

CompTIA SecurityX (CASP+)

CompTIA SecurityX (CASP+) is an advanced certification that focuses on enterprise security, risk management, and integrating computing, communications, and business disciplines.

SEC-300

What you may learn

Professional, practical, & hands-on live instructor-led training

Advance your skills and graduate as a certified professional, with the skills, experience, and job-search know how to get your career moving.

 Start Today

Possible Career Tracks

Cybersecurity Analyst Information Security Specialist

Network Security Engineer Security Consultant

IT Security Administrator Risk Analyst



Taught by Industry Veterans & World Class Instructors

Introduction to CompTIA SecurityX

Overview

Intellectual Point's CompTIA SecurityX Training Course is meticulously crafted to impart the essential knowledge and competencies required for a successful career in cybersecurity. This course prepares you for the CompTIA SecurityX certification exam, which is integral for entering the cybersecurity domain. With an emphasis on hands-on learning, you'll gain practical experience in identifying and mitigating security threats across diverse IT environments. Whether you're a novice or someone with basic knowledge in IT security, this course addresses all aspects of cybersecurity, from risk management to incident response.

Throughout the training, you will delve into topics such as network security, compliance protocols, identity management, and cryptography. The course includes interactive labs and exercises, allowing you to apply best practices in cybersecurity and bolster your technical skills. By the end of the program, you'll be equipped to tackle cybersecurity challenges and successfully achieve your certification goals.

Skill Outcomes

Network Security Implementation Threat and Vulnerability Management Risk Management
Security Compliance and Regulations Incident Response Techniques
Identity and Access Management System and Application Security
Cryptography and Data Protection SecurityX Exam Preparation

Course Insights

Audience Profile

The CompTIA SecurityX Training Course is ideal for IT professionals, cybersecurity enthusiasts, and those looking to transition into a security-focused career. This program is geared towards individuals with a foundational understanding of IT who are keen to specialize in cybersecurity. Suitable for network administrators, IT support personnel, and recent graduates, the course serves those eager to protect digital environments and enhance their expertise in security strategies. It also benefits professionals aiming to validate their security skills with a globally recognized certification.

Learning Outcomes

By the end of this course, participants will

- 1 Develop proficiency in safeguarding networks and systems from cyber threats.
- 2 Analyze and manage security risks effectively to ensure IT infrastructure integrity.
- 3 Understand and apply compliance standards for regulatory adherence.
- 4 Execute incident response strategies to efficiently handle security breaches.
- 5 Comprehensive readiness for the CompTIA SecurityX certification, enhancing career potential.

Module by Module Learning *Outline*

6 Modules

Module 1: Introduction to Cybersecurity and CompTIA SecurityX

Learning Objectives:

- Understand the foundational concepts of cybersecurity.
- Get familiarized with the CompTIA SecurityX certification and its importance.

Topics Covered

Overview of Cybersecurity:

- Definition and evolution of cybersecurity.
- Importance and impact of cybersecurity in modern IT environments.

CompTIA SecurityX Certification:

- Benefits and opportunities provided by SecurityX certification.
- Exam structure and key topics covered.

Module 2: Network Security Essentials

Learning Objectives:

- Develop skills in implementing and managing secure network architecture.
- Identify and mitigate common network threats.

Topics Covered

Secure Network Design:

- Principles of designing a secure network.
- Implementing firewall, IDS/IPS, and VPNs.

Threats and Countermeasures:

- Common network threats such as DDoS attacks, man-in-the-middle attacks.
- Techniques for threat detection and prevention.

Module 3: Risk Management and Compliance

Learning Objectives:

- Analyze and evaluate risks to implement effective risk management strategies.
- Understand regulatory compliance standards.

Topics Covered

Risk Analysis and Management:

- Identifying and assessing potential security risks.
- Strategies for risk mitigation and control.

Compliance and Regulations:

- Overview of compliance frameworks like GDPR, HIPAA.
- Techniques for ensuring regulatory adherence.

Module 4: Identity and Access Management

Learning Objectives:

- Gain insights into managing identities and access control mechanisms.
- Implement identity verification technologies.

Topics Covered

Identity Management Concepts:

- Principles of identity and access management.
- Implementation of federated identity systems.

Access Control Strategies:

- Role-based access control (RBAC) and discretionary access control (DAC).
- Authentication methods: multi-factor, biometric verification.

Module 5: Cryptography and Data Protection

Learning Objectives:

- Understand cryptographic concepts and their applications.
- Implement strong data protection measures.

Topics Covered

Cryptographic Techniques:

- Symmetric vs. asymmetric encryption methods.
- Digital signatures and certificates.

Data Protection Practices:

- Techniques for securing data at rest and in transit.
- Backup and recovery strategies for data integrity.

Module 6: SecurityX Exam Preparation

Learning Objectives:

- Prepare effectively for the CompTIA SecurityX certification exam.
- Develop test-taking strategies and reinforce key cybersecurity concepts.

Topics Covered

Review of Core Topics:

- Highlighting key exam objectives and focus areas.
- Practice scenarios and application of knowledge.

Exam Strategies:

- Time management and question analysis techniques.
- Practice exams and evaluation of readiness.