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.

In addition, this course covers the duties of those who are responsible for monitoring and detecting security incidents in information systems and networks, and for executing a proper response to such incidents. Depending on the size of the organization, this individual may act alone or may be a member of a cybersecurity incident response team (CSIRT).

The course introduces delegates to tools and tactics to manage cybersecurity risks, identify various types of common threats, evaluate the organization's security, collect and analyse cybersecurity intelligence, and handle incidents as they occur. Ultimately, the course promotes a comprehensive approach to security aimed towards those on the front lines of defence.

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+ CS0-002 exam by providing 100% coverage of the objectives and content examples listed on the syllabus. After completing the CompTIA CySA+ course, delegates will have the skills and knowledge to:

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

COURSE OUTLINE

COURSE CONTENT

Lesson 1: Explaining the Importance of Security Controls and Security Intelligence
- Identify Security Control Types
- Explain the Importance of Threat Data and Intelligence

Lesson 2: Utilizing Threat Data and Intelligence
- Classify Threats & Threat Actor Types
- Utilize Attack Frameworks & Indicator Management
- Utilize Threat Modelling & Hunting Methodologies

Lesson 3: Analysing Security Monitoring Data
- Analyse Network Monitoring Output
- Analyse Appliance Monitoring Output
- Analyse Endpoint Monitoring Output
- Analyse Email Monitoring Output

Lesson 4: Collecting and Querying Security Monitoring Data
- Configure Log Review and SIEM Tools
- Analyse and Query Logs and SIEM Data

Lesson 5: Utilizing Digital Forensics and Indicator Analysis Techniques
- Identify Digital Forensics Techniques
- Analyse Network-related IoCs
- Analyse Host-related IoCs
- Analyse Application-Related IoCs
- Analyse Lateral Movement and Pivot IoCs

Lesson 6: Applying Incident Response Procedures
- Explain Incident Response Processes
- Apply Detection and Containment Processes
- Apply Eradication, Recovery, and Post-Incident Processes

Lesson 7: Applying Risk Mitigation and Security Frameworks
- Apply Risk Identification, Calculation, and Prioritization Processes
- Explain Frameworks, Policies, and Procedures

Lesson 8: Performing Vulnerability Management
- Analyse Output from Enumeration Tools
- Configure Infrastructure Vulnerability Scanning Parameters
- Analyse Output from Infrastructure Vulnerability Scanners
- Mitigate Vulnerability Issues

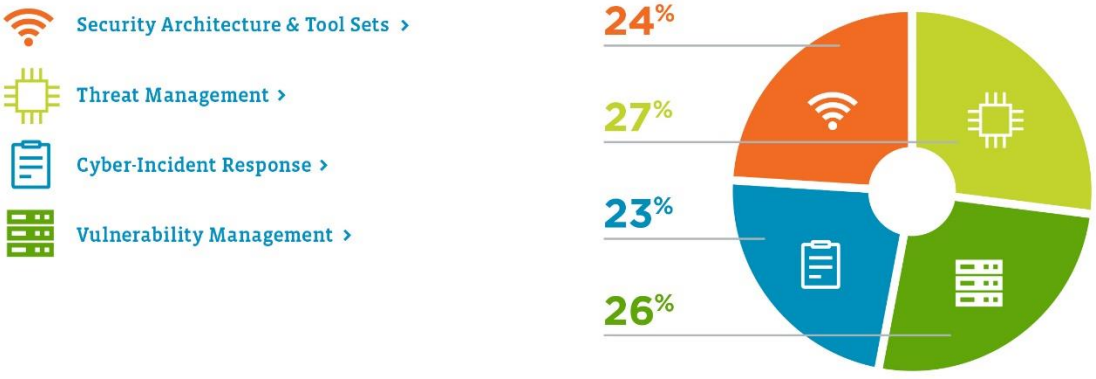
Lesson 9: Applying Security Solutions for Infrastructure Management
- Apply Identity and Access Management Security Solutions
- Apply Network Architecture and Segmentation Security Solutions
- Explain Hardware Assurance Best Practices
- Explain Vulnerabilities Associated with Specialized Technology

Lesson 10: Understanding Data Privacy and Protection
- Identify Non-Technical Data and Privacy Controls
- Identify Technical Data and Privacy Controls

Lesson 11: Applying Security Solutions for Software Assurance
- Mitigate Software Vulnerabilities and Attacks
- Mitigate Web Application Vulnerabilities and Attacks
- Analyse Output from Application Assessments

Lesson 12: Applying Security Solutions for Cloud and Automation
- Identify Cloud Service and Deployment Model Vulnerabilities
- Explain Service-Oriented Architecture
- Analyse Output from Cloud Infrastructure
- Compare Automation Concepts and Technologies

SKILLS AND COMPETENCIES COVERED



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 CS0-002 international examination. Successfully passing this exam will result in the achievement of the CompTIA Cybersecurity Analyst (CySA+) certification.