COMPTIA SECURITY+

Duration: 5 Days

PROGRAM OVERVIEW

This course is an internationally recognised validation of foundation-level security skills and knowledge and is used by organiations and security professionals around the globe. The participant will have the knowledge and skills required to identify risk and participate in risk mitigation activities; provide infrastructure, application, operational and information security; apply security controls to maintain confidentiality, integrity and availability; identify appropriate technologies and products; and operate with an awareness policies, laws and regulations.

LEARNING OUTCOMES

The participant will:

- proactively implement sound security protocols to mitigate security risks
- quickly respond to security issues
- retroactively identify where security breaches may have occurred
- design the network, onsite or in the cloud with security mind

WHO SHOULD ATTEND?

- Security Architect/Engineer/Consultant/Specialist
- Information Assurance Technician
- System/Network Administrator

COURSE CONTENTS

i) Networking Security
- Explain the security function and purpose of network devices and technologies
- Apply and implement secure network administration principles
- Distinguish and differentiate network design elements and compounds
- Implement and use common protocols
- Identify commonly used default network ports
- Implement wireless network in a secure manner

ii) Compliance and Operational Security
- Explain risk related concepts
- Carry out appropriate risk mitigation strategies
- Execute appropriate incident response procedures
- Explain the importance of security related awareness and training
- Compare and contrast aspects of business continuity
- Explain the impact and proper use of environmental controls
- Execute disaster recovery plans and procedures
- Exemplify the concepts of confidentiality, integrity and availability (CIA)

iii) Threats And Vulnerabilities
- Analyse and differentiate among types of malwares
- Analyse and differentiate among types of attacks
- Analyse and differentiate among types of social engineering attacks
- Analyse and differentiate among types of wireless attacks
- Analyse and differentiate among types of application attacks
- Analyse and differentiate among types of mitigation and deterrent techniques
- Implement assessment tools and techniques to discover security threats and vulnerabilities
- Within the realm of vulnerability assessments, explain the proper use of penetration testing versus vulnerability scanning

iv) Application, data and host security
- Explain the importance of application security
- Carry out appropriate procedures to establish host security
- Explain the importance of data security

v) Access control and identity management
- Explain the function and purpose of authentication services
- Explain the fundamental concepts and best practices related to authentication, authorisation and access control
- Implement appropriate security controls when performing account management

vi) Cryptography
- Summarise general cryptography concepts
- Use and apply appropriate cryptographic tools and products
- Explain the concepts of public key infrastructure
- Implement PKI, certificate management and associated components

SIRIM Academy
3rd Floor, Building 3, SIRIM Complex
1, Persiaran Dato' Menteri
PO Box 7035, Section 2
40700 Shah Alam
Selangor
Tel : +603 5544 6000 / 6211
sirimacademy@sirim.my
www.sirimacademy.my

HRDCORP CLAIMABLE

Find us on: