Syllabus

Security + SY0-701

Program Description.

This course will prepare students to assess, monitor, and secure enterprise environments, apply security solutions in hybrid environments, comprehend regulations and policies, and effectively respond to security events and incidents.

Modules will cover a wide range of essential concepts in the field of cybersecurity and key domains, including threats, attacks, and vulnerabilities; technologies and tools; architecture and design; identity and access management; risk management; cryptography and Public Key Infrastructure; secure networking and protocols; operational security; and security governance and compliance. By mastering these domains, students can gain a comprehensive understanding of cybersecurity principles, best practices, and technologies. The SY0-701 course serves as a crucial step in obtaining the CompTIA Security+ certification, which validates the ability to secure networks, systems, and data, making professionals well-equipped to tackle the challenges of cybersecurity in today's digital world.

Prerequisites.

- None

Class Schedule.

Classes will be held Monday through Friday in four-hour blocks, two blocks per day, for one week.

*Please check your local class time in your registration email.

There will be no mealtime breaks, but there will be six 10-minute breaks taken throughout the class sessions.

Course Hours.

Course Number	Course Title	Contact Hours
SY0-701	Security+	40

The approximate time required to complete this program is 10 days.

Required Tools.

- ACI Student Learning Portal (LMS)
- Practice Labs

Prepares for Industry Recognized Certification Exam/s:

- CompTIA Network+ N10-008

Student Responsibilities.

Course Agreement

The signed enrollment paperwork the student submitted or the online purchase of a course from ACI Learning represents an agreement between the student and ACI Learning. It is the student's responsibility to know and follow the policies and procedures of the course as presented in this syllabus and to ask for clarification as necessary.

Communication

Early and prompt communication is essential to success in all classes. Questions and problems cannot be addressed if we are not aware of them. The student must communicate with their instructor or the Support team to ensure that any assistance needed is made available.

Absence

Attendance is expected. The student must notify us if they are going to miss class by emailing Support@acilearning.com.

Attendance

Attendance is checked in the first 30 minutes of class. If the student is going to be late, they must notify Support@acilearning.com to ensure that late arrival is not counted as an absence for the full day's class. Students have to maintain 80% attendance or more to take the End- Course Assessment.

Email

Every student must have an active email account that is checked regularly, as we send all communication regarding classes via email.

Student Conduct

Any inappropriate/offensive communication or behavior the instructor or ACI Learning deems unfit for the classroom may have academic consequences. The student is expected to be respectful at all times. The Student Conduct Policy is located in the “References” tile in the Learning Portal.

Class Participation

The student is expected to attend 100% of class and must participate, attend, and utilize all resources for class to be successful.

Technology

If the student is taking classes from home, it is their responsibility to have all technical requirements to participate effectively in class (computer, internet connection, microphone, webcam, and noise-canceling headset).

Assessments.

Assessment activities are designed to evaluate the knowledge and skills the student has obtained throughout their course.

Mid-course and end-course assessments will be conducted electronically through the ACI Learning Portal. Mid-course and end-course assessments will be proctored.

The end-course assessment links objectives and learning outcomes covered during the course. It is designed to evaluate the knowledge and skills the student has obtained by the completion of their course.

Assessment Policy.

- All ACI students must complete a 60-minute timed assessment on the last day of each class.
- Assessments will be proctored by the instructor in both on-campus and virtual classroom classes.
- If the student scores below 70%, they will be given an opportunity to take a re- assessment on the same day after the instructor reviews the first assessment.
- If the student does not attend and complete the assessment on the last day of

class due to a documented unforeseen circumstance outside of their control (emergency, medical, weather), permission may be granted to reschedule the assessment if the student contacts Support@acilearning.com within 24 hours of their absence.

- If the student does not attend and complete the assessment on the last day of class, with no documented unforeseen circumstance outside of their control (emergency, medical, weather) or with no communication to ACI Learning, the student may not receive participation for the last day of class and may need to retake the class to earn completion and be granted another opportunity to take the assessment.

Mid-Course Assessment Information:

- The mid-course assessment will include 25 questions, and 60 minutes will be given for the assessment.
- The purpose of the mid-course assessment is to serve as a check-in on progress and focus study efforts.
- The outcome of the mid-course assessment does not affect enrollment status.
- Students who earn below 70% on the mid-course assessment will receive a notification email and information about how to schedule time with instructor mentors.

