CompTIA CySA+ Course Outline

EXAM NUMBER: CS0-004

Security Operations (34%)

- **Explain system and network architecture concepts in security operations:** Security architecture components, identity concepts, and logging practices that support secure environments.
- **Analyze indicators of potential malicious activity:** Suspicious activity across networks, endpoints, cloud, and identity systems.
- **Use tools to determine malicious activity:** SIEM, EDR, packet analysis tools, and threat intelligence platforms.
- **Explain threat intelligence and threat-hunting concepts:** Frameworks, data sources, and methods used to identify and investigate threats.
- **Describe efficiency and process improvement in security operations:** Automation, workflows, and processes used to improve operational efficiency.
- **Summarize concepts related to the use of AI in security operations:** Use cases, risks, and governance considerations.

Vulnerability Management (26%)

- **Implement the appropriate vulnerability scanning method:** Tools and techniques used to identify vulnerabilities across systems, networks, and applications.
- **Analyze output from vulnerability assessment tools:** Vulnerabilities, findings, and security gaps identified through scan results.
- **Prioritize and mitigate vulnerabilities:** Risk-based approaches using scoring systems, threat intelligence, and business context.
- **Explain concepts related to control types, risks, and vulnerability management:** Controls, policies, and compliance practices used to manage risk.

Incident Response and Management (24%)

- **Summarize concepts related to attack methodology frameworks:** Models such as MITRE ATT&CK and the Cyber Kill Chain.
- **Outline the incident response process:** Phases including preparation, detection, analysis, containment, eradication, and recovery.
- **Implement incident response techniques:** Triage, evidence handling, escalation, remediation, and root cause identification.

Reporting and Communication (16%)

- **Explain vulnerability management reporting and communication:** Reports, dashboards, and communication activities used to present findings and support escalation during security events.

- **Describe security operations, incident response reporting, and communication:** Incident documentation, post-incident reviews, and metrics such as detection time, response time, and remediation effectiveness.

Describe security operations, incident response reporting, and communication: Incident documentation, post-incident reviews, and metrics such as detection time, response time, and remediation effectiveness.

•