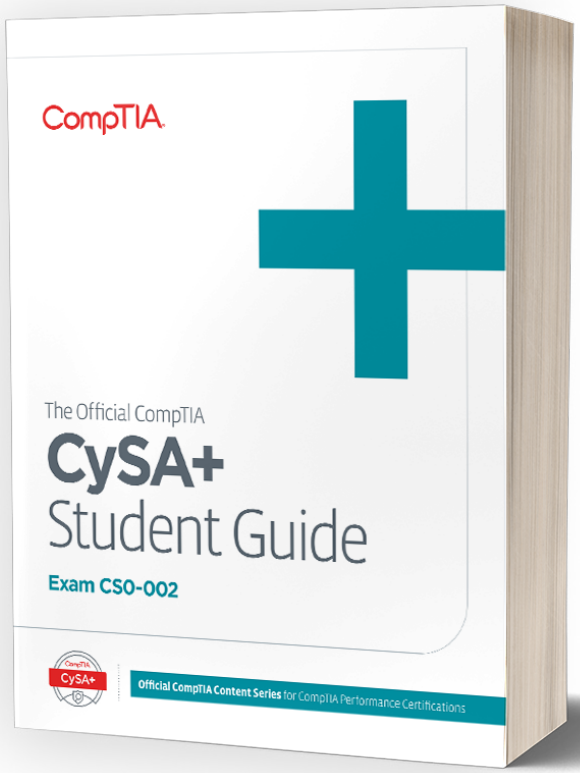
CompTIA



Official CompTIA learning resources 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+ Guides (Exam CS0-002) The Official CompTIA CySA+ Guides (Exam CS0-002) are designed for cybersecurity analysts who apply behavioral analytics to networks to improve the overall state of security through identifying and combating malware and advanced persistent threats. These materials focus on teaching an IT professional the ability to proactively defend and continuously improve the security of an organization through leveraging intelligence and threat detection techniques, analyzing and interpreting data, identifying and addressing vulnerabilities, and effectively responding to and recovering from incidents. The CySA+ guide will sufficiently prepare candidates to take the CompTIA CySA+ certification exam.

OFFICIAL LEARNING RESOURCES

- The Official CompTIA CySA+ Instructor Guide (Exam CS0-002)
- The Official CompTIA CySA+ Student Guide (Exam CS0-002)
- CompTIA Learning Center – Digital Learning Platform – included with purchase of print and eBook
- CompTIA CySA+ (Exam CS0-002) CompTIA Labs
- CertMaster Learn for Instructor-Led Training
- CertMaster Practice

WHY ARE OFFICIAL COMPTIA LEARNING RESOURCES DIFFERENT?

- **For Exam Takers by the Exam Developer** - Official CompTIA learning resources are the only study material exclusively developed by CompTIA for the CompTIA certification candidate.
- **Developed with the instructor in mind** - Official CompTIA learning resource's focus on instruction are unique, providinginstructors ease and flexibility to teach to any audience within any modality.
- **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.

KEY FEATURES AND BENEFITS

- **Designed and Tested Specifically for Instructor-led Training**
  The Official CompTIA CySA+ Guides are specifically designed and tested for expert-facilitated delivery. The Instructor Guide is designed to make implementation easy and support instructors with course-specific technical and setup information, delivery notes, and tips and best practices to foster an excellent learning experience for students.

- **Support the Modern Learner**
  The Official CompTIA CySA+ Guides are designed with the modern student and classroom in mind. The content has been tested to ensure success whether the course format is co-located or remote, synchronous or asynchronous, continuous or modular. In addition, instructors will find best practices and recommendations within the margin of their Instructor Guide specific to the various course formats.

- **Focused on Job Roles and Objectives**
  The Official CompTIA Guides are organized into Courses, Lessons, and Topics and align training to work in the real world. Courses such as CySA+ reflect a real job role, Lessons refer to functional areas within that job role, and Topics relate to discrete job tasks.

