CompTIA CySA+ CS0-003

Duration: **5 Days**

Prerequisites:

To ensure your success in this course, you should have four years of hands-on experience as an incident response analyst or security operations center (SOC) analyst. CompTIA Network+, Security+, or the equivalent knowledge is strongly
recommended.

Course Description:

This course can benefit you in two ways. If you intend to pass the CompTIA CySA+ (Exam CS0-003) certification examination, this course can be a significant part of your preparation. But certification is not the only key to professional success in the field of security analyst. Today's job market demands individuals with demonstrable skills, and the information and activities in this course can help you build your security analyst skill set so that you can confidently perform your duties in any security analyst role.

Course Objectives:

On course completion, you will be able to do the following:

- 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.

Intended Audience:

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.

Course Outlines:

Lesson 1: Understanding Vulnerability Response, Handling, and Management

- Topic 1A: Understanding Cybersecurity Leadership Concepts
- Topic 1B: Exploring Control Types and Methods
- Topic 1C: Explaining Patch Management Concepts

Lesson 2: Exploring Threat Intelligence and Threat Hunting Concepts

- Topic 2A: Exploring Threat Actor Concepts
- Topic 2B: Identifying Active Threats
- Topic 2C: Exploring Threat-Hunting Concepts

Lesson 3: Explaining Important System and Network Architecture Concepts

- Topic 3A: Reviewing System and Network Architecture Concepts
- Topic 3B: Exploring Identity and Access Management (IAM
- Topic 3C: Maintaining Operational Visibility

Lesson 4: Understanding Process Improvement in Security Operations

- Topic 4A: Exploring Leadership in Security Operations
- Topic 4B: Understanding Technology for Security Operations

Lesson 5: Implementing Vulnerability Scanning Methods

- Topic 5A: Explaining Compliance Requirements
- Topic 5B: Understanding Vulnerability Scanning Methods
- Topic 5C: Exploring Special Considerations in Vulnerability Scanning

Lesson 6: Performing Vulnerability Analysis

- Topic 6A: Understanding Vulnerability Scoring Concepts
- Topic 6B: Exploring Vulnerability Context Considerations

Lesson 7: Communicating Vulnerability Information

- Topic 7A: Explaining Effective Communication Concepts
- Topic 7B: Understanding Vulnerability Reporting Outcomes and Action Plans

Lesson 8: Explaining Incident Response Activities

- Topic 8A: Exploring Incident Response Planning
- Topic 8B: Performing Incident Response Activities

Lesson 9: Demonstrating Incident Response Communication

- Topic 9A: Understanding Incident Response Communication
- Topic 9B: Analyzing Incident Response Activities

Lesson 10: Applying Tools to Identify Malicious Activity

- Topic 10A: Identifying Malicious Activity
- Topic 10B: Explaining Attack Methodology Frameworks
- Topic 10C: Explaining Techniques for Identifying Malicious Activity

Lesson 11: Analyzing Potentially Malicious Activity

- Topic 11A: Exploring Network Attack Indicators
- Topic 11B: Exploring Host Attack Indicators
- Topic 11C: Exploring Vulnerability Assessment Tools

Lesson 12: Understanding Application Vulnerability Assessment

- Topic 12A: Analyzing Web Vulnerabilities
- Topic 12B: Analyzing Cloud Vulnerabilities

Lesson 13: Exploring Scripting Tools and Analysis Concepts

- Topic 13A: Understanding Scripting Languages
- Topic 13B: Identifying Malicious Activity Through Analysis

Lesson 14: Understanding Application Security and Attack Mitigation Best Practices

- Topic 14A: Exploring Secure Software Development Practices
- Topic 14B: Recommending Controls to Mitigate Successful Application Attack
- Topic 14C: Implementing Controls to Prevent Attacks