AISECT LEARN
Better Education. Better Careers.

LIVE + SELF-PACED

CERTIFIED CLOUD SECURITY PROFESSIONAL COURSE (CCSPC)

COURSE OVERVIEW

The Certified Cloud Security Professional Course (CCSPC) is designed to empower participants with a comprehensive understanding of cloud security principles, strategies, and best practices. This course aims to equip individuals with the knowledge and skills required to ensure the security, privacy, and compliance of cloud environments. Participants will delve into various cloud service models and deployment architectures, learning to implement robust security measures to protect sensitive data, applications, and resources from potential threats and vulnerabilities. Through hands-on training and real-world scenarios, students will gain the expertise needed to effectively design, implement, and manage secure cloud solutions, making them adept in safeguarding cloud-based assets against unauthorized access and cyberattacks.

COURSE OBJECTIVE

This course aims to provide learners with advanced expertise and methodologies to effectively secure cloud environments and protect critical data from evolving cyber threats. Participants will gain comprehensive knowledge of cloud security principles, practices, and technologies, enabling them to implement robust security measures within various cloud platforms.

WHAT YOU WILL LEARN

In the Cloud Security Professional Course (CCSPC), participants will gain comprehensive knowledge and expertise in securing cloud environments. They will delve into the intricacies of cloud computing, learning to identify potential security risks and vulnerabilities specific to cloud-based services. Throughout the course, participants will explore various cloud deployment models and cloud service providers, understanding how to implement robust security controls for data protection, access management, and compliance.

Participants will become proficient in designing and implementing cloud security architectures, including secure cloud infrastructure and network configurations. They will learn to evaluate and select appropriate security solutions, such as encryption mechanisms, identity and access management (IAM) tools, and monitoring systems to ensure continuous cloud security.

Additionally, the course will cover threat detection and incident response in cloud environments, equipping participants with the skills to identify and mitigate cloud-based attacks effectively. By the end of the CCSPC course, participants will be well-prepared to face the dynamic challenges of cloud security, demonstrating their ability to safeguard cloud data, applications, and services against cyber threats.

COURSE SKILL SET

- Understanding the importance of cybersecurity
- Familiarity with security policies and procedures
- Knowledge of common hacking methodologies and techniques
- Awareness of risk management principles and methodologies
- Ability to design and implement secure architectures for systems and networks
- Understanding network protocols, OSI layers, and IP addressing
- Knowledge of network security controls and intrusion detection systems
- Conducting penetration testing and vulnerability assessments
- Understanding and implementing cybersecurity controls and frameworks
- Knowledge of different types of cyber threats and attack methods
- Familiarity with incident management and response processes
- Understanding the legal and regulatory aspects of cybersecurity
- Knowledge of computer forensics principles and investigation techniques
- Understanding the role and configuration of firewalls
- Understanding cloud computing fundamentals and architecture
- Knowledge of cloud security principles and best practices
- Awareness of identity and access management in the cloud
- Understanding of data security and privacy in the cloud
- Knowledge of cloud-based risk assessment and management
- Awareness of cloud-based incident response and recovery processes

Instructor - **Ajay Gautam | Cyber Security Expert**

Instructor - **Aman Roy | Cyber Security Expert**

Duration - 1 Month

Eligibility - Any graduate with a Science stream

No. of Modules – 08 Modules

Language - English

Shareable certificate - Yes

PROGRAM SYLLABUS

Module 1 Introduction to Cybersecurity
Session 1.1 Introduction
Session 1.2 Why Cyber Security is Important?
Session 1.3 Role of cyber security enginner
Session 1.4 CIA Triad
Session 1.5 The Hacking Methodology
Session 1.6 The WhoIS Query
Session 1.7 Social Engineering
Session 1.8 Brute Force Attacks
Session 1.9 Phishing
Session 1.10 Bots and Botnets
Session 1.11 DoS and DDoS
Session 1.12 Pings
Session 1.13 Man in the Middle Attacks (MITM)

Module 2 Cyber Security Building blocks
Session 2.1 Malicious Codes and Terminologies
Session 2.2 Cybersecurity Breaches
Session 2.3 Penetration Testing and Methodologies
Session 2.4 Frameworks and Standards for Cybersecurity
Session 2.5 Hardware and Software Elements of Computer Systems
Session 2.6 Introduction to Networks and Reference Models
Session 2.7 OSI layers
Session 2.8 Network Protocol
Session 2.9 IP Address and Subnet Classes
Session 2.10 Network Devices
Session 2.11 Packet Sniffing
Session 2.12 Sniffing Using Scapy
Session 2.13 Packet Spoofing
Session 2.14 Packet Spoofing Using Scapy

