

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:

- 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.

Course Outline:

- Understanding Vulnerability Response, Handling, and Management
 - Understanding Cybersecurity Leadership Concepts.
 - Exploring Control Types and Methods
 - Explaining Patch Management Concepts
- Exploring Threat Intelligence and Threat Hunting Concepts
 - Exploring Threat Actor Concepts
 - Identifying Active Threats
 - Exploring Threat-Hunting Concepts
- Explaining Important System and Network Architecture Concepts
 - Reviewing System and Network Architecture Concepts
 - Exploring Identity and Access Management (IAM)
 - Maintaining Operational Visibility
- Understanding Process Improvement in Security Operations
 - Exploring Leadership in Security Operations
 - Understanding Technology for Security Operations
- Implementing Vulnerability Scanning Methods
 - Explaining Compliance Requirements
 - Understanding Vulnerability Scanning Methods
 - Exploring Special Considerations in Vulnerability Scanning
- Performing Vulnerability Analysis
 - Understanding Vulnerability Scoring Concepts
 - Exploring Vulnerability Context Considerations
- Communicating Vulnerability Information
 - Explaining Effective Communication Concepts
 - Understanding Vulnerability Reporting Outcomes and Action Plans
- Explaining Incident Response Activities
 - Exploring Incident Response Planning
 - Performing Incident Response Activities
- Demonstrating Incident Response Communication
 - Understanding Incident Response Communication
 - Analyzing Incident Response Activities
- Applying Tools to Identify Malicious Activity
 - Identifying Malicious Activity

- Explaining Attack Methodology Frameworks
- Explaining Techniques for Identifying Malicious Activity
- Analyzing Potentially Malicious Activity
 - Exploring Network Attack Indicators
 - Exploring Host Attack Indicators
 - Exploring Vulnerability Assessment Tools
- Understanding Application Vulnerability Assessment
 - Analyzing Web Vulnerabilities
 - Analyzing Cloud Vulnerabilities
- Exploring Scripting Tools and Analysis Concepts
 - Understanding Scripting Languages
 - Identifying Malicious Activity Through Analysis
- Understanding Application Security and Attack Mitigation Best Practices
 - Exploring Secure Software Development Practices
 - Recommending Controls to Mitigate Successful Application Attacks
 - Implementing Controls to Prevent Attacks

Who Should Attend

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.