LABS

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 180 days after a CompTIA Labs access key is redeemed, providing a post-class resource for students to practice their skills.

Labs Available:

1. Analyzing Output from Network Security Monitoring Tools
2. Analyzing Output from Security Appliance Logs
3. Analyzing Output from Endpoint Security Monitoring Tools
4. Analyzing Email Headers
5. Configuring SIEM Agents and Collectors
6. Analyzing, Filtering, and Searching Event Log and syslog Output
7. Collecting and Validating Digital Evidence
8. Analyzing Network-related IoCs
9. Analyzing Host and Application IoCs
10. Following an Incident Response Process
11. Observing IoCs during a Security Incident
12. Reviewing Risk Management Processes
13. Analyzing Output from Topology and Host Enumeration Tools
14. Testing Credential Security
15. Configuring Vulnerability Scanning and Analyzing Outputs
16. Assessing Vulnerability Scan Outputs
17. Assessing the Impact of Regulation on Vulnerability Management
18. Performing Account and Permissions Audits
19. Configuring Network Segmentation and Security
20. Configuring and Analyzing Share Permissions
21. Assessing the Impact of Web Application Vulnerabilities
22. Analyzing Output from Web Application Assessment Tools
23. Analyzing Output from Cloud Infrastructure Assessment Tools
24. Assessing the Impact of Threats to Cloud Infrastructures

COMPTIA LEARNING CENTER

The CompTIA Learning Center is an intuitive online platform, accompanied with the purchase of an Instructor or Student Guide, that provides access to the eBook and all accompanying resources tosupport Instructor-Led Training and the Official CompTIA curriculum.

Comprehensive **INSTRUCTOR** resources ensure successful course delivery by providing:	Comprehensive **STUDENT** resources engage students by providing:
• **Course-specific delivery tips** provide the instructor with additional insights to deliver the course successfully • **Facilitator notes** in instructor guide • **PowerPoint slides:** A complete set of slides to facilitate the class including lists, tables, diagrams, illustrations, annotated screens and activity summaries • **Solutions** Instructors have solutions to Activities and Discussion Questions embedded within the Instructor Guide • **Setup Guide:** A complete set of instructions for setting up instructor and student computers to complete hands-on activities in the course.	• **eBook:** An interactive online version of the book, along with secure PDF and downloadable versions • **Videos:** Brief videos supplement key topics in the course • **Assessment:** A series of different assessments for each lesson as well an overall self-assessment • **PowerPoint slides** • **Exam objective mapping** • **Solutions** to activities and discussions • **Strengths and Weaknesses Dashboard:** Students assessments results are aggregated in the Strengths and Weaknesses dashboard to provide an indicator of their overall performance in the course.

COMPTIA CERTMASTER LEARN FOR INSTRUCTOR-LED TRAINING

The official eLearning courseware solution that helps learners gain the knowledge and practical skills needed to improve performance and achieve success.

CertMaster Learn for Instructor-led Training empowers instructor and administrator success by providing easy-to-use course management tools, a comprehensive suite of instructor resources, and reporting and analytics options that provide actionable data to help inform instruction. The Boost Dashboard makes tracking individual student and group progress simple and efficient.

COURSE OVERVIEW

This course is for students who are preparing for the CompTIA CySA+ certification exam CS0-002.

The CompTIA Cybersecurity Analyst (CySA+) certification verifies that successful candidates have the knowledge and skills required to leverage intelligence and threat detection techniques, analyze and interpret data, identify and address vulnerabilities, suggest preventative measures, and effectively respond to and recover from incidents.

JOB ROLES

Top CySA+ Job Roles

- **Security Analyst**
  - **Tier II SOC analyst**
  - **Security monitoring**
- **Threat intelligence analyst**
- **Security engineer**
- **Application security analyst**
- **Incident response or handler**
- **Compliance analyst**
- **Threat hunter**

PREREQUISITES

Recommended Network+, Security+ or equivalent knowledge. Minimum of 4 years of hands-on experience in technical cybersecurity role.

