

Course Syllabus

CompTIA CySA+ (CS0-002) Course

Instructor Name: Andrew Ysasi

Instructor Website:

<https://www.linkedin.com/in/andre-wysasi/>

Instructor Contact: N/A

Course Creation Date: 12/04/2020

Course Description and Goals

Course Description: The CompTIA Cybersecurity Analyst (CySA+ CS0-002) is an intermediate cybersecurity analyst certification. The CySA+ prepares professionals to identify and combat malware, advanced persistent threats (APTs) and many other attacks that plague an organization's security. In this course, students will learn about the five major learning domains in the CompTIA CySA+ which include threat and vulnerability management, software and systems security, security operations and monitoring, incident response and compliance and assessment. This course will prepare students to sit for the exam as well as give them an understanding of the topics covered so that they can apply them in real world scenarios. This course pairs video lessons with practices tests and labs to ensure that the students will have the best chance of passing their exam.

Prerequisites: While there are no specific prerequisites for students to take this course or sit for the CompTIA CySA+ exam, it's recommended that students have knowledge of topics covered in the preceding CompTIA certifications such as A+, Network+ and Security+. Students will have the best chance of success if they follow the cybersecurity pathway set up by

Brought to you by:

CYBRARY | FOR BUSINESS

*Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.*

CYBRARY

CompTIA in which they have sat in for these prior exams before taking the CySA+. In addition, students should have computer skills as well as knowledge of computer networking.

Study Resources: In addition to the video lessons, labs will be available through the Cybrary lab platform along with step-by-step guides for each lab. There will be practice tests/quizzes available. Also, the *CompTIA CySA+ Study Guide Exam CS0-002 2nd Edition* (ISBN: 978-1-119-68405-3) by Sybex was used to help build content for this course.

Course Goals: By the end of this course, students should be able to:

- ☐ A Understand threat management and how to apply threat management techniques
- ☐ B Understand vulnerability management and how to apply vulnerability management techniques
- ☐ C Understand the process of cyber incident response
- ☐ D Recognize security architecture and tools sets
- ☐ E Determine which tools and technologies should be used given a specific scenario

Brought to you by:

CYBRARY | FOR BUSINESS

Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.

Course Outline

Module 1 | Course Introduction

Lesson 1.1: Course Introduction

Module 2 | Threat and Vulnerability Management

Lesson 2.1: Reconnaissance and Intelligence Gathering

Lesson 2.2: Threat Classification

Lesson 2.3: Threat Actors

Lesson 2.4: Attack Frameworks

Lesson 2.5: Common Vulnerability Scoring System (CVSS)

Lesson 2.6: Identify Threats

Lesson 2.7: Vulnerability Identification and Validation

Lesson 2.8: Vulnerability Remediation and Mitigation

Lesson 2.9: Vulnerability Assessment Tools

Lesson 2.10: Software Assessment Techniques

Lesson 2.11: Vulnerabilities Associated with Specialized Technology

Lesson 2.12: Cloud Security

Lesson 2.13: Common Attack Types

Lesson 2.14: Malicious Software

Module 3 | Software and Systems Security

Lesson 3.1: Security Solutions for Infrastructure Management

Lesson 3.2: Identity and Access Management (IAM)

Lesson 3.3: Software Assurance Best Practices

Lesson 3.4: Hardware Assurance Best Practices

Brought to you by:

CYBRARY | FOR BUSINESS

Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.

Module 4 | Security Operations and Monitoring

Lesson 4.1: Endpoint Security Operations and Monitoring

Lesson 4.2: Logging

Lesson 4.3: Email Analysis

Lesson 4.4: Improving Security Controls

Module 5 | Incident Response

Lesson 5.1: Understanding Incident Response

Lesson 5.2: Phases of Incident Response

Lesson 5.3: Eradication and Recovery

Lesson 5.4: Post-incident Activities

Lesson 5.5: Network-Related Attack Indicators

Lesson 5.6: Host-Related Attack Indicators

Lesson 5.7: Software-related Attack Indicators

Module 6 | Compliance and Assessment

Lesson 6.1: Understanding Data Privacy vs Security

Lesson 6.2: Non-technical Data Privacy Controls

Lesson 6.3: Technical Data Privacy Controls

Lesson 6.4: Risk Management

Lesson 6.5: Frameworks

Lesson 6.6: Policies

Lesson 6.7: Procedures

Lesson 6.8: Controls

Module 7 | Course Wrap-Up

Lesson 7.1: Course Wrap-Up

Brought to you by:

CYBRARY | FOR BUSINESS

*Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.*