CERTIFICATION GUIDE

CompTIA Security+

What is it?

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

Why is it different?

- **More choose Security+** – chosen by more corporations and defense organizations than any other certification on the market to validate core security skills and for fulfilling DoD 8570 compliance.
- **Security+ proves hands-on skills** – the only baseline cybersecurity certification emphasizing vendor-neutral, hands-on practical skills, ensuring the security professional is better prepared to problem solve a wider variety of today's complex issues.
- **More job roles turn to Security+ to supplement skills** – baseline cybersecurity skills are applicable across more of today's job roles to secure systems, software and hardware.
- **Security+ is aligned to the latest trends and techniques** – covering the most core technical skills in risk assessment and management, incident response, forensics, enterprise networks, hybrid/cloud operations, and security controls, ensuring high-performance on the job.

About the exam

CompTIA Security+ is the first security certification a candidate 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 troubleshooting, ensuring candidates have practical security problem-solving skills required to:

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

Security+ is compliant with ISO 17024 standards and approved by the US DoD to meet directive 8140/8570.01-M requirements.

Exam #
SY0-601

Release Date
November 2020

Price
$349

Languages
English

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?

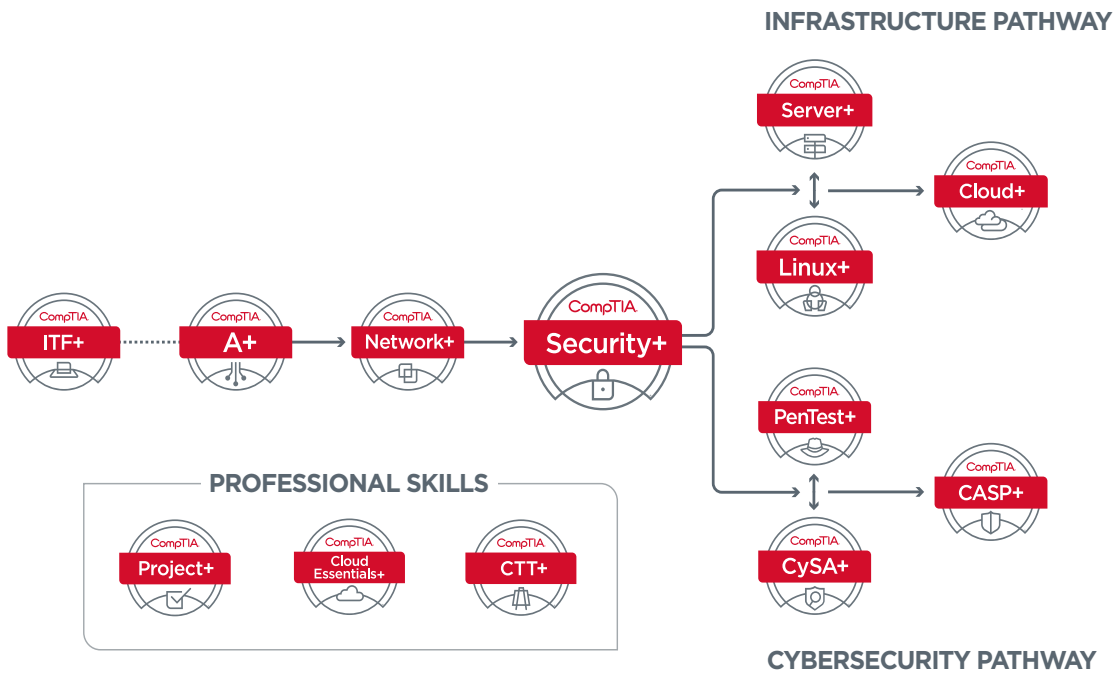
Cybersecurity attacks continue to grow. Increasingly, more job roles are tasked with baseline security readiness and response to address today's threats. Updates to Security+ reflect skills relevant to these job roles and prepare candidates to be more proactive in preventing the next attack.

New updates to the Security+ exam domains:

- Attacks, Threats and Vulnerabilities – Includes updated coverage of the latest threats, attacks, and vulnerabilities, such as IoT device weaknesses, newer DDoS attacks, and social engineering techniques based on current events.
- Architecture and Design - Includes coverage of enterprise environments and reliance on the cloud, which is growing quickly as organizations transition to hybrid networks.
- Implementation – Has been expanded to focus on administering identity, access management, PKI, basic cryptography, wireless, and end-to-end security.
- Operations and Incident Response - Includes organizational security assessment and incident response procedures, such as basic threat detection, risk mitigation techniques, security controls, and basic digital forensics.
- Governance, Risk, and Compliance - Expanded to support organizational risk management and compliance to regulations, such as PCI-DSS, SOX, HIPAA, GDPR, FISMA, NIST, and CCPA.

