CompTIA Cybersecurity Analyst (CySA+) Bootcamp

Length: 5 days
Format: Bootcamp
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. Ultimately, the course promotes a comprehensive approach to security aimed toward those on the front lines of defense.

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 pathway.

Required Exams

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 teamâ€”everyone from help desk staff to the Chief

Information Officerâ€”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:Â Assessing Information Security RiskÂ Topic A:Â Identify the Importance of Risk Management

Â Topic B:Â Assess Risk

Â Topic C:Â Mitigate Risk

Â Topic D:Â Integrate Documentation into Risk Management

Â Lesson 2:Â Analyzing the Threat LandscapeÂ Topic A:Â Classify Threats and Threat Profiles

Â Topic B:Â Perform Ongoing Threat Research

Â Lesson 3:Â Analyzing Reconnaissance Threats to Computing and Network EnvironmentsÂ Topic A:Â Implement Threat Modeling

Â Topic B:Â Assess the Impact of Reconnaissance Incidents

Â Topic C:Â Assess the Impact of Social Engineering

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

Â Topic B:Â Assess the Impact of Web-Based Attacks

Â Topic C:Â Assess the Impact of Malware

Â Topic D:Â Assess the Impact of Hijacking and Impersonation Attacks

Â Topic E:Â Assess the Impact of DoS Incidents

Â Topic F:Â Assess the Impact of Threats to Mobile Security

Â Topic G:Â Assess the Impact of Threats to Cloud Security

Â Lesson 5:Â Analyzing Post-Attack TechniquesÂ Topic A:Â Assess Command and Control Techniques

Â Topic B:Â Assess Persistence Techniques

Â Topic C:Â Assess Lateral Movement and Pivoting Techniques

Â Topic D:Â Assess Data Exfiltration Techniques

Â Topic E:Â Assess Anti-Forensics Techniques

Â Lesson 6:Â Managing Vulnerabilities in the OrganizationÂ Topic A:Â Implement a Vulnerability Management Plan

Â Topic B:Â Assess Common Vulnerabilities

Â Topic C:Â Conduct Vulnerability Scans

Â Lesson 7:Â Implementing Penetration Testing to Evaluate SecurityÂ Topic A:Â Conduct Penetration Tests on Network Assets

Â Topic B:Â Follow Up on Penetration Testing

Â Lesson 8:Â Collecting Cybersecurity IntelligenceÂ Topic A:Â Deploy a Security Intelligence Collection and Analysis Platform

Â Topic B:Â Collect Data from Network-Based Intelligence Sources

Â Topic C:Â Collect Data from Host-Based Intelligence Sources

Â Lesson 9:Â Analyzing Log DataÂ Topic A:Â Use Common Tools to Analyze Logs

Â Topic B:Â Use SIEM Tools for Analysis

Â Topic C:Â Parse Log Files with Regular Expressions

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

Â Topic B:Â Analyze Incidents with Linux-Based Tools

Â Topic C:Â Analyze Malware

Â Topic D:Â Analyze Indicators of Compromise

Â Lesson 11:Â Responding to Cybersecurity IncidentsÂ Topic A:Â Deploy an Incident Handling and Response Architecture

Â Topic B:Â Mitigate Incidents

Â Topic C:Â Prepare for Forensic Investigation as a CSIRT

Â Lesson 12:Â Investigating Cybersecurity IncidentsÂ Topic A:Â Apply a Forensic Investigation Plan

Â Topic B:Â Securely Collect and Analyze Electronic Evidence

Â Topic C:Â Follow Up on the Results of an Investigation

Â Lesson 13:Â Addressing Security Architecture IssuesÂ Topic A:Â Remediate Identity and Access Management Issues

Â Topic B:Â Implement Security During the SDLC