CompTIA CySA+ Course Outline

EXAM NUMBER: CS0-003

Security Operations

- Explain the importance of system and network architecture concepts in security operations.
- Given a scenario, analyze indicators of potentially malicious activity.
- Given a scenario, 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

- Given a scenario, implement vulnerability scanning methods and concepts.
- Given a scenario, analyze output from vulnerability assessment tools.
- Given a scenario, analyze data to prioritize vulnerabilities.
- Given a scenario, recommend controls to mitigate attacks and software vulnerabilities.
- Explain concepts related to vulnerability response, handling, and management.

Incident Response and Management

- Explain concepts related to attack methodology frameworks.
- Given a scenario, perform incident response activities.
- Explain the preparation and post-incident activity phases of the incident management life cycle.

Reporting and Communication

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