

CompTIA Security+ SY0-701

Duration 5 Days

CompTIA Security+ Certification is an excellent entry point for a career in information security. CompTIA Security plus SY0-701 exam expands coverage of cybersecurity threats, risk management, and IoT threats. CompTIA Security+ course equips teams with the knowledge and skills required to assess the security posture of an enterprise environment, 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; identity, analyze, and respond to security events and incidents.

CompTIA Security+ training course is designed to provide learners with the knowledge and skills necessary to pass the exam and earn the certification. CompTIA Security+ prep course is an intensive program that includes instructor-led training, hands-on exercises, and practice exams. Our experienced instructors will guide you through the material and provide personalized attention to help you succeed.

Course Objectives

- Understand and compare various types of security controls and fundamental security principles.
- Analyze and respond to indicators of malicious activity and implement appropriate security solutions.
- Apply security principles to secure enterprise infrastructure and protect data.

- Understand the security implications of different architecture models and resilience strategies.
- Manage hardware, software, and data assets effectively to enhance security.
- Conduct vulnerability management activities and understand security alerting and monitoring tools.
- Implement and maintain identity and access management controls.
- Operate within applicable regulations and policies, understanding governance, risk, and compliance principles.

Target Audience:

Designed for a broad audience, The CompTIA Security+ SY0-701 course targets individuals ranging from the early stages of their cybersecurity careers to seasoned IT professionals looking to specialize further or validate their skills. It's ideal for those aspiring to roles such as security specialists, systems administrators, or security administrators. Additionally, IT professionals transitioning from other areas into security-focused positions will find this certification particularly beneficial.

The course also caters to current cybersecurity professionals aiming to keep their skills sharp and credentials updated. The globally recognized nature of this certification makes it appealing to anyone looking to position themselves competitively in the IT security job market, whether they're entering the field or seeking to ascend to higher, more specialized roles.

Security Administrator

- Network Administrator
- Security Consultant

Prerequisites

Basic understanding of computer networks and systems, including familiarity with the internet, devices, and technology.

- Knowledge of foundational IT skills will be helpful, preferably backed by experience or prior certifications (e.g., CompTIA Network+ or equivalent).
- A grasp of basic security concepts or experience in IT support roles with exposure to security tasks.
- Commitment to continuous learning and staying updated on new cybersecurity threats and technologies.

Course Outline

Module 1: General Security Concepts

- Compare and contrast various types of security controls.
- Summarize fundamental security concepts.
- Explain the importance of change management processes and the impact to security.
- Explain the importance of using appropriate cryptographic solutions.

Module 2: Security Operations

- Given a scenario, apply common security techniques to computing resources.
- Explain the security implications of proper hardware, software, and data asset management.
- Explain various activities associated with vulnerability management.
- Explain security alerting and monitoring concepts and tools.
- Given a scenario, modify enterprise capabilities to enhance security.
- Given a scenario, implement and maintain identity and access management.
- Explain the importance of automation and orchestration related to secure operations.
- Explain appropriate incident response activities.
- Given a scenario, use data sources to support an investigation.

Module 3: Security Architecture

- Compare and contrast security implications of different architecture models.
- Given a scenario, apply security principles to secure enterprise infrastructure.
- Compare and contrast concepts and strategies to protect data.

- Explain the importance of resilience and recovery in security architecture.

Module 4: Threats, Vulnerabilities, and Mitigations

- Compare and contrast common threat actors and motivations.
- Explain common threat vectors and attack surfaces.
- Explain various types of vulnerabilities.
- Given a scenario, analyze indicators of malicious activity.
- Explain the purpose of mitigation techniques used to secure the enterprise.

Module 5: Security Program Management and Oversight

- Summarize elements of effective security governance.
- Explain elements of the risk management process
- Explain the processes associated with third-party risk assessment and management.
- Summarize elements of effective security compliance.
- Explain types and purposes of audits and assessments.
- Given a scenario, implement security awareness practices.

CompTIA Security+

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

Open the Door to Your Cybersecurity Career with Security+

- **Launch a Successful Cybersecurity Career.** Develop a core foundation of essential skills, paving the way for a fulfilling career. More job roles use Security+ for baseline cybersecurity skills than any other certification in the industry.
- **Assess On-the-Job Skills.** Security+ is the most widely adopted ISO/ANSI-accredited early career cybersecurity certification on the market with hands-on, performance-based questions on the certification exam. These practical questions assess your ability to effectively problem solve in real-life situations and demonstrate your expertise to potential employers immediately.
- **Embrace the Latest Trends.** Understand and use the most recent advancements in cybersecurity technology, terms, techniques, and tools. By acquiring early career skills in the latest trends such as automation, zero trust, risk analysis, operational technology, and IoT, you will be well-equipped to excel in the ever-evolving cybersecurity landscape.

Prove Your Skills with Security+

CompTIA Security+ is the first early career cybersecurity certification a candidate should earn.

It equips cybersecurity professionals with the foundational security skills necessary to safeguard networks, detect threats, and secure data through performance-based questions—helping them open the door to a cybersecurity career and become a trusted defender of digital environments. The CompTIA Security+ 701 exam verifies the candidate has the knowledge and 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, Internet of Things (IoT), and operational technology.
- Operate with an awareness of applicable regulations and policies, including principles of governance, risk, and compliance.
- Identify, analyze, and respond to security events and incidents.



