layers of network segmentation, and once access is gained in one segment, the latest pivoting techniques are required to reach the next segment.

Many of the challenges will require outside-the-box thinking and customization of scripts and exploits to get into the innermost segments of the network. The key to be a highly skilled penetration tester is to go up against a variety of targets that are configured in a variety of ways. The ECCAPT consists of entire network segments that replicate an enterprise network — this is not a computer game simulation; this is an accurate representation of an enterprise network that will present the latest challenges to the pen tester. Since the targets and technology continue to change, the ECCAPT is dynamic and machines and defenses will be added as they are observed in the wild. Finally, the targets and segments are progressive in nature, once one gets into one machine and or segment, the next one will challenge one even more.

The final range consists of challenges that will require the skills and concepts that have been covered in the course and consist of multiple visible as well as hidden subnets to prepare one for the possible challenges of the LPT (Master) range.

Finally, the ranges are designed to teach professional-level skills to identify the attack surface of targets within a required time frame and, once this has been accomplished, to gain access to the machines and escalate privileges as required. The greater the variety of targets one encounters with and without defenses, the better of a professional penetration tester one will become.

The practical environment ranges progress in difficulty and reflect real enterprise network architecture. This environment includes defenses and challenges which one must defeat and overcome.

This is not one typical flat network! As one progress through the range levels, each encounter will present the top defenses of today and one will learn the best and latest evasion techniques.

This training format has helped thousands of penetration testers globally and is proven to be effective. The ECCAPT is 100% hands-on. Everything presented in the course is through an enterprise network environment that must be attacked, exploited, evaded, and defended.

TARGET AUDIENCE AND PRE-REQUISITES

To be eligible to apply to attempt the LPT (Master) Exam, candidate must either:

- be an CPENT member in good standing;
- or, Attend the Advanced Penetration Testing course.
- or, possess a minimum of 2 years of Penetration Testing work experience in Penetration Testing;
- or, possess any other industry equivalent certifications such as OSCP or GPEN cert.

L|PT (Master) certified professionals can:

- Demonstrate a repeatable and measurable approach to Penetration Testing
- Perform advanced techniques and attacks to identify SQL injection, Cross site scripting (XSS),
- LFI, RFI vulnerabilities in web applications
- Perform privilege escalation to gain root access to a system Demonstrate 'Out-of-the-box'
- and 'lateral' thinking
- Get access to proprietary EC-Council Penetration Testing methodologies
- Exploit vulnerabilities in Operating systems such as Windows, Linux
- Identify and bypass perimeter protections: In an enterprise network their will be protections, one will learn how to identify the protections in place and bypass them to extract the data even when protected with IPS and endpoint protections
- Perl, Python and Ruby scripting for the penetration tester: As a practitioner one have to be able to modify and change the methods of attacking an enterprise network, this requires custom scripting to defeat signature and anomaly-based protection mechanisms
- Advanced post exploitation and persistence: Gaining access is a small part of a professional penetration test, once one have the access, the ability to move laterally, and exfiltrate the data from the enterprise requires post exploitation skills
- Extending Metasploit with custom modules and exploits: To use open source code in a penetration test requires knowledge of the modules, and the ability to customize them based on the data one have obtained from the targets
- Pivoting from external into internal networks: Virtually all enterprise networks have external facing machines as well as internal intranet machines, the preferred way to access these is through pivoting and using the initial source of access to leverage one way into the enterprise intranet
- Avoiding the most common mistakes when drafting a professional penetration testing report: Having skills is one thing, but being able to provide tangible findings to the enterprise client is critical for a professional penetration tester

DURATION

24 hours

EXAM



Exam Title: LPT (Practical) Exam:

- Number of challenges: 9
- Duration: 18 hours
- Availability: ECCAPT
- Test Format: iLabs ECCAPT cyber range
- Passing Score: 5 out of 9 challenges
- Submission: penetration testing report

OUTLINE

Module 1. Introduction to Vulnerability Assessment and
Module 2. Penetration Testing
Module 3. Information Gathering Methodology
Module 4. Scanning and Enumeration
Module 5. Identify Vulnerabilities
Module 6. Exploitation
Module 7. Post Exploitation
Module 8. Advanced Tips and Techniques
Module 9. Preparing a Report

EC-Council



EC-Council Certified DevSecOps Engineer v1

EC-Council Certified DevSecOps Engineer (ECDE) is a hands-on, instructor-led comprehensive DevSecOps certification program which helps professionals to build essential knowledge and abilities in designing, developing, maintaining a secure applications and infrastructure.

WHAT IS E|CDE

This course is blended with both theoretical knowledge as well as the practical implementation of DevSecOps in one on-prem and cloud-native (AWS and Azure) environment. The course covers integration and automation of all the major and widely used tools, processes, and methodologies of DevSecOps that help organizations to build secure applications rapidly in a DevOps environment.

The EC-Council Certified DevSecOps (Development, Security, and Operations) Engineer (E|CDE) is an instructor-led certification training program that equips professionals with the necessary skills to design, develop, and maintain secure applications and infrastructure using DevSecOps principles. This comprehensive course combines theoretical knowledge with hands-on experience, enabling participants to effectively apply DevSecOps practices in on-premises and cloud environments like AWS and Azure.

EC-Council

EC-Council Certified DevSecOps Engineer

What Makes E|CDE Different?

- 80+ Labs
- On-premises and cloud-native coverage
- Security and tools integration at eight DevOps stages
- Covers cloud environments, including AWS and Microsoft Azure
- Mapped with real-time job roles

EC-Council

E|CDE
EC-Council Certified DevSecOps Engineer

Transform your Software Cybersecurity in On-Premises And Cloud-Based Environments With E|CDE.

A Hands-On Program with 70% of the Curriculum Dedicated to Labs

Become an EC-Council Certified DevSecOps Engineer

COURSE OBJECTIVES

By completing the course, participants will become proficient in integrating and automating essential tools, processes, and methodologies, allowing organizations to expedite the development of secure applications within a DevOps ecosystem. Main objectives are:

- Understand the DevOps culture and its principles, fostering collaboration and continuous improvement within organizations.
- Gain an introduction to DevSecOps, integrating security practices into the DevOps framework for enhanced application and infrastructure security.
- Develop proficiency in planning and implementing a DevSecOps pipeline, covering various stages from code development to release and deployment.
- Learn to apply security measures in each stage of the DevSecOps pipeline, ensuring secure code, build, testing, release, deployment, and ongoing monitoring.
- Acquire hands-on experience with tools, technologies, and methodologies used in DevSecOps, including planning, code analysis, testing, and monitoring tools.
- Understand the importance of continuous monitoring and feedback loops to identify vulnerabilities and mitigate security risks in real-time.
- Apply best practices for secure operations and monitoring within a DevSecOps environment, ensuring ongoing security and resilience for applications and infrastructure.
- Prepare for the EC-Council Certified DevSecOps certification exam to validate one knowledge and expertise in DevSecOps practices.



TARGET AUDIENCE

- Software Engineers
- Application Security Professionals
- DevOps Engineers
- Software Engineers/Testers
- IT Security Professionals
- Cyber security engineer/Analyst
- Anyone having prior knowledge in application security and wants to build their career in DevSecOps

PRE-REQUISITES

- Good understanding of Linux OS and basic Linux commands
- Understanding of one of the Cloud Service Providers like AWS or Azure, or GCP
- Understanding of security concepts and architecture
- Basic understanding of SDLC Lifecycle and automation

DURATION

24 hours

EXAM

Exam Title: EC-COUNCIL Certified DevSecOps Engineer (ANSI)

Number of Questions: 100

Duration: 4 hours

Test Format: Multiple Choice

Exam Prefix: 312-97 (ECC EXAM), 312-50 (VUE)

Passing Score: 70%

OUTLINE

Module 01: Understanding DevOps Culture
Module 02: Introduction to DevSecOps
Module 03: DevSecOps Pipeline-Plan Stage
Module 04: DevSecOps Pipeline-Code Stage
Module 05: DevSecOps Pipeline-Build and Test Stage
Module 06: DevSecOps Pipeline-Release and Deploy Stage
Module 07: DevSecOps Pipeline-Operate and Monitor Stage





EC-Council Certified SOC Analyst v1

The Certified Soc Analyst (CSA) is a certification hosted by the EC-Council that validates IT security professionals' skills and expertise to join a Security Operation Centre (SOC). SOC is a team of Cybersecurity professionals responsible for monitoring and responding to an organization's security threats. The credential is mainly developed for aspiring Level 1 and Level 2 SOC analysts to understand various SOC processes and provide them with the necessary skills to operate efficiently within a SOC team. It can also aid network security professionals in handling the operations related to network security.



WHAT IS C|SA

The course content thoroughly covers the fundamentals of SOC operations, in-depth understanding of log management and correlation, deployment of SIEM solutions, detection, and incident response methodologies. EC-Council Certified SOC Analyst Training Program will help one to master over trending and in-demand technical skills like

- Knowledge of SOC processes, procedures of these processes, technologies, and workflows
- basic understanding and detailed knowledge of security threats, attacks, vulnerabilities, attacker's behaviours, cyber kill chain, etc.

