CompTIA SecurityX Certification Training

Days: 5

Audience: This course is designed for experienced cybersecurity professionals seeking to earn the CompTIA SecurityX (formerly CASP+) certification. Ideal for security architects, senior security engineers, and technical leads responsible for securing complex enterprise environments.

Prerequisites: Candidates should have at least 10 years of general IT experience, including a minimum of 5 years of hands-on cybersecurity experience. Familiarity with enterprise security, risk management, and architecture is essential.

Description: This advanced-level course prepares learners to architect, engineer, integrate, and implement secure solutions across diverse enterprise environments. Participants will gain expertise in governance and compliance, security architecture, operations, engineering, and automation. The training aligns with the CAS-005 exam objectives and covers hands-on scenarios to reinforce critical thinking and problem-solving.

Course Objectives: In this course, you will:

- Apply governance, risk, and compliance (GRC) frameworks
- Architect secure systems and networks
- Engineer proactive detection, response, and access controls
- Implement cryptographic techniques and emerging technologies
- Lead enterprise-wide security operations and automation initiatives

OUTLINE:

CHAPTER 1: GOVERNANCE AND COMPLIANCE
Module A: Security governance
Module B: Regulatory compliance
Module C: Standards and frameworks

CHAPTER 2: SECURITY PROGRAM DESIGN
Module A: Controls and procedures
Module B: Security program management

CHAPTER 3: RISK MANAGEMENT
Module A: Risk assessment
Module B: Risk management strategies

CHAPTER 4: THREAT MANAGEMENT
Module A: Threats and vulnerabilities
Module B: Threat intelligence sources
Module C: Applied intelligence

CHAPTER 5: CRYPTOGRAPHIC TECHNIQUES
Module A: Cryptographic principles
Module B: Ciphers and hashes

CHAPTER 6: APPLIED CRYPTOGRAPHY
Module A: Public key infrastructure
Module B: Cryptographic protocols

CHAPTER 7: AUTHENTICATION AND AUTHORIZATION
Module A: Access control components
Module B: Authentication technologies

CHAPTER 8: SECURE ARCHITECTURE
Module A: Hardware security
Module B: Resilient architecture

CHAPTER 9: AUTOMATED SYSTEMS
Module A: Security automation
Module B: Artificial intelligence

CHAPTER 10: PROTECTING HOSTS AND DATA
Module A: Host security tools
Module B: Securing endpoints and servers
Module C: Data security

CHAPTER 11: NETWORK SECURITY ARCHITECTURE
Module A: Network security infrastructure
Module B: Secure network configuration

CHAPTER 12: THREAT DETECTION
Module A: Threat detection systems
Module B: Network sensors

CHAPTER 13: THREAT ANALYSIS
Module A: Data aggregation and analysis
Module B: Forensic analysis

CHAPTER 14: SPECIALIZED INFRASTRUCTURE SECURITY
Module A: Specialized systems
Module B: Secure cloud infrastructure

CompTIA SecurityX Certification Training