Compuserve Pvt Ltd.

Course Duration : 40 Hrs

CompTIA
CySA+ Student Guide (Exam CS0-002)

COURSE BROCHURE

www.cometcompuserve.com

Overview

CompTIA is a not-for-profit trade association with the purpose of advancing the interests of IT professionals and IT channel organizations, and its industry-leading IT certifications are an important part of that mission. **CompTIA CyberSecurity Analyst (CySA+) certification** is an intermediate-level certification designed to demonstrate the knowledge and competencies of a security analyst or specialist with four years' experience in the field.

This course covers the duties of cybersecurity analysts who are responsible for monitoring and detecting security incidents in information systems and networks, and for executing a proper response to such incidents. The course introduces tools and tactics to manage cybersecurity risks, identify various types of common threats, evaluate the organization's security, collect and analyze cybersecurity intelligence, and handle incidents as they occur. The course will also prepare you for the **CompTIA CySA+ (Exam CS0-002)** certification examination.

Course Objective

In this course, you will assess and respond to security threats and operate a systems and network security analysis platform. You will:

- Collect and use cybersecurity intelligence and threat data.
- Identify modern cybersecurity threat actors types and tactics, techniques, and procedures.
- Analyze data collected from security and event logs and network packet captures.
- Respond to and investigate cybersecurity incidents using forensic analysis techniques.
- Assess information security risk in computing and network environments.
- Implement a vulnerability management program.
- Address security issues with an organization‘s network architecture.
- Understand the importance of data governance controls.
- Address security issues with an organization‘s software development life cycle.
- Address security issues with an organization‘s use of cloud and service-oriented architecture.

Audience Profile

This course is primarily designed for students who are seeking the CompTIA CySA+ certification and who want to prepare for the CompTIA CySA+ CS0-002 certification exam. The course more generally supports candidates working in or aiming for job roles such as security operations center

(SOC) analyst, vulnerability analyst, cybersecurity specialist, threat intelligence analyst, security engineer, and cybersecurity analyst.

Prerequisites

To ensure your success in this course, you should meet the following requirements:

- At least two years‘ experience in computer network security technology or a related field
- The ability to recognize information security vulnerabilities and threats in the context of risk management
- Foundation-level operational skills with the common operating systems for PCs, mobile devices, and servers
- Foundation-level understanding of some of the common concepts for network environments, such as routing and switching
- Foundational knowledge of TCP/IP networking protocols, including IP, ARP, ICMP, TCP, UDP, DNS, DHCP, HTTP/HTTPS, SMTP, and POP3/IMAP
- Foundational knowledge of the concepts and operational framework of common assurance safeguards in computing environments. Safeguards include authentication and authorization, resource permissions, and antimalware mechanisms.
- Foundational knowledge of the concepts and operational framework of common assurance safeguards in network environments, such as firewalls, IPS, NAC, and VPNs

You can obtain this level of skill and knowledge by taking the following Official CompTIA courses:

- The Official CompTIA Network+ (Exam N10-007) Guide
- The Official CompTIA Security+ (Exam SY0-501) Guide

Table of Contents

Lesson 7: Applying Risk Mitigation and Security Frameworks

- Topic 7A: Apply Risk Identification, Calculation, and Prioritization Processes
- Topic 7B: Explain Frameworks, Policies, and Procedures

Lesson 8: Performing Vulnerability Management

- Topic 8A: Analyze Output from Enumeration Tools
- Topic 8B: Configure Infrastructure Vulnerability Scanning Parameters
- Topic 8C: Analyze Output from Infrastructure Vulnerability Scanners
- Topic 8D: Mitigate Vulnerability Issues

Lesson 9 Applying Security Solutions for Infrastructure Management

- Topic 9A: Apply Identity and Access Management Security Solutions
- Topic 9B: Apply Network Architecture and Segmentation Security Solutions
- Topic 9C: Explain Hardware Assurance Best Practices
- Topic 9D: Explain Vulnerabilities Associated with Specialized Technology

Lesson 10: Understanding Data Privacy and Protection

- Topic 10A: Identify Non-Technical Data and Privacy Controls
- Topic 10B: Identify Technical Data and Privacy Controls

Lesson 11: Applying Security Solutions for Software Assurance

- Topic 11A: Mitigate Software Vulnerabilities and Attacks
- Topic 11B: Mitigate Web Application Vulnerabilities and Attacks
- Topic 11C: Analyze Output from Application Assessments

Lesson 12: Applying Security Solutions for Cloud and Automation

- Topic 12A: Identify Cloud Service and Deployment Model Vulnerabilities
- Topic 12B: Explain Service-Oriented Architecture
- Topic 12C: Analyze Output from Cloud Infrastructure Assessment Tools
- Topic 12D: Compare Automation Concepts and Technologies

Our Students Testimonials

CONTACT US

Mobile : +91 9940068251 / 58251

Mail : ramesh@cometcompuserve.com / ilanchezhian@cometcompuserve.com