Through this SOC Analyst Certification Training our expert trainers offer in-depth knowledge with enhanced level capabilities for dynamic contribution to a SOC team.

CSA Training Course has been especially designed to help one learn :

- The basics of SOC operations,
- log management and correlation,
- SIEM deployment,
- advanced incident detection, and incident response

This SOC Analyst course will also help one to improve one knowledge regarding performance of enhanced threat detection using the predictive capabilities of Threat Intelligence.

COURSE OBJECTIVES

Participants will learn the following topics during their CSA training:

- SOC processes, operations, technologies, and workflows
- Get in-depth knowledge about various threats, attacks, vulnerabilities and methodologies and actions taken by an attacker
- Understand centralized log management process and how to monitor logs, alerts from various sources
- Learn how to implement, architect, tune and administer SIEM solutions like Splunk, AlienVault, OSSIM
- Monitoring threat patterns and perform a threat analysis
- Interpreting use cases regarding SIEM deployment and learning alert triage process
- Knowing how to formulate reports and use service desk ticketing system
- Integrating threat intelligence into SIEM solutions
- Learning advanced threat detection and incidence response process



TARGET AUDIENCE

- Soc Analysts (Tier 1, 2)
- Network Administrators
- Network Security Engineers
- Cybersecurity Analysts
- Entry Level Cybersecurity Professionals
- Network Security Operators
- Network Security Specialists
- Network Defense Analysts
- anyone interested in becoming a part of the SOC team

PRE-REQUISITES

The participants should have one year of experience in the network security or Network Administration domain. The participants who have opted for official training from EC-Council or one of its accredited training Centers need not submit any proof of work experience.

DURATION

24 hours

EXAM

Exam Title: Certified SOC Analyst (CSA) (ANSI)

Number of Questions: 100

Duration: 3 hours

Test Format: Multiple Choice

Exam Prefix: 312-39

Passing Score: 70%

OUTLINE

The Certified SOC Analyst training course comprises of six modules that are mentioned below with their exam weightage:

Module 1: Security Operations and Management (5%)
Module 2: Understanding Cyber threats, IoCs, and attack methodologies (11%)
Module 3: Incidents, Events, and Logging (21%)
Module 4: Incident Detection with Security Information and Event Management (SIEM) (26%)
Module 5: Enhanced Incident Detection with Threat Intelligence (8%)
Module 6: Incidence Response (29%)





EC-Council Certified Incident Handler v2

EC-Council's Certified Incident Handler v2 (E|CIH) certification and training imparts and validates extensive skills to address post-security breach consequences in the organization by condensing the financial and reputational impact of the incident. This E|CIH program has been devised by globally recognized cybersecurity and incident handling & response practitioners. The certification is highly ranked and helps enhance the employability of cybersecurity professionals worldwide.

WHAT IS E|CIH

EC-Council's Certified Incident Handler v2 (E|CIH) certification and training imparts and validates extensive skills to address post-security breach consequences in the organization by condensing the financial and reputational impact of the incident. This E|CIH program has been devised by globally recognized cybersecurity and incident handling & response practitioners. The certification is highly ranked and helps enhance the employability of cybersecurity professionals worldwide.



COURSE OBJECTIVES

The E|CIH V2 certification and training targets to explain:

- Combating various kinds of cybersecurity threats and attack vectors
- Core incident management fundamentals that include incident signs and costs
- Basics of vulnerability management, risk management, and threat assessment
- Automation and orchestration of Incident Response
- Best practices of incident handling and response
- Understanding cybersecurity frameworks, standards, acts, laws, and compliance
- Core essentials of computer forensics

- Importance of procedure of the first response
- Collecting and analyzing evidence, packaging, storing, transportation, and data acquisition
- Anti-forensics techniques adopted by attackers to discover cover-ups for cybersecurity incident
- Learn to differentiate between cybersecurity incidents such as malware, network threats, and insider threat-related incidents

TARGET AUDIENCE

- Penetration Testers
- Application Security Engineers
- Vulnerability Assessment Auditors
- Cyber Forensic Investigators and SOC Analysts
- Risk Assessment Administrators
- System Administrators/ Engineers
- Network Administrators
- Firewall Administrators
- Network Managers/ IT Managers

PRE-REQUISITES

- At least 1 year managing Windows/ Unix/ Linux
- In-depth understanding of network and security services

DURATION

24 hours

EXAM

Exam Title: EC-Council Certified Incident Handler (ANSI)

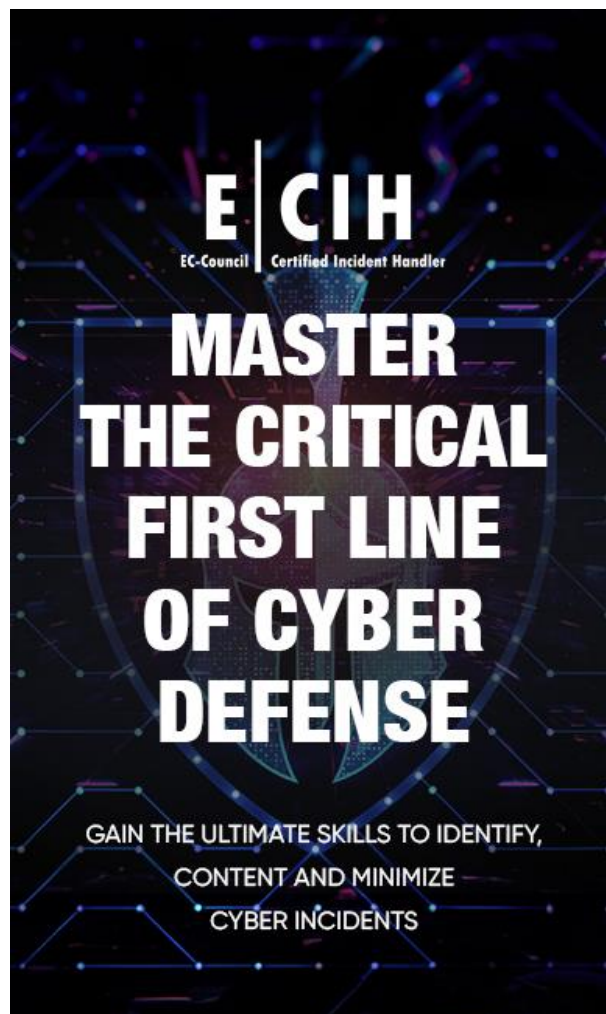
Number of Questions: 100

Duration: 3 hours

Test Format: Multiple Choice

Exam Prefix: 212-89

Passing Score: 70%



OUTLINE

Module 01: Introduction to Incident Handling and Response	Module 06: Handling and Responding to Network Security Incidents
Module 02: Incident Handling and Response Process	Module 07: Handling and Responding to Web Application Security Incidents
Module 03: Forensic Readiness and First Response	Module 08: Handling and Responding to Cloud Security Incidents
Module 04: Handling and Responding to Malware Incidents	Module 09: Handling and Responding to Insider Threats
Module 05: Handling and Responding to Email Security Incidents	

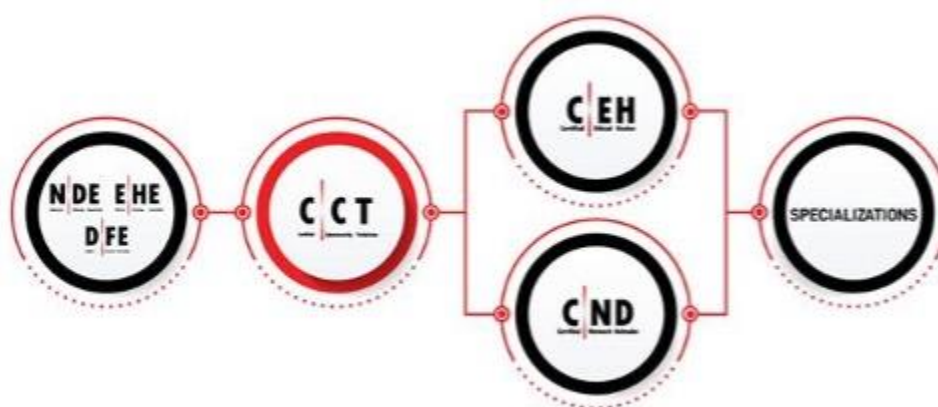


EC-Council Certified Cybersecurity Technician v1

CCT is an entry-level cybersecurity program that is engineered by the creators of the Certified Ethical Hacker program to respond to the global need and demand for cybersecurity technicians.

The C|CT certification program is the world's-only entry-level program to provide total foundational cybersecurity domain coverage with 85 hands-on labs (three times more than any other entry-level certification), ensuring realistic, practical skill development.