CySA+ will verify the successful candidate has the knowledge and skills required to:

- Leverage intelligence and threat detection techniques
- Analyze and interpret data
- Identify and address vulnerabilities
- Suggest preventative measures
- Effectively respond to and recover from incidents

TABLE OF CONTENTS

Lesson 1: Explaining the Importance of Security Controls and Security Intelligence: Topic 1A: Identify Security Control Types Topic 1B: Explain the Importance of Threat Data and Intelligence	**Lesson 2: Utilizing Threat Data and Intelligence:** Topic 2A: Classify Threats and Threat Actor Types Topic 2B: Utilize Attack Frameworks and Indicator Management Topic 2C: Utilize Threat Modeling and Hunting Methodologies	**Lesson 3: Analyzing Security Monitoring Data:** Topic 3A: Analyze Network Monitoring Output Topic 3B: Analyze Appliance Monitoring Output Topic 3C: Analyze Endpoint Monitoring Output Topic 3D: Analyze Email Monitoring Output
Lesson 4: Collecting and Querying Security Monitoring Data: Topic 4A: Configure Log Review and SIEM Tools Topic 4B: Analyze and Query Logs and SIEM Data	**Lesson 5: Utilizing Digital Forensics and Indicator Analysis Techniques:** Topic 5A: Identify Digital Forensics Techniques Topic 5B: Analyze Network-related IOCs Topic 5C: Analyze Host-related IOCs Topic 5D: Analyze Application-related IOCs Topic 5E: Analyze Lateral Movement and Pivot IOCs	**Lesson 6: Applying Incident Response Procedures:** Topic 6A: Explain Incident Response Processes Topic 6B: Apply Detection and Containment Processes Topic 6C: Apply Eradication, Recovery, and Post-incident Processes
Lesson 7: Applying Risk Mitigation and Security Frameworks: Topic 7A: Apply Risk Identification, Calculation, and Prioritization Processes Topic 7B: Explain Frameworks, Policies, and Procedures	**Lesson 8: Performing Vulnerability Management:** Topic 8A: Analyze Output from Enumeration Tools Topic 8B: Configure Infrastructure Vulnerability Scanning Parameters Topic 8C: Analyze Output from Infrastructure Vulnerability Scanners Topic 8D: Mitigate Vulnerability Issues	**Lesson 9: Applying Security Solutions for Infrastructure Management:** Topic 9A: Apply Identity and Access Management Security Solutions Topic 9B: Apply Network Architecture and Segmentation Security Solutions Topic 9C: Explain Hardware Assurance Best Practices Topic 9D: Explain Vulnerabilities Associated with Specialized Technology
Lesson 10: Understanding Data Privacy and Protection: Topic 10A: Identify Non-technical Data and Privacy Controls Topic 10B: Identify Technical Data and Privacy Controls	**Lesson 11: Applying Security Solutions for Software Assurance:** Topic 11A: Mitigate Software Vulnerabilities and Attacks Topic 11B: Mitigate Web Application Vulnerabilities and Attacks Topic 11C: Analyze Output from Application Assessments	**Lesson 12: Applying Security Solutions for Cloud and Automation:** Topic 12A: Identify Cloud Service and Deployment Model Vulnerabilities Topic 12B: Explain Service-oriented Architecture Topic 12C: Analyze Output from Cloud Infrastructure Assessment Tools Topic 12D: Compare Automation Concepts and Technologies

PURCHASE EVERYTHING IN ONE PLACE

Official CompTIA learning resources are available on the CompTIA Store at https://store.comptia.org/, which means partners will be able to obtain Official CompTIA learning resources, CompTIA CertMaster products and exam vouchers all in one place. Please contact your CompTIA business development representative for more information.

CompTIA