Document Generated: 12/15/2025

Learning Style: Virtual Classroom

Technology: CompTIA

Difficulty: Advanced

Course Duration: 5 Days

Next Course Date: February 23, 2026

CompTIA SecurityX (CAS-005)

About this Course:

CompTIA SecurityX (formerly CASP+) is the only advanced-level, hands-on cybersecurity certification designed for senior security engineers and architects who lead cybersecurity readiness, design secure architectures, and implement resilient

enterprise defenses.

SecurityX is the capstone certification in the CompTIA Cybersecurity Pathway and now forms part of the CompTIA Xpert Series. This updated CAS-005 version includes performance-based questions and maps to 19 NICE Framework roles and 19 DoD Cyber Workforce roles, making it an ideal credential for defense contractors and enterprise security leaders alike.
What Is Included

Course Objectives:

This advanced certification course prepares experienced professionals to assess cyber readiness, design enterprise-wide security architectures, and implement secure solutions across hybrid environments. You'll also gain the skills to respond to incidents, lead forensic analysis, and prove compliance against frameworks such as CMMC, NIST, GDPR, and more.

Key learning outcomes include:

- Architect secure solutions in hybrid cloud and zero trust environments
- Perform advanced threat management and digital forensics
- Lead cybersecurity readiness assessments across the enterprise
- Evaluate and meet compliance for major regulatory frameworks
- Implement cryptographic solutions and security engineering controls

Audience:

- Aspiring cybersecurity professionals seeking a foundational certification
- IT support technicians and helpdesk staff transitioning into security roles
- Network and systems administrators responsible for securing infrastructure
- Junior security analysts and SOC team members
- Anyone preparing for the CompTIA SecurityX® (CAS-005) exam

Prerequisites:

- 10+ years of general IT experience
- 5+ years of hands-on cybersecurity experience

- Knowledge equivalent to CompTIA Network+, Security+, CySA+, Cloud+, and PenTest+

Course Outline:

Pre-Assessment

- Baseline skills evaluation
- Familiarity with CAS-005 domains

Governance, Risk, and Compliance

- Prove cyber resiliency metrics
- Map controls to regulations (e.g., CMMC, NIST, GDPR)
- Risk mitigation strategies

Security Architecture

- Design hybrid and cloud-secure architectures
- Integrate Zero Trust security models
- Advanced virtualization and mobility controls

Security Engineering and Cryptography

- Implement enterprise-wide PKI
- Configure endpoint, mobile, and cloud security
- Apply secure protocols and encryption

Security Operations and Incident Response

- Vulnerability management and threat hunting
- Lead digital forensic investigations
- Coordinate response and remediation

CAS-005 Exam Preparation and Practice Materials

- Practice questions and timed drills
- Performance-based scenario exercises
- Final readiness assessment