Following Essentials Program, and after C|CT, one can follow a intermediate course like C|EH (Certified Ethical Hacker - Red Team) or C|ND (Certified Network Defender – Blue Team).



WHAT IS C|CT

CCT develops foundational multi-disciplinary cybersecurity skills across network defense, ethical hacking, digital forensics, and security operations to kickstart a cybersecurity career. The CCT certification/credential is obtained through a comprehensive performance-based exam that combines live cyber range activities with a variety of knowledge assessments proving a grasp of both the knowledge and applied skills required to be successful in a cyber technician role. CCT Course is perfectly designed for anyone who is seeking to kickstart their Professional career journey in the field of Cybersecurity or add a strong foundational understanding of Cyber Security domains, and tactics required to be effective on the job.

COURSE OBJECTIVES

1. To facilitate entry into the world of cybersecurity as a cybersecurity technician
2. To provide a professional fundamental skill and solidifies the concepts of information security, network security, computer forensics, risk management, and incident handling
3. To provide best practices to improve organizational security posture
4. To enhance skills as a cybersecurity specialist and increases employability
5. To provide hands-on practical skills that will use on the job every day as a cyber security technician, or any role in IT with administrative privileges where security should be considered and practiced.

TARGET AUDIENCE

- IT Support Specialist
- IT Networking Specialist
- Cybersecurity Technicians
- Network Administrator
- SOC Analyst
- Network Engineers
- IT Managers
- Facility Administrators
- Career Starters, Career Changers, and Career Advancers– Students, Recent Graduates/IT Professionals, IT Managers



PRE-REQUISITES

- No specific prerequisites are required for CCT Certification.
- Having knowledge and experience in IT Networking with a Cyber-Security focus can be an advantage.
- Candidates should have knowledge of computers and computer networks prior to challenging the CCT program, though core technologies are covered in the curriculum.

DURATION

24 hours

EXAM

Exam Title: Certified Cybersecurity Technician (ANSI)

Number of Questions: 60

Duration: 3 hours

Test Format: Multiple Choice

Exam Prefix: 212-82

Passing Score: 70%

OUTLINE

1 - Information Security Threats and Vulnerabilities	12 - Wireless Network Security
2 - Information Security Attacks	13 - Mobile Device Security
3 - Network Security Fundamentals	14 - IoT and OT Security
4 - Identification, Authentication, and Authorization	15 - Cryptography
5 - Network Security Controls – Administrative Controls	16 - Data Security
6 - Network Security Controls – Physical Controls	17 - Network Troubleshooting
7 - Network Security Controls – Technical Controls	18 - Network Traffic Monitoring
8 - Network Security Assessment Techniques and Tools	19 - Network Logs Monitoring and Analysis
9 - Business Continuity and Disaster Recovery	20 - Incident Response
10 - Application Security	21 - Computer Forensics
11 - Virtualization and Cloud Computing	22 - Risk Management





EC-Council Certified Network Defender v2

The Certified Network Defender (C|ND) certification program focuses on creating Network Administrators who are trained on protecting, detecting and responding to the threats on the network.

The C|ND Program is a skills-based, lab intensive program based on a job-task analysis and cybersecurity education framework presented by the National Initiative of Cybersecurity Education (NICE).



WHAT IS C|ND

Network administrators are usually familiar with network components, traffic, performance and utilization, network topology, location of each system, security policy, etc.

A C|ND will get the fundamental understanding of the true construct of data transfer, network technologies, software technologies so that they understand how networks operate, understand what software is automating and how to analyze the subject material.

In addition, network defense fundamentals, the application of network security controls, protocols, perimeter appliances, secure IDS, VPN and firewall configuration, intricacies of network traffic signature, analysis and vulnerability scanning are also covered which will help the Network Administrator design greater network security policies and successful incident response plans.

These skills will help the Network Administrators foster resiliency and continuity of operations during attacks.

COURSE OBJECTIVES

CND v2 is the first course in the new Vulnerability Assessment and Penetration Testing (VAPT) Track developed by EC-Council. EC-Council has added and removed domains to focus on a comprehensive approach to deal with current network security issues in the latest version. The course authenticates your understanding of critical and core concepts of network and information security.

CND Course Benefits:

- A dedicated focus on IoT security
- Network virtualization practices for the remote workforce
- Enhanced Cloud Security & IoT and Operational Technology (OT) Modules
- Introduction to threat intelligence
- In-depth Attack Surface Analysis



TARGET AUDIENCE

- Network Administrators
- Network security Administrators
- Network Security Engineer
- Network Defense Technicians
- CND Analyst
- Security Analyst
- Security Operator
- Anyone who involves in network operations

PRE-REQUISITES

Basic idea of networking and its components.



DURATION

40 hours

EXAM

Exam Title: Certified (ANSI)

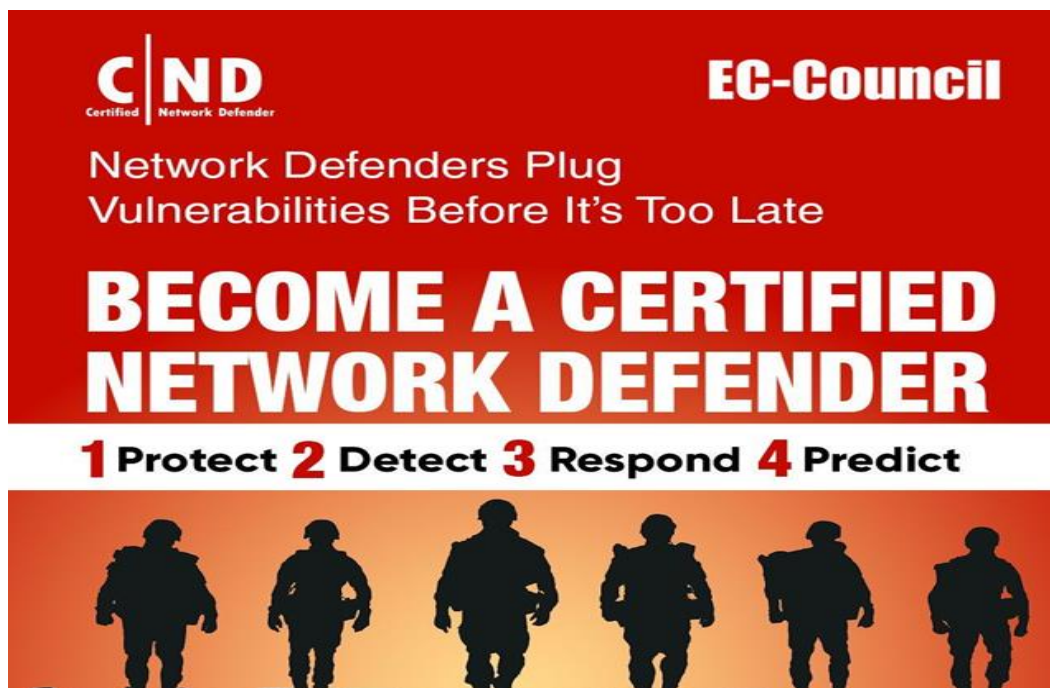
Number of Questions: 100

Duration: 4 hours

Test Format: Multiple Choice

Exam Prefix: 312-38

Passing Score: ANSI cut scores can range from 60% to 85% depending on form.



OUTLINE

Module 01: Network Attacks and Defense Strategies	Module 11: Enterprise Virtual Network Security
Module 02: Administrative Network Security	Module 12: Enterprise Cloud Network Security
Module 03: Technical Network Security	Module 13: Enterprise Wireless Network Security
Module 04: Network Perimeter Security	Module 14: Network Traffic Monitoring and Analysis
Module 05: Endpoint Security-Windows Systems	Module 15: Network Logs Monitoring and Analysis
Module 06: Endpoint Security-Linux Systems	Module 16: Incident Response and Forensic Investigation
Module 07: Endpoint Security- Mobile Devices	Module 17: Business Continuity and Disaster Recovery
Module 08: Endpoint Security-IoT Devices	Module 18: Risk Anticipation with Risk Management
Module 09: Administrative Application Security	Module 19: Threat Assessment with Attack Surface Analysis
Module 10: Data Security	Module 20: Threat Prediction with Cyber Threat Intelligence

EC-Council

EC-Council Certified Threat Intelligence Analyst v1

Certified Threat Intelligence Analyst (C|TIA) from EC-Council is a credentialing certification and training program. This highly valued certification has been exclusively devised in collaboration with threat intelligence and cybersecurity experts worldwide to empower organizations effectively to identify and mitigate security risks with extensive processing and analysis of available threat information.

The C|TIA is a specialist level training and certification that demonstrates security professionals the structured approach to acquiring threat intelligence. The C|TIA certified candidates attain a competitive edge over other information security professionals. This threat intelligence certification course delivers standards-based, intensive practical skills to the most essentially required threat intelligence across information security.



