Course overview

# CompTIA Security+ (Exam SY0-401)

(G634eng)

## Target Audience

This 5-day course is intended for those wishing to qualify with CompTIA Security+ Certification. Security+ is foundation-level certification designed for IT administrators with 2 years' experience whose job role is focused on system security.

> *The CompTIA Security+ exam will certify that the successful candidate has the knowledge and skills required to identify risk, to participate in risk mitigation activities, and to provide infrastructure, application, information, and operational security. In addition, the successful candidate will apply security controls to maintain confidentiality, integrity, and availability, identify appropriate technologies and products, troubleshoot security events and incidents, and operate with an awareness of applicable policies, laws, and regulations.*
>
> *CompTIA A+ Syllabus*

## Courseware with Integrated Learning from Professor Messer

Professor Messer has long been a web hero for CompTIA certification students. For many years, Professor Messer has provided video-based training courses for CompTIA certifications. With professionally-produced lessons covering the full exam objectives and online forums, Professor Messer is a trusted online source for exam information.

Now, gtslearning has partnered with Professor Messer to take this learning to a new level. You will be able to study from the gtslearning courseware and link to the appropriate training video (by QR code, hyperlink or typing short URL) for further explanation. Equally, a student studying from the Professor Messer video course will be able to easily follow his video presentations using the same CompTIA CAQC Official courseware.

## Certification track

This courseware bears the seal of CompTIA Approved Quality Content. This seal signifies this content covers 100% of the exam objectives and implements important instructional design principles. CompTIA recommends multiple learning tools to help increase coverage of the learning objectives. The contents of this training material were created for the CompTIA Security+ Certification SY0-401 exam covering the covering the 2014 Edition Security+ certification exam objectives.

CompTIA APPROVED QUALITY CONTENT

OFFICIAL

MULTI-LAYERED LEARNING TOOLS INCLUDED

## Target audience and course prerequisites

CompTIA Security+ is aimed at IT professionals with job roles such as security architect, security engineer, security consultant/specialist, information assurance technician, security administrator, systems administrator, and network administrator.

Ideally, you should have successfully completed the "CompTIA Network+ Support Skills" course and have around 24 months' experience of networking support or IT administration. It is not *necessary* that you pass the Network+ exam before completing Security+ certification, but it is *recommended*.

Regardless of whether you have passed Network+, it is recommended that you 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).
- Know basic network terminology and functions (such as OSI Model, Topology, Ethernet, TCP/IP, switches, routers).
- Understand TCP/IP addressing, core protocols, and troubleshooting tools.

## Course outcomes

This course will teach you the fundamental principles of identifying risk and implementing security controls and help you to progress a career in IT security administration. It will prepare you to take the CompTIA Security+ exam by providing 100% coverage of the objectives and content examples listed on the syllabus. Study of the course can act as groundwork for more advanced training.

On course completion, you 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 cryptographic standards and products.
- Identify network- and host-based security technologies and practices.
- Describe how wireless and 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.

## Course contents

The course consists of a study volume, containing indexed notes and review questions, plus exam objectives mapping, exam information, and a comprehensive glossary. The course also comes with an online practice exam, pre-requisites test, pre-/post-unit assessment tests plus written scenarios to test students' ability to select appropriate controls and configuration options for given tasks. An optional hands-on labs volume is also available to purchase separately.

An instructor edition of the course is available with margin notes and tips for the trainer. Access to course resources (setup guides and data, PowerPoint slides, timetables, and extra exam information) is also available, subject to meeting minimum order requirements.

**Module 1 – Security Threats and Controls**

- **Security Controls** • Why is Security Important? • Security Policy • Security Controls • Identification • Authentication • Authorization • Basic Authorization Policies • Accounting • Labs • Hyper-V
- **Threats and Attacks** • Vulnerability, Threat, and Risk • Social Engineering • Phishing • Malware • Trojans and Spyware • Preventing Malware • Anti-Virus Software • Removing Malware • Labs • Trojans and Malware Protection
- **Network Attacks** • Network Fundamentals • Sniffers and Protocol Analyzers • ARP Attacks • IP Spoofing and Hijacking • Network Mappers and Port Scanners • Denial of Service Attacks • Labs • Network Vulnerabilities
- **Assessment Tools and Techniques** • Vulnerability Assessments and Pentests • Security Assessment Techniques • Vulnerability Scanners • Honeypots and Honeynets • **Labs** • Baseline Security Analyzer

