CompTIA

CySA +

Objectives

1.0 Threat and Vulnerability Management.

- 1.1 Explain the importance of threat data and intelligence.
- 1.2 Given a scenario, utilize threat intelligence to support organizational security.
- 1.3 Given a scenario, perform vulnerability management activities.
- 1.4 Given a scenario, analyze the output from common vulnerability assessment tools.
- 1.5 Explain the threats and vulnerabilities associated with specialized technology.
- 1.6 Explain the threats and vulnerabilities associated with operating in the cloud.
- 1.7 Given a scenario, implement controls to mitigate attacks and software vulnerabilities.

2.0 Software and Systems Security.

- 2.1 Given a scenario, apply security solutions for infrastructure management.
- 2.2 Explain software assurance best practices.
- 2.3 Explain hardware assurance best practices

3.0 Security Operations and monitoring.

- 3.1 Given a scenario, analyze data as part of security monitoring activities.
- 3.2 Given a scenario, implement configuration changes to existing controls to improve security.
- 3.3 Explain the importance of proactive threat hunting.
- 3.4 Compare and contrast automation concepts and technologies.

4.0 Incident Response.

- 4.1 Explain the importance of the incident response pro
- 4.2 Given a scenario, apply the appropriate incident response procedure.
- 4.3 Given an incident, analyze potential indicators of compromise.
- 4.4 Given a scenario, utilize basic digital forensics techniques.

5.0 Compliance and Assessment.

- 5.1 Understand the importance of data privacy and protection.
- 5.2 Given a scenario, apply security concepts in support of organizational risk mitigation.
- 5.3 Explain the importanceof frameworks, policies, procedures, and controls.