Current Technologies
Computer Learning Centers

+1 (219) 764-3800
6210 Central Ave, Portage IN
sales@ctclc.com
www.ctclc.com

Cisco Partner
Platinum Learning

WHERE GREAT TRAINING HAPPENS EVERYDAY!

Understanding Cisco Cybersecurity Operations Fundamentals (CCNACBR)

Understanding Cisco Cybersecurity Operations Fundamentals (CCNACBR)

The Understanding Cisco Cybersecurity Operations Fundamentals training provides an understanding of the network infrastructure devices, operations, and vulnerabilities of the TCP/IP protocol suite, and basic information security concepts, common network application operations and attacks, the Windows and Linux operating systems, and the types of data that are used to investigate security incidents. After completing this training, 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 (SOC).

This training prepares you for the 200-201 CCNACBR v1.2 exam. If passed, you earn the Cisco Certified Network Associate (CCNA) Cybersecurity certification and the role of a junior or entry-level cybersecurity operations analyst in a SOC. This training also earns you 28 Continuing Education (CE) credits toward recertification

How you'll benefit

This class will help you:

- Gain fundamental skills and hands-on practice to prevent and defend against cyberattacks as part of a SOC team
- Acquire the basic knowledge required to perform as an associate-level cybersecurity analyst in a threat-centric SOC
- Understand key security concepts including operating systems, endpoint security, network monitoring, cryptography, and cloud security fundamentals
- Develop practical skills in threat detection, incident investigation, and using SOC playbooks and response plans through labs and simulations
- Prepare for the 200-201 CCNACBR v1.2 exam
- Earn 28 CE credits toward recertification

Course Duration

5 days

Course Price

$4,395.00 or 44 CLCs

Methods of Delivery

- Instructor Led
- Virtual ILT
- On-Site

Why Attend with Current Technologies CLC

- Our Instructors are in the top 10% rated by Cisco
- Our Lab has a dedicated 1 Gig Fiber Connection for our Labs
- Our Labs run up to Date Code for all our courses

Who Should Attend

The primary audience for this course is as follows:

- Associate-Level Cybersecurity Analysts

Prerequisites

There are no prerequisites for this training. However, the knowledge and skills you are recommended to have before attending this training are:

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

OUTLINE

Module 1: Security Operations

Module 2: Security Principles

Module 3: Access Control Models

Module 4: Cloud Security Models

Module 5: Cryptography for Security Operations

Module 6: Windows OS Basics

Module 7: Linux OS Basics

Module 8: CLIs in Security

Module 9: Network Protocols

Module 10: Network Security Controls

Module 11: IDS and IPS

Module 12: Endpoint Security

Module 13: Threat Actors

Module 14: Cyber Kill Chain Model

Module 15: MITRE Attack Framework

Module 16: Social Engineering Attacks

Module 17: Network Attack Fundamentals

Module 18: Advanced Threat Landscape

Module 19: Network Security Monitoring (NSM) Data

Module 20: Log Data Sources

Module 21: NetFlow for Security Monitoring

Module 22: Web Application Attacks

Module 23: Module 1: Advanced Log Analysis

Module 24: Packet Capture and Forensics

Module 25: Malware and Threat Intelligence

Module 26: Security Information and Event Management (SIEM)

Module 27: Security Orchestration, Automation, and Response (SOAR)

Module 28: Extended Detection and Response (XDR)

Module 29: Incident Response Planning

Module 30: CSIRT Roles and Operations

Module 31: Security Monitoring Playbooks

Module 32: Threat Hunting Methodologies

Lab Outline

Lab 1: Explore Cryptographic Technologies
Lab 2: Explore the Windows Operating System
Lab 3: Explore the Linux Operating System
Lab 4: Explore Endpoint Security
Lab 5: Investigate Hacker Methodology
Lab 6: Explore TCP/IP Attacks
Lab 7: Investigate Advanced Persistent Threats
Lab 8: Use NSM Tools to Analyze Data Categories
Lab 9: Analyze Suspicious DNS Activity
Lab 10: Investigate Browser-based Attacks
Lab 11: Correlate Event Logs, PCAPs, and Alerts of an Attack
Lab 12: Explore SOC Playbooks
Lab 13: Hunt Malicious Traffic