Brought to you by **iEnabler – THE IT ENABLING COMPANY**

CompTIA Security+

(Exam Code: SY0-601)

Course Objective :

The CompTIA Security+ course establishes 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, analyze, and respond to security events and incidents.

Prerequisite :

Basic computer literacy & Basic PC operating system navigation skills. CompTIA Network+ Certification is recommended.

Certificate Of Attendance :

e-Certificate Of Attendance will be awarded to participants completing the course achieving minimum 75% attendance.

Training Duration :

Full-time: 5 weekdays
Time : 9.30am – 5.30pm

Course & Exam Fee :

Course Fee : S$2800
Regn Fee : S$50

Course fee excludes CompTIA Security+ Exam.
All fees subject to prevailing GST.

Training Methodology & Materials:

- Practical hands-on sessions to enhance security concept.
- Well-designed lab sessions to enhance further understanding of the courseware.

DETAILED COURSE OUTLINE

The table below lists the domain areas measured by this examination and the approximate extent to which they are represented in the examination:

Domain	% of Examination
1.0 Attacks, Threats, and Vulnerabilities	24%
2.0 Architecture and Design	21%
3.0 Implementation	25%
4.0 Operations and Incident Response	16%
5.0 Governance, Risk, and Compliance	14%
Total	100%

Course Outline

1.0 Threats, Attacks and Vulnerabilities

1.1 Compare and contrast different types of social engineering techniques
1.2 Given a scenario, analyze potential indicators to determine the type of attack
1.3 Given a scenario, analyze potential indicators associated with application attacks
1.4 Given a scenario, analyze potential indicators associated with network attacks
1.5 Explain different threat actors, vectors, and intelligence sources
1.6 Explain the security concerns associated with various types of vulnerabilities
1.7 Summarize the techniques used in security assessments
1.8 Explain the techniques used in penetration testing

2.0 Architecture and Design

2.1 Explain the importance of security concepts in an enterprise environment
2.2 Summarize virtualization and cloud computing concepts
2.3 Summarize secure application development, deployment and automation concepts
2.4 Summarize authentication and authorization design concepts
2.5 Given a scenario, implement cybersecurity resilience
2.6 Explain the security implications of embedded and specialized systems
2.7 Explain the importance of physical security controls
2.8 Summarize the basics of cryptographic concepts
2.9 Given a scenario, select the appropriate control to meet the goals of security

3.0 Implementation

3.1 Given a scenario, implement secure protocols
3.2 Given a scenario, implement host or application security solutions
3.3 Given a scenario, implement secure network designs
3.4 Given a scenario, install and configure wireless security settings
3.5 Given a scenario, implement secure mobile solutions
3.6 Given a scenario, apply cybersecurity solutions to the cloud
3.7 Given a scenario, implement identity and account management controls
3.8 Given a scenario, implement authentication and authorization solutions
3.9 Given a scenario, implement public key infrastructure

4.0 Operations and Incident Response

4.1 Given a scenario, use the appropriate tool to assess organizational security
4.2 Summarize the importance of policies, processes and procedures for incident response
4.3 Given an incident, utilize appropriate data sources to support an investigation
4.4 Given an incident, apply mitigation techniques or controls to secure an environment
4.5 Explain the key aspects of digital forensics

5.0 Governance, Risk and Compliance

5.1 Explain the importance of applicable regulations, standards or frameworks that impact organizational security posture
5.2 Explain the importance of policies to organizational security
5.3 Summarize risk management processes and concepts
5.4 Explain privacy and sensitive data concepts in relation to security