CompTIA CySA+ (Exam CS0-003), Videos & Skill Labs Set

Course Specifications

Course Number: ACI77-006VL_rev1.0
Video and Lab Length: Approximately 27 hours, 11 minutes

Course Introduction

The CompTIA CySA+ is an industry recognized certification that aims to validate the skills and knowledge of cybersecurity analysts. This course is meant to help you prepare for the exam and covers a wide range of topics, including threat intelligence, vulnerability management, and incident response. Other topics covered includes: - Analyzing security logs and events - Identifying and responding to security incidents - Managing security vulnerabilities - Communicating security findings The skills validated by the CySA+ certification makes it a valuable asset for anyone looking to advance their career in cybersecurity.

Video Enhanced Learning

(15h 11m * 4 Modules * 58 Episodes)

We've enhanced select lab sets with targeted video content to strengthen student readiness and improve lab success. With focused video learning, students get reinforcement of core concepts before they enter the lab, giving them the confidence and context needed to apply skills effectively. Support diverse learning styles, improve lab readiness, and drive stronger outcomes across today's most in-demand skills.

Video Topics

1. Course Overview
2. Common Log Ingestion Concepts
3. Common Operating System Concepts
4. Common Infrastructure Concepts
5. Common IAM Concepts
6. Common Encryption Concepts
7. Protecting Sensitive Data
8. Common Network Architecture
9. Malicious Network Activity
10. Malicious Host Activity

11. Malicious Application Activity
12. Other Malicious Activity
13. Packet Capture Tools
14. Log Analysis Tools
15. Endpoint Detection and Response
16. DNS and IP Reputation Tools
17. File Analysis Tools
18. Sandboxing Tools
19. Email Analysis Tools
20. User and Entity Behavior Analytics
21. Scripting and Programming
22. Threat Actor Types
23. TTPs
24. CTI Confidence Levels
25. CTI Sources
26. CTI Sharing
27. Threat Hunting
28. Process Standardization
29. Streamlining Operations
30. Integrating Tools and Technology Into Security Operations
31. Asset Discovery and Mapping
32. Vulnerability Scanning Types and Considerations
33. Vulnerability Scanning Frameworks
34. Analyze Vulnerability Assessment Scanner Output
35. CVSS
36. Vulnerability Prioritization
37. Software Vulnerability Mitigations
38. SDLC
39. Threat Modeling
40. Compensating Controls
41. System Maintenance Procedures
42. Risk Management Principles
43. Policies, Governance, and SLOs
44. Prioritization and Escalation

45. Attack Surface Management
46. Secure Coding Best Practices
47. Attack Methodology Frameworks
48. Detection and Analysis
49. Containment, Eradication, and Recovery
50. Preparation Phase
51. Post-Incident Activity
52. Communicate Vulnerability Management Reporting
53. Communicate Incident Response Metrics and KPIs
54. Communicate Compliance Reporting
55. Communicate Inhibitors to Remediation
56. Communicate Incident Response Reports
57. Communicate Root Cause Analysis
58. Communicate Vulnerability Metrics and KPIs

Skill Labs

(12h * 12 Labs)

A **skills lab** is a guided, hands-on learning environment that allows students to practice real-world tasks in a safe, virtual setting. Instead of simply reading or watching videos, learners actively do the work—navigating realistic scenarios, applying concepts, troubleshooting issues, and building confidence through practical experience. This ensures that theory becomes usable skill. Skill labs are essential for developing true workplace readiness because they mirror real systems, tools, and challenges, helping learners bridge the gap between knowledge and performance. By completing a skills lab, students gain the hands-on competence employers expect and are better prepared for both assessments and real job responsibilities.

Skill Labs Topics

1. System & Network Security Implementation Concepts (CS0-003)
2. Threat Intelligence & Threat Gathering Concepts (CS0-003)
3. Techniques to Determine Malicious Activity (CS0-003)
4. Vulnerability Scanning Tools & Techniques (CS0-003)
5. Identifying & Analyzing Malicious Activity (CS0-003)
6. Tools for Identifying Malicious Activity (CS0-003)
7. Attack Methodology Frameworks (CS0-003)
8. Vulnerability Data Analysis and Prioritization (CS0-003)

9. Incident Response Management Techniques (CS0-003)
10. Incident Response Communication & Reporting (CS0-003)
11. Vulnerability Reporting Concepts (CS0-003)
12. Vulnerability Patching & Attack Surface Management (CS0-003)