WHAT IS CTIA

Certified Threat Intelligence Analyst (CTIA) is designed and developed in collaboration with cybersecurity and threat intelligence experts across the globe to help organizations identify and mitigate business risks by converting unknown internal and external threats into known threats. It is a comprehensive, specialist-level program that teaches a structured approach for building effective threat intelligence.

In the ever-changing threat landscape, CTIA is an essential program for those who deal with cyber threats on a daily basis. Organizations today demand a professional-level cybersecurity threat intelligence analyst who can extract the intelligence from data by implementing various advanced strategies. Such professional-level programs can only be achieved when the core of the curricula maps with and is compliant to government and industry published threat intelligence frameworks.

COURSE OBJECTIVES

- Detailed understanding of threat intelligence and analysis
- Hands-on exposure to modern techniques and best practices
- Curriculum mapped to CTIA certification exam
- Certified instructors having several years of information security expertise
- Primary issues threatening the information security world
- Role of threat intelligence
- Implementing threat intelligence in risk management, incident response, and SIEM
- Cyber threats and threat factors
- Objectives of diverse cybersecurity attacks
- Basics of threat intel including types, capabilities, strategy, lifecycle, maturity model, and frameworks
- Implementing the cyber kill chain methodology
- Advanced Persistent Threat (APT) lifecycle
- Tactics, Techniques, and Procedures (TTPs)
- Indicators of Compromise (IOS) and the pyramid of pain
- Steps to Planning a threat intel program including taking requirements, planning, directing, and review
- Types of data feeds and methods to collect data
- Threat intelligence data collection by using Cyber Counterintelligence (CCI), Open Source Intelligence (OSINT), Human Intelligence (HUMINT), and Indicators of Compromise (IOS)
 - Bulk data collection, data structuring, processing, normalizing, sampling, storing, and creating visualizations
 - Types of data analysis techniques such as Statistical Data Analysis, Analysis Structured Analysis of Competing Hypotheses (SACH), and of Competing Hypotheses (ACH)
 - Threat analysis process including threat modeling, evaluation, fine-tuning, creating a knowledge base and runbook
- Threat intelligence dissemination, dissemination preferences
- Intelligence collaboration and Malware analysis
- Types of TI exchange and threat intelligence sharing formats
- Tools for threat intelligence, threat modeling, data analysis
- Disseminating threat intelligence and sharing protocols, dissemination preferences, sharing rules and models, intelligence collaboration
 - TI exchange architecture and types, sharing relationships
 - threat intelligence standards and formats for sharing
 - Threat intelligence reporting
 - Platforms and regulations to share operational, strategic, tactical, and technical intelligence

PRE-REQUISITES

Working experience of minimum 2 years in information security.

TARGET AUDIENCE

- Security professionals and ethical hackers
- Security Analysts and architects
- SOC professionals, cybersecurity forensic experts and malware analysts
- Security consultants and threat hunters

DURATION

24 hours

EXAM

Exam Title: Certified Threat Intelligence Analyst (ANSI)

Number of Questions: 50

Duration: 4 hours

Test Format: Multiple Choice

Exam Prefix: 312-85

Passing Score: 70%



 CERTIFIED THREAT INTELLIGENCE ANALYST		
What Is CJTIA Certified Threat Intelligence Analyst (CJTIA) is a brand-new threat intelligence training program that is designed and developed in collaboration with cybersecurity and threat intelligence experts across the globe to help organizations identify and mitigate various business risks by converting unknown internal and external threats into known threats. It is a comprehensive specialist-level program that teaches a structured approach for building effective threat intelligence. CJTIA is a method-driven course which gives a holistic approach covering vast concepts concerning organizational threat intelligence that are highly essential while building an effective threat intelligence that can secure organizations from future threats or attacks.	Course Content This program addresses all the stages involved in Threat Intelligence Life Cycle, and this attention towards the realistic and futuristic approach makes CJTIA one of the most comprehensive threat intelligence certifications on the market today. This program provides solid professional knowledge that is required for a career in threat intelligence, and it enhances your skills as a Threat Intelligence Analyst, increasing your employability.	Who Is it For? This program is designed for cybersecurity professionals, especially ethical hackers, security practitioners/engineers/analysts/specialist/architects/managers, threat intelligence analysts/associates/researchers/consultants, threat hunters, SOC professionals, digital forensic and malware analysts, and incident response team members. As well as any mid-level to high-level cybersecurity professionals with a minimum of 3-5 years of experience. Individuals from the information security profession and who want to enrich their skills and knowledge in the field of cyber threat intelligence and individuals interested in preventing cyber threats can also benefit from this program.
Why Become a CJTIA • Built in Compliance with the NICE and CREST Framework • Helps Increase Employability • Developed by SMEs • Follows a Detect, Respond, Defeat Methodology • Holistic Approach to Threat Intelligence • Helps Professionals Combat Cyber Threats	Course Information Course Duration: 3 Days (9:00 AM to 5:00 PM) or 24 hours Certification: The CJTIA exam can be challenged post the completion of attending the complete official CJTIA course. Candidates that successfully pass the exam will receive their CJTIA certificate and membership privileges. Members are required to adhere to the policies of EC-Council's Continuing Education Policy.	Exam Information • Exam Title: Certified Threat Intelligence Analyst • Exam Code: 312-85 • Number of Questions: 50 • Duration: 2 hours • Availability: EC-Council Exam Portal • Test Format: Multiple Choice • Passing Score: 70%
https://www.eccouncil.org/programs/certified-threat-intelligence-analyst/ For More Information on Certification: https://cert.eccouncil.org/application-process-eligibility.html		
EC-Council Hackers are here. Where are you?		

OUTLINE

Domain 1: Introduction to Threat Intelligence	Domain 4: Data Collection and Processing
Domain 2: Cyber Threats and Kill Chain Methodology	Domain 5: Data Analysis
Domain 3: Requirements, Planning, Direction, and Review	Domain 6: Dissemination and Reporting of Intelligence



EC-Council Certified Responsible AI Governance & Ethics (C|RAGE)

DESCRIPTION

C|RAGE is EC-Council's credential for professionals who lead AI governance, ethics and compliance. It covers oversight, risk management, regulatory alignment and accountability across the AI lifecycle, aligned with the NIST AI RMF and ISO/IEC 42001, with a focus on building audit-ready AI governance programs — highly relevant for the EU AI Act.

OUTLINE

Module 1. AI Foundations and Technology Ecosystem
Module 2. AI Concerns, Ethical Principles and Responsible AI
Module 3. AI Strategy and Planning
Module 4. AI Governance and Frameworks
Module 5. AI Regulatory Compliance
Module 6. AI Risk and Threat Management
Module 7. Third-Party AI Risk Management and Supply Chain Security
Module 8. AI Security Architecture and Controls
Module 9. Building Privacy, Trust and Safety in AI Systems
Module 10. AI Incident Response and Business Continuity
Module 11. AI Assurance, Testing and Auditing

TARGET AUDIENCE

- CISOs and Data Protection Officers
- GRC, risk and compliance professionals
- Privacy and data governance professionals
- Internal and technology auditors
- AI program managers

PRE-REQUISITES

- No technical AI experience required
- Familiarity with governance, risk or compliance concepts recommended

DURATION

Approximately 10 hours of instruction (live online, in-person or on-demand)

EXAM

Certification exam administered by EC-Council (see cert.eccouncil.org for current exam details).

Official EC-Council course delivered by ScorpionShield, EC-Council Accredited Training Center (ATC).



EC-Council Certified Offensive AI Security Professional (C|OASP)

DESCRIPTION

C|OASP is EC-Council's hands-on offensive AI security certification for professionals who red-team LLMs, exploit AI agents and pipelines, and build defences against those attacks. Aligned with MITRE ATLAS and the OWASP Top 10 for LLM Applications, it includes 30 lab exercises, 20+ offensive AI techniques and 20+ testing tools.

OUTLINE

Module 1. Offensive AI and AI System Hacking Methodology
Module 2. AI Reconnaissance and Attack Surface Mapping
Module 3. AI Vulnerability Scanning and Fuzzing
Module 4. Prompt Injection and LLM Application Attacks
Module 5. Adversarial Machine Learning and Model Privacy Attacks
Module 6. Data and Training Pipeline Attacks
Module 7. Agentic AI and Model-to-Model Attacks
Module 8. AI Infrastructure and Supply Chain Attacks
Module 9. AI Security Testing, Evaluation and Hardening
Module 10. AI Incident Response and Forensics

TARGET AUDIENCE

- Penetration testers and red team operators
- SOC, detection and incident response analysts
- AI/ML, GenAI and DevSecOps engineers
- AI security architects

PRE-REQUISITES

- Foundational cybersecurity knowledge (not a beginner course)

DURATION

Approximately 9 hours of instruction, plus 6 months of lab access

EXAM

Exam Title: Certified Offensive AI Security Professional

Number of Questions: 70 (65 multiple choice + 5 practical challenges)

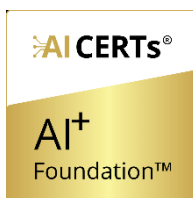
Duration: 6 hours, live-proctored

Test Format: Multiple choice and practical assessment

Exam Provider: EC-Council

Passing Score: As defined by EC-Council

Official EC-Council course delivered by ScorpionShield, EC-Council Accredited Training Center (ATC).



