CompTIA PUBLIC SECTOR NETWORK Certified B Corporation

CompTIA Security+ Certification Course

TRAINING

Secure Your Future: Elevate Your Career

Online → September 23 - 27, 2024 | 9AM - 5PM AEST

Overview

In an era where digital threats loom larger by the day, the demand for skilled cybersecurity professionals is skyrocketing. CompTIA Security+ stands as a critical milestone for IT professionals seeking to affirm their expertise in the world of cybersecurity.

This globally recognised certification validates your skills in securing applications, networks, and devices. It also proves your ability to proactively address security incidents with confidence and precision.

Designed with the latest cybersecurity trends and risk management techniques in mind, CompTIA Security+ covers essential domains such as threats, attacks, and vulnerabilities; technologies and tools; architecture and design.

Beyond theoretical knowledge, CompTIA Security+ emphasises practical, hands-on skills to ensure that you're not just prepared to pass an exam, but also to implement real-world cybersecurity solutions.

Whether you're looking to start a career in IT security, seeking to advance in your current role, or aiming to broaden your understanding of cybersecurity, CompTIA Security+ is your gateway to success.

Learning Outcomes

- **Assess the security posture of an enterprise environment and recommend and implement appropriate security solutions**
- **Monitor and secure hybrid environments, including cloud, mobile, and Internet of Things (IoT)**
- **Operate with an awareness of applicable regulations and policies, including principles of governance, risk, and compliance**
- **Identify, analyse, and respond to security events and incidents**

Who Should Attend

- **Security Administrator**
- **Cyber security analyst**
- **Information security analyst**
- **Systems Administrator**
- **Helpdesk Manager/Analyst**
- **Security Analyst**
- **Network/Cloud Engineer**
- **IT Auditors**
- **Security Engineer**
- **IT Project Manager**
- **Security Officer**
- **Information Security Manager**
- **DevOps/Software Developer**
- **Security Architect**

Why Attend

- **Step up an advance your career in cyber and information security**
- **Validate and build skills as a cyber security professional (and or equivalent).**
- **Prepare for the CompTIA Security Plus Exam and the opportunity to gain an internationally recognised certification**
- **Equip yourself with the knowledge, skills, and credentials to stand out in a competitive job market and make a lasting impact.**
- **Build practical, hands-on skills to ensure that you're not just prepared to pass an exam, but also to implement real-world cybersecurity solutions.**
- **Instructor-led**

Explore the Key Sessions

This program will be delivered across 5 days from 23 to 27 September 2024, 9am to 5pm with breaks for morning tea, lunch and afternoon tea.

Threats, Attacks, and Vulnerabilities

- Identifying different types of cybersecurity threats and attacks, such as viruses, malware, phishing, social engineering, and advanced persistent threats (APTs)
- Understanding the techniques used for exploiting vulnerabilities in systems and networks, including common attack vectors
- Analysing potential indicators of compromise and determining the types of malware and their impact on systems

Technologies and Tools

- Utilising security technologies and tools such as firewalls, VPNs, IDS/IPS, and encryption to protect network and information systems
- Implementing secure network architecture concepts and systems design to mitigate risks and vulnerabilities
- Applying security configurations to network, application, and endpoint devices

Architecture and Design

- Applying fundamental principles of security architecture and design to develop secure information systems and networks
- Understanding the importance of security frameworks, policies, and best practices in establishing a secure organisational environment
- Incorporating cloud, virtualisation, and mobile security considerations into organisational security planning

Identity and Access Management

- Managing identity and access control mechanisms to ensure the confidentiality, integrity, and availability of information
- Implementing effective authentication, authorisation, and accounting practices to safeguard against unauthorised access
- Understanding biometric systems, multifactor authentication, and the principles of least privilege and need-to-know access

Risk Management

- Identifying and analysing risks to organisational security and applying appropriate risk management strategies
- Understanding compliance regulations, legal requirements, and privacy laws that impact organisational security policies and procedures
- Developing and implementing policies and procedures for data security, incident response, and disaster recovery

Cryptography and PKI

- Understanding the principles of cryptography and its applications in securing data in transit, at rest, and in use
- Understanding cryptographic algorithms, key management practices, and common cryptographic attacks Applying digital signatures, hashing algorithms, and steganography for data integrity and authentication

PUBLIC SECTOR NETWORK

Certified B Corporation

Get In Contact

CONNECTING GOVERNMENT

PUBLICSECTORNETWORK.COM

AUSTRALIA / NEW ZEALAND

P +61 2 9057 9070

E info@publicsectornetwork.com

USA / CANADA

P +1 (510) 556-0789

E contact@publicsectornetwork.com

JOIN THE SOCIAL LEARNING PLATFORM FOR FREE AT PUBLICSECTORNETWORK.COM