https://www.ituonline.com/

# CompTIA Cybersecurity Analyst (CySA+)

## Module 1: Threat Management

Introduction
Given a scenario, apply environmental reconnaissance techniques using appropriate tools and processes Part 1
Given a scenario, apply environmental reconnaissance techniques using appropriate tools and processes Part 2
Given a scenario, apply environmental reconnaissance techniques using appropriate tools and processes Part 3
Given a scenario, apply environmental reconnaissance techniques using appropriate tools and processes Part 4
Given a scenario, apply environmental reconnaissance techniques using appropriate tools and processes Part 5
Given a scenario, apply environmental reconnaissance techniques using appropriate tools and processes Part 6
Given a scenario, apply environmental reconnaissance techniques using appropriate tools and processes Part 7
Given a scenario, apply environmental reconnaissance techniques using appropriate tools and processes Part 8
Given a scenario, apply environmental reconnaissance techniques using appropriate tools and processes Part 9
Given a scenario, analyze the results of a network reconnaissance Part 1
Given a scenario, analyze the results of a network reconnaissance Part 2
Given a scenario, analyze the results of a network reconnaissance Part 3
Given a scenario, analyze the results of a network reconnaissance Part 4
Given a scenario, analyze the results of a network reconnaissance Part 5
Given a network-based threat, implement or recommend the appropriate response and countermeasure Part 1
Given a network-based threat, implement or recommend the appropriate response and countermeasure Part 2
Given a network-based threat, implement or recommend the appropriate response and countermeasure Part 3
Given a network-based threat, implement or recommend the appropriate response and countermeasure Part 4
Explain the purpose of practices used to secure a corporate environment Part 1
Explain the purpose of practices used to secure a corporate environment Part 2
Explain the purpose of practices used to secure a corporate environment Part 3
Explain the purpose of practices used to secure a corporate environment Part 4

## Module 2: Vulnerability Management

Given a scenario, implement an information security vulnerability management process Part 1
Given a scenario, implement an information security vulnerability management process Part 2
Given a scenario, implement an information security vulnerability management process Part 3
Given a scenario, implement an information security vulnerability management process Part 4
Given a scenario, implement an information security vulnerability management process Part 5
Given a scenario, implement an information security vulnerability management process Part 6
Given a scenario, implement an information security vulnerability management process Part 7
Given a scenario, analyze the output resulting from a vulnerability scan Part 1
Given a scenario, analyze the output resulting from a vulnerability scan Part 2
Compare and contrast common vulnerabilities found in the following targets within an organization Part 1
Compare and contrast common vulnerabilities found in the following targets within an organization Part 2
Compare and contrast common vulnerabilities found in the following targets within an organization Part 3

## Module 3: Cyber Incident Response

Given a scenario, distinguish threat data or behavior to determine the impact of an incident Part 1
Given a scenario, distinguish threat data or behavior to determine the impact of an incident Part 2
Given a scenario, distinguish threat data or behavior to determine the impact of an incident Part 3
Given a scenario, prepare a toolkit and use appropriate forensic tools during an investigation Part 1
Given a scenario, prepare a toolkit and use appropriate forensic tools during an investigation Part 2
Given a scenario, prepare a toolkit and use appropriate forensic tools during an investigation Part 3
Given a scenario, prepare a toolkit and use appropriate forensic tools during an investigation Part 4
Given a scenario, prepare a toolkit and use appropriate forensic tools during an investigation Part 5
Explain the importance of communications during the incident response process
Given a scenario, analyze common symptoms to select the best course of action to support incident response Part 1
Given a scenario, analyze common symptoms to select the best course of action to support incident response Part 2
Given a scenario, analyze common symptoms to select the best course of action to support incident response Part 3
Given a scenario, analyze common symptoms to select the best course of action to support incident response Part 4
Summarize the incident recovery and post-incident response process Part 1
Summarize the incident recovery and post-incident response process Part 2
Summarize the incident recovery and post-incident response process Part 3
Summarize the incident recovery and post-incident response process Part 4

## Module 4: Security Architecture and Tool Sets

Explain the relationship between frameworks, common policies, controls, and procedures Part 1
Explain the relationship between frameworks, common policies, controls, and procedures Part 2
Explain the relationship between frameworks, common policies, controls, and procedures Part 3
Explain the relationship between frameworks, common policies, controls, and procedures Part 4
Given a scenario, use data to recommend remediation of security issues related to identity and access management

Part 1
Given a scenario, use data to recommend remediation of security issues related to identity and access management

Part 2
Given a scenario, use data to recommend remediation of security issues related to identity and access management

Part 3
Given a scenario, use data to recommend remediation of security issues related to identity and access management

Part 4
Given a scenario, review security architecture and make recommendations to implement compensating controls Part

1
Given a scenario, review security architecture and make recommendations to implement compensating controls Part

2
Given a scenario, review security architecture and make recommendations to implement compensating controls Part

3
Given a scenario, use applications security best practices while participating in the Software Development Life Cycle

(SDLC) Part 1
Given a scenario, use applications security best practices while participating in the Software Development Life Cycle

(SDLC) Part 2
Overview

## Conclusion