CompTIA Cybersecurity Analyst (CS0-003)

Duration 5 Days

COURSE OVERVIEW

CompTIA Cybersecurity Analyst (CySA+) is a certification for cyber professionals tasked with incident detection, prevention and response through continuous security monitoring. This 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. This course may earn a Credly Badge.

COURSE OBJECTIVES

With completion of this course you will be prepared to:

- Detect and analyze indicators of malicious activity
- Understand threat hunting and threat intelligence concepts
- Use appropriate tools and methods to manage, prioritize and respond to attacks and vulnerabilities
- Perform incident response processes
- Understand reporting and communication concepts related to vulnerability management and incident response activities

COURSE OUTLINE

Lesson 1: Understanding Vulnerability Response, Handling, And Management

- Understanding Cybersecurity Leadership Concepts
- Exploring Control Types and Methods
- Explaining Patch Management Concepts

Lesson 2: Exploring Threat Intelligence And Threat Hunting Concepts

- Exploring Threat Actor Concepts
- Identifying Active Threats
- Exploring Threat-Hunting Concepts

Lesson 3: Explaining Important System And Network Architecture Concepts

- Reviewing System and Network Architecture Concepts
- Exploring Identity and Access Management (IAM)
- Maintaining Operational Visibility

Lesson 4: Understanding Process Improvement In Security Operations

- Exploring Leadership in Security Operations
- Understanding Technology for Security Operations

Lesson 5: Implementing Vulnerability Scanning Methods

- Explaining Compliance Requirements
- Understanding Vulnerability Scanning Methods
- Exploring Special Considerations in Vulnerability Scanning

Lesson 6: Performing Vulnerability Analysis

- Understanding Vulnerability Scoring Concepts
- Exploring Vulnerability Context Considerations

Lesson 7: Communicating Vulnerability Information

- Explaining Effective Communication Concepts
- Understanding Vulnerability Reporting Outcomes and Action Plans

Lesson 8: Explaining Incident Response Activities

- Exploring Incident Response Planning
- Performing Incident Response Activities

Lesson 9: Demonstrating Incident Response Communication

- Understanding Incident Response Communication
- Analyzing Incident Response Activities

Lesson 10: Applying Tools To Identify Malicious Activity

- Identifying Malicious Activity
- Explaining Attack Methodology Frameworks
- Explaining Techniques for Identifying Malicious Activity

Lesson 11: Analyzing Potentially Malicious Activity

- Exploring Network Attack Indicators
- Exploring Host Attack Indicators
- Exploring Vulnerability Assessment Tools

Lesson 12: Understanding Application Vulnerability Assessment

- Analyzing Web Vulnerabilities
- Analyzing Cloud Vulnerabilities

Lesson 13: Exploring Scripting Tools And Analysis Concepts

- Understanding Scripting Languages
- Identifying Malicious Activity Through Analysis

Lesson 14: 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 suited to Security Analyst Security Operations Center (SOC) Analyst Incident Response Analyst Vulnerability Management Analyst Security Engineer.

PREREQUISITES

Prior to this course you should have taken CompTIA Network+ and CompTIA Security+ courses or have the equivalent knowledge. A minimum of 4 years of hands-on information security or related experience is recommended.