

CompTIA SecurityX (CASP+)

Demonstrate fundamental cybersecurity concepts related to the defense of software, systems, and data, enabling robust threat protection and risk management.

 Certificate Included

[View Official Website](#) 

What you may learn


Simple and straight-to-the-point live classes

Our simple and direct-to-the-point classes are designed to help students learn faster and understand better.

 Start Today

Possible Career Tracks


 Security Engineer

 Penetration Tester

 GRC Specialist

 Threat Intelligence Analyst

 Security Architect

 Security Analyst



Taught by Industry Veterans & World Class Instructors

Introduction to CompTIA SecurityX


Overview

This certification is an opportunity for you to demonstrate advanced-level cybersecurity knowledge and skills. As a candidate for this certification, you should have familiarity with the self-paced or instructor-led learning material.

This certification is open to individuals from various IT security backgrounds. While there isn't a strict prerequisite for specialized experience, having a strong foundation in topics like enterprise security operations, risk management, and incident response is beneficial.


You can use CompTIA Security X to enhance your qualifications for roles such as security architect, senior security engineer, or security consultant. However, SecurityX isn't a prerequisite for any other specific certification.

Skills measured

 Foundations of Cybersecurity

 Threat Analysis & Mitigation

 Incident Response

 Network Security & Access Control

 Governance, Risk & Compliance (GRC)

Course Insights

Audience Profile

The CompTIA SecurityX course is designed for anyone interested in understanding the core principles and practices of cybersecurity. You don't need to have any experience with advanced security tools before taking this course, but a basic familiarity with operating systems, networking, and the Internet is assumed. Some of the concepts covered in the course require a foundational understanding of security best practices—such as password policies and encryption fundamentals.

The course includes hands-on activities that involve investigating security incidents, configuring security tools, and exploring real-world scenarios. Although prior experience with command-line interfaces or scripting isn't mandatory, having these skills can make the labs more approachable and maximize your learning experience.

Learning Outcomes

By the end of this course, participants will

1 Recognize the core principles of cybersecurity and common attack vectors.

2 Implement essential security controls to protect networks, systems, and data.

3 Apply fundamental risk management and compliance concepts to real-world scenarios.

4 Understand incident response procedures and threat mitigation tactics.

5 Explore encryption methods and access control strategies for secure operations.

Module Learning *Path*

4 Modules

Module 1: Introduction to Cybersecurity Concepts

Learning Objectives:

- Understand the fundamental principles of cybersecurity (Confidentiality, Integrity, Availability).
- Explore common types of cyber threats and vulnerabilities.

Topics Covered

Overview of Cybersecurity

- Core principles (CIA triad).
- Common attack types (phishing, malware, ransomware).

Understanding the Threat Landscape

- Threat actors and motivations.
- Vulnerabilities and exploits in various systems.

Hands-On Lab: Cybersecurity Baseline Assessment

- Identifying basic security controls on a local or virtual environment.
- Conducting a quick vulnerability scan.

Module 2: Network Security & Access Control

Learning Objectives:

- Learn the essentials of network protocols and security mechanisms.
- Implement access control methods to safeguard data and resources.

Topics Covered

Network Security Fundamentals

- TCP/IP overview and common ports.
- Firewalls, proxies, and intrusion detection/prevention systems.

Access Control

- Authentication, Authorization, and Accounting (AAA).
- Multi-factor authentication (MFA) and identity management.

Hands-On Lab: Firewall and IDS Configuration

- Configuring firewall rules in a lab environment.
- Implementing intrusion detection to monitor network traffic.

Module 3: Threat Analysis, Incident Response & Forensics

Learning Objectives:

- Identify and analyze potential threats and vulnerabilities using various tools.
- Understand the stages of incident response and basic forensic techniques.

Topics Covered

Threat Analysis Tools

- Vulnerability scanners (e.g., Nessus), endpoint protection platforms.
- Penetration testing basics.

Incident Response

- Incident response lifecycle (Preparation, Detection, Containment, Eradication, Recovery).
- Evidence preservation and chain of custody in digital forensics.

