CompTIA SecurityX Day

Length: 9 days
Format: Classroom
Time: Day

About This Course

The CompTIA SecurityX Certification course is designed for experienced cybersecurity professionals ready totake their expertise to the next level. SecurityX is part of CompTIAs Xpert series and focuses on the skillsrequired of senior security engineers and architects who lead enterprise-level cybersecurity initiatives. Thiscourse equips learners with the advanced knowledge needed to design and implement secure solutions acrosscomplex environments, preparing them to meet todays evolving threat landscape head-on.

Throughout the course, students will engage with real-world scenarios that mirror the challenges faced byprofessionals in high-stakes cybersecurity roles. Topics include digital security architecture, enterprise riskmanagement, governance, and advanced threat mitigation strategies. Whether you're aiming to validate yourskills or step into a leadership role in cybersecurity, this course offers the depth and rigor needed to succeedon the SecurityX exam and beyond.

Click here to find your place on the CompTIA Roadmap.

Required Exams

To earn the CompTIA SecurityX certification, students must pass exam CAS-005.

Audience Profile

This course is designed for IT professionals in the cybersecurity industry whose primary job responsibility is tosecure complex enterprise environments. The target student should have real-world experience with thetechnical administration of these enterprise environments. This course is also designed for students who areseeking the CompTIA SecurityX certification.

Course Objectives

* Design, implement, and integrate secure solutions across complex environments to support a resilient enterprise in security architecture and engineering.
* Use automation, monitoring, detection, and incident response to proactively support ongoing security operations.
* Apply security practices to cloud, on-premises, and hybrid environments to ensure enterprise-wide protection.
* Utilize cryptographic technologies and techniques while evaluating the impact of emerging trends, such as

artificial intelligence, on information security.
* Implement governance, compliance, risk management, and threat modeling strategies across the enterprise.
* Validate advanced, hands-on skills in security architecture and senior security engineering within live environments.

Outline

Module 1: Introduction * Preassessment

Module 2: Summarizing Governance Risk and Compliance * Implement Appropriate Governance Components
* Explain Legal Compliance
* Apply Risk Management Strategies

Module 3: Implementing Architecture and Design * Apply Software Development
* Integrate Software Architecture
* Support Operational Resilience
* Implement Cloud Infrastructure
* Integrate Zero Trust Concepts
* Troubleshoot using AAA and IAM

Module 4: Understanding Security Engineering * Enhance Endpoint Security
* Configure Network Infrastructure
* Initiate Security Automation
* Apply Cryptography Concepts

Module 5: Applying Security Operations and * Incident Response
* Perform Threat Modeling
* Examine Security Monitoring
* Analyze Known Attack Methods and Associated Mitigations
* Apply Threat Hunting Tools and Technologies
* Evaluate Incident Analysis and Response