AVWSQ-CySA+

WSQ - CompTIA Cybersecurity Analyst (CySA+)

5 Days Course • Instructor-Led Training (English)

About The Course

This course covers the duties of cybersecurity analysts who are responsible for monitoring and detecting security incidents in information systems and networks, and for executing a proper response to such incidents. The course introduces 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.

Audience Profile

The course more generally supports candidates working in or moving into job roles such as security operations centre (SOC) analyst, vulnerability analyst, cybersecurity specialist, threat intelligence analyst, security engineer, and cybersecurity analyst.

Course Outcome

- Collect and use cybersecurity intelligence and threat data
- Identify modern cybersecurity threat actors 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

Pre-Requisites

- The ability to recognize information security vulnerabilities and threats in the context of risk management
- Foundational knowledge of the concepts and operational framework of common assurance safeguards in computing environments. Safeguards include authentication and authorization, resource permissions, and antimalware mechanisms
- Foundational knowledge of the concepts and operational framework of common assurance safeguards in network environments, such as firewalls, IPS, NAC, and VPNs.

Course Outline

12 Lessons

Lesson 01 - Explaining the Importance of Security Controls and Security Intelligence

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

Lesson 02: Utilizing Threat Data and Intelligence

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

Lesson 03: Analyzing Security Monitoring Data

- Analyze Network Monitoring Output
- Analyze Appliance Monitoring Output
- Analyze Endpoint Monitoring Output
- Analyze Email Monitoring Output

Lesson 04: Configuring and Managing Virtual Networks

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

Lesson 05: Collecting and Querying Security Monitoring Data

- Identify Digital Forensics Techniques
- Analyze Network-related IoCs
- Analyze Host-related IoCs
- Analyze Application-related IoCs
- Analyze Lateral Movement and Pivot IoCs

Lesson 06: Applying Incident Response Procedures

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

Lesson 07: Applying Risk Mitigation and Security Frameworks

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

Lesson 08: Performing Vulnerability Management

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

Lesson 09: 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
- Analyze Output from Application Assessments

Lesson 12: Applying Security Solutions for Cloud and Automation

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