

CompTIA SecurityX (CAS-005)

Course Description

CompTIA SecurityX serves as the capstone certification in the CompTIA Cybersecurity Career Pathway, intended to be the final certification for those seeking to prove their mastery of advanced cybersecurity skills. Targeted at professionals with 5 to 10 years of experience, SecurityX represents the pinnacle of cybersecurity certifications. It is specifically designed for senior security engineers and security architects tasked with leading and improving an enterprise's cybersecurity readiness.

Course Duration

5 days

Prerequisites

Target audience: Minimum 10 years general hands-on IT experience, 5 years being hands-on security, with Network+, Security+, CySA+, Cloud+ and PenTest+ or equivalent knowledge.

Objectives

- Individuals who have passed this exam have proven that they can design and implement effective cybersecurity solutions on complex enterprise networks that exist on premises and in the cloud.
- SecurityX certification communicates that learners have the mastery-level skills of an enterprise-level Security Architect and Senior Security Engineer. They can design, assess, fix, automate, and operate a secure enterprise network while complying with various governance, risk, and compliance requirements.
- Earning the SecurityX certification gives learners an internationally recognized, vendor-neutral credential. They can demonstrate their competency in technical integration of enterprise business goals, secure systems design, senior engineering, and security architecture.
- Information security threats are rising around the world, leaving organizations increasingly concerned over lack of adequately trained IT security staff. A SecurityX certification qualifies learners to assess, manage, and protect their enterprise-wide cybersecurity needs using the latest techniques and best practices.¹

Course Outline

- Supporting IT Governance and Risk Management
- Leveraging Collaboration to Support Security
- Using Research and Analysis to Secure the Enterprise
- Integrating Advanced Authentication and Authorization Techniques
- Implementing Cryptographic Techniques
- Implementing Security Controls for Hosts
- Implementing Security Controls for Mobile Devices
- Implementing Network Security
- Implementing Security in the Systems and Software Development Lifecycle
- Integrating Assets in a Secure Enterprise Architecture
- Conducting Security Assessments. Responding to and Recovering from Incidents

Who Should Attend

- Security Architect
- Senior Security Engineer
- Information Security Officer