SCORPIONSHIELD ACADEMY

INFORMATION SECURITY AND CYBERSECURITY

ABOUNT 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 ISACA

ISACA is an international professional association focused on IT (information technology) governance. It is known as the Information Systems Audit and Control Association, although ISACA now goes by its acronym only. ISACA currently offers 8 certification programs as well as other micro-certificates.

ABOUT SCORPIONSHIELD AND ISACA

SCORPIONSHIELD is an **ISACA Accredited Training Organization (ATO)**, and an **APMG International Certified** for providing two certified courses: CISM and CISA. Certified Information Security Manager (CISM) is targeted for Information Security middle Managers and Certified Chief Information Security Officers (CISOs). And Certified Information Systems Auditor (CISA) is targeted for auditors in the Information Security field. While the CISA qualification is aimed at professionals involved in auditing and assurance of information systems, the CISM certification is better suited for those involved in information security management and strategy.

ABOUT (ISC)2

The International Information System Security Certification Consortium, or (ISC)2, is a non-profit organization which specializes in training and certifications for cybersecurity professionals. The most widely known certification offered by (ISC)2 is the Certified Information Systems Security Professional (CISSP) certification, which is considered one of the most difficult certification exams in the world of information security and cybersecurity, directed to CISO's Certified Chief Information Security Officers and Middle Managers. Also, the CC Certified in Cybersecurity course, is a newly popular entry level for starters in Cybersecurity.

EC-Council Certified Chief Information Security Officer v3

DESCRIPTION

EC-Council's CCISO Program has certified leading information security professionals around the world. The CCISO Advisory Board contributed by forming the foundation of the program and outlining the content that would be covered by the exam, body of knowledge and training. Some members of the Board contributed as authors, others as exam writers, others as quality assurance checks and still others as trainers. Each segment of the program was developed with the aspiring CISO in mind and looks to transfer the knowledge of seasoned professionals to the next generation in the areas that are most critical in the development and maintenance of a successful information security program. The Certified CISO (CCISO) program is the first of its kind training and certification program aimed at producing top-level information security executives.

The CCISO does not focus solely on technical knowledge but on the application of information security management principles from an executive management point of view. The program was developed by sitting CISOs for current and aspiring CISOs. In order to sit for the CCISO exam and earn the certification, candidates must meet the basic CCISO requirements. Candidates who do not yet meet the CCISO requirements but are interested in information security management can pursue EC-COUNCIL Information Security Management (EISM) certification
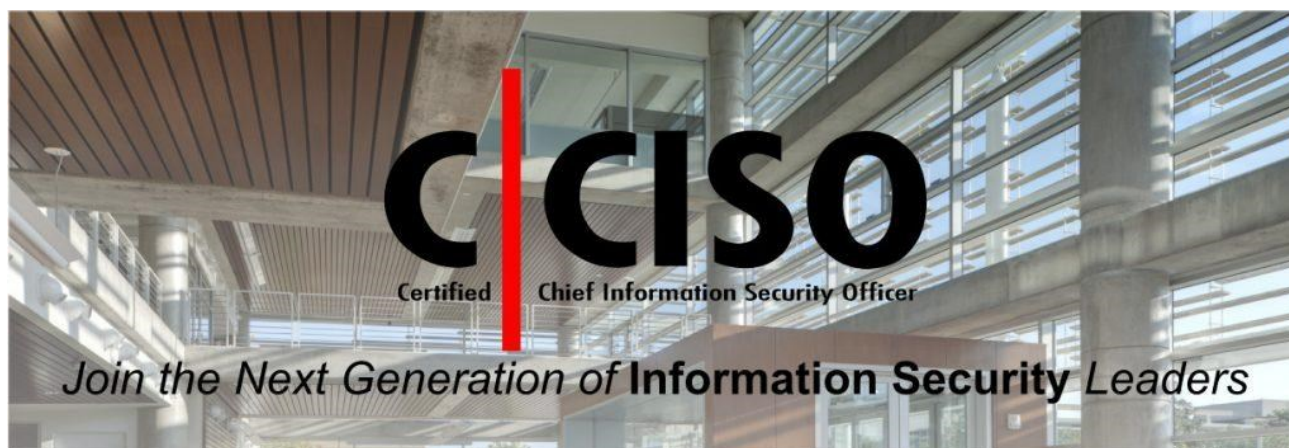
TOPICS

