CompTIA Cybersecurity Analyst (CySA+) (CS0-003)

Course Description

CompTIA Cybersecurity Analyst (CySA+) is a certification for cybersecurity professionals tasked with incident detection, prevention and response through continuous security monitoring.

The skills that today's security analysts need to protect organizations are different than the skills they had just a few years ago. CompTIA Cybersecurity Analyst (CySA+) certification has evolved to help organizations address, monitor and respond to threats and manage risk. Specifically, learners will gain skills in security operations, vulnerability management, incident response and management, and reporting and communication. CySA+-certified professionals are able to confidently lead incident detection, prevention and response in job roles like security analyst, Security Operations Center (SOC) analyst, incident response analyst, vulnerability management analyst, security engineer and threat hunter.

Course Duration:

5 days

Prerequisites:

Network+, Security+, or equivalent knowledge, with a minimum of 4 years of hands-on experience as an incident response analyst, security operations center (SOC) analyst, or equivalent experience.

Objectives:

After you successfully complete this course, expect to be able 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
- Lesson 2: Exploring Threat Intelligence and Threat Hunting Concepts
- Lesson 3: Explaining Important System and Network Architecture Concepts
- Lesson 4: Understanding Process Improvement in Security Operations
- Lesson 5: Implementing Vulnerability Scanning Methods
- Lesson 6: Performing Vulnerability Analysis
- Lesson 7: Communicating Vulnerability Information
- Lesson 8: Explaining Incident Response Activities
- Lesson 9: Demonstrating Incident Response Communication
- Lesson 10: Applying Tools to Identify Malicious Activity

- Lesson 11: Analyzing Potentially Malicious Activity
- Lesson 12: Understanding Application Vulnerability Assessment
- Lesson 13: Exploring Scripting Tools and Analysis Concepts
- Lesson 14: Understanding Application Security and Attack Mitigation Best Practices

Who Should Attend

This course is designed for experienced tech professionals who are looking to expand and validate their skill set. Job roles that CySA+ maps to:

- Security Analyst
- Security Operations
- Center (SOC) Analyst
- Security Administrator
- Incident Response Analyst
- Vulnerability Management Analyst
- Security Engineer