CERTIFICATION GUIDE

CompTIA Security+

What is it?

CompTIA Security+ is a global certification that validates the baseline skills necessary to perform core security functions and pursue an IT security career.

Why is it different?

- No other certification that assesses baseline cybersecurity skills has performance-based questions on the exam. Security+ emphasizes hands-on practical skills, ensuring the security professional is better prepared to problem solve a wider variety of issues.
- More choose Security+ for DoD 8570 compliance than any other certification.
- Focuses on the latest trends and techniques in risk management, risk mitigation, threat management and intrusion detection.
- The new Security+ certification covers the Junior IT Auditor/Penetration Tester job role, in addition to the previous job roles for Systems Administrator, Network Administrator, and Security Administrator.

Key Benefits

- Security+ is the first security certification IT professionals should earn. It establishes the core knowledge required of any cybersecurity role and provides a springboard to intermediate-level cybersecurity jobs.
- Security+ incorporates best practices in hands-on trouble-shooting to ensure security professionals have practical security problem-solving skills. Cybersecurity professionals with Security+ know how to address security incidents – not just identify them.
- Recent updates ensure the exam keeps pace with the evolving security landscape. Security+ is developed by leading IT experts and industry-wide survey feedback.
- Security+ is compliant with ISO 17024 standards and approved by the US DoD to meet directive 8140/8570.01-M requirements.

Exam #
SY0-501

Release Date
October, 2017

List Price
$320

Languages
English
(Japanese and Portuguese in Q2, 2018)

CE Required?
Yes

Accreditation
Accredited by ANSI to show compliance with the ISO 17024 Standard. It is also approved by the DoD for Directive 8140/8570.01-M.

What's in this version?

Version SY0-501 is designed to better reflect today's best practices for risk management and risk mitigation. The updated exam covers a greater emphasis on a security professional's practical and hands-on ability to both identify and address security threats, attacks and vulnerabilities.

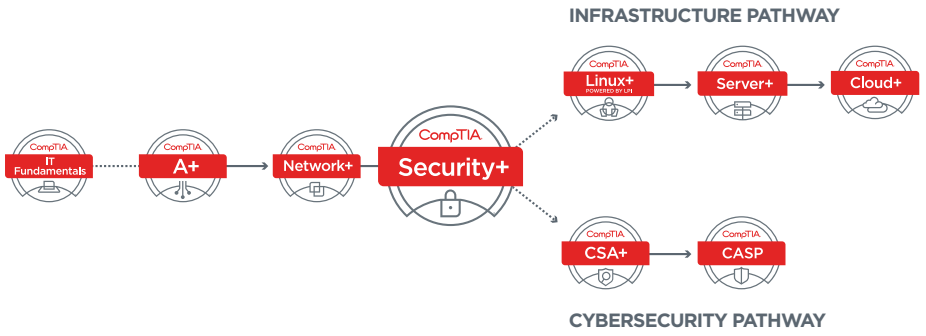
The new version has also been updated to reflect how cybersecurity jobs are becoming more specialized. As new skills (like security analytics) become more prevalent, skills covered in Security+ have become a baseline for all cybersecurity jobs. Because of this, the importance of and demand for Security+ has increased for a broader variety of job roles.

How does Security+ Compare to Alternatives?

	CompTIA Security+	CISCO	CEH Certified Ethical Hacker	GSEC
Certification	**Security+**	**CCNA Security**	**EC-Council Certified Ethical Hacker (CEH)**	**GIAC Security Essentials (GSEC)**
Performance-based Questions	Yes	No	No	No
Exam Length	1 exam, 90 min	1 exam, 90 min	1 exam, 4 hrs	1 exam, 5 hrs
Experience Level	Entry-level cybersecurity	Intermediate	Intermediate	Entry-level cybersecurity
Pre-requisites	CompTIA A+ and Network+ recommended	CCENT, CCNA Routing and Switching, OR CCIE certification	CEH Training, 2 years information security experience, Endorsement	None
Price	$320	$250	$700	$659

CompTIA Certification Pathway

CompTIA certifications align with the skillsets needed to support and manage IT infrastructure. Enter where appropriate for you. Consider your experience and existing certifications or course of study.



