CO-CYSA

COMPTIA CYBERSECURITY ANALYST

DURATION	LEVEL	TECHNOLOGY	DELIVERY METHOD	TRAINING CREDITS
5 Days	Intermediate	Cybersecurity	Instructor Led	NA

INTRODUCTION

The CompTIA Cybersecurity Analyst (CySA+) course is an international, vendor-neutral cybersecurity certification that applies behavioural analytics to improve the overall state of IT security. The CySA+ course validates knowledge and skills that are required to prevent, detect and combat cybersecurity threats.

CompTIA CySA+ proves candidates can detect and analyze indicators of malicious activity using the most up-to-date methods and tools, such as threat intelligence, security information and event management (SIEM), endpoint detection and response (EDR) and extended detection and response (XDR). IT pros gain unique skills sought after by organizations to protect and detect their networks.

AUDIENCE PROFILE

This course is designed primarily 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 defence 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, from help desk staff to the Chief Information Officer, understand their role in these security processes.

PREREQUISITES

To get the most out of the CompTIA CySA+ Study Guide and be able to prepare for your exam you should have successfully earned the CompTIA Network+ certification and CompTIA Security+ certification or have equivalent knowledge. Specifically, it is recommended that you have the following skills and knowledge before starting this course:

- Know basic network terminology and functions (such as OSI Model, Topology, Ethernet, Wi-Fi, switches, routers).
- Understand TCP/IP addressing, core protocols, and troubleshooting tools
- Identify network attack strategies and defences.
- Know the technologies and uses of cryptographic standards and products
- Identify network- and host-based security technologies and practices.
- Describe the standards and products used to enforce security on web and communications technologies.

COURSE OBJECTIVES

CompTIA CySA+ will teach you the fundamental principles of using threat and vulnerability analysis tools plus digital forensics tools. It will prepare you to take the CompTIA CySA+ CS0-003 exam by providing 100% coverage of the objectives and content examples listed on the syllabus.

- Security Operations
- Vulnerability Management
- Incident Response and Management
- Reporting and Communication

COURSE CONTENT

Lesson 1: Understanding Vulnerability Response, Handling, and Management

- Understanding Cybersecurity Leadership Concepts
- Exploring Control Types and Methods
- Explaining Patch Management Concepts

Lesson 2: Exploring Threat Intelligence and Threat Hunting Concepts

- Exploring Threat Actor Concepts
- Identifying Active Threats
- Exploring Threat-Hunting Concepts

Lesson 3: Explaining Important System and Network Architecture Concepts

- Reviewing System and Network Architecture Concepts
- Exploring Identity and Access Management (IAM)
- Maintaining Operational Visibility

Lesson 4: Understanding Process Improvement in Security Operations

- Exploring Leadership in Security Operations
- Understanding Technology for Security Operations

Lesson 5: Implementing Vulnerability Scanning Methods

- Explaining Compliance Requirements
- Understanding Vulnerability Scanning Methods
- Exploring Special Considerations in Vulnerability Scanning

Lesson 6: Performing Vulnerability Analysis

Understanding Vulnerability Scoring Concepts

Exploring Vulnerability Context Considerations

Lesson 7: Communicating Vulnerability Information

- Explaining Effective Communication Concepts
- Understanding Vulnerability Reporting Outcomes and Action Plans

Lesson 8: Explaining Incident Response Activities

- Exploring Incident Response Planning
- Performing Incident Response Activities

Lesson 9: Demonstrating Incident Response Communication

- Understanding Incident Response Communication
- Analyzing Incident Response Activities

SKILLS AND COMPETENCIES COVERED

Security Operations 33%

- Explain the importance of system and network architecture concepts in security operations.
- Analyze indicators of potentially malicious activity.
- Use appropriate tools or techniques to determine malicious activity.
- Compare and contrast threat-intelligence and threat-hunting concepts.
- Explain the importance of efficiency and process improvement in security operations.

Vulnerability Management 30%

- Implement vulnerability scanning methods and concepts.
- Analyze output from vulnerability assessment tools.
- Analyze data to prioritize vulnerabilities.
- Recommend controls to mitigate attacks and software vulnerabilities.
- Explain concepts related to vulnerability response, handling and management.

Incident Response Management 20%

- Explain concepts related to attack methodology frameworks.
- Perform incident response activities.
- Explain the preparation and post-incident activity phases of the incident management lifecycle.

Reporting and Communication 17%

- Explain the importance of vulnerability management reporting and communication.
- Explain the importance of incident response reporting and communication.

ASSOCIATED CERTIFICATIONS & EXAM

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

This course is designed to prepare students to take the CompTIA CS0-003 international examination. Successfully passing this exam will result in the achievement of the CompTIA Cybersecurity Analyst (CySA+) certification.