CompTIA Cybersecurity Analyst (CySA+) Certification

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.

Prerequisite Comments

Network+, Security+ or equivalent knowledge. Minimum of 3-4 years of hands-on information security or related experience. While there is no required prerequisite, CySA+ is intended to follow CompTIA Security+ or equivalent experience and has a technical, hands-on focus.

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

Assessing Information Security Risk

- Identify the Importance of Risk Management
- Assess Risk
- Mitigate Risk
- Integrate Documentation into Risk Management

Analyzing Reconnaissance Threats to Computing and Network Environments

- Assess the Impact of Reconnaissance Incidents
- Assess the Impact of Social Engineering

Analyzing Attacks on Computing and Network Environments

- Assess the Impact of System Hacking Attacks
- Assess the Impact of Web-Based Attacks
- Assess the Impact of Malware
- Assess the Impact of Hijacking and Impersonation Attacks
- Assess the Impact of DoS Incidents
- Assess the Impact of Threats to Mobile Security
- Assess the Impact of Threats to Cloud Security

Analyzing Post-Attack Techniques

- Assess Command and Control Techniques
- Assess Persistence Techniques
- Assess Lateral Movement and Pivoting Techniques
- Assess Data Exfiltration Techniques
- Assess Anti-Forensics Techniques

Managing Vulnerabilities in the Organization

- Implement a Vulnerability Management Plan
- Assess Common Vulnerabilities
- Conduct Vulnerability Scans
- Conduct Penetration Tests on Network Assets
Collecting Cybersecurity Intelligence

Deploy a Security Intelligence Collection and Analysis Platform
Collect Data from Network-Based Intelligence Sources
Collect Data from Host-Based Intelligence Sources

Analyzing Log Data

Use Common Tools to Analyze Logs
Use SIEM Tools for Analysis

Performing Active Asset and Network Analysis

Analyze Incidents with Windows-Based Tools
Analyze Incidents with Linux-Based Tools
Analyze Malware
Analyze Indicators of Compromise

Responding to Cybersecurity Incidents

Deploy an Incident Handling and Response Architecture
Mitigate Incidents
Prepare for Forensic Investigation as a CSIRT

Investigating Cybersecurity Incidents

Apply a Forensic Investigation Plan
Securely Collect and Analyze Electronic Evidence
Follow Up on the Results of an Investigation

Addressing Security Architecture Issues

Remediate Identity and Access Management Issues
Implement Security During the SDLC

Related Courses, Certifications, Exams

- CompTIA Network+ Certification
- CompTIA Security+ Certification
- CompTIA A+ Certification (Exams 220-901 and 220-902)
- CS0-001 - CompTIA Cybersecurity Analyst (CSA+) Certification