Performing CyberOps Using Cisco Security Technologies (CBRCOR) v1.0

Duration 5 Days

COURSE DESCRIPTION

The Performing CyberOps Using Cisco Security Technologies (CBRCOR) v1.0 course guides you through cybersecurity operations fundamentals, methods, and automation. The knowledge you gain in this course will prepare you for the role of Information Security Analyst on a Security Operations Center (SOC) team. You will learn foundational concepts and their application in real-world scenarios, and how to leverage playbooks in formulating an Incident Response (IR). The course teaches you how to use automation for security using cloud platforms and a SecDevOps methodology. You will learn the techniques for detecting cyberattacks, analyzing threats, and making appropriate recommendations to improve cybersecurity.

This course also earns you 40 Continuing Education (CE) credits towards recertification and prepares you for the 350-201 CBRCOR core exam.

COURSE OUTLINE

- Understanding Risk Management and SOC Operations
- Understanding Analytical Processes and Playbooks
- Investigating Packet Captures, Logs, and Traffic Analysis
- Investigating Endpoint and Appliance Logs
- Understanding Cloud Service Model Security Responsibilities
- Understanding Enterprise Environment Assets
- Implementing Threat Tuning
- Threat Research and Threat Intelligence Practices
- Understanding APIs
- Understanding SOC Development and Deployment Models
- Performing Security Analytics and Reports in a SOC
- Malware Forensics Basics
- Threat Hunting Basics
- Performing Incident Investigation and Response

PREREQUISITES

Although there are no mandatory prerequisites, to fully benefit from this course, you should have the following knowledge:

- Familiarity with UNIX/Linux shells (bash, csh) and shell commands
- Familiarity with the Splunk search and navigation functions
- Basic understanding of scripting using one or more of Python, JavaScript, PHP or similar.

Recommended Cisco offerings that may help you prepare for this course:

- Understanding Cisco Cybersecurity Operations Fundamentals (CBROPS)
- Implementing and Administering Cisco Solutions (CCNA)

Recommended third-party resources:

- Splunk Fundamentals 1

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

- Blue Team Handbook: Incident Response Edition by Don Murdoch
- Threat Modeling- Designing for Security y Adam Shostack
- Red Team Field Manual by Ben Clark
- Blue Team Field Manual by Alan J White
- Purple Team Field Manual by Tim Bryant
- Applied Network Security and Monitoring by Chris Sanders and Jason Smith
-

WHO SHOULD ATTEND

Although there are no mandatory prerequisites, the course is particularly suited for the following audiences:

- Cybersecurity engineer
- Cybersecurity investigator
- Incident manager
- Incident responder
- Network engineer
- SOC analysts currently functioning at entry level with a minimum of 1 year of experience

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