CASP+ (CAS-004)

Overview:

Prepare for the CompTIA CASP+ exam with the course CASP+ CompTIA Advanced Security Practitioner (CAS-004). The course contains assessment questions, test sets, interactive lessons with knowledge checks and quizzes, and labs to provide a hands-on learning experience of security in a safe, online environment. It provides complete coverage of the CAS-004 exam objectives and it is designed to give you insight into the working world of IT security. It describes the types of tasks and activities that a security professional with 5–10 years of experience carries out.

Here's what you will get:

The CompTIA CASP+ (CAS-004) certification is a globally recognized widely-trusted vendor-neutral credential. CASP+ covers the technical knowledge and skills required to architect, engineer, integrate, and implement secure solutions across complex environments to support a resilient enterprise while considering the impact of governance, risk, and compliance requirements. It is an advanced-level cybersecurity certification for security architects and senior security engineers charged with leading and improving an enterprise’s cybersecurity readiness.

Lessons

11 Lessons
410 Exercises
200 Quizzes
313 Flashcards
209 Glossary of terms

TestPrep

90 Pre Assessment Questions
2 Full Length Tests
90 Post Assessment Questions
180 Practice Test Questions

Lab

31+ Performance Labs
31 video tutorials
Course Outline

Chapter 1: Introduction

- Before You Begin the CompTIA CASP+ Certification Exam
- Who Should Read This Course
- What You Will Learn
- How This Course Is Organized
- How to Use This Course
- Tips for Taking the CASP+ Exam
- CompTIA CASP+ Study Guide Exam Objectives
- The CASP+ Exam Objective Map

Chapter 2: Risk Management

- Risk Terminology
- The Risk Assessment Process
- Policies Used to Manage Employees
- Cost-Benefit Analysis
- Continuous Monitoring
- Enterprise Security Architecture Frameworks and Governance
- Training and Awareness for Users
- Best Practices for Risk Assessments
- Business Continuity Planning and Disaster Recovery
- Reviewing the Effectiveness of Existing Security Controls
- Conducting Lessons Learned and After-Action Reviews
- Creation, Collection, and Analysis of Metrics
- Analyzing Security Solutions to Ensure They Meet Business Needs
- Testing Plans
- Internal and External Audits
- Using Judgment to Solve Difficult Problems
- Summary
- Exam Essentials

Chapter 3: Configure and Implement Endpoint Security Controls

- Hardening Techniques
- Trusted Operating Systems
- Compensating Controls
- Summary
- Exam Essentials

Chapter 4: Security Operations Scenarios

- Threat Management
- Actor Types
- Intelligence Collection Methods
- Frameworks
- Indicators of Compromise
- Response

- Summary
- Exam Essentials

Chapter 5: Security Ops: Vulnerability Assessments and Operational Risk

- Terminology
- Vulnerability Management
- Vulnerabilities
- Inherently Vulnerable System/Application
- Proactive Detection
- Summary
- Exam Essentials

Chapter 6: Data Analysis and Statistics

- Shared Responsibility in Cloud Computing
- Security Concerns of Integrating Diverse Industries
- Regulations, Accreditations, and Standards
- Contract and Agreement Types
- Third-Party Attestation of Compliance
- Legal Considerations
- Summary
- Exam Essentials

Chapter 7: Cryptography and PKI

- The History of Cryptography
- Cryptographic Goals and Requirements
- Supporting Security Requirements
- Risks with Data
- Hashing
- Symmetric Algorithms
- Asymmetric Encryption
- Public Key Infrastructure Hierarchy
- Digital Certificates
- Implementation of Cryptographic Solutions
- Recognizing Cryptographic Attacks
- Troubleshooting Cryptographic Implementations
- Summary
- Exam Essentials

Chapter 8: Incident Response and Forensics

- The Incident Response Framework
- Forensic Concepts

- Forensic Analysis Tools
- Summary
- Exam Essentials

Chapter 9: Security Architecture

- Security Requirements and Objectives for a Secure Network Architecture
- Organizational Requirements for Infrastructure Security Design
- Integrating Applications Securely into an Enterprise Architecture
- Data Security Techniques for Securing Enterprise Architecture
- Security Requirements and Objectives for Authentication and Authorization Controls
- Summary
- Exam Essentials

Chapter 10: Secure Cloud and Virtualization

- Implement Secure Cloud and Virtualization Solutions
- How Cloud Technology Adoption Impacts Organization Security
- Summary
- Exam Essentials

Chapter 11: Secure Cloud and Virtualization

- Emerging Technologies and Their Impact on Enterprise Security and Privacy
- Secure Enterprise Mobility Configurations
- Security Considerations for Technologies, Protocols, and Sectors
- Summary
- Exam Essentials