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

TARGET AUDIENCE AND PRE-REQUISITES

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

WAIVERS PER DOMAIN

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

DURATION

40 hours

EXAM

C|CISO™
Certified | Chief Information Security Officer

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

Module 1. Governance
Information program security management
Information security governance program
Regulatory and legal compliance
Risk management
Module 2. Is Risk, Controls & Auditing Management
Design, Deploy and Manage Security Controls
Security Control Types and Objectives
Implement Control Assurance Frameworks Audit Management
Module 3. Information Security Leadership – Projects & Operations
The role of the CISO
Information security projects
Integration of security into processes (change management, version control, disaster recovery, etc.)
Module 4. Information Security Core Competencies
Access controls
Physical security
Disaster recovery and business continuity planning
Network security
Threat and vulnerability management
Application security
Encryption
Vulnerability assessments and penetration testing
Computer forensics and incident response
Module 5. Strategic Planning & Finance
Security Strategic Planning and Alignment with Business Goals and Risk Tolerance
Key Performance Indicators (KPI)
Financial Planning
Development of business cases for security
Analyzing, forecasting, and developing a capital expense budget and an operating expense budget
Return on investment (ROI) and cost-benefit analysis
Vendor management and integrating security into contractual agreement and procurement process

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 C|HFI

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

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 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 technics, commonly used by hackers.

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 C|EH

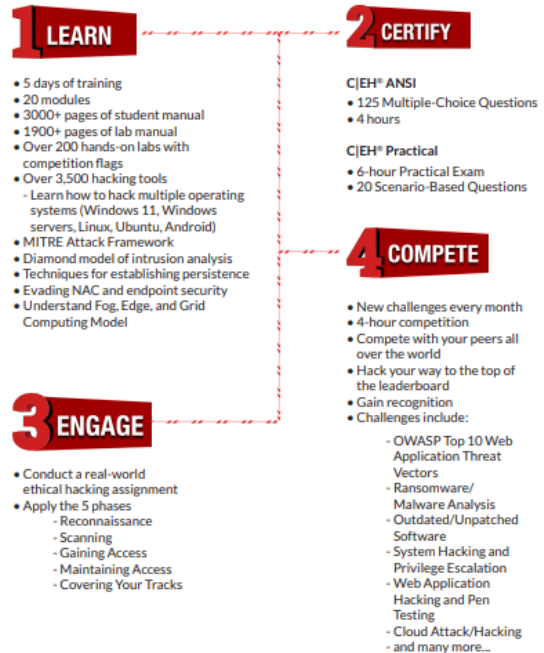| |
|---|
| **Module 01: Introduction to Ethical Hacking** |
| **Module 02: Footprinting and Reconnaissance** |
| **Module 03: Scanning Networks** |
| **Module 04: Enumeration** |
| **Module 05: Vulnerability Analysis** |
| **Module 06: System Hacking** |
| **Module 07: Malware Threats** |
| **Module 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, handson 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.

1 LEARN
Gain Skills

2 CERTIFY
Gain Recognition

3 ENGAGE
Gain Experience

4 COMPETE
Gain Respect

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

1 LEARN
- 5 days of training
- 20 modules
- 3000+ pages of student manual
- 1900+ pages of lab manual
- Over 200 hands-on labs with competition flags
- Over 3,500 hacking tools
  - Learn how to hack multiple operating systems (Windows 11, Windows servers, Linux, Ubuntu, Android)
- MITRE Attack Framework
- Diamond model of intrusion analysis
- Techniques for establishing persistence
- Evading NAC and endpoint security
- Understand Fog, Edge, and Grid Computing Model

