CompTIA Security+ Exam Prep: Master SY0-701 with Expert Guidance

28 February – 4 March 2027
Bangkok

AGILE LEADERS
Training Center

AGILE LEADERS
Training Center

CompTIA Security+ Exam Prep: Master SY0-701 with Expert Guidance

Ref: 103600442_109371 **Date:** 28 February – 4 March 2027 **Location:** Bangkok **Fees:** 6000 Euro

Course Overview:

This CompTIA Security+ SY0-701 Exam Preparation Course is designed to help participants develop the essential skills and knowledge needed to pass the CompTIA Security+ certification exam. It covers topics such as security controls, threats and vulnerabilities, network security, risk management, and incident response. This course will equip learners with real-world insights to apply in securing systems and managing risks within an organization. Whether you are preparing for the SY0-701 exam or want to advance your cybersecurity certification journey, this training provides the comprehensive understanding necessary to pass the exam and secure an IT role.

- Learn about CompTIA Security+ exam objectives, security operations, vulnerability management, and much more.
- Master Security+ SY0-701 practice tests and study materials to prepare for the certification.
- Review essential CompTIA Security+ certification tips and exam questions.

Target Audience:

- IT professionals
- Security administrators
- Network administrators
- Systems administrators
- Anyone looking to pass the CompTIA Security+ SY0-701 exam

Targeted Organizational Departments:

- IT Security
- Network Security
- Risk Management
- Compliance & Governance
- Incident Response & Cybersecurity Operations

AGILE LEADERS
Training Center

Targeted Industries:

- Information Technology
- Financial Services
- Healthcare
- Government & Defense
- Education
- Cloud Providers & Tech Startups

Course Offerings:

By the end of this course, participants will be able to:

- Assess the security posture of an enterprise environment and recommend security solutions.
- Monitor and secure cloud environments, mobile devices, and IoT.
- Operate with an understanding of governance, compliance, and risk management principles.
- Analyze security incidents, apply mitigation techniques, and respond effectively to cybersecurity events.

Training Methodology:

This course will use a mix of interactive lectures, hands-on exercises, practice exams, and group discussions to help participants learn and apply cybersecurity concepts. We will also include real-life case studies and exam objectives mapping to ensure a deep understanding of the course materials.

- Case studies from various industries
- Security+ SY0-701 practice questions and exam simulations
- Interactive sessions on network security, cryptography, and identity management

Course Toolbox:

Participants will have access to:

- Study Guides and CompTIA Security+ practice exams
- CompTIA Security+ syllabus
- Online resources and video tutorials
- Access to security tools e.g., encryption software, firewalls, etc. used in real-world cybersecurity practices

AGILE LEADERS
Training Center

Course Agenda:

Day 1: Security Fundamentals

- **Topic 1:** Introduction to the CompTIA Security+ SY0-701 Exam Objectives
- **Topic 2:** General Security Concepts CIA Triad: Confidentiality, Integrity, Availability
- **Topic 3:** Risk Management and Governance Frameworks
- **Topic 4:** Security Controls: Types Preventive, Detective, Corrective, Compensating
- **Topic 5:** Authentication Methods and Access Control
- **Topic 6:** Security Operations and Understanding Incident Response
- **Reflection & Review:** Review key concepts from Day 1 and apply Security+ exam prep to real-world scenarios.

Day 2: Threats, Vulnerabilities & Mitigation

- **Topic 1:** Types of Malware Attacks Ransomware, Trojans, Worms
- **Topic 2:** Social Engineering Attacks Phishing, Smishing, Vishing
- **Topic 3:** Threat Vectors and Attack Surfaces Email, Wireless, Removable Media
- **Topic 4:** Cryptography Basics Encryption, Hashing, PKI
- **Topic 5:** Vulnerability Management Identifying, Analyzing, Mitigating
- **Topic 6:** Security Tools for Threat Detection and Incident Response
- **Reflection & Review:** Analyze case studies and threat mitigation techniques using Security+ practice questions.

Day 3: Security Architecture

- **Topic 1:** Network Security Architecture Firewalls, VPNs, IDS/IPS
- **Topic 2:** Cloud Security and Hybrid Environments
- **Topic 3:** Zero Trust Architecture and Principles of Secure Design
- **Topic 4:** Cryptographic Protocols Public Key Infrastructure, Key Management
- **Topic 5:** Incident Response Frameworks and Security Monitoring
- **Topic 6:** Data Protection Strategies and Resilience in Security Architecture
- **Reflection & Review:** Simulate network and cloud security vulnerabilities and defenses with Security+ exam practice.

Day 4: Security Operations & Incident Response

- **Topic 1:** Security Monitoring and Alerting in Security Operations
- **Topic 2:** Vulnerability Management and Patch Management
- **Topic 3:** Security Compliance GDPR, HIPAA, SOX
- **Topic 4:** Incident Detection and Response Strategies
- **Topic 5:** Data Privacy and Legal Considerations
- **Topic 6:** Security Automation and Orchestration in Incident Response
- **Reflection & Review:** Practice handling cybersecurity incidents using Security+ exam objectives and simulations.

Day 5: Exam Preparation & Review

- **Topic 1:** Review all CompTIA Security+ SY0-701 domains and exam objectives
- **Topic 2:** CompTIA Security+ Exam Questions and Test-Taking Strategies
- **Topic 3:** Review Security+ Practice Exams for all domains
- **Topic 4:** Final Discussion on Security+ Certification Tips and Exam Resources
- **Topic 5:** Common Mistakes to avoid during the Security+ Exam
- **Topic 6:** Post-Exam Strategy: Continuing your learning path post-certification
- **Reflection & Review:** Answer Security+ exam prep questions, engage in group discussions, and review key topics for the final exam.

FAQ:

What specific qualifications or prerequisites are needed for participants before enrolling in the course?

Participants should have at least 2 years of IT administration experience, with a focus on security, and an understanding of basic networking concepts.

How long is each day's session, and is there a total number of hours required for the entire course?

Each day's session typically lasts around 4-5 hours, totaling approximately 20-25 hours of instruction over 5 days.

What is the best way to prepare for the exam after completing this course?

Practice using CompTIA Security+ SY0-701 practice tests, refer to the CompTIA Security+ study guide, and continue studying using the exam objectives to ensure success.

AGILE LEADERS
Training Center

How This Course is Different from Other CompTIA Security+ SY0-701 Exam Prep Courses:

Unlike other CompTIA Security+ certification training programs, this course offers an integrated approach, combining exam-specific knowledge with practical insights into real-world security issues. Participants will not only pass the exam but will also gain actionable knowledge applicable in enterprise environments. Additionally, the course includes exclusive access to exam preparation tools and practice tests designed to simulate the actual Security+ exam experience, helping learners build confidence.