CompTIA Cybersecurity Analyst

Duration 5 Days

COURSE OVERVIEW

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.

COURSE OBJECTIVES

In this course, you will assess and respond to security threats and operate a systems and network security analysis platform. You will:

- Assess information security risk in computing and network environments.
- Analyze the cybersecurity threat landscape. Analyze reconnaissance threats to computing and network environments.
- Analyze attacks on computing and network environments.
- Analyze post-attack techniques on computing and network environments.
- Implement a vulnerability management program.
- Evaluate the organization's security through penetration testing.
- Collect cybersecurity intelligence.
- Analyze data collected from security and event logs. Perform active analysis on assets and networks.
- Respond to cybersecurity incidents. Investigate cybersecurity incidents.
- Address security issues with the organization's technology architecture.

WHO SHOULD ATTEND

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.

PREREQUISITES

Network+, Security+ or equivalent knowledge. Minimum of 3-4 years of hands-on information security or related experience. While there is no required prerequisite, CySA+ is intended to follow CompTIA Security+ or equivalent experience and has a technical, hands-on focus.

COURSE OUTLINE

Assessing information security risk

- Identify the importance of risk management
- Assess risk
- Mitigate risk
- Integrate documentation into risk management

NETWORK TRAINING CENTER CO.,LTD. (NTC) | www.trainingcenter.co.th
Call us today 0-2634-7993-4
177/1 BUI Bldg., 14th Fl., Unit 1, 3 & 4, Surawongse Rd., Suriyawongse, Bangrak, Bangkok, THAILAND | Email: sales@trainingcenter.co.th

Analyzing the threat landscape
- Classify threats and threat profiles
- Perform ongoing threat research

Analyzing reconnaissance threats to computing and network environments
- Implement threat modeling
- Assess the impact of reconnaissance incidents
- Assess the impact of social engineering

Analyzing attacks on computing and network environments
- Assess the impact of system hacking attacks
- Assess the impact of web-based attacks
- Assess the impact of malware
- Assess the impact of hijacking and impersonation attacks
- Assess the impact of dos incidents
- Assess the impact of threats to mobile security
- Assess the impact of threats to cloud securty

Analyzing post-attack techniques
- Assess command and control techniques
- Assess persistence techniques
- Assess lateral movement and pivoting techniques
- Assess data exfiltration techniques
- Assess anti-forensics techniques

Managing vulnerabilities in the organization
- Implement a vulnerability management plan
- Assess common vulnerabilities
- Conduct vulnerability scans

Implementing penetration testing to evaluate security
- Conduct penetration tests on network assets
- Follow up on penetration testing

Collecting cybersecurity intelligence
- Deploy a security intelligence collection and analysis platform
- Collect data from network-based intelligence sources
- Collect data from host-based intelligence sources

Analyzing log data
- Use common tools to analyze logs
- Use siem tools for analysis
- Parse log files with regular expressions

Performing active asset and network analysis
- Analyze incidents with windows-based tools
- Analyze incidents with linux-based tools
- Analyze malware
- Analyze indicators of compromise

Responding to cybersecurity incidents
- Deploy an incident handling and response architecture
- Mitigate incidents
- Prepare for forensic investigation as a csirt

Investigating cybersecurity incidents
- Apply a forensic investigation plan
- Securely collect and analyze electronic evidence
- Follow up on the results of an investigation

Addressing security architecture issues
- Remediate identity and access management issues
- Implement security during the sdlc

NETWORK TRAINING CENTER CO.,LTD. (NTC) | www.trainingcenter.co.th
Call us today 0-2634-7993-4
177/1 BUI Bldg., 14th Fl., Unit 1, 3 & 4, Surawongse Rd., Suriyawongse, Bangrak, Bangkok, THAILAND | Email: sales@trainingcenter.co.th