

**uCertify**

# Course Outline

**CompTIA Security+ (SY0-701)**



11 May 2024

1. Course Objective
2. Pre-Assessment
3. Exercises, Quizzes, Flashcards & Glossary  
Number of Questions
4. Expert Instructor-Led Training
5. ADA Compliant & JAWS Compatible Platform
6. State of the Art Educator Tools
7. Award Winning Learning Platform (LMS)
8. Chapter & Lessons  
Syllabus  
Chapter 1: Introduction  
Chapter 2: Today's Security Professional  
Chapter 3: Cybersecurity Threat Landscape  
Chapter 4: Malicious Code  
Chapter 5: Social Engineering and Password Attacks  
Chapter 6: Security Assessment and Testing  
Chapter 7: Application Security  
Chapter 8: Cryptography and the PKI  
Chapter 9: Identity and Access Management  
Chapter 10: Resilience and Physical Security  
Chapter 11: Cloud and Virtualization Security  
Chapter 12: Endpoint Security  
Chapter 13: Network Security  
Chapter 14: Wireless and Mobile Security  
Chapter 15: Monitoring and Incident Response  
Chapter 16: Digital Forensics  
Chapter 17: Security Governance and Compliance  
Chapter 18: Risk Management and Privacy

Videos and How To

9. Practice Test

Here's what you get

Features

10. Live labs

Lab Tasks

Here's what you get

11. Post-Assessment

## 1. Course Objective

The CompTIA Security+ (SY0-701) course covers the SY0-701 exam objectives and provides knowledge in areas such as covering in-demand skills related to current threats, automation, zero trust, IoT, risk, and more, this course represents the forefront of cybersecurity education. Learn and use the newest developments in cybersecurity technology, terminology, techniques, and tools. The CompTIA Security+ study guide will help you get a full understanding of the challenges you'll face as a security professional.

## 2. Pre-Assessment

Pre-Assessment lets you identify the areas for improvement before you start your prep. It determines what students know about a topic before it is taught and identifies areas for improvement with question assessment before beginning the course.

## 3. Exercises

There is no limit to the number of times learners can attempt these. Exercises come with detailed remediation, which ensures that learners are confident on the topic before proceeding.



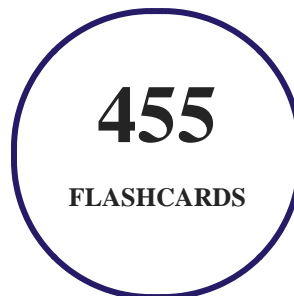
## 4. Quizzes

Quizzes test your knowledge on the topics of the exam when you go through the course material. There is no limit to the number of times you can attempt it.



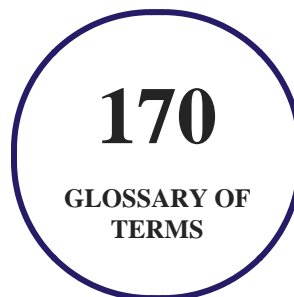
## 5. flashcards

Flashcards are effective memory-aiding tools that help you learn complex topics easily. The flashcard will help you in memorizing definitions, terminologies, key concepts, and more. There is no limit to the number of times learners can attempt these. Flashcards help master the key concepts.



## 6. Glossary of terms

uCertify provides detailed explanations of concepts relevant to the course through Glossary. It contains a list of frequently used terminologies along with its detailed explanation. Glossary defines the key terms.



## 7. Expert Instructor-Led Training

uCertify uses the content from the finest publishers and only the IT industry's finest instructors. They have a minimum of 15 years real-world experience and are subject matter experts in their fields. Unlike a live class, you can study at your own pace. This creates a personal learning experience and gives you all the benefit of hands-on training with the flexibility of doing it around your schedule 24/7.

## 8. ADA Compliant & JAWS Compatible Platform

uCertify course and labs are ADA (Americans with Disability Act) compliant. It is now more accessible to students with features such as:

- Change the font, size, and color of the content of the course
- Text-to-speech, reads the text into spoken words
- Interactive videos, how-tos videos come with transcripts and voice-over
- Interactive transcripts, each word is clickable. Students can clip a specific part of the video by clicking on a word or a portion of the text.

JAWS (Job Access with Speech) is a computer screen reader program for Microsoft Windows that reads the screen either with a text-to-speech output or by a Refreshable Braille display. Student can easily navigate uCertify course using JAWS shortcut keys.

## 9. State of the Art Educator Tools

uCertify knows the importance of instructors and provide tools to help them do their job effectively. Instructors are able to clone and customize course. Do ability grouping. Create sections. Design grade scale and grade formula. Create and schedule assessments. Educators can also move a student from self-paced to mentor-guided to instructor-led mode in three clicks.

