Tel +441273622272
info@siliconbeachtraining.co.uk

What is CompTIA Security+ Certification?

Enhance your computer security knowledge with our CompTIA Security+ course.

Through this CompTIA Security training course, you will learn the key fundamentals of IT security and the common practices. This training course features hands-on experience with the components you will have to familiarise yourself with when using this knowledge in the workplace environment.

The CompTIA Security is a globally recognised qualification which is highly sought after. To obtain that qualification you will have to enrol in this training course and pass the exam (not included).

This training course will teach you the fundamental principles of using security, threats and vulnerability analysis tools plus digital forensics tools. It will prepare you to take the CompTIA Cybersecurity Analyst+ CS0-001 exam by providing 100% coverage of the objectives and content examples listed on the syllabus. Study of the course can also help to build the prerequisites to study more advanced IT security qualifications, including CompTIA Advanced Security Practitioner (CASP) and ISC's CISSP (Certified Information Systems Security Professional).

What are the objectives of CompTIA Security+ Certification?

On certification completion, you will be able to:

- Identify tools and techniques to perform an environmental reconnaissance of a target network or security system.
- Collect, analyze, and interpret security data from multiple log and monitoring sources.
- Use network host and web application vulnerability assessment tools and interpret the results to provide effective mitigation.
- Understand and remediate identity management, authentication, and access control issues.
- Participate in a senior role within an incident response team and use forensic tools to identify the source of an attack.
- Understand the use of frameworks, policies, and procedures and report on security architecture with recommendations for effective compensating controls.

Who is CompTIA Security+ Certification intended for?

This training course is intended for those wishing to qualify for CompTIA Cybersecurity Analyst+ Certification (CSA+). CompTIA's CSA+ Certification is an intermediate-level certificate for IT professionals with previous experience of working in the field of IT security. The CompTIA Cybersecurity Analyst+ examination is designed for IT security analysts, vulnerability analysts, or threat intelligence analysts.The CS0-001 exam will certify that the successful candidate has the knowledge and skills required to configure and use threat detection tools, perform data analysis, and interpret the results to identify vulnerabilities, threats, and risks to an organisation with the end goal of securing and protecting applications and systems within an organisation.

Ideally, you should have successfully completed "CompTIA Network+ Certification" and "CompTIA Security+ Certification" courses or have equivalent knowledge. Specifically, it is recommended that you have the following skills and knowledge before starting this course:

- Know basic network terminology and functions (such as OSI Model, Topology, Ethernet, Wi-Fi, switches and routers).
- Understand TCP/IP addressing, core protocols, and troubleshooting tools.
- Identify network attack strategies and defences.
- Know the technologies and uses of cryptographic standards and products.
- Identify network- and host-based security technologies and practices.
- Describe the standards and products used to enforce security on the web and communications technologies.

CompTIA Security+ Certification Exam

This CompTIA Security+ does not include the exam.

This exam will cover topics such as threats and vulnerabilities with IT security, it will also deal with the security of networks as well.

The exam lasts for a duration of 90 minutes with a total of 90 questions in the paper. The pass mark is 750/900.

Ideally, you should have successfully completed "CompTIA Network+ Certification" and "CompTIA Security+ Certification" courses or have equivalent knowledge. Specifically, it is recommended that you have the following skills and knowledge before starting this course:

- Know basic network terminology and functions (such as OSI Model, Topology, Ethernet, Wi-Fi, switches and routers).
- Understand TCP/IP addressing, core protocols, and troubleshooting tools.
- Identify network attack strategies and defences.
- Know the technologies and uses of cryptographic standards and products.
- Identify network- and host-based security technologies and practices.
- Describe the standards and products used to enforce security on the web and communications technologies.

Identifying Security Threats

- Identify Social Engineering Attacks
- Classify Network Attacks
- Classify Software Based Attacks

Hardening Internal Systems

- Harden Base Operating Systems and Directory Services
- DHCP Services
- DHCP Servers

- Network File
- Print Servers

Internetwork Devices and Services

- Hardening Internetwork Connection Devices
- DNS and BIND Servers
- Web Servers and FTP Servers
- Email Servers

Securing Network Communications

- Secure Network Traffic Using IP Security (IPSec)
- Wireless Traffic
- Client Internet Access
- Remote Access Channel

Public Key Infrastructure

- Install a Certificate Authority (CA) Hierarchy
- Back Up Certificate Authorities
- Restore a Certificate Authority

Monitoring the Security Infrastructure

- Scan For Vulnerabilities
- Monitor For Intruders
- Respond to Security Incidents

Enforcing Organisational Security Policy

- Enforce Corporate Security Policy Compliance
- Legal Compliance
- Physical Security Compliance

Educate Users

Enhance your computer security knowledge with our CompTIA Security+ course.

Through this CompTIA Security training course, you will learn the key fundamentals of IT security and the common practices. This training course features hands-on experience with the components you will have to familiarise yourself with when using this knowledge in the workplace environment.