Module 3 Basic Concepts of Vulnerability
Session 3.1 Types of Hackers & Hacktivism
Session 3.2 Understanding Terminologies
Session 3.3 Vulnerability & Pentesting
Session 3.4 Cyber Security Controls
Session 3.5 Cyber Security Policies
Session 3.6 CVE & CVSS

Module 4 Security Basics
Session 4.1 Attacks & Threats
Session 4.2 Architecture & Design
Session 4.3 Implementation
Session 4.4 Operations & Incident Response
Session 4.5 Governance, Risk & Compliance
Session 4.6 Firewalls
Session 4.7 Encryption
Session 4.8 Biometrics
Session 4.9 Anti Virus
Session 4.10 Password Management
Session 4.11 What is Cyber Kill Chain?
Session 4.12 Reconnaissance & Weaponization
Session 4.13 Delivery & Exploitation
Session 4.14 Installation, Command and control (C2) & Actions on Objectives

Module 5 Computer Forensics
Session 5.1 Computer Forensics investigation process
Session 5.2 Data Acquisition & Duplication
Session 5.3 Introduction to Windows Forensics
Session 5.4 Lab: Capturing Windows Memory
Session 5.5 Browser Forensics using Encase
Session 5.6 Lab: WebHistorian
Session 5.7 Memory Forensics
Session 5.8 Lab: Analysing USB data
Session 5.9 Lab: Analysing Malware using Volatility
Session 5.10 Introduction to Indian Cyber Law

Module 6 Cloud Security
Session 6.1 Introduction
Session 6.2 Understanding cloud computing concepts
Session 6.3 Describe Cloud Reference Architecture
Session 6.4 Understand Security Concepts Relevant to Cloud Computing
Session 6.5 Understand design principles of secure cloud computing
Session 6.6 Evaluate Cloud Service Providers
Session 6.7 Describe Cloud Data Concepts
Session 6.8 Design and Implement Cloud Data Storage Architectures

Session 6.9 Design and Apply Data Security Technologies and Strategies
Session 6.10 Implement Data Discovery
Session 6.11 Implement Data Classification
Session 6.12 Design and Implement Information Rights Management (IRM)
Session 6.13 Plan and Implement Data Retention, Deletion and Archiving Policies
Session 6.14 Data Events
Session 6.15 Comprehend Cloud Infrastructure Components
Session 6.16 Design a Secure Data Center
Session 6.17 Analyze Risks Associated with Cloud Infrastructure
Session 6.18 Design and Plan Security Controls
Session 6.19 Plan Disaster Recovery (DR) and Business Continuity (BC)
Session 6.20 Advocate Training and Awareness for Application Security
Session 6.21 Describe the Secure Software Development Life Cycle (SDLC) Process
Session 6.22 Apply the Secure Software Development Life Cycle (SDLC)
Session 6.23 Apply Cloud Software Assurance and Validation
Session 6.24 Use Verified Secure Software
Session 6.25 Comprehend the Specifics of Cloud Application Architecture
Session 6.26 Design Appropriate Identity and Access Management (IAM) Solutions
Session 6.27 Implement and Build Physical and Logical Infrastructure for Cloud
Session 6.28 Operate Physical and Logical Infrastructure for Cloud Environment-Part 1
Operate Physical and Logical Infrastructure for Cloud Environment-Part 2
Session 6.29 Implement Operational Controls and Standards
Session 6.30 Support Digital Forensics
Session 6.31 Manage Communication with Relevant Parties
Session 6.32 Manage Security Operations
Session 6.34 Understand Privacy Issues
Session 6.35 Understand Audit Process, Methodologies, and Required Adaptations- Part 1
Understand Audit Process, Methodologies, and Required Adaptations- Part 2

Session 6.36 Understand Implications of Cloud to Enterprise Risk Management
Session 6.37 Understand Outsourcing and Cloud Contract Design

Module 7 Python Essentials
Session 7.1 Python Introduction
Session 7.2 Installation of Anaconda Navigator
Session 7.3 Jupyter Notebook Interface
Session 7.4 How to Open, Save, and Rename a file
Session 7.5 Variables and Data Types
Session 7.6 Python Strings
Session 7.7 Loops (Conditional)
Session 7.8 Loops (iterative while)

Module 8 Job roles
Session 8.2 Analyst Application Security
Session 8.3 Engineer Trainee
Session 8.5 Security Analyst
Session 8.7 Analyst Security Operations Centre

AISECT LEARN
Better Education. Better Careers.

Sign up for

Webinars, Free courses and Paid Courses

starting from ₹**499/-** onwards only

Contact Us

+91 9111177800

learn@aisectlearn.com

www.courses.aisectlearn.com