COMPTIA CYBERSECURITY ANALYST / CySA+ (CSO-001)

Who Should Attend

The CompTIA CySA+ exam is an internationally targeted validation of intermediate-level security skills and knowledge. While there is no required prerequisite, the CompTIA CySA+ certification is intended to follow CompTIA Security+ or equivalent experience and has a technical, "hands-on" focus on IT security analytics.

It is recommended for CompTIA CySA+ certification candidates to have the following:

- 3-4 years of hands-on information security or related experience
- Network+, Security+ or equivalent knowledge

Course Objectives

As attackers have learned to evade traditional signature-based solutions such as firewalls, an analytics-based approach within the IT security industry is increasingly important for most organizations. The behavioral analytics skills covered by CySA+ identify and combat malware, and advanced persistent threats (APTs), resulting in enhanced threat visibility across a broad attack surface.

Upon successful completion of this course, students will be able to:

- Configure and use threat detection tools.
- Perform data analysis.
- Interpret the results to identify vulnerabilities, threats and risks to an organization

Course Outline

Threat Management

- Given a scenario, apply environmental reconnaissance techniques using appropriate tools and processes.
- Given a scenario, analyze the results of a network reconnaissance.
- Given a network-based threat, implement or recommend the appropriate response and countermeasure.
- Explain the purpose of practices used to secure a corporate environment.

Vulnerability Management

- Given a scenario, implement an information security vulnerability management process.
- Given a scenario, analyze the output resulting from a vulnerability scan.
- Compare and contrast common vulnerabilities found in the following targets within an organization.

Cyber Incident Response

- Given a scenario, distinguish threat data or behavior to determine the impact of an incident.
- Given a scenario, prepare a toolkit and use appropriate forensics tools during an investigation.
- Explain the importance of communication during the incident response process.
- Given a scenario, analyze common symptoms to select the best course of action to support incident response.
- Summarize the incident recovery and post-incident response process.

Security Architecture and Tool Sets

- Explain the relationship between frameworks, common policies, controls, and procedures.
- Given a scenario, use data to recommend remediation of security issues related to identity and access management.
- Given a scenario, review security architecture and make recommendations to implement compensating controls.
- Given a scenario, use application security best practices while participating in the Software Development Life Cycle (SDLC).
- Compare and contrast the general purpose and reasons for using various cybersecurity tools and technologies.