AI+ Foundation™ (AF-101)

DESCRIPTION

A beginner-friendly introduction to artificial intelligence: core principles, practical tools, real-world applications and ethics. Participants learn how AI works, how to interact with it through effective prompts and how it is reshaping business, work and careers, with hands-on activities in every module.

OUTLINE

Module 1. Introduction to AI and Its Impact
Module 2. Prompt Engineering: Interacting with AI
Module 3. AI in Business and Industry Applications
Module 4. AI Ethics and Bias
Module 5. The Future of AI and Career Opportunities
Module 6. Optional: AI Agents for Foundation

TARGET AUDIENCE

- Business professionals
- AI enthusiasts
- Technology leaders
- Ethics professionals
- Students and new graduates

PRE-REQUISITES

- Basic familiarity with using technology
- Curiosity about AI applications across industries
- No prior AI knowledge required

DURATION

4 hours

EXAM

Exam Title: AI+ Foundation™

Number of Questions: 50 (multiple choice / multiple response)

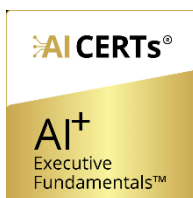
Duration: 90 minutes

Test Format: Online, proctored

Exam Provider: AI CERTs®

Passing Score: 70% (35/50)

Official AI CERTs® course delivered by ScorpionShield, AI CERTs® Authorized Training Partner in Portugal.



AI+ Executive Fundamentals™ (AC-110)

DESCRIPTION

Designed for business leaders who want to use AI strategically. The course covers AI fundamentals, business applications, ethical and legal considerations, and how to lead organisational change and manage AI projects, ending with an interactive workshop.

OUTLINE

Module 1. Understanding Artificial Intelligence
Module 2. AI Technologies and Business Implications
Module 3. AI Strategy for Executives
Module 4. Ethical, Legal and Societal Considerations
Module 5. Managing AI Projects
Module 6. AI and the Future of Work
Module 7. Department-Specific AI Applications
Module 8. Interactive Workshop

TARGET AUDIENCE

- Business leaders and executives
- IT managers
- Technology consultants
- Data scientists and analysts

PRE-REQUISITES

- Business awareness
- Comfort with technology
- Openness to AI-driven decision-making

DURATION

8 hours (1 day)

EXAM

Exam Title: AI+ Executive Fundamentals™

Number of Questions: 50 (multiple choice / multiple response)

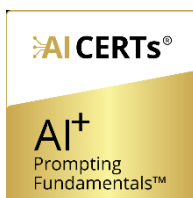
Duration: 90 minutes

Test Format: Online, proctored

Exam Provider: AI CERTs®

Passing Score: 70% (35/50)

Official AI CERTs® course delivered by ScorpionShield, AI CERTs® Authorized Training Partner in Portugal.



AI+ Prompting Fundamentals™ (AC-130)

DESCRIPTION

Covers core AI concepts such as machine learning, natural language processing and neural networks, then focuses on designing, refining and troubleshooting prompts. Participants work hands-on with leading text and image models and address AI ethics, privacy and regulatory compliance.

OUTLINE

Module 1. Foundations of AI and Prompt Engineering
Module 2. Principles of Effective Prompting
Module 3. Introduction to AI Tools and Models
Module 4. Mastering Prompt Engineering Techniques
Module 5. Mastering Image Model Techniques
Module 6. Project-Based Learning Session
Module 7. Ethical Considerations and the Future of AI

TARGET AUDIENCE

- Business leaders and strategists
- Data scientists and analysts
- Developers and programmers
- Research scientists

PRE-REQUISITES

- Basic understanding of AI and how it is used
- No technical skills required

DURATION

8 hours (1 day)

EXAM

Exam Title: AI+ Prompting Fundamentals™

Number of Questions: 50 (multiple choice / multiple response)

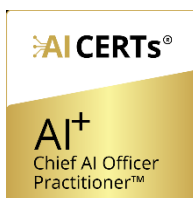
Duration: 90 minutes

Test Format: Online, proctored

Exam Provider: AI CERTs®

Passing Score: 70% (35/50)

Official AI CERTs® course delivered by ScorpionShield, AI CERTs® Authorized Training Partner in Portugal.



AI+ Chief AI Officer Practitioner™ (AP-910)

DESCRIPTION

Prepares C-suite executives to lead AI-driven innovation: building a strategic AI roadmap, assembling high-performance AI teams, governing AI risk and ethics, and driving organisation-wide adoption, with a capstone project that applies the concepts to a real business context.

OUTLINE

Module 1. Foundations of AI and Leadership in the Digital Era
Module 2. Crafting a Strategic AI Roadmap
Module 3. Building a High-Performance AI Team
Module 4. Ethics in AI Governance and Risk Management
Module 5. Data-Driven Decision-Making and Business Impact Assessment
Module 6. Driving Organisation-Wide Adoption of AI
Module 7. Leveraging Generative AI for Business Innovation
Module 8. Capstone Project

TARGET AUDIENCE

- CTOs, CIOs and CDOs
- CEOs and founders
- COOs and operations executives
- Senior managers preparing for AI leadership roles

PRE-REQUISITES

- Basic understanding of business management
- Experience in a leadership or business administration role
- Familiarity with fundamental AI concepts (recommended)

DURATION

8 hours (1 day)

EXAM

Exam Title: AI+ Chief AI Officer Practitioner™

Number of Questions: 50 (multiple choice / multiple response)

Duration: 90 minutes

Test Format: Online, proctored

Exam Provider: AI CERTs®

Passing Score: 70% (35/50)

Official AI CERTs® course delivered by ScorpionShield, AI CERTs® Authorized Training Partner in Portugal.



Executive Introduction to RSAIF DESCRIPTION

An executive primer on AI governance, security and compliance based on the RSAIF framework, co-developed by AI CERTs® and the Cyber Future Foundation. It helps leaders oversee AI initiatives that are responsible, transparent and secure, with attention to risk management and regulations such as the GDPR and the EU AI Act.

OUTLINE

Module 1. AI Security Frameworks: Safeguarding AI Systems Across Industries
Module 2. Simplifying AI Governance
Module 3. The Executive's Role in AI Security
Module 4. Understanding the RSAIF MOSAIC Framework
Module 5. Governance, Oversight and Compliance
Module 6. Identifying AI Risks and Red Flags
Module 7. Learning from Real-World Successes and Failures

TARGET AUDIENCE

- C-suite executives (CEO, CTO, CIO)
- CISOs and IT security leaders
- Risk and compliance managers
- Policy makers
- AI project managers

PRE-REQUISITES

- None required
- A basic understanding of AI governance and security is recommended

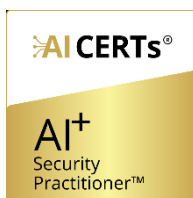
DURATION

4 hours

CERTIFICATION

Certificate of completion issued by AI CERTs®.

Official AI CERTs® course delivered by ScorpionShield, AI CERTs® Authorized Training Partner in Portugal.



AI+ Security Practitioner™ (AT-2101)

DESCRIPTION

Covers AI-driven cybersecurity from the ground up: security principles, threats and controls in AI-enabled environments, AI for threat detection and hunting, LLM security and offensive testing of AI systems. Aimed at entry-level to intermediate cybersecurity roles, with scenario-based exercises and hands-on projects.

OUTLINE

Module 1. Computing, Linux and Operating System Foundations
Module 2. Networking Fundamentals and Traffic Analysis
Module 3. Python for Security and Automation
Module 4. Cybersecurity Foundations and Threat Landscape
Module 5. Cryptography, Authentication and Identity Security
Module 6. Introduction to AI and Machine Learning
Module 7. AI Applied to Security Detection and Threat Hunting
Module 8. AI Security, LLM Security and Responsible AI
Module 9. Offensive Security for AI Systems
Module 10. Security Operations, Incident Response and Malware Analysis

TARGET AUDIENCE

- Cybersecurity professionals and security analysts
- IT, network and system administrators
- Risk and compliance professionals
- Ethical hackers and security researchers

PRE-REQUISITES

- Basic cybersecurity and networking knowledge
- Basic AI knowledge
- Basic programming skills

DURATION

40 hours (5 days)

EXAM

Exam Title: AI+ Security Practitioner™

Number of Questions: 50 (multiple choice)

Duration: 90 minutes

Test Format: Online, proctored

Exam Provider: AI CERTs®

Passing Score: 70% (35/50)

Official AI CERTs® course delivered by ScorpionShield, AI CERTs® Authorized Training Partner in Portugal.