## 10. Award Winning Learning Platform (LMS)

uCertify has developed an award winning, highly interactive yet simple to use platform. The SIIA CODiE Awards is the only peer-reviewed program to showcase business and education technology's finest products and services. Since 1986, thousands of products, services and solutions have been

recognized for achieving excellence. uCertify has won CODiE awards consecutively for last 7 years:

- **2014**

1. Best Postsecondary Learning Solution

- **2015**

1. Best Education Solution
2. Best Virtual Learning Solution
3. Best Student Assessment Solution
4. Best Postsecondary Learning Solution
5. Best Career and Workforce Readiness Solution
6. Best Instructional Solution in Other Curriculum Areas
7. Best Corporate Learning/Workforce Development Solution

- **2016**

1. Best Virtual Learning Solution
2. Best Education Cloud-based Solution
3. Best College and Career Readiness Solution
4. Best Corporate / Workforce Learning Solution
5. Best Postsecondary Learning Content Solution
6. Best Postsecondary LMS or Learning Platform
7. Best Learning Relationship Management Solution

- **2017**

1. Best Overall Education Solution
2. Best Student Assessment Solution
3. Best Corporate/Workforce Learning Solution
4. Best Higher Education LMS or Learning Platform

- **2018**

1. Best Higher Education LMS or Learning Platform

2. Best Instructional Solution in Other Curriculum Areas
3. Best Learning Relationship Management Solution

- **2019**

1. Best Virtual Learning Solution
2. Best Content Authoring Development or Curation Solution
3. Best Higher Education Learning Management Solution (LMS)

- **2020**

1. Best College and Career Readiness Solution
2. Best Cross-Curricular Solution
3. Best Virtual Learning Solution

## 11. Chapter & Lessons

uCertify brings these textbooks to life. It is full of interactive activities that keeps the learner engaged. uCertify brings all available learning resources for a topic in one place so that the learner can efficiently learn without going to multiple places. Challenge questions are also embedded in the chapters so learners can attempt those while they are learning about that particular topic. This helps them grasp the concepts better because they can go over it again right away which improves learning.

Learners can do Flashcards, Exercises, Quizzes and Labs related to each chapter. At the end of every lesson, uCertify courses guide the learners on the path they should follow.

## Syllabus

### Chapter 1: Introduction

- The Security+ Exam
- What Does This Course Cover?
- Exam SY0-701 Exam Objectives

- SY0-701 Certification Exam Objective Map

## Chapter 2: Today's Security Professional

- Cybersecurity Objectives
- Data Breach Risks
- Implementing Security Controls
- Data Protection
- Summary
- Exam Essentials

## Chapter 3: Cybersecurity Threat Landscape

- Exploring Cybersecurity Threats
- Threat Data and Intelligence
- Summary
- Exam Essentials

## Chapter 4: Malicious Code

- Malware
- Summary

- Exam Essentials

## Chapter 5: Social Engineering and Password Attacks

- Social Engineering and Human Vectors
- Password Attacks
- Summary
- Exam Essentials

## Chapter 6: Security Assessment and Testing

- Vulnerability Management
- Vulnerability Classification
- Penetration Testing
- Audits and Assessments
- Vulnerability Life Cycle
- Summary
- Exam Essentials

## Chapter 7: Application Security

- Software Assurance Best Practices

- Designing and Coding for Security
- Software Security Testing
- Injection Vulnerabilities
- Exploiting Authentication Vulnerabilities
- Exploiting Authorization Vulnerabilities
- Exploiting Web Application Vulnerabilities
- Application Security Controls
- Secure Coding Practices
- Automation and Orchestration
- Summary
- Exam Essentials

## Chapter 8: Cryptography and the PKI

- An Overview of Cryptography
- Goals of Cryptography
- Cryptographic Concepts
- Modern Cryptography
- Symmetric Cryptography

- Asymmetric Cryptography
- Hash Functions
- Digital Signatures
- Public Key Infrastructure
- Asymmetric Key Management
- Cryptographic Attacks
- Emerging Issues in Cryptography
- Summary
- Exam Essentials

## Chapter 9: Identity and Access Management

- Identity
- Authentication and Authorization
- Authentication Methods
- Accounts
- Access Control Schemes
- Summary
- Exam Essentials

## Chapter 10: Resilience and Physical Security

- Resilience and Recovery in Security Architectures
- Response and Recovery Controls
- Physical Security Controls
- Summary
- Exam Essentials

## Chapter 11: Cloud and Virtualization Security

- Exploring the Cloud
- Virtualization
- Cloud Infrastructure Components
- Cloud Security Issues
- Hardening Cloud Infrastructure
- Summary
- Exam Essentials

