MYCOMPUTER CAREER
TRAINING FOR A BETTER LIFE

CyberSecurity Analyst Syllabus
CompTIA CySA+ (CSO-002)

Course Description

CyberSecurity Analyst: In this course, students will learn the skills to develop a comprehensive approach to executing the duties of cybersecurity analysts who are responsible for monitoring and detecting security incidents in information systems and networks and executing a proper response to such incidents. Students will obtain knowledge of the tools and tactics to manage cybersecurity risks, identify common threats, evaluate an organization's security, collect and analyze cybersecurity intelligence, and handle incident responses.

The class will begin at 8:00 A.M. EST each instructional day on Saturdays and conclude at 6:00 P.M. EST each session. The course consists of a total of 40 hours.

Saturday 1

Morning Session: Security Controls, Intelligence, & Network Monitoring Output

- Topics
  - Lesson 1: Explaining the Importance of Security Controls and Security Intelligence
  - Lesson 2: Utilizing Threat Data and Intelligence
  - Lesson 3A: Analyze Network Monitoring Output
- Activities and Demonstrations
  - Frameworks, Controls, Policies and Procedures (Skillsoft Lab)
  - Threat Data (Skillsoft Demo Lab)
- End of Class Review

Afternoon Session: Analyzing Security Monitoring Data

- Topics
  - Lesson 3B: Analyze Appliance Monitoring Output
  - Lesson 3C: Analyze Endpoint Monitoring Output
  - Lesson 3D: Analyze E-mail Monitoring Output
- Activities and Demonstrations
  - Log Monitoring and Review (Skillsoft Demo Lab)
  - Security Monitoring Activities (Skillsoft Lab)
- End of Class Review

Saturday 2

Morning Session: Collecting & Querying Security Data and Digital Forensics

- Topics
  - Lesson 4A: Configure Log Review and SIEM Tools

    - Lesson 4B: Analyze and Query Logs and SIEM Data
    - Lesson 5A: Identify Digital Forensics Techniques
    - Lesson 5B: Analyze Network-related IoCs
- Activities and Demonstrations
    - Digital Forensics Techniques (Skillsoft Lab)
    - Scripting (Skillsoft Demo Lab)
- End of Class Review

Afternoon Session: Digital Forensics & Incident Response Procedures

- Topics
    - Lesson 5C: Analyze Host-related IoCs
    - Lesson 5D: Analyze Application-related IoCs
    - Lesson 5E: Analyze Lateral Movement and Pivot IoCs
    - Lesson 6A: Explain Incident Response Processes
    - Lesson 6B: Apply Detection and Containment Processes
- Activities and Demonstrations
    - Importance of Incident Response (Skillsoft Demo Lab)
    - Initial Phases of Incident Response (Skillsoft Lab)
- End of Class Review

Saturday 3

Morning Session: Incident Response Procedures, Applying Risk Mitigation and Security Frameworks & Vulnerability Management

- Topics
    - Lesson 6C: Apply Eradication, Recovery, and Post-incident Processes
    - Lesson 7A: Apply Risk Identification, Calculation, and Prioritization Processes
    - Lesson 7B: Explain Frameworks, Policies, and Procedures
    - Lesson 8A: Analyze Output from Enumeration Tools
- Activities and Demonstrations
    - Later Phases of Incident Response (Skillsoft Lab)
    - Enumeration (Skillsoft Demo Lab)
- End of Class Review

Afternoon Session: Vulnerability Management & Infrastructure Security Management

- Topics
    - Lesson 8C: Analyze Output from Infrastructure Vulnerability Scanners
    - Lesson 8D: Mitigate Vulnerability Issues
    - Lesson 9A: Apply Identity and Access Management Security Solutions
    - Lesson 9B: Apply Network Architecture and Segmentation Security Solutions

    - Lesson 9C: Explain Hardware Assurance Best Practices
- Activities and Demonstrations
    - Infrastructure Vulnerability Scanners (Skillsoft Lab)
    - Vulnerability Identification and Remediation (Skillsoft Demo Lab)
- End of Class Review

Saturday 4

Morning Session: Data Privacy and Protection & Security Solutions for Software Assurance

- Topics
    - Lesson 9D: Explain Vulnerabilities Associated with Specialized Technology
    - Lesson 10A: Identify Non-technical Data and Privacy Controls
    - Lesson 10B: Identify Technical Data and Privacy Controls
    - Lesson 11A: Mitigate Software Vulnerabilities and Attacks
    - Lesson 11B: Mitigate Web Application Vulnerabilities and Attacks
    - Lesson 11C: Analyze Output from Application Assessments
- Activities and Demonstrations
    - Vulnerabilities in Specialized Technology (Skillsoft Demo Lab)
    - Vulnerabilities (Skillsoft Lab)
- End of Class Review

Afternoon Session: Security Solutions for Cloud and Automation & Course Review

- Topic
    - Lesson 12A: Identify Cloud Service and Deployment Model Vulnerabilities
    - Lesson 12B: Explain Service-oriented Architecture
    - Lesson 12C: Analyze Output from Cloud Infrastructure Assessment Tools
    - Lesson 12D: Compare Automation Concepts and Technologies
- Activities and Demonstrations
    - Automation Concepts (Skillsoft Lab)
    - Infrastructure Solutions (Skillsoft Lab)
- End of Course Review
        - Student-focused Q&A for Understanding