**Module 2 – Cryptography and Access Control**

- **Cryptography** • Uses of Cryptography • Cryptographic Terminology and Ciphers • Encryption Technologies • Cryptographic Hash Functions • Symmetric Encryption • Asymmetric Encryption • Diffie-Hellman • ECC and Quantum Cryptography • Transport Encryption • Cryptographic Attacks • Steganography • **Labs** • Steganography
- **Public Key Infrastructure** • PKI and Certificates • Certificate Authorities • Implementing PKI • Creating Keys • Key Recovery Agents • Key Status and Revocation • PKI Trust Models • Cryptographic Standards • PGP / GPG • **Labs** • Configuring Certificate Services
- **Password Authentication** • LAN Manager / NTLM • Kerberos • PAP and CHAP • Password Protection • Password Attacks • **Labs** • Password Sniffing
- **Strong Authentication** • Token-based Authentication • Biometric Authentication • Common Access Card • Extensible Authentication Protocol • RADIUS and TACACS+ • Federation and Trusts
- **Authorization and Account Management** • Privilege Policies • Directory Services • Lightweight Directory Access Protocol • Windows Active Directory • Creating and Managing User Accounts • Managing Group Accounts • Account Policy Enforcement • User Rights, Permissions, and Access Reviews

**Module 3 – Network Security**

- **Secure Network Design** • Secure Network Topologies • Demilitarized Zones • Other Security Zones • Network Device Exploitation • Switches and VLANs • Switch Vulnerabilities and Exploits • Routers • Network Address Translation
- **Security Appliances and Applications** • Basic Firewalls • Stateful Firewalls • Proxies and Gateways • Implementing a Firewall or Gateway • Web and Email Security Gateways • Intrusion Detection Systems • IDS Analysis Engines • Monitoring System Logs
- **Wireless Network Security** • Wireless LANs • WEP and WPA • Wi-Fi Authentication • Additional Wi-Fi Security Settings • Wi-Fi Site Security
- **VPN and Remote Access Security** • Remote Access • Virtual Private Networks • IPSec • Remote Access Servers • Remote Administration Tools • Hardening Remote Access Infrastructure • **Labs** • Configuring a VPN
- **Network Application Security** • Application Layer Security • DHCP Security • DNS Security • SNMP Security • Storage Area Network Security • IPv4 versus IPv6 • Telephony • **Labs** • Attacks Against DHCP and DNS

**Module 4 – Host, Data, and Application Security**

- **Host Security** • Computer Hardening • Host Security Management Plan • OS Hardening • Patch Management • Endpoint Security • Network Access Control • **Labs** • Network Access Protection
- **Data Security** • Data Handling • Data Encryption • Data Loss Prevention • Backup Plans and Policies • Backup Execution and Frequency • Restoring Data and Verifying Backups • Data Wiping and Disposal • **Labs** • Data Leakage Prevention
- **Web Services Security** • HyperText Transport Protocol • SSL / TLS • Web Servers • Load Balancers • File Transfer • **Labs** • HTTP and HTTPS
- **Web Application Security** • Web Application Technologies • Web Application Databases • Web Application Exploits • Web Application Browser Exploits • Secure Web Application Design • Auditing Web Applications • Web Browser Security • **Labs** • Web Application Vulnerabilities
- **Virtualization and Cloud Security** • Virtualization Technologies • Virtual Platform Applications • Virtualization Best Practices • Cloud Computing • Risks of Cloud Computing

**Module 5 – Operational Security**

- **Site Security** • Site Layout and Access • Gateways and Locks • Alarm Systems • Surveillance • Hardware Security • Environmental Controls • Hot and Cold Aisles • RFI / EMI • Fire Prevention and Suppression
- **Mobile and Embedded Device Security** • Static Environments • Mitigating Risk in Static Environments • Mobile Device Security • Mobile Device Management • BYOD Concerns • Mobile Application Security • Bluetooth and NFC
- **Risk Management** • Business Continuity Concepts • Risk Calculation • Risk Mitigation • Integration with Third Parties • Service Level Agreements • Change and Configuration Management
- **Disaster Recovery** • Disaster Recovery Planning • IT Contingency Planning • Clusters and Sites
- **Incident Response and Forensics** • Incident Response Procedures • Preparation • Detection, and Analysis • Containment • Eradication, and Recovery • Forensic Procedures • Collection of Evidence • Handling and Analyzing Evidence • **Labs** • Computer Forensic Tools
- **Security Policies and Training** • Corporate Security Policy • Operational Policies • Privacy and Employee Policies • Standards and Best Practice • Security Policy Training and User Habits • **Labs** • Scenario Questions