skillsoft global knowledge™

COMPTIA CYSA+ CERTIFICATION PREP COURSE - CYBERSECURITY ANALYST

Course Code: 5867

Learn how to analyze, monitor, and protect critical infrastructures using threat-detection and threat-analysis tools.

Gain the tools and tactics to manage cybersecurity risks, identify various types of common threats, evaluate an organization's security, collect and analyze cybersecurity intelligence, and handle incidents as they occur. This is a comprehensive approach to security aimed toward those on the front lines of defense.
This course is designed to assist students in preparing for the CompTIA CySA+ - Cybersecurity Analyst+ (CS0-003) certification exam.

CompTIA's CySA+ is a global, vendor-neutral certification covering intermediate-level knowledge and skills required by information security analyst job roles. It helps identify a cybersecurity professional's ability to proactively defend an organization using secure monitoring, threat identification, incident response and teamwork. The CompTIA CySA+ CS0-003 certification exam ensures the 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

This course includes an exam voucher.

What You'll Learn

- Explain the Importance of Security Controls and Security Intelligence
- Utilize Threat Data and Intelligence
- Analyze Security Monitoring Data
- Collect and Query Security Monitoring Data
- Utilize Digital Forensics and Indicator Analysis Techniques
- Apply Incident Response Procedures
- Apply Risk Mitigation and Security Frameworks

- Perform Vulnerability Management
- Apply Security Solutions for Infrastructure Management
- Understand Data Privacy and Protection
- Apply Security Solutions for Software Assurance
- Apply Security Solutions for Cloud and Automation

Who Needs to Attend

- IT Security Analyst
- Security Operations Center (SOC) Analyst
- Vulnerability Analyst
- Cybersecurity Specialist
- Threat Intelligence Analyst
- Security Engineer

Prerequisites

To ensure your success in this course, you should meet the following requirements:

- At least two years (recommended) of experience in computer network security technology or a related field.
- The ability to recognize information security vulnerabilities and threats in the context of risk management.
- Foundation-level operational skills with some of the common operating systems for computing environments.
- Foundational knowledge of the concepts and operational framework of common assurance safeguards in computing environments. Safeguards include, but are not limited to, basic authentication and authorization, resource permissions, and anti-malware mechanisms.
- Foundation-level understanding of some of the common concepts for network environments, such as routing and switching.
- Foundational knowledge of major TCP/IP networking protocols including, but not limited to, TCP, IP, UDP, DNS, HTTP, ARP, ICMP, and DHCP.
- Foundational knowledge of the concepts and operational framework of common assurance safeguards in network environments. Safeguards include, but are not limited to, firewalls, intrusion prevention systems, and VPNs.

skillsoft global knowledge™

COMPTIA CYSA+ CERTIFICATION PREP COURSE - CYBERSECURITY ANALYST

Course Code: 5867

CLASSROOM LIVE	$3,095 USD	5 Day

skillsoft global knowledge™

COMPTIA CYSA+ CERTIFICATION PREP COURSE - CYBERSECURITY ANALYST

Course Code: 5867

VIRTUAL CLASSROOM LIVE	$3,095 USD	5 Day

Virtual Classroom Live Outline

- Lesson 1: Understanding Vulnerability Response, Handling, and Management
- Lesson 2: Exploring Threat Intelligence and Threat Hunting Concepts
- Lesson 3: Explaining Important System and Network Architecture Concepts
- Lesson 4: Understanding Process Improvement in Security Operations
- Lesson 5: Implementing Vulnerability Scanning Methods
- Lesson 6: Performing Vulnerability Analysis
- Lesson 7: Communicating Vulnerability Information
- Lesson 8: Explaining Incident Response Activities
- Lesson 9: Demonstrating Incident Response Communication
- Lesson 10: Applying Tools to Identify Malicious Activity
- Lesson 11: Analyzing Potentially Malicious Activity
- Lesson 12: Understanding Application Vulnerability Assessment
- Lesson 13: Exploring Scripting Tools and Analysis Concepts
- Lesson 14: Understanding Application Security and Attack Mitigation Best Practices
- Appendix A: Mapping Course Content to CompTIA CySA+ (CS0-003)

Virtual Classroom Live Labs

- Assisted Lab: Exploring the Lab Environment
- Assisted Lab: Configuring Controls
- Assisted Lab: Reviewing IoC and Threat Intelligence Sources
- Assisted Lab: Performing Threat Hunting
- Assisted Lab: Configuring Centralized Logging
- APPLIED LAB: Performing System Hardening
- Assisted Lab: Assess Time Synch Errors
- Assisted Lab: Configuring Automation

- Assisted Lab: Performing Asset Discovery
- Assisted Lab: Performing Vulnerability Scanning
- Assisted Lab: Performing Passive Scanning
- Assisted Lab: Establishing Context Awareness
- Assisted Lab: Analyzing Vulnerability Reports
- Assisted Lab: Detecting Legacy Systems
- APPLIED LAB: Performing Post-Incident Forensic Analysis
- APPLIED LAB: Performing IoC Detection and Analysis
- ADAPTIVE LAB: Performing Playbook Incident Response
- APPLIED LAB: Collecting Forensic Evidence
- Assisted Lab: Performing Root Cause Analysis
- APPLIED LAB: Using Network Sniffers
- APPLIED LAB: Researching DNS and IP Reputation
- Assisted Lab: Using File Analysis Techniques
- Assisted Lab: Analyzing Potentially Malicious Files
- Assisted Lab: Using Nontraditional Vulnerability Scanning Tools
- APPLIED LAB: Performing Web Vulnerability Scanning
- Assisted Lab: Exploiting Weak Cryptography
- Assisted Lab: Performing and Detecting Directory Traversal and Command Injection
- Assisted Lab: Performing and Detecting Privilege Escalation
- Assisted Lab: Performing and Detecting XSS
- Assisted Lab: Performing and Detecting LFI/RFI
- Assisted Lab: Performing and Detecting SQLi
- Assisted Lab: Performing and Detecting CSRF
- APPLIED LAB: Detecting and Exploiting Security Misconfiguration

Jun 2 - 6, 2025 | 11:30 AM - 7:30 PM EDT

Jun 9 - 13, 2025 | 8:30 AM - 4:30 PM EDT

Jul 28 - Aug 1, 2025 | 8:30 AM - 4:30 PM EDT

Aug 4 - 8, 2025 | 8:30 AM - 4:30 PM EDT

Sep 15 - 19, 2025 | 8:30 AM - 4:30 PM EDT

Oct 6 - 10, 2025 | 8:30 AM - 4:30 PM EDT

Nov 3 - 7, 2025 | 8:30 AM - 4:30 PM EST

Dec 1 - 5, 2025 | 8:30 AM - 4:30 PM EST

Dec 8 - 12, 2025 | 11:30 AM - 7:30 PM EST

Jan 12 - 16, 2026 | 8:30 AM - 4:30 PM EST

COMPTIA CYSA+ CERTIFICATION PREP COURSE - CYBERSECURITY ANALYST

Course Code: 5867

PRIVATE GROUP TRAINING	5 Day

Visit us at www.globalknowledge.com or call us at 1-866-716-6688.

Date created: 5/9/2025 12:47:12 AM