Exam #

SY0-701

Release Date

November 7, 2023

Languages

English

CE Required?

Yes

Accreditation

Accredited by ANSI to show compliance with the ISO 17024 Standard.

How does CompTIA Security+ compare to alternatives?

		 Systems Security Certified Practitioner		 Certified Ethical Hacker	 Systems Security Certified Practitioner
Certification	CompTIA Security+	ISC2 Systems Security Certified Practitioner (SSCP)	GIAC Security Essentials (GSEC)	EC-Council Certified Ethical Hacker (CEH)	ISC2 Certified in Cybersecurity
Performance-Based Questions	Yes	No	Yes	No	No
Vendor Neutral	Yes	Yes	Yes	Yes	Yes
Experience Level	Early Career	Early career	Early career	Early career	Entry level
Exam Focus	Baseline cybersecurity skills, core cybersecurity knowledge	Security administrator job role	Security administrator job role	Pen testing and ethical hacking	Cybersecurity terms and concepts
Training Products	Full suite of online test prep tools, LOT, books	Self-paced online, LOT, courseware, mobile toolkit	In-person training and online	Online review course and answers database, courseware	Self-paced online, LOT

Jobs that use CompTIA Security+

- Security Specialist
- Security Administrator
- Systems Administrator
- Help Desk Analyst
- Security Analyst
- Security Engineer

The great majority of candidates with IT certifications are more confident in their abilities (92%). Furthermore, most have more confidence to explore new job opportunities (81).

PearsonVUE

2023 Value of IT Certification Candidate Report; 2021 Value of IT Certification Employer Report

Technical skills covered in the certification and training

General Security Concepts 12% • Compare and contrast various types of security controls. • Summarize fundamental security concepts. • Explain the importance of change management processes and the impact to security. • Explain the importance of using appropriate cryptographic solutions.	Threats, Vulnerabilities & Mitigations 22% • Compare and contrast common threat actors and motivations. • Explain common threat vectors and attack surfaces. • Explain various types of vulnerabilities. • Given a scenario, analyze indicators of malicious activity. • Explain the purpose of mitigation techniques used to secure the enterprise.	Security Architecture 18% • Compare and contrast security implications of different architecture models. • Given a scenario, apply security principles to secure enterprise infrastructure. • Compare and contrast concepts and strategies to protect data. • Explain the importance of resilience and recovery in security architecture.
Security Operations 28% • Given a scenario, apply common security techniques to computing resources. • Explain the security implications of proper hardware, software, and data asset management. • Explain various activities associated with vulnerability management. • Explain security alerting and monitoring concepts and tools. • Given a scenario, modify Enterprise capabilities to enhance security. • Given a scenario, implement and maintain identity and access management. • Explain the importance of automation and orchestration related to secure operations. • Explain appropriate incident response activities. • Given a scenario, use data sources to support an investigation.		Security Program Management & Oversight 20% • Summarize elements of effective security governance. • Explain elements of the risk management process. • Explain the processes associated with third-party risk assessment and management. • Summarize elements of effective security compliance. • Explain types and purposes of audits and assessments. • Given a scenario, implement security awareness practices.

Nearly all IT managers (97%) recognize the value certified professionals bring to the organization such as boosting productivity, helping to meet client requirements and closing organizational gaps.

Organizations That Contributed to the Development of CompTIA Security+

- Blue Chip Talent
- Brotherhood Mutual
- Contentful
- Cyber Warfare Tactics LLC
- Deakin University
- Deloitte
- Fidelis Risk Advisory
- Fidelity Investments
- Five9
- General Dynamics IT (GDIT)
- Growth Arbor
- Johns Hopkins University Applied Physics Laboratory
- L3Harris
- Linford and Company LLC
- Lippert Components
- Microsoft
- MindPoint Group
- Nationwide
- Organon
- SecureWorks
- SenseOn
- SS&C Technologies
- U.S. Navy Center for Information Dominance
- Washington State Patrol
- Wells Fargo
- Zoom

Research and Statistics

Security+ is In Demand 24% of the total employed cybersecurity workforce in the U.S. are Security+ certified.¹

Well-Paying Positions Security+ job roles have a **median pay of \$80,000** in 2023.²

Job Openings In 2023, **13% of total cybersecurity job openings** request Security+ in the job requirements.³

★ 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 ISO/ANSI accreditation, the standard for personnel certification programs. CompTIA has awarded more than 3 million ISO/ANSI-accredited certifications in areas such as cybersecurity, networking, cloud computing, and technical support.

★ What does it mean to be a “vendor-neutral” certification?

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 to just one technology.

★ Prepare for your exam with Official CompTIA Content.

First and foremost, we're an education company. CompTIA offers everything you need to get ready for your Security+ certification exam. Explore training developed by CompTIA with options that fit various learning styles and timelines.

¹ Cyberseek

² Bureau of Labor Statistics, Occupational Outlook 2023, Network & Computer Systems Administrator

³ Cyberseek

