CompTIA Cybersecurity Analyst (CySA+) Day

Length: 9 days
Format: Classroom
Time: Day

About This Course

CompTIA Cybersecurity Analyst (CySA+) is an international, vendor-neutral IT professional certification that applies behavioral analytics to improve the overall state of IT security. It validates the knowledge and skills required to configure and use threat detection tools, perform data analysis and interpret the results to identify vulnerabilities, threats and risks to an organization, with the end goal of securing and protecting applications and systems within an organization.

This course covers the duties of those who are responsible for monitoring and detecting security incidents in information systems and networks, and for executing a proper response to such incidents. Depending on the size of the organization, this individual may act alone or may be a member of a cybersecurity incident response team (CSIRT). 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.

To learn more about the course objectives and opportunities in the industry for CySA+ certified professionals, view our CySA+ Certification Info Session.

Click here to find your place on the CompTIA Roadmap.

Required Exams

CySA+ Certification Exam

Audience Profile

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 the cybersecurity threat landscape.
* 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.
* Evaluate the organization\'s security through penetration testing.
* 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.

Outline

Lesson 1:Assessing Information Security RiskTopic A:Identify the Importance of Risk Management

Topic B:Assess Risk

Topic C:Mitigate Risk

Topic D:Integrate Documentation into Risk Management

Lesson 2:Analyzing the Threat LandscapeTopic A:Classify Threats and Threat Profiles

Topic B:Perform Ongoing Threat Research

Lesson 3:Analyzing Reconnaissance Threats to Computing and Network EnvironmentsTopic A:Implement Threat Modeling

Topic B:Assess the Impact of Reconnaissance Incidents

Topic C:Assess the Impact of Social Engineering

Lesson 4:Analyzing Attacks on Computing and Network EnvironmentsTopic A:Assess the Impact of System Hacking Attacks

Topic B:Assess the Impact of Web-Based Attacks

Topic C:Assess the Impact of Malware

Topic D:Assess the Impact of Hijacking and Impersonation Attacks

Topic E:Assess the Impact of DoS Incidents

Topic F:Assess the Impact of Threats to Mobile Security

Topic G:Assess the Impact of Threats to Cloud Security

Lesson 5:Analyzing Post-Attack TechniquesTopic A:Assess Command and Control Techniques

Topic B:Assess Persistence Techniques

Topic C:Assess Lateral Movement and Pivoting Techniques

Topic D:Assess Data Exfiltration Techniques

Topic E:Assess Anti-Forensics Techniques

Lesson 6:Managing Vulnerabilities in the OrganizationTopic A:Implement a Vulnerability Management Plan

Topic B:Assess Common Vulnerabilities

Topic C:Conduct Vulnerability Scans

Lesson 7:Implementing Penetration Testing to Evaluate SecurityTopic A:Conduct Penetration Tests on Network Assets

Topic B:Follow Up on Penetration Testing

Lesson 8:Collecting Cybersecurity IntelligenceTopic A:Deploy a Security Intelligence Collection and Analysis Platform

Topic B:Collect Data from Network-Based Intelligence Sources

Topic C:Collect Data from Host-Based Intelligence Sources

Lesson 9:Analyzing Log DataTopic A:Use Common Tools to Analyze Logs

Topic B:Use SIEM Tools for Analysis

Topic C:Parse Log Files with Regular Expressions

Lesson 10:Performing Active Asset and Network AnalysisTopic A:Analyze Incidents with Windows-Based Tools

Topic B:Analyze Incidents with Linux-Based Tools

Topic C:Analyze Malware

Topic D:Analyze Indicators of Compromise

Lesson 11:Responding to Cybersecurity IncidentsTopic A:Deploy an Incident Handling and Response Architecture

Topic B:Mitigate Incidents

Topic C:Prepare for Forensic Investigation as a CSIRT

Lesson 12:Investigating Cybersecurity IncidentsTopic A:Apply a Forensic Investigation Plan

Topic B:Securely Collect and Analyze Electronic Evidence

Topic C:Follow Up on the Results of an Investigation

Lesson 13:Addressing Security Architecture IssuesTopic A:Remediate Identity and Access Management Issues

Topic B:Implement Security During the SDLC