AI+ Security Expert™ (AT-2102)

DESCRIPTION

An intermediate credential focused on securing AI applications: AI threat modelling, GenAI security controls, prompt injection and adversarial testing, RAG and model pipeline security, secure cloud and API deployment, and AI security monitoring, incident response and governance.

OUTLINE

Module 1. AI Security Context, Scope and Opportunities
Module 2. AI Application Architecture and Threat Modelling
Module 3. Applied Python Automation for AI Security Evidence
Module 4. GenAI Application Security Controls
Module 5. Prompt Injection, LLM Risk Testing and Adversarial Attacks
Module 6. RAG and Knowledge System Security
Module 7. AI Data, Model, ML Pipeline and Detection Security
Module 8. Secure AI Deployment: Cloud, API and Identity
Module 9. AI Security Monitoring and Incident Response
Module 10. AI Governance, Privacy and Compliance

TARGET AUDIENCE

- Cybersecurity professionals
- Cloud architects and engineers
- Software developers
- Security consultants and risk specialists

PRE-REQUISITES

- Basic understanding of cybersecurity concepts and practices
- Familiarity with AI and machine learning fundamentals
- Knowledge of cloud computing and application security

DURATION

40 hours (5 days)

EXAM

Exam Title: AI+ Security Expert™

Number of Questions: 50 (multiple choice)

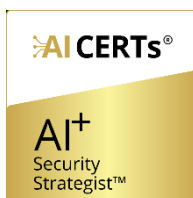
Duration: 90 minutes

Test Format: Online, proctored

Exam Provider: AI CERTs®

Passing Score: 70% (35/50)

Official AI CERTs® course delivered by ScorpionShield, AI CERTs® Authorized Training Partner in Portugal.



AI+ Security Strategist™ (AT-2103)

DESCRIPTION

An advanced certification on AI-driven cybersecurity strategy and engineering: machine learning and deep learning for threat detection, adversarial AI, AI for network, endpoint, cloud and identity security, and secure AI system engineering in complex enterprise environments.

OUTLINE

Module 1. Foundations of AI and ML for Security Engineering
Module 2. ML for Threat Detection and Response
Module 3. Deep Learning for Security Applications
Module 4. Adversarial AI in Security
Module 5. AI in Network Security
Module 6. AI in Endpoint Security
Module 7. Secure AI System Engineering
Module 8. AI for Cloud and Container Security
Module 9. AI and Blockchain for Security
Module 10. AI in Identity and Access Management (IAM)

TARGET AUDIENCE

- Security architects and IT managers
- Cybersecurity and risk management specialists
- Ethical hackers and penetration testers
- Aspiring AI security experts

PRE-REQUISITES

- AI+ Security Practitioner™ and AI+ Security Compliance Practitioner™ (recommended)
- Intermediate to advanced Python, including TensorFlow or PyTorch
- Advanced cybersecurity and Linux skills

DURATION

40 hours (5 days)

EXAM

Exam Title: AI+ Security Strategist™

Number of Questions: 50 (multiple choice)

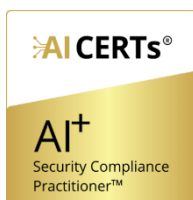
Duration: 90 minutes

Test Format: Online, proctored

Exam Provider: AI CERTs®

Passing Score: 70% (35/50)

Official AI CERTs® course delivered by ScorpionShield, AI CERTs® Authorized Training Partner in Portugal.



AI+ Security Compliance Practitioner™ (AT-230)

DESCRIPTION

Combines cybersecurity compliance fundamentals with practical AI applications: using AI to interpret security standards, assess risk and compliance gaps, manage policies, controls and evidence, oversee third parties and support monitoring and audits — highly relevant for NIS2, DORA and ISO/IEC 27001 programmes.

OUTLINE

Module 1. Foundations of AI-Enabled Security Compliance
Module 2. Using AI to Interpret Security Standards and Requirements
Module 3. AI-Assisted Security Risk and Compliance Gap Assessment
Module 4. AI for Security Policy and Procedure Management
Module 5. AI for Control Implementation and Evidence Management
Module 6. AI for Third-Party Security Compliance
Module 7. AI for Compliance Monitoring, Incident Management and Auditing
Module 8. AI-Powered Security Compliance Programme and Capstone

TARGET AUDIENCE

- Compliance officers
- Risk management specialists
- IT security analysts
- Cybersecurity and audit professionals

PRE-REQUISITES

- Basic cybersecurity knowledge
- Familiarity with standards, policies, audits and risk management
- Introductory AI knowledge, including generative AI

DURATION

40 hours (5 days)

EXAM

Exam Title: AI+ Security Compliance Practitioner™

Number of Questions: 50 (multiple choice)

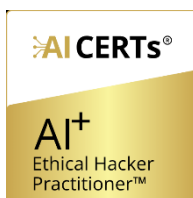
Duration: 90 minutes

Test Format: Online, proctored

Exam Provider: AI CERTs®

Passing Score: 70% (35/50)

Official AI CERTs® course delivered by ScorpionShield, AI CERTs® Authorized Training Partner in Portugal.



AI+ Ethical Hacker Practitioner™ (AT-220)

DESCRIPTION

Applies AI techniques to ethical hacking across offensive testing and defence: AI-enhanced reconnaissance and attack-surface mapping, AI-assisted penetration testing of web, API, cloud and AI applications, adversarial machine learning, AI-driven SOC operations and incident response.

OUTLINE

Module 1. Cybersecurity, Ethical Hacking and AI Foundations
Module 2. Networking, Linux, Web Technologies and Reconnaissance
Module 3. AI-Enhanced Reconnaissance and Attack Surface Mapping
Module 4. Vulnerability Assessment and Risk Prioritisation
Module 5. AI-Assisted Penetration Testing
Module 6. LLM, RAG and AI Application Security
Module 7. Machine Learning for Cybersecurity and Adversarial AI
Module 8. Threat Hunting, Detection Engineering and AI-Driven SOC Operations
Module 9. Incident Response, Digital Forensics and AI-Assisted Investigations
Module 10. Identity Security, Zero Trust and Cloud Security

TARGET AUDIENCE

- Ethical hackers and penetration testers
- Cybersecurity professionals
- Technology leaders and decision makers
- Aspiring cybersecurity students

PRE-REQUISITES

- Basic programming or scripting (e.g. Python)
- Networking and cybersecurity fundamentals
- Familiarity with Windows, Linux and web technologies

DURATION

40 hours (5 days)

EXAM

Exam Title: AI+ Ethical Hacker Practitioner™

Number of Questions: 50 (multiple choice)

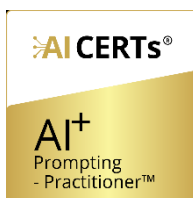
Duration: 90 minutes

Test Format: Online, proctored

Exam Provider: AI CERTs®

Passing Score: 70% (35/50)

Official AI CERTs® course delivered by ScorpionShield, AI CERTs® Authorized Training Partner in Portugal.



AI+ Prompting Practitioner™ (AC-1302)

DESCRIPTION

Teaches developers to design, refine and optimise prompts across AI applications, from advanced prompt design and experimentation to integration with development tools, combining hands-on labs, real-world case studies and project-based learning.

OUTLINE

Module 1. Introduction to Prompt Engineering for Developers
Module 2. Advanced Prompt Design and Engineering
Module 3. Experimentation and Optimisation
Module 4. Designing Advanced Strategies for Prompt Engineering
Module 5. Integration with Development Tools
Module 6. Applications of Prompt Engineering in Various Domains
Module 7. Project-Based Learning: Real-World AI Projects

TARGET AUDIENCE

- AI developers
- Tech professionals and AI practitioners
- Machine learning enthusiasts
- Students and new graduates

PRE-REQUISITES

- Familiarity with at least one programming language (Python recommended)
- Basic knowledge of REST services and APIs
- Basic understanding of AI concepts and language models

DURATION

40 hours (5 days)

EXAM

Exam Title: AI+ Prompting Practitioner™

Number of Questions: 50 (multiple choice / multiple response)

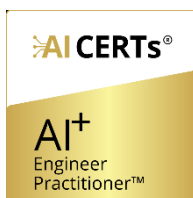
Duration: 90 minutes

Test Format: Online, proctored

Exam Provider: AI CERTs®

Passing Score: 70% (35/50)

Official AI CERTs® course delivered by ScorpionShield, AI CERTs® Authorized Training Partner in Portugal.



AI+ Engineer Practitioner™ (AT-330)

DESCRIPTION

Covers the full AI engineering stack — AI architecture, neural networks, large language models, generative AI and natural language processing — with hands-on transfer learning using Hugging Face, GUI design for AI solutions and deployment pipelines for scalable AI systems.