Recommended experience: CompTIA A+ and CompTIA Network+

Top Security+ Job Roles

- Systems Administrator
- Network Administrator
- Security Administrator
- Junior IT Auditor/ Penetration Tester
- Security Specialist
- Security Consultant
- Security Engineer

Technical Areas Covered in the Certification

Threats, Attacks and Vulnerabilities

21%

- Analyze indicators of compromise and determine types of malware
- Compare and contrast types of attacks
- Explain threat actor types and attributes
- Explain penetration testing concepts
- Explain vulnerability scanning concepts
- Explain the impact of types of vulnerabilities

Technologies and Tools

22%

- Install and configure network components, both hardware and software-based, to support organizational security
- Use appropriate software tools to assess the security posture of an organization
- Trouble-shoot common security issues
- Analyze and interpret output from security technologies
- Deploy mobile devices securely
- Implement secure protocols

Architecture and Design

15%

- Explain use cases and purposes for frameworks, best practices and secure configuration guides
- Implement secure network architecture concepts
- Implement secure systems design
- Explain the importance of secure staging deployment concepts
- Explain the security implications of embedded systems
- Summarize secure application development and deployment concepts
- Summarize cloud and virtualization concepts
- Explain how resiliency and automation strategies reduce risk
- Explain the importance of physical security controls

Identity and Access Management

16%

- Compare and contrast identity and access management concepts
- Install and configure identity and access services
- Implement identity and access management controls
- Differentiate common account management practices

Risk Management

14%

- Explain the importance of policies, plans and procedures related to organizational security
- Summarize business impact analysis concepts
- Explain risk management processes and concepts
- Follow incident response procedures
- Summarize basic concepts of forensics
- Explain disaster recovery and continuity of operations concepts
- Compare and contrast various types of controls
- Carry out data security and privacy practices

Cryptography and PKI

12%

- Compare and contrast basic concepts of cryptography
- Explain cryptography algorithms and their basic characteristics
- Install and configure wireless security settings
- Implement public key infrastructure

Organizations that have contributed to the development of Security+

- Northrop Grumman
- State of Minnesota
- Nationwide
- Southeastern Louisiana University
- Norfolk University
- Office of the Comptroller of the Currency
- Agile Defense, Inc.
- The Johns Hopkins University Applied Physics Laboratory
- Modern Technology Solutions, Inc. (MTSI)
- Archdiocese of Philadelphia
- Fayetteville Technical Community College
- Brotherhood Mutual
- The Joint Commission

Research and Statistics

Security Even Higher Priority

About 8 in 10 managers responsible for security at their firms across 12 countries covered in CompTIA's *International Trends in Cybersecurity* **expect security to become an even higher priority** over the next two years.†

Importance of Testing

Nearly all managers believe it is important to **test after IT security training** to confirm knowledge gains (96% net very important + somewhat important).†

Risk of Human Error

58% of organizations report **human error a major contributor to security risk.** Top sources of human cybersecurity error include (1) general carelessness, (2) failure to get up to speed on new threats, (3) lack of expertise with websites and applications, (4) end user failure to follow policies and procedures, (5) lack of expertise with networks, servers and other infrastructure, and (6) IT staff failure to follow policies and procedures.†

Serious Breaches Common

While nearly three-quarters of organizations report experiencing at least one security incident, about 6 in 10 had **one or more serious breaches**.†

"I needed to establish my career. In this profession, a person who has certifications is more recognized in the market."

Wanderley Martins
Security+ Certified

"When I got out of the Marine Corps, I realized a lot of potential employers require CompTIA Security+. You need more than just job training – you need certifications."

Michael Bays
Security+ Certified

† International Trends in Cybersecurity – CompTIA, April 2016

CompTIA