

CompTIA CySA+ (CS0-003)

Overview

CompTIA Cybersecurity Analyst (CySA+) is a certification for cybersecurity professionals tasked with incident detection, prevention and response through continuous security monitoring.

The skills that today's security analysts need to protect organizations are different than the skills they had just a few years ago. CompTIA Cybersecurity Analyst (CySA+) certification has evolved to help organizations address, monitor and respond to threats and manage risk. Specifically, learners will gain skills in security operations, vulnerability management, incident response and management, and reporting and communication. CySA+-certified professionals are able to confidently lead incident detection, prevention and response in job roles like security analyst, Security Operations Center (SOC) analyst, incident response analyst, vulnerability management analyst, security engineer and threat hunter.

This course is designed for experienced tech professionals who are looking to expand and validate their skill set. Job roles that CySA+ maps to:

- Security Analyst
- Security Operations
- Center (SOC) Analyst
- Security Administrator
- Incident Response Analyst
- Vulnerability Management Analyst
- Security Engineer

CompTIA CySA+ is compliant with ISO/ANSI 17024 standards and maps to 10 DCWF work roles used by U.S. DoD Directive 8140.03M. View the approved work roles at [CompTIA.org/blog/putting-8140-to-work-upskilling-the-dod-workforce](https://www.comptia.org/blog/putting-8140-to-work-upskilling-the-dod-workforce)

Key Features

Training Delivery Options

- Private Cohort
- Self-Paced
- Mentored Learning
- Instructor-Led Training

Training Duration Options

- 5 Days
- 8 Weeks
- 13 Weeks
- Custom Option

Available Product Options

- CertMaster Learn + Labs
- CertMaster Learn
- CertMaster Lab
- Instructor and Student Guides

Prerequisite Courses / Knowledge

Network+, Security+, or equivalent knowledge, with a minimum of 4 years of hands-on experience as an incident response analyst, security operations center (SOC) analyst, or equivalent experience.

Knowledge and Skills

The CompTIA Cybersecurity Analyst (CySA+) certification exam will certify the successful candidate has the knowledge and skills required to:

- Detect and analyze indicators of malicious activity
- Understand threat hunting and threat intelligence concepts
- Use appropriate tools and methods to manage, prioritize, and respond to attacks and vulnerabilities
- Perform incident response processes
- Understand reporting and communication concepts related to vulnerability management and incident response activities

Lesson Outline

Lesson 1: Understanding Vulnerability Response, Handling, and Management	Lesson 9: Demonstrating Incident Response Communication
Lesson 2: Exploring Threat Intelligence and Threat Hunting Concepts	Lesson 10: Applying Tools to Identify Malicious Activity Lesson 11: Analyzing Potentially Malicious Activity
Lesson 3: Explaining Important System and Network Architecture Concepts	Lesson 12: Understanding Application Vulnerability Assessment
Lesson 4: Understanding Process Improvement in Security Operations	Lesson 13: Exploring Scripting Tools and Analysis Concepts
Lesson 5: Implementing Vulnerability Scanning Methods Lesson 6: Performing Vulnerability Analysis	Lesson 14: Understanding Application Security and Attack Mitigation Best Practices
Lesson 7: Communicating Vulnerability Information	Appendix 0: Student Resources
Lesson 8: Explaining Incident Response Activities	Appendix 1: Instructor Resources

Learner Outcomes

Learners who successfully earn the CompTIA CySA+ certification demonstrate the ability to proactively monitor and detect malicious activity using advanced tools and techniques like threat intelligence, SIEM, EDR, and XDR. They are equipped to effectively respond to threats, attacks, and vulnerabilities by applying incident response and vulnerability management processes, while showcasing strong communication skills essential for security analysis and compliance. Additionally, they exhibit a deep understanding of current trends impacting security analysts, including expertise in cloud and hybrid environments, proving their value in addressing modern cybersecurity challenges.

Exam Details

Launch Date: June 6, 2023

Number of Questions: Maximum of 85 questions

Type of Questions: Multiple choice and performance-based
Length of Test: 165 Minutes

Passing Score: 750 (on a scale of 100-900)