2 CERTIFY
C|EH® ANSI
- 125 Multiple-Choice Questions
- 4 hours

C|EH® Practical
- 6-hour Practical Exam
- 20 Scenario-Based Questions

4 COMPETE
- New challenges every month
- 4-hour competition
- Compete with your peers all over the world
- Hack your way to the top of the leaderboard
- Gain recognition
- Challenges include:
  - OWASP Top 10 Web Application Threat Vectors
  - Ransomware/ Malware Analysis
  - Outdated/Unpatched Software
  - System Hacking and Privilege Escalation
  - Web Application Hacking and Pen Testing
  - Cloud Attack/Hacking
  - and many more...

3 ENGAGE
- Conduct a real-world ethical hacking assignment
- Apply the 5 phases
  - Reconnaissance
  - Scanning
  - Gaining Access
  - Maintaining Access
  - Covering Your Tracks

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 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 C|EH MASTER

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

Earning the CEH Master designation is 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 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 C|PENT

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.
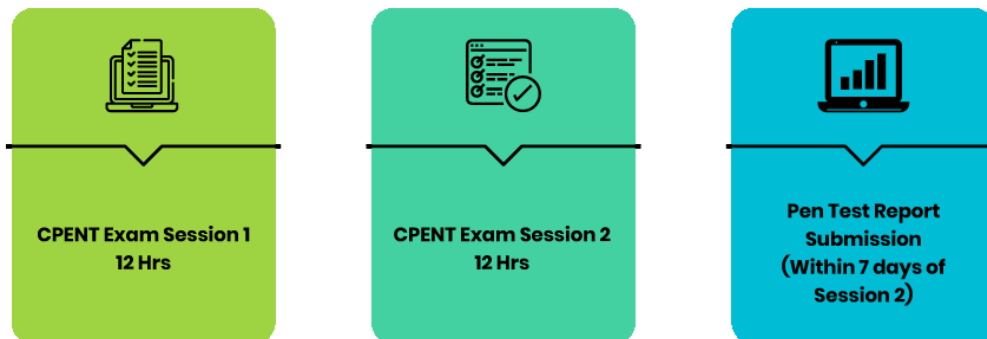
TARGET AUDIENCE AND PRE-REQUISITES

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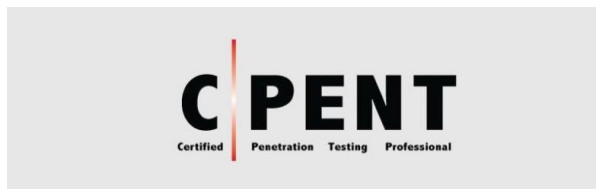
DURATION

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.

CPENT Exam Session 1
12 Hrs

CPENT Exam Session 2
12 Hrs

Pen Test Report Submission
(Within 7 days of Session 2)

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 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 (L|PT MASTER)

