CompTIA Cybersecurity Analyst (CYSA+)

Duration: 5 days

Prerequisites: This course assumes that you have some applied knowledge of computers, networks, and cybersecurity principles. Knowledge equivalent to the CompTIA Security+ certification is helpful but not necessary. To ensure your success in this course, you should meet the following requirements:

- At least two years (recommended) of experience in computer network security technology or a related field.
- The ability to recognize information security vulnerabilities and threats in the context of risk management.
- Foundation-level operational skills with some of the common operating systems for computing environments.
- Foundational knowledge of the concepts and operational framework of common assurance safeguards in computing environments. Safeguards include, but are not limited to, basic authentication and authorization, resource permissions, and anti-malware mechanisms.
- Foundation-level understanding of some of the common concepts for network environments, such as routing and switching.
- Foundational knowledge of major TCP/IP networking protocols, including, but not limited to TCP, IP, UDP, DNS, HTTP, ARP, ICMP, and DHCP.
- Foundational knowledge of the concepts and operational framework of common assurance safeguards in network environments. Safeguards include, but are not limited to, firewalls, intrusion prevention systems, and VPNs.

Audience: This course is designed primarily for cybersecurity practitioners who perform job functions related to protecting information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This course focuses on the knowledge, ability, and skills necessary to provide for the defense of those information systems in a cybersecurity context, including protection, detection, analysis, investigation, and response processes. In addition, the course ensures that all members of an IT team—everyone from help desk staff to the Chief Information Officer—understand their role in these security processes.

Description: This course covers the duties of those who are responsible for monitoring and detecting security incidents in information systems and networks, and for executing a proper response to such incidents. Depending on the size of the organization, this individual may act alone or may be a member of a cybersecurity incident response team (CSIRT). The course introduces tools and tactics to manage cybersecurity risks, identify various types of common threats, evaluate the organization's security, collect and analyze cybersecurity intelligence, and handle incidents as they occur. Ultimately, the course promotes a comprehensive approach to security aimed toward those on the front lines of defense. This course is designed to prepare for the CompTIA® Cybersecurity Analyst+ (Exam CS0-002) certification examination. What you learn and practice in this course can be a significant part of your preparation. In addition, this course can help students who are looking to fulfill DoD directive 8570.01 for information assurance (IA) training. This program is designed for personnel performing IA functions, establishing IA policies, and implementing security measures and procedures for the Department of Defense and affiliated information systems and networks.

CompTIA Cybersecurity Analyst (CYSA+)

OUTLINE:

CHAPTER 1: UNDERSTANDING THREATS

Module A: Threats and vulnerabilities
Module B: Threat intelligence
Module C: Automation technologies

CHAPTER 2: POLICY DESIGN

Module A: Security policies
Module B: Controls and procedures

CHAPTER 3: VULNERABILITY MANAGEMENT

Module A: Risk management programs
Module B: Vulnerability assessment
Module C: Vulnerability management programs

CHAPTER 4: RECOGNIZING VULNERABILITIES

Module A: Attack strategies
Module B: System vulnerabilities
Module C: Application exploits

CHAPTER 5: NETWORK THREATS

Module A: Network vulnerabilities
Module B: Cloud vulnerabilities

CHAPTER 6: RECONNAISSANCE

Module A: Reconnaissance techniques
Module B: Active reconnaissance
Module C: Analyzing scan results

CHAPTER 7: NETWORK SECURITY SYSTEMS

Module A: Network security systems
Module B: Logging and monitoring

CHAPTER 8: NETWORK DEFENSE TECHNIQUES

Module A: Data analysis
Module B: Threat hunting

CHAPTER 9: SECURE INFRASTRUCTURE MANAGEMENT

Module A: Data protection
Module B: Hardening networks
Module C: Cryptographic security
Module D: Identity systems

CHAPTER 10: SECURE SYSTEM DESIGN

Module A: Hardware assurance
Module B: Hardening hosts and devices
Module C: Software assurance

CHAPTER 11: INCIDENT RESPONSE

Module A: Incident response planning
Module B: Incident response procedures
Module C: Forensic toolkits