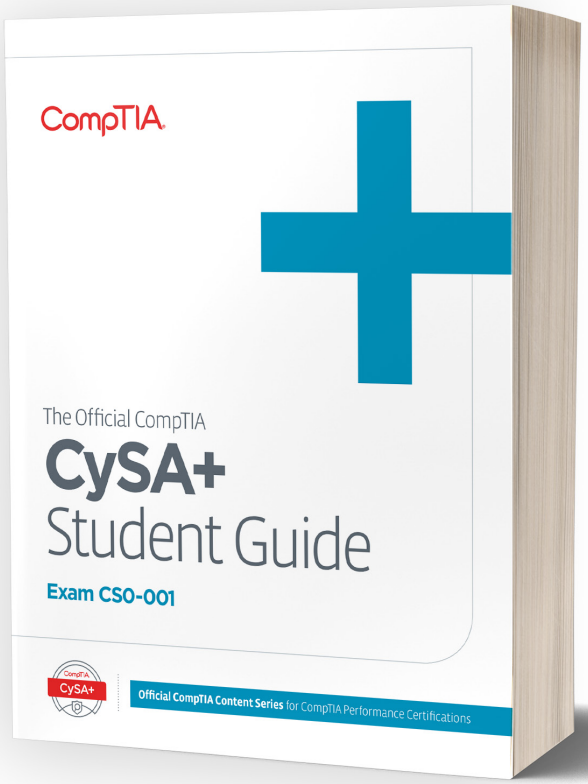
CompTIA



Official CompTIA Content for Instructor-Led Training:

CompTIA CySA+

Official CompTIA Content for Instructor-Led Training is designed with the instructor in mind, providing insights and tools for successfully training learners pursuing their CompTIA CySA+ certification.

Overview

The Official CompTIA CySA+ Guide (Exam CS0-001) is developed for cybersecurity practitioners who perform job functions related to protecting information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. These materials focus 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. It provides full coverage of the objectives for the CompTIA CySA+ certification and will help prepare students to take the exam.

Official Content:

- The Official CompTIA CySA+ Instructor Guide (Exam CS0-001)
- The Official CompTIA CySA+ Student Guide (Exam CS0-001)
- CompTIA CHOICE Digital Learning Platform
  - Online resources included with purchase of Guides
- CompTIA CySA+ (Exam CS0-001) CompTIA Labs
- CompTIA CertMaster Practice for CySA+ (Exam CS0-001)

Why is Official CompTIA Content different?

- **For exam takers, by the exam developer** - Official CompTIA Content is the only study material exclusively developed by CompTIA for the CompTIA certification candidate.
- **Complete Library** - No other content library covers all exam objectives for all certifications. It provides complete breadth, depth and currency of material unavailable with competitors.
- **Developed with the instructor in mind** - Official CompTIA Content's focus on instruction is unique, providing instructors ease and flexibility to teach to any audience within any modality.

Key Features and Benefits

- **Designed and Class-tested for Instructor-Led Training** using proven instructional design. Topics are presented in a hierarchy that offers knowledge, procedural tasks and hand-on activities that require students put knowledge into practice. This approach keeps student engaged and ensures success.
- **Comprehensive instructor resources enhanced through CompTIA CHOICE platform** ensures a successful course delivery. Resources to download include:
  - **Course setup** notes describe hardware and software requirements
  - Course-specific **delivery tips** with insights to deliver the course material
  - **Presentation planners** help plan and schedule coursed based on different course lengths
  - **PowerPoint slides**
  - **Facilitator notes** in instructor manual
  - **Solutions** to activities and discussions
- **Comprehensive student resources enhanced through CompTIA CHOICE platform** engages students by providing:
  - **Classroom:** A link to the training provider's classroom environment
  - **eBook:** An interactive online version of the book, along with secure PDF and downloadable versions
  - **Files:** Any course files available to download
  - **Videos:** Brief animated videos that enhance and extend the classroom learning experience
  - **Assessment:** Questions designed for self-assessment of the course content
  - **Checklists:** Step by step procedures for recurring IT tasks that are part of the course objectives and as post-class references
  - **Links:** Helpful links to certification exam information, CompTIA's IT Careers blog, and additional resources for test prep
  - **Locker:** A resource allowing for secure file exchange with students
- **Focused on job roles and 100% coverage of exam objectives** means content is practical, based on real performance scenarios. In addition, content is aligned to certification exam objectives.
- **Active Learning** is integrated with one activity per topic designed to enable students to practice guidelines and procedures as well as solidify understanding of the informational material presented in the course.
- **Flexible and customizable based on course format** whether the course is co-located or remote, synchronous or asynchronous. Class resources can be easily configured based on modality.