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

THE LEARNING TRACK

Knowledge   Skill   Ability
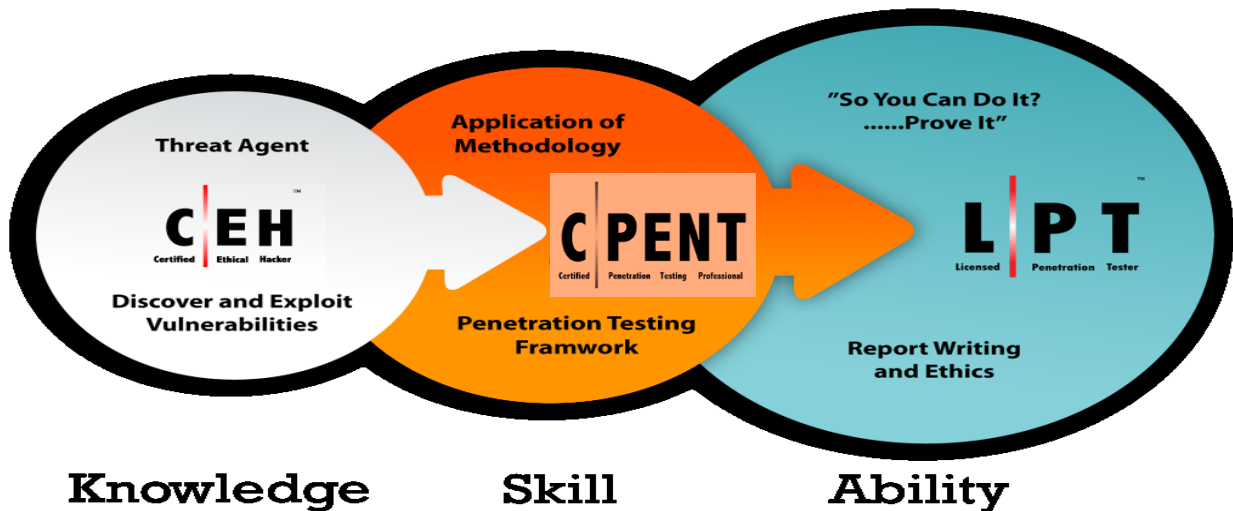
The Advanced Penetration Testing Course by EC-Council was created as the progression after the CPENT (Practical) to prepare those that want to challenge the Licensed Penetration Tester (Master) certification and be recognized as elite penetration testing professionals. Our training has been designed 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 v
arious 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)
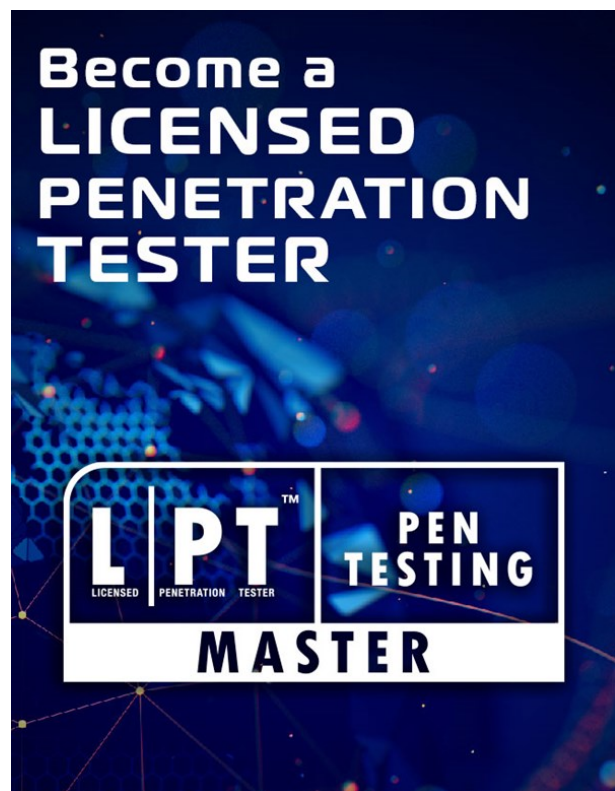
The Advanced Penetration Testing course from EC-Council is built on the backbone of the Advanced Penetration Testing Cyber Range (ECCAPT) and this was designed by experts who each have more than 25 years of professional security testing across the globe.

