CISCO CYBEROPS ASSOCIATE (CCNA CYBEROPS)

Our Learning Exclusive

- Custom exam prep software and materials
- Exam delivery in classroom with 98% success
- Course specific thinQtank® Learning publications to promote a fun exciting learning
- Extended hours of training including immersive hands-on exercises
- WE DO NOT "TEACH THE TEST" We always deliver valuable hands-on experience
- Receive all reading material and study guides when you register
- All courses taught by expert information security professionals

Course Duration

- Five days of instructor-led training + 1 day self-study
- 60% lecture, 40% demonstrations

Prerequisites

To ensure your success in this course, you should meet the following requirements:

- Familiarity with Ethernet and TCP/IP networking
- Working knowledge of the Windows and Linux operating systems
- Familiarity with basics of networking security concepts

Target Audience

- This course is designed for an associate-level cybersecurity analyst who is working in security operation centers.

Exam Information

- 200-201 – Cisco CBROPS Exam

Delivery Methods

- Instructor-Led Training
- Immersive Live-Online Training
- On-Site and Custom Delivery

Exclusive Learning Package

- Cisco-approved CBROPS training program
- After-course instructor coaching benefits
- Complete KALI Linux Build with VMWare
- Custom interactive study materials that assure success on the exam – FIRST ATTEMPT!
- **Exam voucher included and exam delivered in the classroom with a guaranteed pass.**

Course Overview

thinQtank® Learning is offering an industry-unique five-day training camp during which students can receive the Cisco Understanding Cisco Cybersecurity Operations Fundamentals (CBROPS) certification. As with our Cisco Training Experiences, exams are delivered in the classroom.

The Understanding Cisco Cybersecurity Operations Fundamentals course teaches an understanding of the network infrastructure devices, operations, and vulnerabilities of the Transmission Control Protocol/Internet Protocol (TCP/IP) protocol suite. You will learn basic information about security concepts, common network application operations and attacks, the Windows and Linux operating systems, and the types of data used to investigate security incidents. After completing this course, you will have the basic knowledge required to perform the job role of an associate-level cybersecurity analyst in a threat-centric security operations center to strengthen network protocol, protect your devices and increase operational efficiency. This course prepares you for the Cisco Certified CyberOps Associate certification.

Please note that this course is a combination of Instructor-Led and Self-Paced Study - 5 days in the classroom and approx. 1 day of self-study. The self-study content will be provided as part of the digital courseware that you will receive at the beginning of the course and should be part of your preparation for the exam.

Course Objectives

After completing this course, you should be able to:

- Explain how a SOC operates and describe the different types of services that are performed from a Tier 1 SOC analyst's perspective.
- Explain Network Security Monitoring (NSM) tools available.
- Explain the data that is available to the network security analyst.
- Describe the basic concepts and uses of cryptography.
- Describe security flaws in TCP/IP and how to attack networks.
- Understand common endpoint security technologies.
- Understand the kill chain and the diamond models.
- Identify resources for hunting cyber threats.
- Explain the need for event data normalization and event correlation.
- Identify the common attack vectors.
- Identify malicious activities.
- Identify patterns of suspicious behaviors and conduct investigations.
- Explain the use of a typical playbook in the SOC.
- Explain the use of SOC metrics to measure effectiveness of the SOC.
- Explain the use of a workflow management system and automation.
- Describe a typical incident response plan and functions of a CSIRT.

CISCO CYBEROPS ASSOCIATE (CCNA CYBEROPS)

Course Outline

O

- Outline: Understanding Cisco Cybersecurity Operations Fundamentals (CBROPS)
- Defining the Security Operations Center
- Understanding Network Infrastructure and Network Security Monitoring Tools
- Exploring Data Type Categories
- Understanding Basic Cryptography Concepts
- Understanding Common TCP/IP Attacks
- Understanding Endpoint Security Technologies
- Understanding Incident Analysis in a Threat-Centric SOC
- Identifying Resources for Hunting Cyber Threats
- Understanding Event Correlation and Normalization
- Identifying Common Attack Vectors
- Identifying Malicious Activity
- Identifying Patterns of Suspicious Behavior
- Conducting Security Incident Investigations
- Using a Playbook Model to Organize Security Monitoring
- Understanding SOC Metrics
- Understanding SOC Workflow and Automation
- Describing Incident Response
- Understanding the Use of VERIS
- Understanding Windows Operating System Basics
- Understanding Linux Operating System Basics

Labs Outline

L

- Configure the Initial Collaboration Lab Environment
- Use NSM Tools to Analyze Data Categories
- Explore Cryptographic Technologies
- Explore TCP/IP Attacks
- Explore Endpoint Security
- Investigate Hacker Methodology
- Hunt Malicious Traffic
- Correlate Event Logs, PCAPs, and Alerts of an Attack
- Investigate Browser-Based Attacks
- Analyze Suspicious DNS Activity
- Explore Security Data for Analysis
- Investigate Suspicious Activity Using Security Onion
- Investigate Advanced Persistent Threats
- Explore SOC Playbooks
- Explore the Windows Operating System
- Explore the Linux Operating System

CISCO CYBEROPS ASSOCIATE (CCNA CYBEROPS)

thinQtank® Global, Inc. dba thinQtank® Learning P.O. Box 803215, Valencia, CA 91380 USA
Tel 855-TO-THINQ Fax 208-979-0668 www.thinqtanklearning.com