CompTIA Advanced Security Practitioner (CASP)

Modality: On Demand

Duration: 23 Hours

This course prepares you for the CAS-003 Exam leading to CAS-003 Certification. This course does not include the Official Exam Voucher, however, you can request to purchase the Official Exam Voucher separately.

About this course:

The CompTIA Advanced Security Practitioner (CASP) certification training establishes knowledgeable professionals in the field of advanced security practices. Students will first learn about the enterprise security architecture, security technology and resource technology. Students will then learn security design and solutions, application security design, managing risk, security policies, security procedures and enterprise security integration. Finally, they will learn about security research and analysis, disaster recovery and business continuity, managing risk in projects, legal issues and judgment and decision-making. This certification course will help the students in the preparation for CompTIA CAS-002 & CAS-003 exam.

The average salary for CompTIA Advanced Security Practitioners and related IT security certification is **$79,730** per year.

Course Objective:

After completing this course, students will be able to:

- Successfully prepare for the CompTIA Advanced Security Practitioner (CASP) Certification Exam
- Investigate enterprise storage requirements
- Examine risk management security policies and procedures
- Research potential threats and identify appropriate countermeasures
- Evaluate collaboration methodologies for security communications

Audience:

This course is intended for:

- IT security professional who has a minimum of 10 years experience in IT administration

Prerequisites:

- Ten years of IT administration experience, including at least five years of hands-on technical security experience

Suggested prerequisites courses:

- Certified Security Leadership Officer
- Certified Information Security Manager (CISM)

Course Outline:

- Course Introduction
- Chapter 01 - Understanding Risk Management
- Chapter 02 - Network and Security Components and Architecture
- Chapter 03 - Implementing Advanced Authentication and Cryptographic Techniques
- Chapter 04 - Implementing Security for Systems, Applications, and Storage
- Chapter 05 - Implementing Security for Cloud and Virtualization Technologies
- Chapter 06 - Utilizing Security Assessments and Incident Response
- Course Closure