COURSE OVERVIEW

Course Name:
(SY0-601)
CompTIA Security+

COURSE DURATION: 5 Day

Gauteng:
3rd Floor, 34 Whitely Road
Melrose Arch
Johannesburg
2196

Gauteng:
192 on Bram
192 Bram Fischer Drive
Ferndale, Randburg
Johannesburg
2160

Cape Town:
3rd Floor, Thomas Pattullo Building
19 Jan Smuts St
Cape Town
8000

Durban:
9 Mountview Close
Broadlands
Mount Edgecombe
Durban
4302

087 941 5764
sales@impactful.co.za
impactful.co.za

INTRODUCTION

The Official CompTIA Security+ Instructor and Student Guides (SY0-601) have been developed by CompTIA for the CompTIA certification candidate. Rigorously evaluated to validate coverage of the CompTIA Security+ (SY0-601) exam objectives, The Official CompTIA Security+ Instructor and Student Guides teach students the knowledge and skills required to assess the security posture of an enterprise environment and recommend and implement appropriate security solutions; monitor and secure hybrid environments, including cloud, mobile, and IoT; operate with an awareness of applicable laws and policies, including principles of governance, risk, and compliance; identify, analyse, and respond to security events and incidents.

DELIVERY METHOD

Our courses have flexible delivery options:

- In-person classroom training at the Impactful training facilities
  - Johannesburg, Durban, Cape Town
- Virtual instructor-led training
- Nationally: on-site at the client

IMPACTFUL
Powered by LRMG

INTENDED AUDIENCE

- Security Administrator
- Systems Administrator
- Helpdesk Manager / Analyst
- Security Analyst
- Network / Cloud Engineer
- IT Auditors • Security Engineer
- IT Project Manager
- Security Officer
- Information Security Manage

PREREQUISITES

Students should have basic Windows user skills and a fundamental understanding of computer and networking concepts. Achievement of CompTIA A+ and Network+ certifications, plus two years of experience with IT administration with a security focus

COURSE OBJECTIVES

This course is for students who are preparing to take the CompTIA Security+ certification exam SY0-601. This course is aimed towards IT professionals who install and configure systems to secure applications, networks, and devices; perform threat analysis and respond with appropriate mitigation techniques; participate in risk mitigation activities; and operate with an awareness of applicable policies, laws, and regulations.

COURSE CONTENT

Lesson 1: Comparing Security Roles and Security Controls
Topic 1A: Compare and Contrast Information Security Roles
Topic 1B: Compare and Contrast Security Control and Framework Types
Topic 1C: Compare and Contrast Social Engineering Attack Types
Topic 1D: Determine Malware Type

Lesson 2: Explaining Threat Actors and Threat Intelligence
Topic 2A: Explain Threat Actor Types and Attack Vectors
Topic 2B: Explain Threat Intelligence Sources

Lesson 3: Performing Security Assessments
Topic 3A: Assess Organizational Security with Network Reconnaissance Tools
Topic 3B: Explain Security Concerns with General Vulnerability Types
Topic 3C: Summarize Vulnerability Scanning Techniques
Topic 3D: Explain Penetration Testing Concept

Lesson 4: Identifying Social Engineering and Malware
Topic 4A: Compare and Contrast Social Engineering Techniques
Topic 4B: Analyse Indicators of Malware-Based Attacks

Lesson 5: Summarizing Basic Cryptographic Concepts
Topic 5A: Compare and Contrast Cryptographic Ciphers
Topic 5B: Summarize Cryptographic Modes of Operation
Topic 5C: Summarize Cryptographic Use Cases and Weaknesses
Topic 5D: Summarize Other Cryptographic Technologies

Lesson 6: Implementing Public Key Infrastructure
Topic 6A: Implement Certificates and Certificate Authorities
Topic 6B: Implement PKI Management

Lesson 7: Implementing Authentication Controls
Topic 7A: Summarize Authentication Design Concepts
Topic 7B: Implement Knowledge-Based Authentication
Topic 7C: Implement Authentication Technologies
Topic 7D: Summarize Biometrics Authentication Concepts

Lesson 8: Implementing Identity and Account Management Controls
Topic 8A: Implement Identity and Account Types
Topic 8B: Implement Account Policies
Topic 8C: Implement Authorization Solutions
Topic 8D: Explain the Importance of Personnel Policies

Lesson 9: Implementing Secure Network Designs
Topic 9A: Implement Secure Network Designs
Topic 9B: Implement Secure Switching and Routing
Topic 9C: Implement Secure Wireless Infrastructure
Topic 9D: Implement Load Balancer

Lesson 10: Implementing Network Security Appliances
Topic 10A: Implement Firewalls and Proxy Servers
Topic 10B: Implement Network Security Monitoring
Topic 10C: Summarize the Use of SIEM

Lesson 11: Implementing Secure Network Protocols
Topic 11A: Implement Secure Network Operations Protocols
Topic 11B: Implement Secure Application Protocols
Topic 11C: Implement Secure Remote Access Protocol

Lesson 12: Implementing Host Security Solutions
Topic 12A: Implement Secure Firmware
Topic 12B: Implement Endpoint Security

Lesson 13: Implementing Secure Mobile Solutions
Topic 13A: Implement Mobile Device Management
Topic 13B: Implement Secure Mobile Device Connection

Lesson 14: Summarizing Secure Application Concepts
Topic 14A: Analyse Indicators of Application Attacks
Topic 14B: Analyse Indicators of Web Application Attacks
Topic 14C: Summarize Secure Coding Practices
Topic 14D: Implement Secure Script Environments
Topic 14E: Summarize Deployment and Automation Concepts

Lesson 15: Implementing Secure Cloud Solutions
Topic 15A: Summarize Secure Cloud and Virtualization Services
Topic 15B: Apply Cloud Security Solutions
Topic 15C: Summarize Infrastructure as Code Concepts

Lesson 16: Explaining Data Privacy and Protection Concepts
Topic 16A: Explain Privacy and Data Sensitivity Concepts
Topic 16B: Explain Privacy and Data Protection Controls