Contact:
Info@silverlake.sg
+65 - 65882456

CompTIA Security+ Certification

Course#:CompTIA-SecC
Duration:1 Day
Price:0.00

Course Description

Security is among the fastest growing fields in the IT industry and certified security professionals are much in demand. In such a scenario, a reputed certification such as CompTIA Security+ can propel your career to new heights.

Certification from CompTIA stands out because of its accreditation by ANSI and its wide recognition by high profile companies like Hitachi Information Systems, CSC, IBM, Motorola and others. It is a well-rounded exam that covers all concepts of IT security and its integration in an organization.

Our course covers all the objectives of the CompTIA Security+ certification exam including the principles of protecting a system against attack and managing risk. Important topics of the exam such as access control, identity management and cryptography will be covered in detail.

You will receive hands-on training in implementing security strategies that will also help you polish your practical skills in areas of cloud computing, BYOD and SCADA.

Objectives

What you will learn:

Understand all security essentials from cryptography to risk management
Demonstrate your knowledge in the field of security concepts and tools and their implementation
Be part of the much-sought after group of certified security professionals
Learn how to detect and avert security threats
Help your organization avoid huge economic losses due to potential security breaches
Earn the certification that is also recognized by the U.S. Department of Defence
Be eligible to work in any portfolio from security analyst to security engineer
Learn about network management, performance tuning, testing and troubleshooting

Audience

-

Prerequisites

CompTIA recommends that candidates have Network+ certification though it is not mandatory, and a minimum of two years of experience in IT administration with a focus on security.

Content

General security concepts
Operational organizational security
Legal issues, privacy, and ethics
Cryptography
Public key infrastructure
Standards and protocols
Physical security
Infrastructure security
Remote access and authentication
Intrusion detection systems
Security baselines
Types of attacks and malicious software
E-mail and instant messaging
Web components
Disaster recovery and business continuity
Risk, change, and privilege management
Computer forensics