CompTIA CASP+¬ Training

Course: **00064**
Filter: **Beginner**
Duration: **4 days**
Category:: **Gouvernance, Risk and Compliance**
Price: **3000,00 €**

About Course

This CASP+ Training course prepares you for the CompTIA CASP+ certification exam (CAS-004) and demonstrates your knowledge and skills in enterprise security, risk management, research and analysis, and the integration of computing, communications, and business disciplines. You will learn through a CompTIA-approved CASP+ training program and receive after-course instructor coaching and an exam voucher. The course is available in-person or online, with virtual instructor-led training and virtual classroom options, providing a flexible and convenient learning experience. Passing the CompTIA CASP+ Certification Exam meets U.S. DoD Directive 8140/8570.01 Technical (IAT) Level-III, Management (IAM) Level-II and Information Assurance Security Architect/Engineer (IASAE) Level-I and Level II requirements.

What you'll learn

- Experience an Official CompTIA- CASP+ training program.
- Receive after-course instructor coaching and an exam voucher.
- 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 secure communications.
- Continue learning and face new challenges with after-course one-on-one instructor coaching.

Pre-requisites

- CompTIA Security+® Training, or equivalent experience
- Ten years of IT (Information Technology) administration experience, including at least five years of hands-on technical security experience

Curriculum

Module 1: Enterprise Security

- Identifying security concerns in scenarios
- Distinguishing between cryptographic concepts
- Securing enterprise storage
- Analyzing network security architectures
- Troubleshooting security controls for hosts
- Differentiating application vulnerabilities

Module 2: Risk Management and Incident Response

- Interpreting business and industry influences and risks
- Executing risk mitigation planning, strategies, and control
- Privacy policies and procedures
- Conduct incident response and recovery procedures

Module 3: Research, Analysis, and Assessment

- Determining industry trends impact to the enterprise
- Appropriate security document usage
- Evaluating scenarios to determine how to secure the enterprise
- Conducting an assessment and analyzing the results

Module 4: Integrating Computing, Communications, and Business Disciplines

- Collaborating across diverse business units to achieve security goals

- Selecting controls for secure communications
- Implementing security across the technology life cycle

Module 5: Technical Integration of Enterprise Components

- Integrate devices into a secure enterprise architecture
- Securing data following existing security standards
- Applying technical deployment models
- Integrating storage and applications into the enterprise
- Integrating advanced authentication and authorization technologies
- Implementing certificate-based and SSO authentication
- Applying federation solutions