Cybersecurity Analyst
Exam CS0-002

Overview
CompTIA Cybersecurity Analyst (CySA+) is an IT workforce certification that applies behavioral analytics to networks and devices to prevent, detect and combat cybersecurity threats through continuous security monitoring.
CySA+ is the only intermediate high-stakes cybersecurity analyst certification with performance-based questions that cover core security analyst skills while emphasizing software and application security, automation, threat hunting, and IT regulatory compliance.

What skills will you learn?
- Threat and Vulnerability Management. Utilize and apply proactive threat intelligence to support organizational security and perform vulnerability management activities.
- Software and systems security. Apply security solutions for infrastructure management and explain software & hardware assurance best practices.
- Compliance and assessment. Apply security concepts in support of organizational risk mitigation and understand the importance of frameworks, policies, procedures, and controls.
- Security Operations and Monitoring. Analyze data as part of continuous security monitoring activities and implement configuration changes to existing controls to improve security.
- Incident response. Apply the appropriate incident response procedure, analyze potential indicators of compromise, and utilize basic digital forensics techniques.

Course Length
5 days

Prerequisites
CompTIA Network+ candidates are recommended to have the following experience:
- Network+, Security+ or equivalent knowledge. Minimum of 4 years of hands-on information security or related experience.

Course Contents

- Lesson 1: Explaining the Importance of Security Controls and Security Intelligence
- Lesson 2: Utilizing Threat Data and Intelligence
- Lesson 3: Analyzing Security Monitoring Data
- Lesson 4: Collecting and Querying Security Monitoring Data
- Lesson 5: Utilizing Digital Forensics and Indicator Analysis Techniques
- Lesson 6: Applying Incident Response Procedures
- Lesson 7: Applying Risk Mitigation and Security Frameworks
- Lesson 8: Performing Vulnerability Management
- Lesson 9: Applying Security Solutions for Infrastructure Management
- Lesson 10: Understanding Data Privacy and Protection
- Lesson 11: Applying Security Solutions for Software Assurance
- Lesson 12: Applying Security Solutions for Cloud and Automation

Certification Information

Exam CS0-002