CompTIA

Security Origin

The Official CompTIA

Security+ Study Guide

Exam SY0-601

www.securityorigin.com

Index:

- Overview
- Why you should choose Security+
- Target Audience?
- Exam Information
- Prerequisites
- Course Objectives
- What will you learn?

CompTIA Security+

Your Gateway to a Fulfilling Career in IT Security!"

Achieving the CompTIA Security+ certification signifies possessing fundamental competencies vital for pursuing a career in IT security. For numerous up-and-coming cybersecurity enthusiasts, attaining this widely sought-after entry-level certification serves as an initial stride towards a lucrative and high-demand profession.

Empower Your Cybersecurity Future: Secure, Analyze, Mitigate, Comply

The Security+ certification program equips individuals with the necessary knowledge and skills to effectively secure applications, networks, and devices through proficient installation and configuration techniques. Participants learn to conduct thorough threat analyses and employ appropriate mitigation strategies to counter emerging cybersecurity challenges. Moreover, the program emphasizes active participation in risk mitigation activities, ensuring proactive defense measures are in place. By fostering an understanding of relevant policies, laws, and regulations, candidates are prepared to navigate the complex regulatory landscape with confidence. With Security+, individuals are empowered to achieve their cybersecurity goals by mastering essential competencies and staying abreast of industry best practices.

Overview:

The latest iteration of CompTIA Security+ (SY0-701) encapsulates cutting-edge cybersecurity knowledge, addressing prevalent threats, automation, zero-trust principles, IoT integration, risk management, and more. Upon certification, candidates gain a profound understanding of essential job skills, enhancing their employability as employers recognize their proficiency.

The Security+ exam validates competencies in:

- Evaluating the security stance of an organizational setup and suggesting and implementing suitable security measures.
- Safeguarding hybrid environments effectively, spanning cloud, mobile, IoT, and operational technology realms.
- Operating while adhering to relevant regulations and policies, encompassing governance, risk management, and compliance principles.
- Recognizing, dissecting, and responding to security incidents and events promptly.

CompTIA Security+ adheres to ISO 17024 standards and holds approval from the U.S. Department of Defense to fulfill Directive 8140.03M requirements. ANSI accreditation is pivotal as it instills confidence and trust in the accredited program's outcomes, with over 3 million CompTIA ISO/ANSI-accredited exams administered since January 1, 2011.

Why you should choose CompTIA Security+:

Comprehensive Foundation: Develop essential skills forming the backbone of a successful cybersecurity career, providing a solid foundation for advancement.

Industry Recognition: Security+ is the most preferred early-career certification, recognized by employers across various job roles, ensuring your skills align with industry standards.

Practical Assessment: Gain hands-on experience through performance-based questions, reflecting real-world scenarios, allowing you to demonstrate your problem-solving abilities effectively.

Stay Ahead of Trends: Stay abreast of the latest cybersecurity trends, including automation, zero trust, risk analysis, operational technology, and IoT, ensuring you're equipped to tackle contemporary challenges.

Immediate Employability: Armed with Security+, you'll be prepared to embark on a cybersecurity career journey with confidence, ready to meet the demands of the rapidly evolving cybersecurity landscape.

Launch your cybersecurity career with confidence through Security+. Gain a comprehensive understanding of core skills, validate your expertise with practical assessments, and stay ahead of industry trends, ensuring immediate employability in today's dynamic cybersecurity landscape.

Target Audience:

CompTIA Security+ caters to individuals with following categories:

- **Systems Administrator:** Manages and maintains an organization's IT infrastructure, including servers, operating systems, and software applications.
- **Network Administrator**: Oversees the setup, operation, and maintenance of an organization's network infrastructure, ensuring connectivity and security.
- **Security Administrator:** Implements and manages security measures to protect an organization's systems, networks, and data from cyber threats.
- **Junior IT Auditor/Penetration Tester:** Conducts audits and penetration tests to identify vulnerabilities in an organization's IT systems and assesses the effectiveness of security controls.
- **Security Specialist:** Specializes in designing, implementing, and managing security solutions to protect against cyber threats and ensure compliance with security policies.
- **Security Consultant**: Provides expert advice and guidance to organizations on improving their security posture, developing security strategies, and mitigating cyber risks.
- **Security Engineer:** Designs, implements, and maintains security infrastructure and systems, such as firewalls and intrusion detection systems, to protect against cyber threats.
- **Anyone who wants to start a career in Cyber Security**: Aspiring cybersecurity professionals seeking to embark on a career in the field.

This certification is tailored for those aiming to initiate or progress their careers within the realm of cybersecurity.

Pre-requisites:

This program seeks IT professionals with a minimum of two years' experience in IT administration, particularly emphasizing security-oriented roles. This experience can be demonstrated during the application process.

Exam Information:

Number of Questions: 90	Test Duration: 1.5 Hours
Test Format: Multiples Choice & Performance Based	Test Delivery: Online Proctored
Exam Prefix: SYO 601 - SYO 701	Passing Score:750 (on scale of 100-900)

Course Objectives:

Module 01: General Security Concepts (12%)

Covers foundational principles and theories of cybersecurity, including confidentiality, integrity, and availability, along with basic security protocols and mechanisms.

Module 02: Threats, Vulnerabilities, and Mitigations (22%)

Focuses on identifying and understanding various cyber threats and vulnerabilities, and implementing appropriate mitigation strategies to address them effectively.

Module 03: Security Architecture (18%)

Explores the design and implementation of secure network architectures and systems, including access control, encryption, and secure protocols, to protect against cyber threats.

Module 04: Security Operations (28%)

Addresses the day-to-day tasks and activities involved in managing and maintaining cybersecurity measures, such as incident response, monitoring, and patch management.

Module 05: Security Program Management and Oversight (20%)

Involves the development, implementation, and oversight of comprehensive cybersecurity programs, including risk management, compliance, and governance, to ensure organizational security goals are met.

Module 17: Business Continuity and Disaster Recovery

-Addresses strategies for ensuring business continuity and recovery from disasters, including the development of contingency plans.

These modules collectively provide a comprehensive overview of network and cybersecurity, covering a wide range of topics to prepare professionals for securing diverse IT environments.

What you will learn:

General Security Concepts
Includes key cybersecurity terminology and concepts up front to provide a foundation for security controls discussed throughout the exam.

Threats, Vulnerabilities & Mitigations
Focuses on responding to common threats, cyberattacks, vulnerabilities, and security incidents and appropriate mitigation techniques to monitor and secure hybrid environments.

Security Architecture
Includes security implications of different architecture models, principles of securing enterprise infrastructure, and strategies to protect data.

Security Operations
Includes applying and enhancing security and vulnerability management techniques, as well as security implications of proper hardware, software, and data management.

Security Program Management & Oversight
Updated to better reflect the reporting and communication skills required for Security+ job roles relating to governance, risk management, compliance, assessment, and security awareness.

www.securityorigin.com