REAL WORLD
TECHNOLOGY TRAINING & SOLUTIONS
"Training You Can Really Use"

CompTIA Cybersecurity Analyst (CySA+)

Duration: 5 Days

Method: Instructor-Led Training (ILT) | Live Online Training

Certification: *CompTIA Cybersecurity Analyst (CySA+)*

Course Description

This course is an international, vendor-neutral cybersecurity certification that applies behavioural analytics to improve the overall state of IT security. The 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 participants 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.

Target Audience

This course is intended for:

- IT professionals with (or seeking) job roles such as
  - IT Security Analyst,
  - Security Operations Center (SOC) Analyst,
  - Vulnerability Analyst,
  - Cybersecurity Analyst/Specialist,
  - Threat Intelligence Analyst
  - Application Security Analyst
  - Compliance Analyst
  - Security Engineer.
- Professionals who wish to attain this intermediate-level certificate.

REAL WORLD
TECHNOLOGY TRAINING & SOLUTIONS
"Training You Can Really Use"

Prerequisites

To attend this course, candidates must have:

- Minimum of four (4) years of hands-on information security or related experience.
- Obtained the *Network*+ and *Security*+ certificates or have equivalent knowledge such as:
  - Knowledge of basic network terminology and functions (such as OSI Model, Topology, Ethernet, Wi-Fi, switches, routers)
  - Understanding of TCP/IP addressing, core protocols, and troubleshooting tools
  - Network attack strategies and defences.
  - Knowledge of the technologies and uses of cryptographic standards and products
  - Network- and host-based security technologies and practices.

Exam Details

Exam Code:	• CS0-003
Length of Exam:	• 165 mins
Number of Questions:	• 85
Passing Score:	• 750 out of 900
Question Format:	• Multiple Choice and Performance-Based

Course Objectives

Upon successful completion of this course, attendees will be able to:

- Collect and use cybersecurity intelligence and threat data.
- Identify modern cybersecurity threat actor types and tactics, techniques, and procedures.
- Analyse data collected from security and event logs and network packet captures.
- Respond to and investigate cybersecurity incidents using forensic analysis techniques.
- Assess information security risk in computing and network environments.
- Implement a vulnerability management program.
- Address security issues with an organization's network architecture.
- Understand the importance of data governance controls.
- Address security issues with an organization's software development life cycle.
- Address security issues with an organization's use of cloud and service-oriented architecture.

REAL WORLD
TECHNOLOGY TRAINING & SOLUTIONS
"Training You Can Really Use"

Course Topics

Module 1: Explaining the Importance of Security Controls and Security Intelligence

- Identify Security Control Types
- Explain the Importance of Threat Data and Intelligence

Module 2: Utilizing Threat Data and Intelligence

- Classify Threats and Threat Actor Types
- Utilize Attack Frameworks and Indicator Management
- Utilize Threat Modelling and Hunting Methodologies

Module 3: Analysing Security Monitoring Data

- Analyse Network Monitoring Output
- Analyse Appliance Monitoring Output
- Analyse Endpoint Monitoring Output
- Analyse Email Monitoring Output

Module 4: Collecting and Querying Security Monitoring Data

- Configure Log Review and SIEM Tools
- Analyse and Query Logs and SIEM Data

Module 5: Utilizing Digital Forensics and Indicator Analysis Techniques

- Identify Digital Forensics Techniques
- Analyse Network-Related Indicators of Compromise (IOCs)
- Analyse Host-Related IOCs
- Analyse Application-Related IOCs
- Analyse Lateral Movement and Pivot IOCs

Module 6: Applying Incident Response Procedures

- Explain Incident Response Processes
- Apply Detection and Containment Processes
- Apply Eradication, Recovery, and Post-Incident Processes

Module 7: Applying Risk Mitigation and Security Frameworks

- Apply Risk Identification, Calculation, and Prioritization Processes
- Explain Frameworks, Policies, and Procedures

Course Topics *Continued*

Module 8: Performing Vulnerability Management

- Analyse Output from Enumeration Tools
- Configure Infrastructure Vulnerability Scanning Parameters
- Analyse Output from Infrastructure Vulnerability Scanners
- Mitigate Vulnerability Issues

Module 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

Module 10: Understanding Data Privacy and Protection

- Identify Non-Technical Data and Privacy Controls
- Identify Technical Data and Privacy Controls

Module 11: Applying Security Solutions for Software Assurance

- Mitigate Software Vulnerabilities and Attacks
- Mitigate Web Application Vulnerabilities and Attacks
- Analyse Output from Application Assessments

Module 12: Applying Security Solutions for Cloud and Automation

- Identify Cloud Service and Deployment Model Vulnerabilities
- Explain Service-Oriented Architecture
- Analyse Output from Cloud Infrastructure Assessment Tools
- Compare Automation Concepts and Technologies

LABS INCLUDED