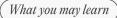# Certified in Cybersecurity (CC)

The Certified in Cybersecurity (CC) course provides foundational training in cybersecurity concepts and practices, ideal for those starting a career in cybersecurity.

SEC-100

What you may learn

Simple and straight-to-the-point live classes

Our simple and direct-to-the-point classes are designed to help students learn faster and understand better.

Start Today

Possible Career Tracks

Cybersecurity Analyst   Information Security Specialist

Network Security Administrator   IT Security Consultant

Security Operations Center (SOC) Analyst

Incident Response Analyst

Taught by Industry Veterans &
World Class Instructors

Introduction to Certified in Cybersecurity (CC)

Overview

The Certified in Cybersecurity (CC) Training Course at Intellectual Point is meticulously curated to equip learners with fundamental cybersecurity knowledge and practical skills essential for entry-level cybersecurity roles. As aligned with ISC2 standards, this course leads you through the core concepts of cybersecurity, encompassing risk management, network defense, threat analysis, and policy implementation. By integrating both theory and hands-on practice, you ensure the mastery of crucial cybersecurity techniques and concepts.

Throughout the training, participants will delve into topics such as threat identification, cybersecurity frameworks, secure network configuration, and incident response protocols. With real-world simulations and labs, you'll gain practical experience in defending systems from cyber threats. By the end of the course, you'll be adept at implementing security measures and prepared to excel in your certification exam.

Skill Outcomes

Risk Management   Network Security   Threat Analysis   Policy Implementation

Incident Response   Cybersecurity Framework Implementation   Intrusion Detection

Vulnerability Assessment   Security Configuration and Management
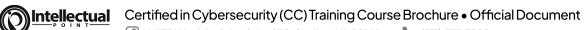

Course Insights

Audience Profile

The Certified in Cybersecurity (CC) Training Course is aimed at individuals eager to launch their careers in cybersecurity or enhance their current IT skills with a focus on security. This includes recent graduates, IT professionals, and career changers who have a basic understanding of information technology and desire to specialize in cybersecurity. Enthusiasts interested in safeguarding digital information and those committed to a career in defensive and proactive information security practices will find this course particularly beneficial. The curriculum suits individuals who crave both foundational learning and recognized certification such as the ISC2 Certified in Cybersecurity to validate their expertise.

Learning Outcomes

By the end of this course, participants will

1. Gain proficiency in identifying and analyzing various cyber threats and vulnerabilities.

2. Demonstrate the ability to implement essential security measures and frameworks effectively.

3. Develop comprehensive strategies to respond to security incidents promptly.

4. Achieve readiness for the Certified in Cybersecurity by (ISC)² certification, enhancing employability.

5. Obtain a recognized (ISC)² Certified in Cybersecurity credential that validates your skills.

Module by Module Learning *Outline*

6 Modules

Module 1: Introduction to Cybersecurity

Learning Objectives:

- Understand the basic principles and importance of cybersecurity.
- Identify various roles within the cybersecurity field and their functions.

Topics Covered

Overview of Cybersecurity:

- Definition and key goals: Confidentiality, integrity, and availability.
- Importance of cybersecurity in today's digital landscape.

Cybersecurity Careers:

- Various roles in cybersecurity and their responsibilities.
- Career pathways and certifications in cybersecurity.

Module 2: Risk Management in Cybersecurity

Learning Objectives:

- Comprehend the fundamentals of risk management and its role in cybersecurity.
- Learn to assess and mitigate risks effectively.

Topics Covered

Risk Assessment Techniques

- Identifying and evaluating information security risks.
- Risk analysis methodologies and frameworks.

Risk Mitigation Strategies

- Approaches to risk reduction and acceptance.
- Developing and implementing risk management plans.

Module 3: Network Security Fundamentals

Learning Objectives:

- Explore key components of network security.
- Understand secure network configurations and protocols.

Topics Covered

Basics of Network Security:

- Network security principles and practices.
- Overview of firewalls, VPNs, and intrusion detection systems.

Securing Networks:

- Best practices for network configuration.
- Tools and techniques for enhancing network defense.

Module 4: Threat Analysis and Response

Learning Objectives:

- Identify various types of cyber threats and vulnerabilities.
- Implement effective incident response strategies.

Topics Covered

Cyber Threats and Vulnerabilities:

- Types of cyber threats: Malware, phishing, DDoS, etc.
- Vulnerability assessment tools and techniques.

Incident Response Protocols

- Steps in developing an incident response plan.
- Practical approaches to carrying out incident response.

Module 5: Policy Implementation and Cybersecurity Frameworks

Learning Objectives:

- Gain insights into cybersecurity policies and frameworks.
- Develop and implement security measures within an organization.

Topics Covered

Cybersecurity Policies:

- Importance and components of a strong cybersecurity policy.
- Processes for creating and enforcing policies.

Cybersecurity Frameworks:

- Overview of frameworks like NIST, ISO, and others.
- Implementation of best practices and controls.

Module 6: Hands-On Labs

Learning Objectives:

- Apply theoretical knowledge in practical scenarios to reinforce learning.
- Prepare effectively for the Certified in Cybersecurity (CC) exam.

Topics Covered

Real-World Simulations:

- Types of cyber threats: Malware, phishing, DDoS, etc.
- Vulnerability assessment tools and techniques.

Exam Preparation

- Review of key exam topics and practice questions.
- Strategies for successful exam completion and obtaining certification.