

# Course overview

## g631eng Security+ Certification (2008 Objectives)

(g631eng)



### Overview and objectives

The aim of this course is to prepare students for CompTIA's Security+ 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

The course has been approved through the CompTIA Authorized Quality Curriculum program.

### Certification track

This course will prepare students to take the SY0-201 CompTIA Security+ exam, for the objectives released in October 2008.

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+. The qualification 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

## g631eng Security+ Certification (2008 Objectives)

(g631eng)



### 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 CompTIA Network+ exam before completing CompTIA Security+, but this is *recommended*.

Regardless of whether students have passed CompTIA 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 and 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 two online practice exams.

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.com 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 • Identification and Authentication • Accounting • Training
- **Threats** • Types and Sources of Threats • What Makes a Network Secure? • Social Engineering • Malware • Network Attack Strategies
- **Operational Security** • Corporate Security Policy • Risk Management • Privilege Policies • Disposal / Destruction Policy • HR Policy • Incident Response Policy

#### Module 2 - Cryptography

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

# Course overview

## g631eng Security+ Certification (2008 Objectives)

(g631eng)



### 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 Interconnections • Switches • Routers • Firewalls • SNMP • Network Access Control
- **Wireless Access Security** • Wireless Technologies • Wireless LAN Security
- **Operating System Security** • Computer Hardening • Hardening Windows • Hardening Other OS • Virtualization Technologies • Services and Protocols • Hardware and Software Updates • Authentication Technologies • Directory Services
- **Application Security** • File and Print Services • Storage Security • Databases • DHCP Security • DNS Security
- **Auditing and Intrusion Detection Systems** • Systems and Performance Monitoring • Audit Logs • Vulnerability Assessments • Intrusion Detection Systems • Honey pots

### 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 Authentication and Confidentiality • Instant Messaging and VoIP • File Transfer
- **Securing Web Services** • HTTP • SSL / TLS • Web Servers • Web Browsers • Desktop Security Applications

### Module 5 - Disaster Recovery and Business Continuity

- **Disaster Recovery and Business Continuity** • Disaster Recovery Planning • Business Continuity • Secure Recovery • Backup Strategies

## CompTIA Certification Update Policy

CompTIA's Certification Update Policy allows candidates holding certification under the previous exam objectives to update their certification by taking a special bridge exam.

The instructor edition of this course contains extensive notes on the differences between the 2008 and 2002 objectives, for those using the course to prepare students to take the bridge exam (BR0-001).