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 get 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 encounter 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 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.
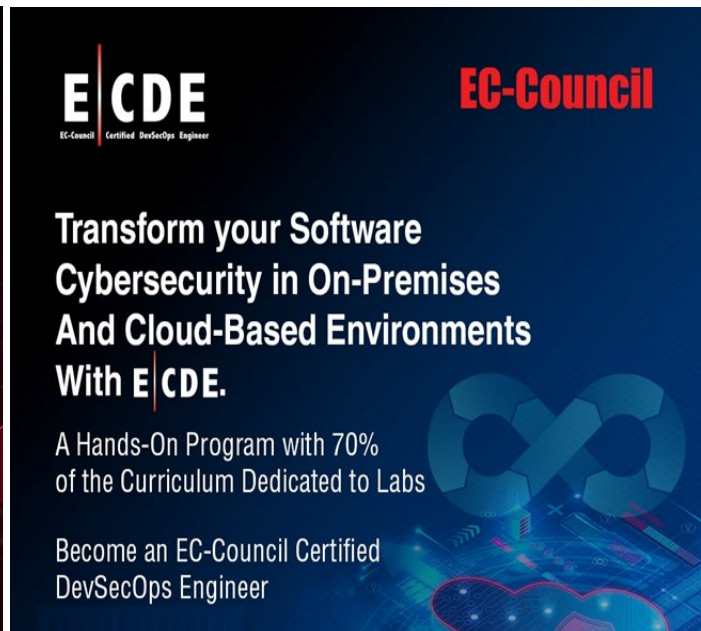
COURSE OBJECTIVES

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 enhances 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 enhances 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
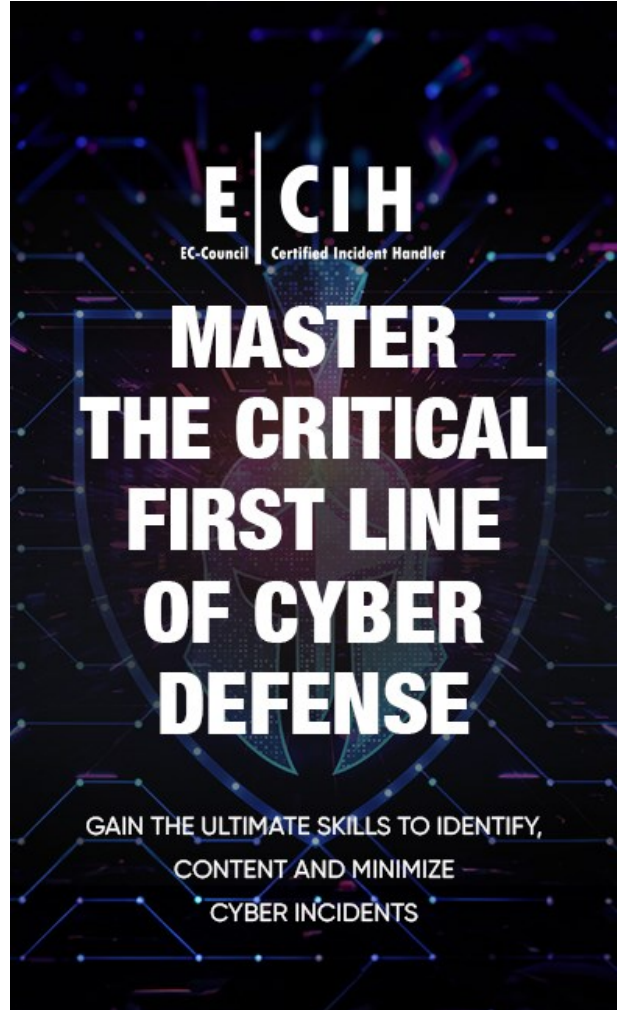- Network Managers/ IT Managers

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).
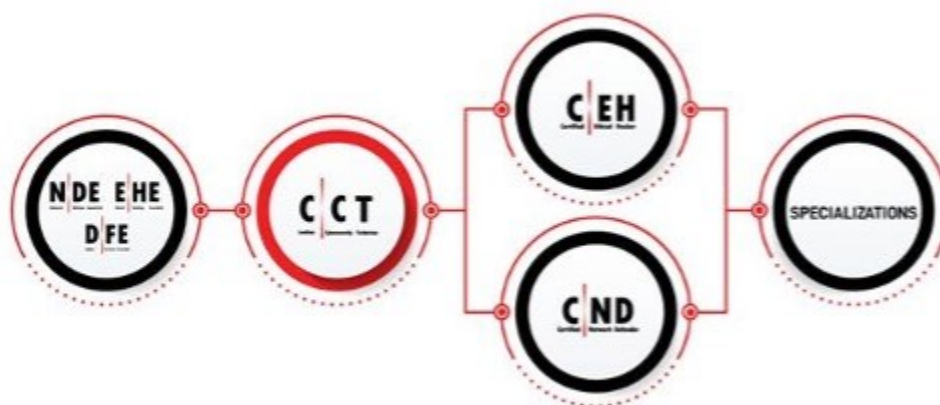
WHAT IS C|CT

