CompTIA Cybersecurity Analyst (CySA+) Certification

Course Overview

This is a 5-day class

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.

Who Should Attend

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.

Upcoming Dates

Date	Time	Where
12/14/2020	9:00AM - 5:00PM	Online LIVE
01/25/2021	9:00AM - 5:00PM	Online LIVE
03/08/2021	9:00AM - 5:00PM	Online LIVE
04/26/2021	9:00AM - 5:00PM	Online LIVE
06/21/2021	9:00AM - 5:00PM	Online LIVE

View All Course Dates & Register Today

Course Outline

1 ASSESSING INFORMATION SECURITY RISK

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

CompTIA Cybersecurity Analyst (CySA+) Certification

2 ANALYZING RECONNAISSANCE THREATS TO COMPUTING AND NETWORK ENVIRONMENTS

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

3 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

4 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

5 MANAGING VULNERABILITIES IN THE ORGANIZATION

Implement a Vulnerability Management Plan
Assess Common Vulnerabilities
Conduct Vulnerability Scans
Conduct Penetration Tests on Network Assets

6 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

7 ANALYZING LOG DATA

Use Common Tools to Analyze Logs
Use SIEM Tools for Analysis

8 PERFORMING ACTIVE ASSET AND NETWORK ANALYSIS

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

9 RESPONDING TO CYBERSECURITY INCIDENTS

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

CompTIA Cybersecurity Analyst (CySA+) Certification

10 INVESTIGATING CYBERSECURITY INCIDENTS

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

11 ADDRESSING SECURITY ARCHITECTURE ISSUES

Remediate Identity and Access Management Issues
Implement Security During the SDLC