

# CompTIA Cybersecurity Analyst (CySA+)

**Duration: 5 Days**

**Course Objectives:**

- Understand and perform incident response and vulnerability management processes.
- Detect and analyze indicators of malicious activity in support of security operations.
- Use appropriate tools, methods, and frameworks to prioritize and manage vulnerabilities and respond to incidents.
- Understand reporting and communication concepts related to vulnerability management and incident response activities.

**Course Outlines:**

**Security Operations**

**Explain concepts related to system and network architecture in security operations.**

- Logging concepts
- Operating system concepts
- Infrastructure/system architecture concepts
- Device management concepts
- Network architecture concepts
- Identity and access management (IAM)
- Encryption techniques
- Data protection concepts
- Critical infrastructure concepts

**Given a scenario, analyze indicators of potential malicious activity.**

- Network-related indicators
- Host-related indicators
- Unauthorized configuration
- Application-related indicators
- Cloud-related indicators
- Social engineering attacks
- Identity-based indicators
- Email-related attacks

**Given a scenario, use tools to determine malicious activity.**

- Tools
- File formats
- Programming/scripting languages

**Explain threat intelligence and threat-hunting concepts.**

- Threat actors
- Tactics, techniques, and procedures (TTPs)
- Confidence-level impacts
- Collection methods and sources
- Indicator of compromise (IoC)
- Threat modeling
- Threat mapping
- Cyber deception

**Explain the importance of efficiency and process improvement in security operations.**

- Standardize processes
- Streamline operations
- Technology and tool integration

**Summarize concepts related to the use of AI in security operations.**

- AI risks
- Governance
- Use cases

**Vulnerability Management**

- Asset inventory
- Given a scenario, implement the appropriate vulnerability scanning method.
- Planning considerations
- Scan types

**Given a scenario, analyze output from vulnerability assessment tools.**

- Network scanning and mapping
- Multipurpose tools
- Web application scanners
- Vulnerability scanners
- Cloud infrastructure assessment tools
- Breach attack simulation (BAS) tools

**Given a scenario, analyze data to prioritize and mitigate vulnerabilities.**

- Criteria
- Scoring methods
- Context awareness
- Mitigation strategies
- Validation of remediation

**Explain concepts related to control types, risks, and vulnerability management.**

- Control types
- Control functions
- Risk concepts
- Risk management strategies
- Policies, governance, and service-level objectives (SLOs)
- Application security
- Third-party risk

**Incident Response and Management**

**Summarize concepts related to attack methodology frameworks.**

- Cyber Kill Chain
- Diamond Model of Intrusion Analysis
- MITRE ATT&CK

**Summarize the incident response process.**

- Preparation
- Detection
- Analysis
- Containment
- Eradication
- Recovery
- Post-incident

**Given a scenario, implement incident response techniques.**

- Developing plans
- Creating playbooks
- Defining roles
- Performing training
- Log collection
- Log correlation
- Log augmentation and enrichment
- Alerts and notifications
- Triage
- Establishment of a timeline
- Determining severity and impact
- Prioritization
- Evidence gathering
- Isolating affected targets
- Escalation
- Remediation and verification
- Release from isolation
- Performing restoration
- Root cause analysis (RCA)
- Corrective action development

**Reporting and Communication**

**Explain the importance of vulnerability management reporting and communication.**

- Vulnerability scan reports
- Compliance findings
- Risk scorecards
- Action plans
- Inhibitors to remediation
- Stakeholder identification and communication
- Metrics and key performance indicators (KPIs)

**Explain the importance of security operations and incident response reporting and communication.**

- Incident declaration and escalation
- Executive summary
- Communication plan
- Operational security awareness
- Post-incident reporting
- Shift/incident handover
- Internal threat intelligence report
- Metrics and KPIs

**REGISTER NOW!**

training@trends.com.ph  
 (+632) 8863-2123  
 www.trendssacademy.com.ph