## Chapter 12: Endpoint Security

- Operating System Vulnerabilities

- Hardware Vulnerabilities
- Protecting Endpoints
- Hardening Techniques
- Operating System Hardening
- Securing Embedded and Specialized Systems
- Asset Management
- Summary
- Exam Essentials

## Chapter 13: Network Security

- Designing Secure Networks
- Secure Protocols
- Network Attacks
- Summary
- Exam Essentials

## Chapter 14: Wireless and Mobile Security

- Building Secure Wireless Networks

- Managing Secure Mobile Devices
- Summary
- Exam Essentials

## Chapter 15: Monitoring and Incident Response

- Incident Response
- Incident Response Data and Tools
- Mitigation and Recovery
- Summary
- Exam Essentials

## Chapter 16: Digital Forensics

- Digital Forensic Concepts
- Conducting Digital Forensics
- Reporting
- Digital Forensics and Intelligence
- Summary
- Exam Essentials

## Chapter 17: Security Governance and Compliance

- Security Governance
- Understanding Policy Documents
- Change Management
- Personnel Management
- Third-Party Risk Management
- Complying with Laws and Regulations
- Adopting Standard Frameworks
- Security Awareness and Training
- Summary
- Exam Essentials

## Chapter 18: Risk Management and Privacy

- Analyzing Risk
- Managing Risk
- Risk Tracking
- Disaster Recovery Planning
- Privacy

- Summary
- Exam Essentials

## 12. Practice Test

uCertify provides full length practice tests. These tests closely follow the exam objectives and are designed to simulate real exam conditions. Each course has a number of test sets consisting of hundreds of items to ensure that learners are prepared for the certification exam.

### Here's what you get

**90**  
PRE-ASSESSMENTS  
QUESTIONS

**2**  
FULL LENGTH TESTS

**90**  
POST-ASSESSMENTS  
QUESTIONS

### Features

Each question comes with detailed remediation explaining not only why an answer option is correct but also why it is incorrect.

#### Unlimited Practice

Each test can be taken unlimited number of times until the learner feels they are prepared. Learner can review the test and read detailed remediation. Detailed test history is also available.

Each test set comes with learn, test and review modes. In learn mode, learners will attempt a question and will get immediate feedback and complete remediation as they move on to the next question. In test mode, learners can take a timed test simulating the actual exam conditions. In review mode,

learners can read through one item at a time without attempting it.

## 13. Live Labs

The benefits of live-labs are:

- Exam based practical tasks
- Real equipment, absolutely no simulations
- Access to the latest industry technologies
- Available anytime, anywhere on any device
- Break and Reset functionality
- No hardware costs

## Lab Tasks

### Malicious Code

- Examining Spyware
- Analyzing Malware Using VirusTotal

### Social Engineering and Password Attacks

- Using Social Engineering Techniques to Plan an Attack
- Cracking a Linux Password Using John the Ripper
- Cracking Passwords

### Security Assessment and Testing

- Scan for Vulnerabilities Using Nikto
- Conducting Vulnerability Scanning Using Nessus
- Consulting a Vulnerability Database

- Gathering Site Information

## **Application Security**

- Fuzzing Using OWASP ZAP
- Performing SQL Injection in DVWA
- Exploiting LFI and RFI Vulnerabilities
- Conducting a Cross-Site Request Forgery Attack
- Performing an XSS Attack in DVWA
- Examining Application Vulnerabilities
- Exploiting an Overflow Vulnerability
- Exploiting a TOCTOU Vulnerability

## **Cryptography and the PKI**

- Using Symmetric Encryption
- Creating Asymmetric Key Pairs
- Creating File Hashes
- Examining PKI Certificates

## **Identity and Access Management**

- Installing a RADIUS Server
- Examining Kerberos Settings
- Enforcing Password Policies
- Using the chmod Command
- Creating Linux Users and Groups

## **Cloud and Virtualization Security**

- Detecting Virtualization

## **Network Security**

- Capturing Credentials On-path
- Launching a DoS Attack

### Wireless and Mobile Security

- Securing a Wi-Fi Hotspot

### Monitoring and Incident Response

- Examining MITRE ATT&CK
- Viewing Linux Event Logs
- Viewing Windows Event Logs

### Digital Forensics

- Completing the Chain of Custody
- Using FTK Imager
- Analyzing Forensic Case with Autopsy

## Here's what you get

**36**

LIVE LABS

**35**

VIDEO TUTORIALS

**01:34**

HOURS

## 14. Post-Assessment

After completion of the uCertify course Post-Assessments are given to students and often used in conjunction with a Pre-Assessment to measure their achievement and the effectiveness of the exam.

**GET IN TOUCH:**

[www.uCertify.com](http://www.uCertify.com)