CompTIA CS0-002 Exam Prep 2026

CompTIA CS0-002 CySA+ 2026. Threat analysis, vulnerability management, and incident response.

IT Certifications Instructor: Jason Miller • 5 sections • 45 lessons • 13.25h total

View this course online Browse all courses

About this course

Preparing for the CompTIA CySA+ (CS0-002) exam can feel overwhelming with so much material to cover. This course cuts through the noise and gives you a focused, step-by-step study plan aligned with the 2026 exam objectives.

You will learn how to tackle each exam domain with practical techniques, including threat analysis, vulnerability management, and incident response. The course includes video lessons, downloadable study guides, real case studies, and practice question sessions.

Course curriculum

Section 1: Foundations and Exam Overview

- Understanding the 2026 CS0-002 Exam Structure (12m)
  Get a clear breakdown of the exam domains and question types to set your study strategy from the start.
- Setting Up Your Study Environment and Tools (8m)
  Learn how to organize your materials and use free resources to create an effective study plan.
- Key Terminology for Cybersecurity Analysts (15m)
  Master essential terms and concepts that appear frequently on the exam, with practical examples.
- How to Read and Analyze Exam Objectives (10m)
  Step-by-step guide to interpreting the official CS0-002 objectives for targeted learning.
- Time Management Strategies for the Exam (11m)
  Techniques to pace yourself during the test, including how to handle performance-based questions.
- Building a 90-Day Study Schedule (18m)
  Downloadable template to create a personalized timeline that balances review and practice.
- Common Pitfalls to Avoid in CS0-002 Preparation (9m)
  Real-case analysis of mistakes candidates make and how to steer clear of them.

Section 2: Core Concepts - Threat and Vulnerability Management

- Applying Threat Intelligence in Real Scenarios (22m)
  Learn how to use threat feeds and data to identify risks, with a downloadable checklist.
- Vulnerability Scanning Tools and Techniques (25m)
  Walk through popular tools and how to interpret scan results for the exam.
- Prioritizing Vulnerabilities with Risk Assessment (14m)
  Step-by-step guide to scoring and ranking vulnerabilities using industry frameworks.
- Analyzing Malware and Attack Vectors (28m)
  Problem-solving session on dissecting malware reports and attack paths.
- Network Security Monitoring Fundamentals (16m)
  How to set up and interpret logs from firewalls and intrusion detection systems.
- Encryption Methods for Data Protection (13m)
  Practical overview of symmetric and asymmetric encryption with exam-focused examples.
- Identity and Access Management Best Practices (20m)
  Real-world case study on implementing MFA and role-based access controls.
- Cloud Security Considerations for CySA+ (19m)
  Key concepts for securing cloud environments, based on 2026 exam updates.
- Hands-On Lab: Vulnerability Assessment Simulation (30m)
  Interactive exercise to scan a mock network and report findings.

Section 3: Deep Dive - Incident Response and Forensics

- Incident Response Lifecycle: Step-by-Step (24m)
  Break down the phases from preparation to recovery, with a downloadable workflow chart.
- Creating an Incident Response Plan (17m)
  Template and guide to draft a plan tailored to your organization's needs.
- Forensic Data Collection Techniques (21m)
  Learn how to preserve evidence without contamination, using real case examples.
- Analyzing Logs for Incident Clues (26m)
  Problem-solving session to trace an attack through system and application logs.
- Containment and Eradication Strategies (15m)
  Practical methods to isolate threats and remove malware from affected systems.
- Post-Incident Reporting and Lessons Learned (12m)
  How to write a clear report that meets compliance and improves future responses.
- Legal and Ethical Considerations in Forensics (18m)
  Discussion on chain of custody and privacy laws relevant to the exam.

Section 4: Advanced Application - Security Operations

- Security Information and Event Management (SIEM) Basics (23m)
  How to configure alerts and dashboards for proactive monitoring.
- Automating Security Tasks with Scripts (27m)
  Intro to Python scripts for log analysis and reporting, with code examples.
- Threat Hunting Methodologies (20m)
  Step-by-step approach to proactively search for threats in your network.
- Disaster Recovery and Business Continuity Planning (19m)
  Real-world case study on creating a recovery plan for a data breach.
- Compliance Frameworks: NIST and ISO (16m)
  How these frameworks apply to CySA+ and exam question strategies.
- Secure Software Development Lifecycle (SDLC) (22m)
  Integrating security into development processes, with a downloadable checklist.
- Mobile and IoT Security Challenges (14m)
  Analysis of common vulnerabilities and mitigation techniques.
- Advanced Network Traffic Analysis (29m)
  Hands-on exercise using Wireshark to identify suspicious activity.
- Social Engineering Defense Strategies (11m)
  Practical tips to train teams and recognize phishing attempts.
- Case Study: Full Security Operations Review (32m)
  Walk through a comprehensive scenario from detection to resolution.

Section 5: Implementation and Exam Success

- Practice Exam Strategies and Review (18m)
  How to take and analyze practice tests to identify weak areas.

- Performance-Based Questions (25m)
  Step-by-step walkthrough of common PBQ formats and tips for success.
- Creating Your Personalized Flashcards (9m)
  Downloadable template for key terms and concepts to reinforce memory.
- Final Review: Domain-by-Domain Checklist (13m)
  A comprehensive list to ensure you've covered all 2026 exam objectives.
- Test Day Preparation and Mindset (10m)
  Practical advice on what to do before and during the exam to stay calm.
- Post-Exam: What to Do After Passing (8m)
  Next steps for certification maintenance and career advancement.
- Study Group and Community Resources (7m)
  How to join forums and groups for ongoing support and updates.
- Updating Your Resume with CySA+ Certification (11m)
  Tips on highlighting your new skills for job applications.
- Long-Term Learning Plan for Cybersecurity (15m)
  Strategies to stay current with evolving threats and technologies.
- Q&A Session: Common Exam Questions Answered (20m)
  Real student questions addressed with detailed explanations.
- Final Mock Exam and Debrief (35m)
  Full-length practice test followed by a problem-solving review session.
- Course Wrap-Up and Next Steps (6m)
  Summary of key takeaways and how to apply your knowledge on the job.