End-Course Assessment Information:

- The end-course assessment will include 25 questions, and 60 minutes will be given for the assessment and any retake attempts.
- The retake of the end-course assessment will be the final score; no additional retakes will be offered unless the student re-sits the entire course.
- End-course assessment scores will be recorded by the instructor and Frontline Administration in the student's electronic file.
- To pass the course, students must earn 70% or higher in the end-course assessment.

Instructional Methods.

- Lectures
- PowerPoint Slides
- Courseware
- Labs (Virtual) and In-Class
- Videos
- Assessments

Course Objectives.

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

SY0-701 Security+

Module 1: Authentication, Access, and Asset Management

- **Objective A:** Identify the pillars of cybersecurity and how they are implemented.
- **Objective B:** Describe the importance of managing network assets.
- **Objective C:** Explain enterprise identity management.

Module 2: Secure Architecture and Devices

- **Objective A:** Outline key components of a secure network architecture.
- **Objective B:** Explain how to monitor and harden network devices.
- **Objective C:** Identify and comply with security governance requirements.

Module 3: Data Protection and Security Solutions

- **Objective A:** Identify ways to maintain and protect enterprise data.
- **Objective B:** Describe how to apply security principles to network devices.

Module 4: Cryptographic Solutions

- **Objective A:** Explain the types and uses of cryptography in the enterprise network.

Module 5: Vulnerability Management, Resilience, and Recovery

- **Objective A:** Discuss the importance of user security awareness.
- **Objective B:** Identify vulnerability management and alerting strategies.
- **Objective C:** Describe network resilience and recovery practices.
- **Objective D:** Differentiate between automation and orchestration uses in the security environment.

Module 6: Malicious Actors, Attacks, and Mitigations

- **Objective A:** Identify different types of attackers.
- **Objective B:** Discuss typical vulnerabilities and attack vectors.
- **Objective C:** List and explain various vulnerability mitigation strategies.
- **Objective D:** Identify indicators of attack and compromise.

Module 7: Compliance, Risk Management, and Incident Response

- **Objective A:** Discuss security compliance.
- **Objective B:** Explain enterprise risk management.
- **Objective C:** Identify methods of conducting vulnerability and compliance audits and assessments.
- **Objective D:** Explain incident response and investigation support.

Course Outline.

Week 1 - 40 hours

Day 1

- Opening and Instructor Introduction
- Course Overview and Expectations
- Courseware, Practice Labs, & ITProTV Introduction
- CompTIA Objectives Introduction
- Student Introductions
- **Module 1: Authentication, Access, and Asset Management**
  - Objectives A – C
- **Module 1** in-class instructor demos, Practice Labs, and discussion questions, as needed
- **Module 2: Secure Architecture and Devices**
  - Objective A (partial)
- **Module 2** in-class instructor demos, Practice Labs, and discussion questions, as needed

Day 2

- Intro/ Recap Day 1
- **Module 2: Secure Architecture and Devices**
  - Objectives A (partial) - C
- **Module 2** in-class instructor demos, Practice Labs, and discussion questions, as needed
- **Module 3: Data Protection and Security**
  - Objectives A - B
- **Module 3** in-class instructor demos, Practice Labs, and discussion questions, as needed

Day 3

- Intro/ Recap Day 2
- **Module 4: Cryptographic Solutions**
  - Objectives A
- **Module 4** in-class instructor demos, Practice Labs, and discussion questions, as needed

- Mid-Course Assessment
- **Module 5: Vulnerability Management, Resilience, and Recovery**
  - Objectives A – D (partial)
- **Module 5** in-class instructor demos, Practice Labs, and discussion questions, as needed

Day 4

- Intro/ Recap Day 3
- **Module 5: Vulnerability Management, Resilience, and Recovery**
  - Objective D (partial)
- **Module 5** in-class instructor demos, Practice Labs, and discussion questions, as needed
- **Module 6: Malicious Actors, Attacks, and Mitigations**
  - Objectives A - D
- **Module 6** in-class instructor demos, Practice Labs, and discussion questions, as needed
- **Module 7: Compliance, Risk Management, and Incident Response**
  - Objective A
- **Module 7** in-class instructor demos, Practice Labs, and discussion questions, as needed

Day 5

- Intro/ Recap Day 4
- **Module 7: Compliance, Risk Management, and Incident Response**
  - Objectives B - D
- **Module 7** in-class instructor demos, Practice Labs, and discussion questions, as needed
- Review course content
- End-course assessment
- Certification exam strategies
- Course review

Grading.

To pass the course, students must earn 70% or higher on the end-course assessment.