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 the 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

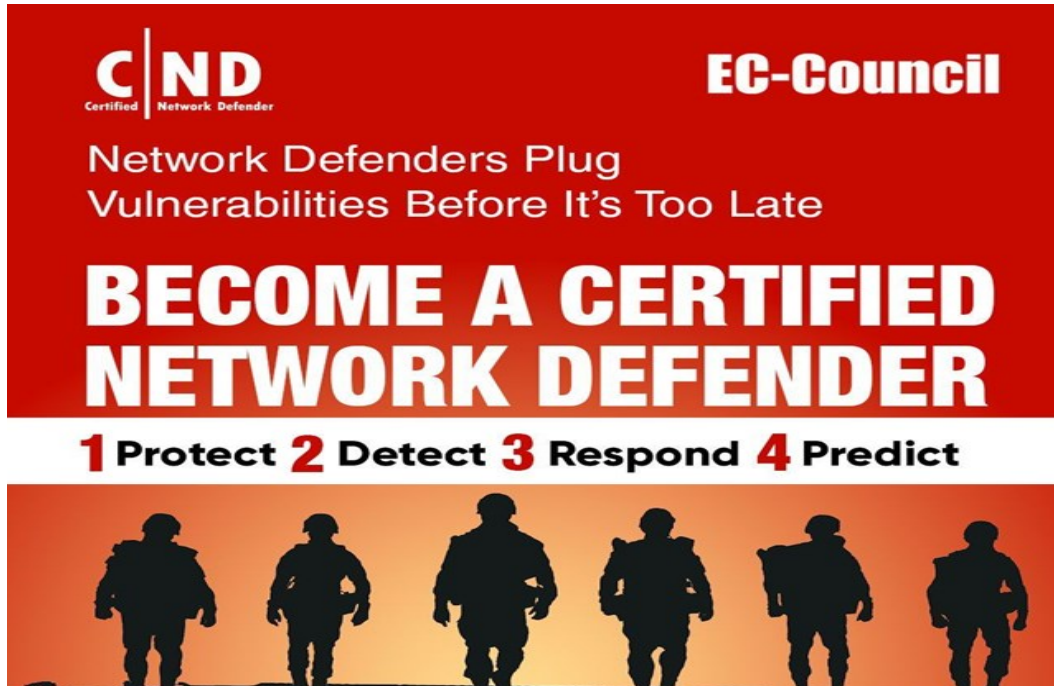40 hours

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 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 C|TIA

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%

CTIA - CERTIFIED THREAT INTELLIGENCE ANALYST

What Is C|TIA

Certified Threat Intelligence Analyst (C|TIA) 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.

C|TIA 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 C|TIA 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 C|TIA

- 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 C|TIA exam can be challenged post the completion of attending the complete official C|TIA course. Candidates that successfully pass the exam will receive their C|TIA 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**

(ISC)2 CISSP Certified Information Systems Security Professional

The Certified Information Systems Security Professional (CISSP) is the most globally recognized certification in the information security market. CISSP validates an information security professional's deep technical and managerial knowledge and experience to effectively design, engineer, and manage the overall security posture of an organization.

CISSP course will cover information security concepts and principles and how these can be aligned to business objectives to help organizations improve their cyber security posture. Proactive identifying cyber security risks and applying the appropriate security controls will help to reduce the impact to business operations. Implementation of appropriate security guidelines and protocols that is aligned to corporate security policies will be covered.

WHAT IS CISSP

CISSP - The World's Premier 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.

With a CISSP, validates expertise and become an ISC2 member, unlocking a broad array of exclusive resources, educational tools and peer-to-peer networking opportunities.

