CompTIA Security+ - Fundamentals of Security

Course CT-03G Five days Instructor-Led, Hands-on

Introduction

The CompTIA Security+ certification confirms that you have the fundamental knowledge required to perform core security functions and pursue a career in IT security. Authored by Ian Neil, a world-class CompTIA Security+ 701 trainer, this course is a best-in-class study guide that fully covers the CompTIA Security+ 701 exam objectives.

Complete with self-assessment scenarios and realistic exam questions, this course will help you master the core concepts to pass the exam the first time you take it. With the help of relevant examples, you'll learn about fundamental security concepts, from certificates and encryption to identity and access management (IAM). You'll then delve into the important domains of the exam, namely, cloud security, threats, attacks and vulnerabilities, technologies and tools, architecture and design, risk management, and cryptography and public key infrastructure (PKI). This course comes with over 600 practice questions with detailed explanations and includes two mock exams to help you test yourself.

By the end of this course, you will understand the application of core Security+ concepts in the real world and be ready to take the exam with confidence.

Audience

If you want to take and pass the CompTIA Security+ SY0-701 exam, even if you are not from an IT background, this course is for you. You'll find this course useful if you want to become a qualified security professional. This course is also ideal for US Government and DOD personnel seeking this certification.

At Course Completion

Upon successful completion of this course, students will learn:

- Get to grips with security fundamentals, from the CIA triad through to IAM
- Explore cloud security and techniques used in penetration testing
- Discover different authentication methods and troubleshoot security issues
- Secure the devices and applications that are used by your company
- Identify and protect against various types of malware and virus
- Protect your environment against social engineering and advanced attacks
- Understand and implement PKI concepts
- Delve into secure application development, deployment, and automation concepts

Contact ISInc for more information at 916.920.1700 or by visiting our website at http://www.isinc.com

Prerequisites

Basic Windows skills and a fundamental understanding of computer and networking concepts are required.

CompTIA A+ and Network+ certifications, or equivalent knowledge, and six to nine months experience in networking, including experience configuring and managing TCP/IP, are strongly recommended. Students can obtain this level of skill and knowledge by taking any of the following ISInc courses:

- CompTIA A+ Certification- Comprehensive for All Exams
- CompTIA Network+-Fundamentals of Networking (

Additional introductory courses or work experience in application development and programming or in network and operating system administration for any software platform or system are helpful but not required.

Course Materials

The student kit includes a comprehensive workbook and other necessary materials for this class.

Course Outline

Module 1: Security Aims and Objectives

- Understanding security fundamentals
- Comparing control types
- Physical security controls
- Understanding digital forensics

Module 2: Implementing Public Key Infrastructure

- PKI Concepts
- Asymmetric and symmetric encryption
- Key stretching algorithms
- Quantum computing
- Blockchain and the public ledger
- Hashing and data integrity
- Comparing and contrasting the basic concepts of cryptography
- Basic cryptographic terminologies
- Cryptography
- Practical exercises

Module 3: Investigating Identity and Access Management

- Understanding identity and access management concepts
- Implementing authentication and authorization solutions

Contact ISInc for more information at 916.920.1700 or by visiting our website at http://www.isinc.com

- Summarizing authentication and authorization design concepts
- Cloud versus on premises
- Common Account Management Policies

Module 4: Exploring Virtualization and Cloud Concepts

- Overview of cloud computing
- Implementing different cloud deployment models
- Understanding cloud service models\
- Understanding cloud computing concepts
- Understanding cloud storage concepts
- Selecting cloud security controls
- Exploring the virtual network environments

Module 5: Monitoring Scanning and Penetration Testing

- Penetration testing concepts
- Passive and active
- Vulnerability scanning concepts
- Syslog/security information and event management
- Security orchestration, automation and response

Module 6: Understanding Secure and Insecure Protocols

- Introduction to protocols
- Insecure protocols and their use cases
- Secure protocols and their use cases
- Additional use cases and their protocols

Module 7: Delving into Network and Security Concepts

- Installing and configuring network components
- Remote access capabilities
- Secure network architecture concepts
- Network segmentation
- Network reconnaissance and discovery
- Forensic tools
- IP Addressing

Module 8: Securing Wireless and Mobile Solutions

- Implementing wireless security
- Wireless access point controllers
- Mobile device connection methods
- Wireless open system authentication
- Deploying mobile services security

Contact ISInc for more information at 916.920.1700 or by visiting our website at http://www.isinc.com

Module 9: Identifying Threats, Attacks and Vulnerabilities

- Virus and malware attacks
- Social engineering attacks
- Threat actors
- Advanced attacks
- Cryptographic attacks

Module 10: Governance, Risk and Compliance

- Risk management processes and concepts
- Threat actors, vectors and intelligence concepts
- Regulations, standards and legislation
- Privacy and sensitive data concepts
- The importance of policies for organizational security

Module 11: Managing Application Security

- Implementing host or application security
- Understanding the security implications or embedded and specialist systems
- Application development
- Deployments and automation

Module 12: Dealing with Incident Response Procedures

- Incident response procedures
- Utilizing data courses to support investigations
- Knowing how to apply mitigation techniques or controls to secure an environment
- Implementing cybersecurity resilience

Module 13: Mock Exam 1

Module 14: Mock Exam 2