Lab option

- CompTIA Labs hosted by Learn on Demand Systems allow students to learn in actual software applications through a remote lab environment. Labs allow students to practice what they are learning using real, hands-on experiences. Students have access to the software environment for 6 months after a CompTIA Labs access key is redeemed, providing a fantastic post-class resource for students to practice their skills.

Exam Prep option

- CertMaster Practice is an online knowledge assessment and remediation tool designed to help students feel more confident and prepared for their CompTIA exam.

Course Overview

This course is for students who are preparing for the CompTIA CySA+ certification exam CS0-001.

This course has been created 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.

Job Roles

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

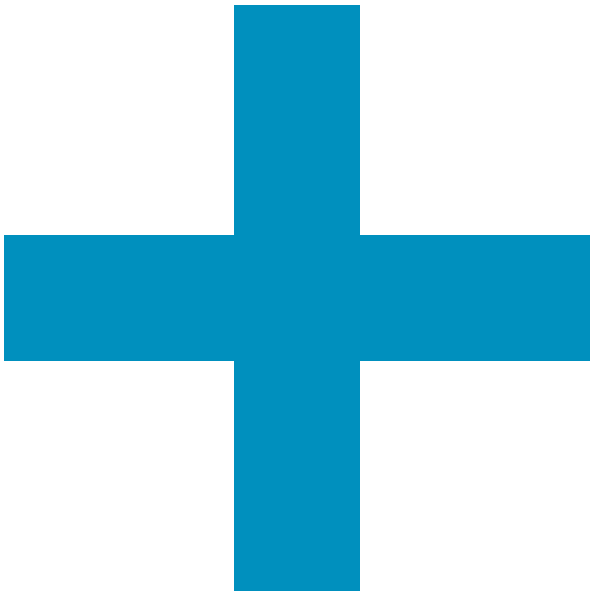
Prerequisites

Students should have at least two years' experience in IT network security plus:

- The ability to recognize information security vulnerabilities and threats in the context of risk management.
- Foundation-level operational skills with common operating systems
- Foundational knowledge of the concepts and framework of common desktop and network security safeguards
- Foundation-level understanding of some of common networking concepts
- Foundational knowledge of major TCP/IP networking protocols

Course content summary

- *Lesson 1: Assessing Information Security Risk:* Identify the Importance of Risk Management • Assess Risk • Mitigate Risk • Integrate Documentation into Risk Management
- *Lesson 2: Analyzing Reconnaissance Threats to Computing and Network Environments:* Assess the Impact of Reconnaissance Incidents • Assess the Impact of Social Engineering
- *Lesson 3: Analyzing Attacks on Computing and Networking Environments:* Assess the Impact of System Hacking Attacks • Assess the Impact of Web-Based Attacks • Assess the Impact of Malware • Assess the Impact of Hijacking and Impersonation Attacks • Assess the Impact of DoS Incidents • Assess the Impact of Threats to Mobile Security • Assess the Impact of Threats to Cloud Security
- *Lesson 4: Analyzing Post-Attack Techniques:* Assess Command and Control Techniques • Assess Persistence Techniques • Assess Lateral Movement and Pivoting Techniques • Assess Data Exfiltration Techniques • Assess Anti-Forensics Techniques
- *Lesson 5: Managing Vulnerabilities in the Organization:* Implement a Vulnerability Management Plan • Assess Common Vulnerabilities • Conduct Vulnerability Scans • Conduct Penetration Tests on Network Assets
- *Lesson 6: Collecting Cybersecurity Intelligence:* Deploy a Security Intelligence Collection and Analysis Platform • Collect Data from Network-Based Intelligence Sources • Collect Data from Host-Based Intelligence Sources
- *Lesson 7: Analyzing Log Data:* Use Common Tools to Analyze Logs • Use SIEM Tools for Analysis
- *Lesson 8: Performing Active Asset and Network Analysis:* Analyze Incidents with Windows-Based Tools • Analyze Incidents with Linux-Based Tools • Analyze Malware • Analyze Indicators of Compromise
- *Lesson 9: Responding to Cybersecurity Incidents:* Deploy an Incident Handling and Response Architecture • Mitigate Incidents • Prepare for Forensic Investigation as a CSIRT
- *Lesson 10: Investigating Cybersecurity Incidents:* Apply a Forensic Investigation Plan • Securely Collect and Analyze Electronic Evidence • Follow Up on the Results of an Investigation
- *Lesson 11: Addressing Security Architecture Issues:* Remediate Identity and Access Management



Purchase Everything in One Place

Official CompTIA Content is available on the CompTIA Store at store.comptia.com, which means partners will be able to obtain Official CompTIA Content, CompTIA CertMaster products and exam vouchers all in one place.

Please contact your CompTIA business development representative for more information.

CompTIA