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 (ISC)² 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 (ISC)² by successfully passing the CISSP examination
    - The Associate of (ISC)² will then have 6 years to earn the 5 years required experience

DURATION

45 hours

EXAM

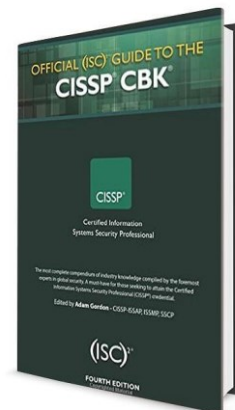**Exam Title:** Certified Information Systems Security Professional
Number of Questions: Adaptative 125+50 (until April 2024)
**Duration:** 4 hours
Test Format: Multiple Choice
Exam Prefix: PUE Pearson Vue (ISC)2 CISSP
Passing Score: 70%

OUTLINE

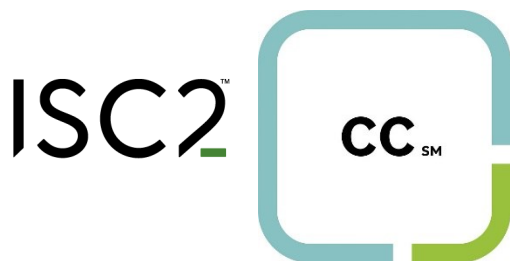|	
Domain 1. Security and Risk Management	**Domain 5. Identity and Access Management (IAM)**
Domain 2. Asset Security	**Domain 6. Security Assessment and Testing**
Domain 3. Security Architecture and Engineering	**Domain 7. Security Operations**
Domain 4. Communication and Network Security	**Domain 8.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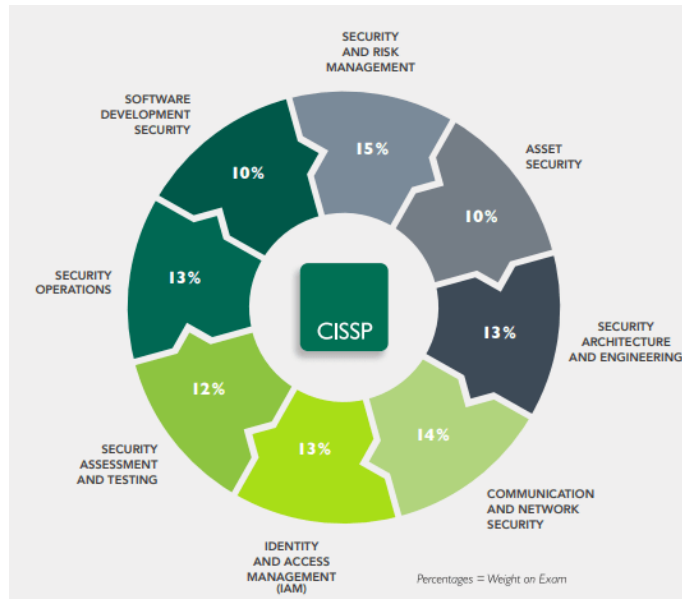
(ISC)2 CC Certified in Cybersecurity

This course is a kickstart in the Cyber security career, entry-level. The new "Certified in Cybersecurity" (CC) certification from (ISC)2 is intended for people who want to begin a career in cybersecurity. Although completing a test covering key cybersecurity subjects like cybersecurity principles, network security, and security operations is required; the certification does not require any prior experience.

WHAT IS CC

CC proves the foundational knowledge, skills and abilities for an entry- or junior-level cybersecurity role. The CC certification may demonstrate fundamental cybersecurity expertise, open job chances, and possibly lead to further professional growth and certification, among other possible advantages.

The first million people who are entering the cybersecurity industry for the first time will receive free CC online self-paced training and examinations from (ISC)2 as part of their "One Million Certified in Cybersecurity" campaign. For individuals who are interested in more training and resources, they are also providing two training bundles with unique bonuses.

