

# Course overview

## CompTIA Security+ Certification Support Skills

(G630eng)



### Overview and objectives

The aim of this course is to help to prepare students for CompTIA's Security+ Certification exam. CompTIA Security+ validates knowledge of communication security, infrastructure security, cryptography, operational security, and general security concepts.

On completion of this course, students will be able to:

- Identify network attack strategies and defenses.
- Understand the principles of organizational security and the elements of effective security policies.
- Know the technologies and uses of encryption standards and products.
- Identify network- and host-based security technologies and practices.
- Describe how remote access security is enforced.
- Describe the standards and products used to enforce security on web and communications technologies.
- Identify strategies for ensuring business continuity, fault tolerance, and disaster recovery

### Certification track

This course will prepare students to take the SY0-101 CompTIA Security+ Certification exam, for the objectives released in November 2002.

Major corporations such as Sun, IBM/Tivoli Software Group, Symantec, Motorola, Hitachi Electronics Services and VeriSign value the CompTIA Security+ certification and recommend or require it of their IT employees.



### Target audience

This course is intended for students wishing to qualify with CompTIA Security+ Certification. Security+ is aimed primarily at networking professionals, but because security is vital to all levels and job roles within an organization, it will also benefit PC support analysts, application developers, and senior managers in accounting, sales, product development, and marketing.

# Course overview

## CompTIA Security+ Certification Support Skills

(G630eng)



### Course prerequisites

Ideally, students should have successfully completed CompTIA Network+ certification and have around 24 months' experience of networking support. It is not *necessary* that students pass the Network+ exam before completing Security+ certification, but this is *recommended*.

Regardless of whether students have passed Network+, it is recommended that they have the following skills and knowledge before starting this course:

- Know the function and basic features of the components of a PC.
- Use Windows to create and manage files and use basic administrative features (Explorer, Control Panel, Management Consoles).
- Basic network terminology (such as OSI Model, Topology, Ethernet, TCP/IP).
- TCP/IP addressing, core protocols, and troubleshooting tools.

### Course contents

The course consists of two volumes, with a study volume, containing indexed notes and review questions, and a companion volume, containing exam objectives mapping, exam information, practical labs, answers to review questions, and a comprehensive glossary. The course also comes with an online practice exam.

An instructor edition of the course is available with margin notes and tips for the trainer. Access to course resources on gtslearning's trainer portal ([www.gtstrainer.com](http://www.gtstrainer.com)) is also available, subject to meeting minimum order requirements. gtstrainer hosts setup guides and data, PowerPoint slides, timetables, and extra exam information.

#### Module 1 - Security Fundamentals

- **Security Concepts** Why is Security Important? • Security Fundamentals • Access Control • Authentication • Accounting • Training
- **Threats** Types and Sources of Threats • What Makes a Network Secure? • Network Attack Strategies • Malware
- **Operational Security** Corporate Security Policy • Risk Identification • Privilege Policies • Disposal / Destruction Policy • HR Policy • Incident Response Policy

#### Module 2 - Cryptography

- **Cryptography** What is Cryptography? • Encryption Technologies • Cryptographic Attacks
- **Public Key Infrastructure** What is PKI? • Implementing PKI • Cryptographic Standards

# Course overview

## CompTIA Security+ Certification Support Skills

(G630eng)



### Module 3 - Implementing Local Security

- **Site Security** Physical Access Controls • Environmental Security
- **Network Security** Secure Network Topologies • Virtual LANs (VLAN) • Network Address Translation • Tunneling • Network Infrastructure • Switches • Routers • Firewalls • Network Management • Servers and Workstations • Removable Media
- **OS and Applications Security** OS Hardening • Directory Services • File and Print Services • Databases • Dynamic Host Configuration Protocol • Name Resolution Using DNS
- **Auditing and Intrusion Detection Systems** Audit Logs • Intrusion Detection Systems • Honey Pots • System Scanning
- **Wireless Access Security** Wireless Networks • Wireless LANs

### Module 4 - Implementing Remote Security

- **Remote Access Security** What is Remote Access? • Remote Access Infrastructure • Remote Connectivity Protocols • Remote Access Server • Enterprise Remote Access Authentication • Remote Authentication Protocols • Hardening Remote Access Infrastructure
- **Securing Email and Messaging Communications** Email Standards • Email Application Security • Email Confidentiality • Instant Messaging and VoIP • Network News Transfer Protocol • File Transfer
- **Securing Web Services** HTTP • SSL / TLS • Web Servers • Web Browsers • WAP and WTLS

### Module 5 - Disaster Recovery and Business Continuity

- **Disaster Recovery and Business Continuity** Disaster Recovery Planning • Fault Tolerance and Redundancy • Backup Strategies