CompTIA Certification Pathway

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



"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

Technical Areas Covered in the Certification

Attacks, Threats and Vulnerabilities
24%

- Compare and contrast different types of social engineering techniques
- Analyze potential indicators to determine the type of attack
- Explain different threat actors, vectors, and intelligence sources
- Explain security concerns associated with various types of vulnerabilities
- Summarize techniques used in security assessments
- Explain techniques used in penetration testing

Architecture and Design
21%

- Explain importance of security concepts in an enterprise environment
- Summarize virtualization and cloud computing concepts, secure application development, deployment, and automation concepts
- Summarize authentication and authorization design concepts and the basics of cryptographic concepts
- Given a scenario, implement cybersecurity resilience
- Explain security implications of embedded and specialized systems and physical security controls

Implementation
25%

- Given a scenario, implement secure protocols, host or application security solutions, and secure network designs
- Comprehend how to install and configure wireless security settings and how to apply cybersecurity solutions to the cloud
- Given a scenario, implement authentication and authorization solutions and identity and account management controls
- Understand implementing public key infrastructure (PKI)

Operations and Incident Response
16%

- Given a scenario, use appropriate tool to assess organizational security
- Summarize importance of policies, processes, and procedures for incident response
- Given an incident, utilize appropriate data sources to support investigations
- Given an incident, apply mitigation techniques or controls to secure an environment
- Explain key aspects of digital forensics

Governance, Risk and Compliance
14%

- Compare and contrast various types of controls
- Explain importance of applicable regulations, standards, or frameworks that impact organizational security posture
- Explain importance of policies to organizational security
- Summarize risk management processes and concepts
- Explain privacy and sensitive data concepts in relation to security

How does Security+ Compare to Alternatives?

Certification	Security+	(ISC)2 Systems Security Certified Practitioner (SSCP)	EC-Council Certified Ethical Hacker (CEH)	GIAC Security Essentials (GSEC)
Performance-based Questions	Yes	No	No	No
Exam Length	1 exam, 90 minutes	1 exam, 180 minutes	1 exam, 4 hours	1 exam, 5 hours
Experience Level	Entry-level	Entry-level	Entry-level	Entry-level
Prerequisites	CompTIA A+ and Network+ recommended	Minimum of one year work experience in one or more domains	CEH Training, 2 years information security experience, Endorsement	None

Top Security+ Job Roles

- Security Administrator
- 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

Organizations that have contributed to the development of Security+

- Target Corp.
- Ricoh
- U.S. Navy Center for Information Dominance
- RxSense
- Johns Hopkins University Applied Physics Laboratory
- Splunk
- General Dynamics IT (GDIT)
- aeSolutions
- Max Life Insurance
- Southeastern Louisiana University
- Netflix
- SecureWorks
- University of Redlands
- Spire Inc.
- Australian Information Security Association / Deakin University

Research and Statistics

Security+ is in Demand

Among IT Professionals that hold CompTIA Certifications in North America, **62%** hold Security+.[1]

Certified Salary

The average salary for a CompTIA certified holder in North America is $93,097.

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

Wanderley Martins
Security+ Certified

CompTIA Certification Exams

What does it mean to be a "high stakes" exam?

An extraordinarily high level of rigor is employed in developing CompTIA certifications. Each question created for a CompTIA exam undergoes multiple layers of quality assurance and thorough psychometric statistical validation, ensuring CompTIA exams are highly representative of knowledge, skills and abilities required of real job roles. This is why CompTIA certifications are a requirement for many professionals working in technology. Hiring managers and candidates alike can be confident that passing a CompTIA certification exam means competence on the job. This is also how CompTIA certifications earn the ANSI/ISO 17024 accreditation, the standard for personnel certification programs. Over 2.3 million CompTIA ISO/ANSI-accredited exams have been delivered since January 1, 2011.

What does it mean to be a "vendor-neutral" exam?

All CompTIA certification exams are vendor-neutral. This means each exam covers multiple technologies, without confining the candidate to any one platform. Vendor-neutrality is important because it ensures IT professionals can perform important job tasks in any technology environment. IT professionals with vendor-neutral certifications can consider multiple solutions in their approach to problem-solving, making them more flexible and adaptable than those with training in just one technology.

What is a Performance Certification?

CompTIA performance certifications validate the skills associated with a particular job or responsibility. They include simulations that require the test taker to demonstrate multi-step knowledge to complete a task. CompTIA has a higher ratio of these types of questions than any other IT certifying body.

1 https://www.globalknowledge.com/us-en/content/salary-report/it-skills-and-salary-report/

CompTIA