COURSE OBJECTIVES

- Gain the knowledge for entry level IT, Cyber Security, roles and job interviews
- Prepare for in-demand Cyber Security entry level certifications
- Understand: Security Principle, Business Continuity Planning (BCP), Disaster Recovery Planning (DRP) and Incident Response Concepts.
- Understand: Access Controls Concepts, Network Security, Security Operations, etc
- Understand: The CIA triad, IAAA, Risk Management, Organizational/IT/Cyber Security Governance.
- Understand: Physical/logical access control, Disaster planning/recovery, Cryptography, Network Security, Malware, and much more.
- Understand: Cyber Security, Information, and IT Security.

TARGET AUDIENCE

- People wanting to get the knowledge for their first job in Cyber Security.
- Anyone who wants to begin a career as a Cyber Security professional.
- Business & IT Managers needing or wanting to learn about Cyber Security.
- Anyone who wants to learn the basics of computer and Cyber Security.
- Entry or Mid-level professionals looking to gain or renew the Fundamentals of Cyber Security for their job or certifications.
- Anyone wanting to pass their Certified in Cybersecurity (CC), CSX-P or ITCA exams.
- Systems, Security and Cyber Security analysts, engineers, managers, administrators, consultants or auditors.

PRE-REQUISITES

- Problem solvers
- Creative
- Analytical and critical thinkers
- Excited by the opportunity to learn

DURATION

24 hours

EXAM

Exam Title: Certified in Cybersecurity
Number of Questions: 100
Duration: 2 hours
Test Format: Multiple Choice
Exam Prefix: (ISC)2 CC

OUTLINE

Domain 1. Security Principles
Domain 2. Business Continuity (BC), Disaster Recovery (DR) & Incident Response Concepts
Domain 3. Access Controls Concepts
Domain 4. Network Security
Domain 5. Security Operations

ISACA CISM Certified Information Security Manager

A Certified Information Security Manager (CISM) is a certification offered by the Information Systems Audit and Control Association (ISACA). Earning a CISM demonstrates an individual's proficiency in best IT security practices. Holders of a CISM can design, implement and oversee a company's entire security network. They can also identify and eliminate potential threats to networks and servers. In the event of a security breach, CISMs can reduce any damage. A CISM is one of the most valued certifications available. As companies increasingly rely on information technology, the need for skilled security professionals has risen. An active CISM certification can show you're dedicated to IT security and have extensive knowledge of the latest information systems trends and developments.

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 risk management
Information security program development and management
Information security 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 Prefix: ISACA CISM
Passing Score: 450 /800

CERTIFICATION

To earn the Certified Information Security Manager (CISM) certification from ISACA, must complete 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: Submit proof of at least five years of information security work experience, including three years in management roles across key CISM areas. This experience must be recent, acquired within five years after passing the exam.
- Substitute Work Experience: ISACA allows for certain substitutions for the work experience requirement, such as holding specific certifications (e.g., CISA, CISSP), possessing a postgraduate degree in a related field, or having completed a specialized management program.
- 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.

ISACA CISA Certified Information Systems Auditor

The Certified Information Systems Auditor (CISA) certification, offered by ISACA (Information Systems Audit and Control Association), is a globally recognized credential for IS audit control, assurance, and security professionals. Being certified as a CISA demonstrates your ability to assess IT and business systems and ensure that they are adequately controlled, monitored, and assessed.

WHAT IS CISM

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 Prefix: ISACA CISA
Passing Score: 450 /800

CERTIFICATION

To earn the Certified Information Systems Auditor (CISA) certification from ISACA, must complete 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: Submit proof of at least five years of information systems auditing, control, or security work experience, which includes specific duties as prescribed by ISACA. This experience must be recent, acquired within five years after passing the exam.
- Substitute Work Experience: ISACA permits certain substitutions for the work experience requirement, such as holding specific certifications (e.g., CISM, CISSP), possessing a postgraduate degree in information systems or a related field, or having completed a specialized program in information systems auditing.
- 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.