OUTLINE

Module 1. Foundations of Artificial Intelligence
Module 2. Introduction to AI Architecture
Module 3. Fundamentals of Neural Networks
Module 4. Applications of Neural Networks
Module 5. Significance of Large Language Models (LLM)
Module 6. Application of Generative AI
Module 7. Natural Language Processing
Module 8. Transfer Learning with Hugging Face
Module 9. Crafting Sophisticated GUIs for AI Solutions
Module 10. AI Communication and Deployment Pipeline

TARGET AUDIENCE

- AI and software engineers
- Data scientists
- IT specialists and system architects
- Students and new graduates

PRE-REQUISITES

- Basic Python programming (mandatory)
- Basic mathematics and computer science fundamentals
- AI+ Data Practitioner™ or AI+ Developer Practitioner™ (recommended)

DURATION

40 hours (5 days)

EXAM

Exam Title: AI+ Engineer Practitioner™

Number of Questions: 50 (multiple choice / multiple response)

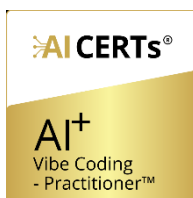
Duration: 90 minutes

Test Format: Online, proctored

Exam Provider: AI CERTs®

Passing Score: 70% (35/50)

Official AI CERTs® course delivered by ScorpionShield, AI CERTs® Authorized Training Partner in Portugal.



AI+ Vibe Coding Practitioner™ (AP-111)

DESCRIPTION

A beginner-friendly programme on AI-assisted coding: core programming concepts, AI coding tools, prompting for code, debugging and testing with AI, and building a simple full-stack application, with attention to code ethics, security and the limits of AI.

OUTLINE

Module 1. Introduction to Vibe Coding and AI Tools
Module 2. Prompting for Code: Basics and Best Practices
Module 3. Debugging and Testing via AI
Module 4. Building a Simple Full-Stack App with Prompts
Module 5. Code Ethics, Security and AI Limits
Module 6. Capstone Project: Prompt-Driven App

TARGET AUDIENCE

- Aspiring programmers and career switchers
- Entrepreneurs and creators
- Tech enthusiasts
- Students and graduates

PRE-REQUISITES

- Basic computer skills
- Logical thinking
- Curiosity about programming

DURATION

8 hours (1 day)

EXAM

Exam Title: AI+ Vibe Coding Practitioner™

Number of Questions: 50 (multiple choice / multiple response)

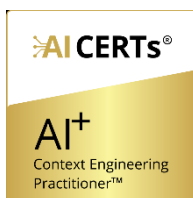
Duration: 90 minutes

Test Format: Online, proctored

Exam Provider: AI CERTs®

Passing Score: 70% (35/50)

Official AI CERTs® course delivered by ScorpionShield, AI CERTs® Authorized Training Partner in Portugal.



AI+ Context Engineering Practitioner™ (AP-3309)

DESCRIPTION

Teaches how to design the instructions, memory, retrieval, tools and multi-agent workflows that make AI systems reliable in production, including RAG and grounding architectures, cost control, scaling and security for enterprise and regulated environments.

OUTLINE

Module 1. Foundations of Context Engineering
Module 2. Context Management Patterns and Techniques
Module 3. Context Pipelines, RAG and Grounding Architecture
Module 4. Optimisation, Scaling and Enterprise Readiness
Module 5. Context Flow Design for Business Users (No-Code AI)
Module 6. Real-World Industry Context Applications
Module 7. Multi-Agent Orchestration and the Future
Module 8. Capstone Project

TARGET AUDIENCE

- AI engineers and LLM developers
- AI and solution architects
- Product managers and technical leaders
- Data and platform engineers

PRE-REQUISITES

- Basic programming knowledge (e.g. Python)
- Understanding of AI and machine learning concepts
- Familiarity with cloud platforms

DURATION

8 hours (1 day)

EXAM

Exam Title: AI+ Context Engineering Practitioner™

Number of Questions: 50 (multiple choice / multiple response)

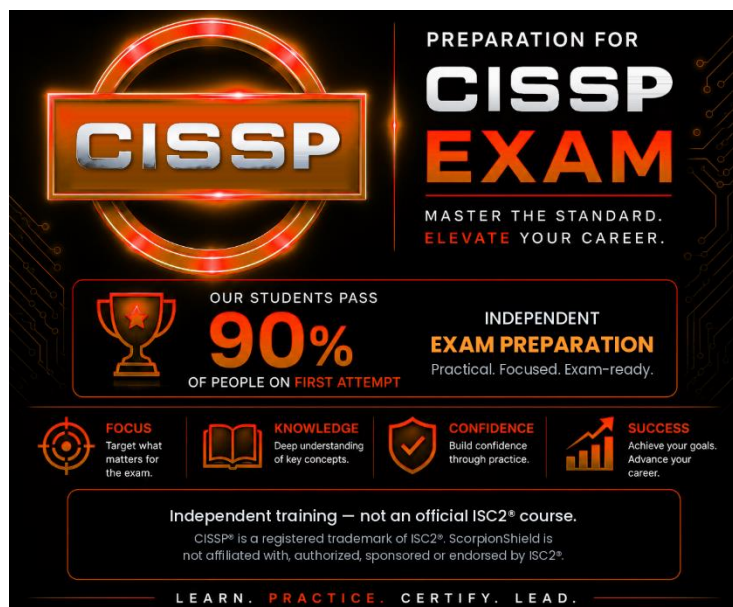
Duration: 90 minutes

Test Format: Online, proctored

Exam Provider: AI CERTs®

Passing Score: 70% (35/50)

Official AI CERTs® course delivered by ScorpionShield, AI CERTs® Authorized Training Partner in Portugal.



CISSP® EXAM PREPARATION

ScorpionShield's independent CISSP® exam preparation course is for experienced security practitioners, architects, managers and consultants who want to prove broad, in-depth expertise in information security. The CISSP® (Certified Information Systems Security Professional) is one of the most widely recognised certifications in the information security market.

The course covers the eight domains of the CISSP® Common Body of Knowledge through practical sessions, exam-style questions and real-world scenarios, so that participants learn to design, implement and manage an enterprise security program with a managerial, risk-based mindset and arrive at the exam well prepared.

WHAT IS CISSP

CISSP® – a leading global cybersecurity certification

Accelerate cybersecurity career with the CISSP certification. Earning the CISSP proves having what it takes to effectively design, implement and manage a best-in-class cybersecurity program.

Holding the CISSP® validates expertise across all eight domains of the CISSP® Common Body of Knowledge and is widely recognised by employers worldwide.

Proving skills, advancing career, gain the support of a community of cybersecurity leaders here to support throughout the career.

COURSE OBJECTIVES

- Relate confidentiality, integrity, availability, non-repudiation, authenticity, privacy and safety to due care and due diligence
- Identify and select security assessment approaches, frameworks and standards
- Relate information security governance to organizational business strategies, goals, missions and objectives
- Identify the different types and categories of information security controls and their use.

- Compare and contrast the security operations characteristics of different types of governance and administrative controls
- Develop incident response policies and plans. Link incident response to needs for security controls and their operational use
- Understand internal, external and third party assessment and testing
- Explain how governance frameworks and processes relate to the operational use of information security controls

TARGET AUDIENCE

- Chief Information Security Officer
- Chief Information Officer
- Director of Security
- IT Director/Manager
- Security Systems Engineer
- Security Analyst
- Security Manager
- Security Auditor
- Security Architect
- Security Consultant
- Network Architect

PRE-REQUISITES

- Practicing security, ICT professional or anyone that has the necessary IT qualifications that wants to enter the field of Information Security
- Below are the certification requirements, if you are taking the course just for knowledge, it is not mandatory to possess the below requirements
 - Candidates must have a minimum of 5 years cumulative work experience in 2 or more of the 8 domains of the CISSP CBK
 - Earning a 4-year college degree or regional equivalent or an additional credential from the ISC2 approved list will satisfy 1 year of the required experience
 - Education credit will only satisfy 1 year of experience.
 - A candidate that doesn't have the required experience to become a CISSP may become an Associate of ISC2 by successfully passing the CISSP examination
 - The Associate of ISC2 will then have 6 years to earn the 5 years required experience

DURATION

45 hours

EXAM

Exam Title: Certified Information Systems Security Professional

Number of Questions: 100–150 (Computerized Adaptive Testing)

Duration: 3 hours

Test Format: Multiple Choice

Exam Provider: ISC2® (delivered via Pearson VUE)

Passing Score: 700/1000

OUTLINE

Domain 1. Security and Risk Management	Domain 5. Identity and Access Management (IAM)
Domain 2. Asset Security	Domain 6. Security Assessment and Testing
Domain 3. Security Architecture and Engineering	Domain 7. Security Operations
Domain 4. Communication and Network Security	Domain 8. Software Development Security

Independent training, not an official ISC2® course. CISSP® is a registered trademark of ISC2®. ScorpionShield is not affiliated with, authorised, sponsored or endorsed by ISC2®.



PREPARATION FOR CISM EXAM

MASTER THE STANDARD. ELEVATE YOUR CAREER.

