CompTIA Cybersecurity Analyst (CySA+) Certification (Exam CS0-002)

Overview

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.

Target Audience

This course is designed primarily for cybersecurity practitioners who perform job functions related to protecting information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This course focuses on the knowledge, ability, and skills necessary to provide for the defense of those information systems in a cybersecurity context, including protection, detection, analysis, investigation, and response processes. In addition, the course ensures that all members of an IT team—everyone from help desk staff to the Chief Information Officer—understand their role in these security processes.

Course Objectives

In this course, you will assess and respond to security threats and operate a systems and network security analysis platform you will...
Assess information security risk in computing and network environments.
Analyze reconnaissance threats to computing and network environments.
Analyze attacks on computing and network environments.
Analyze post-attack techniques on computing and network environments.
Implement a vulnerability management program.
Collect cybersecurity intelligence.
Analyze data collected from security and event logs.
Perform active analysis on assets and networks.
Respond to cybersecurity incidents.
Investigate cybersecurity incidents.
Address security issues with the organization's technology architecture.

Course Outline

1 - Threat and Vulnerability Management

Explain the importance of threat data and intelligence.
Given a scenario, utilize threat intelligence to support organizational security.
Given a scenario, perform vulnerability management activities
Given a scenario, analyze the output from common vulnerability assessment tools.
Explain the threats and vulnerabilities associated with specialized technology.
Explain the threats and vulnerabilities associated with operating in the cloud.
Given a scenario, implement controls to mitigate attacks and software vulnerabilities.

2 - Software and Systems Security

Given a scenario, apply security solutions for infrastructure management.
Explain software assurance best practices.
Explain hardware assurance best practices.

3 - Security Operations and Monitoring

Given a scenario, analyze data as part of security monitoring activities.
Given a scenario, implement configuration changes to existing controls to improve security.
Explain the importance of proactive threat hunting.
Compare and contrast automation concepts and technologies.

4 - Incident Response

Explain the importance of the incident response process.
Given a scenario, apply the appropriate incident response procedure.
Given an incident, analyze potential indicators of compromise.
Given a scenario, utilize basic digital forensics techniques

5 - Compliance and Assessment

Understand the importance of data privacy and protection.
Given a scenario, apply security concepts in support of organizational risk mitigation.
Explain the importance of frameworks, policies, procedures, and controls.

Related Courses, Certifications, Exams

- CompTIA Security+ Certification (SY0-601)
- CompTIA Security+ Certification (SY0-601)