CompTIA CySA+

Course Description

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. With the end goal of proactively defending and continuously improving the security of an organization, CySA+ will verify the successful candidate has the knowledge and skills required to: Leverage intelligence and threat detection techniques; Analyze and interpret data; Identify and address vulnerabilities; Suggest preventative measures; and effectively respond to and recover from incidents.

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 Duration:

5 days

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

Objectives:

After you successfully complete this course, expect to be able to:

- Understand vulnerability response, handling, and management
- Explore threat intelligence and threat hunting concepts
- Explain important system and network architecture concepts
- Understand process improvement in security operations
- Implement vulnerability scanning methods
- Perform vulnerability analysis
- Classify vulnerability information
- Explain incident response activities.Demonstrate incident response
- communication
- Apply tools to identify malicious activity
- Analyze potentially malicious activity
- Understand application vulnerability assessment
- Explore scripting tools and analysis concepts
- Understand application security and attack mitigation best practices

Course Outline:

- Explaining the Importance of Security Controls and Security Intelligence
- Utilizing Threat Data and Intelligence
- Analyzing Security Monitoring Data
- Collecting and Querying Security Monitoring Data
- Utilizing Digital Forensics and Indicator Analysis Techniques
- Applying Incident Response Procedures
- Applying Risk Mitigation and Security Frameworks
- Performing Vulnerability Management
- Applying Security Solutions for Infrastructure Management
- Understanding Data Privacy and Protection
- Applying Security Solutions for Software Assurance
- Applying Security Solutions for Cloud and Automation

Who Should Attend

The Official CompTIA CySA+ (Exam CS0-003) is the primary course you will need to take if your job responsibilities include capturing, monitoring, and responding to network traffic findings, software and application security, automation, threat hunting, and IT regulatory compliance. You can take this course to prepare for the CompTIA CySA+ (Exam CS0-003) certification examination.