OUR STUDENTS PASS **90%** OF PEOPLE ON FIRST ATTEMPT

INDEPENDENT EXAM PREPARATION
Practical. Focused. Exam-ready.

FOCUS Target what matters for the exam.

KNOWLEDGE Deep understanding of key concepts.

CONFIDENCE Build confidence through practice.

SUCCESS Achieve your goals. Advance your career.

Independent training — not an official ISACA® course.
CISA® and CISM® are registered trademarks of ISACA®. ScorpionShield is not affiliated with, authorized, sponsored or endorsed by ISACA®.

LEARN. PRACTICE. CERTIFY. LEAD.

CISM® EXAM PREPARATION

CISM® (Certified Information Security Manager) is a globally recognised certification for information security professionals who manage, implement, monitor and assess information security in an organisation. ScorpionShield's independent CISM® exam preparation course covers the four exam domains: information security governance, information security risk management, the information security program and incident management. The course includes discussions, domain-specific exercises and a mock exam to prepare participants for the CISM® certification exam.

WHAT IS CISM

The Certified Information Security Manager is for information security professionals and managers who want to gain the knowledge and skills to oversee, design, or assess an information security program within an organization.

OUTLINE

Information security governance
Information security risk management
Information security program
Incident management

TARGET AUDIENCE

The target audience for the Certified Information Security Manager (CISM) certification typically includes:

- Information Security Managers: Who oversee and manage a company's information security systems.
- IT and Corporate Security Managers: Professionals responsible for managing and aligning information technology and corporate security.
- IS/IT Consultants: Who advise organizations on information security strategies and implementations.
- Risk Officers: Who assess and mitigate risks related to information security within an organization.

- Auditors: IT auditors who need to understand the workings of information security systems as part of their audit responsibilities.

PRE-REQUISITES

Not every IT professional can take the exam. Someone who aspires to be CISM-certified must have 5 years of experience in information security, with at least 3 years of information security management experience in 3 or more of the CISM domains mentioned above. Moreover, the experience should be gained within 10 years before the application date or within 5 years after passing the exam. After passing the exam, applicants can then apply for CISM certification within 5 years.

DURATION

24 hours

EXAM

Exam Title: Certified Information Security Manager

Number of Questions: 150

Duration: 4 hours

Test Format: Multiple Choice

Exam Provider: ISACA®

Passing Score: 450 /800

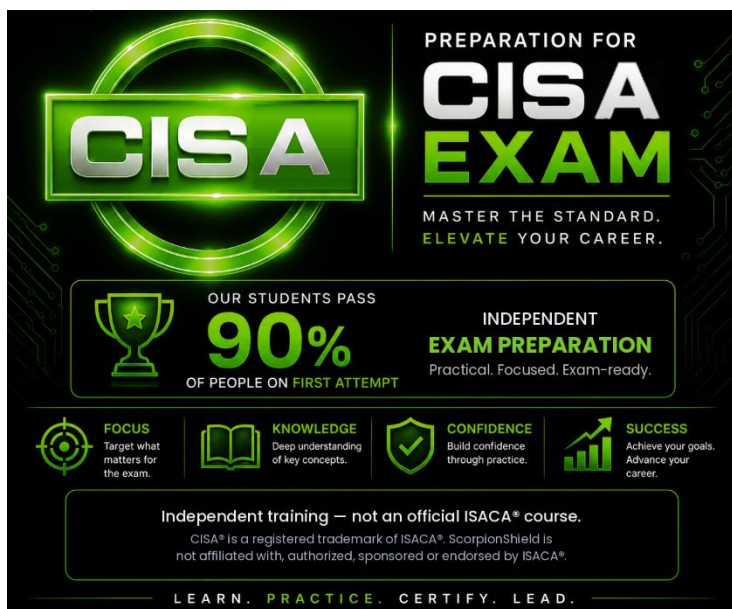
CERTIFICATION

To earn the CISM® certification, candidates must complete these key steps:

- Pass the CISM Exam: Demonstrate your knowledge in information security management by passing the rigorous CISM exam.
- Agree to the Code of Ethics: Commit to adhering to ISACA®'s Code of Professional Ethics to ensure professionalism and continuous proficiency in information security.
- Complete Continuing Education: Fulfill ISACA®'s requirement of 20 hours of Continuing Professional Education (CPE) annually, and 120 hours every 3 years, to maintain up-to-date knowledge in the field.
- Verify Work Experience: Provide proof of at least five years of information security work experience, including at least three years in information security management, gained within the ten years before applying or within five years after passing the exam.
- Substitute Work Experience: Up to two years of the experience requirement can be substituted, for example by holding CISA® or CISSP®, or by a postgraduate degree in information security or a related field.
- Apply for Certification: Once all requirements are met, including the experience criteria with or without substitutions, submit application to ISACA® for verification and approval to receive CISM certification.

This streamlined process ensures that CISM holders have the necessary expertise and experience to manage, design, and oversee their organizations' information security.

Independent training, not an official ISACA® course. CISM® is a registered trademark of ISACA®. ScorpionShield is not affiliated with, authorised, sponsored or endorsed by ISACA®.



CISA

PREPARATION FOR
CISA EXAM

MASTER THE STANDARD.
ELEVATE YOUR CAREER.

OUR STUDENTS PASS
90%
OF PEOPLE ON FIRST ATTEMPT

INDEPENDENT
EXAM PREPARATION
Practical. Focused. Exam-ready.

FOCUS
Target what matters for the exam.

KNOWLEDGE
Deep understanding of key concepts.

CONFIDENCE
Build confidence through practice.

SUCCESS
Achieve your goals. Advance your career.

Independent training — not an official ISACA® course.
CISA® is a registered trademark of ISACA®. ScorpionShield is not affiliated with, authorized, sponsored or endorsed by ISACA®.

LEARN. PRACTICE. CERTIFY. LEAD.

CISA® EXAM PREPARATION

The CISA® (Certified Information Systems Auditor) is a globally recognised certification for professionals in information systems audit, control, assurance and security. ScorpionShield's independent CISA® exam preparation course gets candidates ready for the exam through structured coverage of the five domains, practical exercises and exam-style questions.

WHAT IS CISA

The Certified Information Systems Auditor is for professionals who audit, control, monitor, and assess an organization's information technology and business systems.

OUTLINE

Information System Auditing Process
Governance and Management of IT
Information Systems Acquisition, Development, and Implementation
Information Systems Operations and Business Resilience
Protection of Information Assets

TARGET AUDIENCE

The target audience for the Certified Information Systems Auditor (CISA) certification typically includes:

- IS/IT Auditors: Professionals responsible for auditing information technology and business systems to ensure they are secure, controlled, and effective.
- IT Compliance Managers: Those tasked with ensuring that IT systems comply with regulatory and organizational standards and procedures.
- Chief Compliance Officers: Executives who oversee compliance issues within an organization, particularly concerning IT and security compliance.

- Chief Risk & Privacy Officers: Senior executives responsible for managing risks and ensuring the privacy of information within an organization.
- Security Heads: Professionals who lead security efforts and manage the overall security posture of the organization.

PRE-REQUISITES

Not every IT professional can take the exam. Aspiring CISA-certified individuals must have 5 years of experience in auditing, controlling, or securing information systems, with waivers available for certain educational or professional qualifications. The relevant experience must be obtained within 10 years prior to the application date or within five years from the date of passing the exam.

DURATION

24 hours

EXAM

Exam Title: Certified Information Systems Auditor

Number of Questions: 150

Duration: 4 hours

Test Format: Multiple Choice

Exam Provider: ISACA®

Passing Score: 450 /800

CERTIFICATION

To earn the CISA® certification, candidates must complete these key steps:

- Pass the CISA Exam: Demonstrate your expertise in information systems auditing by successfully passing the rigorous CISA exam.
- Agree to the Code of Ethics: Commit to adhering to ISACA®'s Code of Professional Ethics to ensure professionalism and continuous proficiency in information systems auditing.
- Complete Continuing Education: Fulfill ISACA®'s requirement of 20 hours of Continuing Professional Education (CPE) annually, and 120 hours every 3 years, to maintain up-to-date knowledge in the field.
- Verify Work Experience: Provide proof of at least five years of work experience in information systems audit, control, assurance or security, gained within the ten years before applying or within five years after passing the exam.
- Substitute Work Experience: Up to three years of the experience requirement can be substituted, for example by one year of information systems or non-IS audit experience, a university degree (one or two years, depending on the degree), or a master's degree in information security or IT (one year).
- Apply for Certification: Once all requirements are met, including the experience criteria with or without substitutions, submit your application to ISACA® for verification and approval to receive your CISA certification.

This process ensures that CISA certification holders are highly qualified in the areas of IS audit, control, and security, making them valuable assets to any organization.

Independent training, not an official ISACA® course. CISA® is a registered trademark of ISACA®. ScorpionShield is not affiliated with, authorised, sponsored or endorsed by ISACA®.



SCORPIONSHIELD
FOR A CYBER SECURED WORLD