Hands-On Lab: Simulated Attack & Response

- Running a controlled attack scenario.
- Documenting and analyzing evidence to formulate a recovery plan.

Module 4: Governance, Risk Management & Compliance (GRC)

Learning Objectives:

- Recognize the importance of security governance and compliance frameworks.
- Apply risk assessment and management techniques in a business environment.

Topics Covered

Security Governance & Frameworks

- ISO 27001, NIST, GDPR, and other standards/regulations.
- Organizational security policies and procedures.

Risk Management

- Risk assessment methodologies (qualitative vs. quantitative).
- Implementing control measures and monitoring risk over time.

Hands-On Lab: Compliance Audit & Risk Assessment

- Performing a mini-audit against a chosen standard or framework.
- Creating a risk register with identified vulnerabilities and mitigations.



Hands-on learning with instructor-led classes



Lab platform with over 100+ tests, flashcards and more



Career Services Specialist assistance for your future



Certificate of Completion validated by the industry

A Complete Skillset

The technical skills you will showcase on your resume will provide a detailed overview of your expertise and proficiency in the field.

- Cyber Security Analyst
- Cloud Architect
- Data Analysis
- IT Project Management
- Cyber Fundamentals
- Cyber Forensics
- Advanced Cyber Security
- Advanced Artificial Intelligence

And full support after the pathway from our career specialist services team

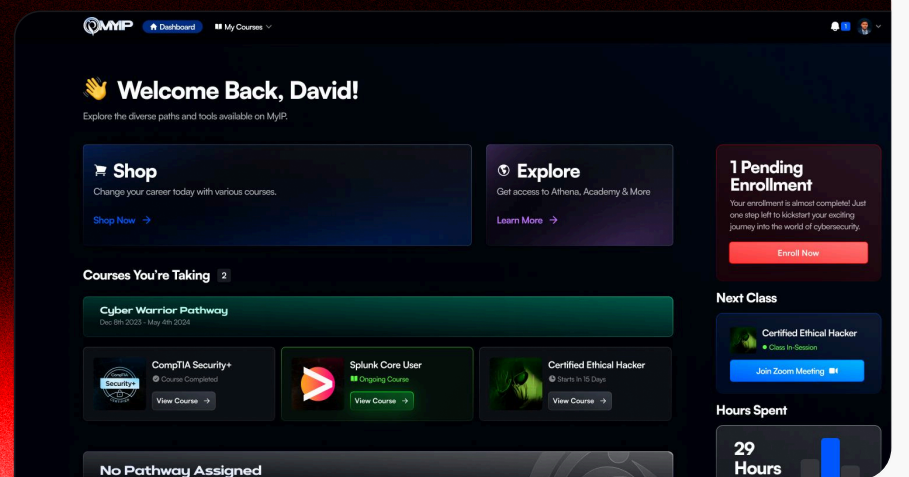
Certificate of Completion

A recognized certification to showcase your learning, demonstrate your skills, and enhance your resume.



Learn from scratch, earn a certificate, and gain valuable skills.

- 2000+ Students trained in 2023
- 70+ Courses available for you to empower your career
- 300+ Simulations available in our exclusive Learn Portal



Student Testimonials

Students Who Empowered Their Career With Our Courses

The next testimonial may be yours! ↓

"I had zero IT background but passed CompTIA Security+ on my first try after a few weeks of training with them. Their program is top-notch, covering simulations, videos, books, and tests thoroughly, plus extra sessions on job prep and study tips."



Nathan W. Student



"I went in to Intellectual Point not knowing what to expect when studying for the Security+ Certification. The instructor I had was very good in breaking the concepts. He was also very helpful during the multiple review sessions prior to exam. I recommend them a lot!"



Victor Eagle Student



"I had an incredible experience at Intellectual Point. The instructors there are true experts in their field, and I owe my success in acing my SEC+ exam to their excellent guidance and teaching."



Raul Ponce Student

