

CompTIA Security+ Certification (SY0-601), Semester B

Credits: 0.5

Course Overview and Goals

CompTIA Security+ Certification (SY0-601), Semester B is the second part of a two-semester course that covers exam objectives of the CompTIA Security+ certification exam SY0-601.

This course begins by identifying application security solutions. You will learn about secure protocols and how to design a secure network. You will learn how to secure wireless networks, mobile devices, cloud, and sensitive data. You will describe account management controls, authentication management solutions, and public key infrastructure (PKI). You will describe processes related to incidence response and incidence investigation. You will identify the tools for digital forensics. Finally, you will describe organizational security and risk management.

By the end of this course, you will be able to do the following:

- ❖ Identify and implement application security solutions.
- ❖ Describe secure protocols and their uses.
- ❖ Describe how to design a secure network.
- ❖ Describe how to secure a wireless network.
- ❖ Describe how to secure mobile devices.
- ❖ Describe security controls and solutions for cloud.
- ❖ Describe how to secure sensitive data and enhance privacy.
- ❖ Identify account management controls.
- ❖ Describe authentication management solutions and access control models.
- ❖ Describe public key infrastructure (PKI) and the types of certificates.
- ❖ Describe the processes and procedures related to incident response.
- ❖ Identify the data sources that support an incident investigation.
- ❖ Describe various mitigation techniques.
- ❖ Explain the main aspects of digital forensics.
- ❖ Compare different security controls.
- ❖ Identify the tools that access organizational security.
- ❖ Describe the regulations, standards, and frameworks related to organizational security.
- ❖ Explain the importance of organizational security policies.
- ❖ Describe the concepts and processes of risk management.

UNIT 1: APPLICATION, NETWORK, AND MOBILE SECURITY (DAYS 1 – 29)

In this unit, you will learn about application security, system hardening techniques, and database security. You will learn about secure protocols, network segmentation, virtual private networks (VPNs), port security, and load balancing. You will describe how to secure a wireless network and mobile devices. You will identify cloud security controls and solutions. Additionally, you will describe the types of data and the impact of vulnerabilities and data breaches.

Lesson	Lesson Objective
Application Security	Identify and implement application security solutions.
Protocol Security	Describe secure protocols and their uses.
Network Security	Describe how to design a secure network.
Wireless Security	Describe how to secure a wireless network.
Mobile Device Security	Describe how to secure mobile devices.
Cloud Security	Describe security controls and solutions for cloud.
Data Security	Describe how to secure sensitive data and enhance privacy.

UNIT 2: ACCOUNT MANAGEMENT AND AUTHENTICATION (DAYS 30 – 44)

In this unit, you will learn about identity, account types, and account policies. You will identify authentication management solutions, authentication technologies, and access control models. Additionally, you will learn about concepts related to public key infrastructure (PKI) and different types of certificates and certificate formats.

Lesson	Lesson Objective
Account Management Controls	Identify account management controls.
Authentication and Authorization Solutions	Describe authentication management solutions and access control models.
Public Key Infrastructure	Describe public key infrastructure (PKI) and the types of certificates.

UNIT 3: INCIDENT RESPONSE AND MITIGATION TECHNIQUES (DAYS 45 – 62)

In this unit, you will describe incident response life cycle, plans, team, and policies. You will describe different tools used in incident investigations including vulnerability scanners, bandwidth monitors, and protocol analyzers. You will also describe security orchestration, automation, and response (SOAR). You will describe various mitigation techniques. In addition, you will describe the procedures and tools involved in digital forensics.

Lesson	Lesson Objective
Incident Response	Describe the processes and procedures related to incident response.
Incident Investigation	Identify the data sources that support an incident investigation.
Mitigation Techniques	Describe various mitigation techniques.
Digital Forensics	Explain the main aspects of digital forensics.

UNIT 4: ORGANIZATIONAL SECURITY AND RISK MANAGEMENT (DAYS 63 – 90)

In this unit, you will describe different types of security controls. You will differentiate between different categories of security controls, including managerial, operational, and technical. You will describe the tools needed for organizational security. You will describe regulations, standards, and legislations related to organizational security. You will describe organizational policies related to personnel, data, and credentials. Additionally, you will describe the types of risks, disasters, and risk management strategies.

Lesson	Lesson Objective
Security Controls	Compare different security controls.
Organizational Security	Identify the tools that access organizational security.
Regulations and Standards	Describe the regulations, standards, and frameworks related to organizational security.
Organizational Security Policies	Explain the importance of organizational security policies.
Risk Management	Describe the concepts and processes of risk management.