Current Technologies
Computer Learning Centers

cisco Partner
Platinum Learning

Understanding Cisco Cybersecurity Operations Fundamentals (CCNACBR)

WHERE GREAT TRAINING HAPPENS EVERYDAY!

Understanding Cisco Cybersecurity Operations Fundamentals (CCNACBR)

Course Duration
5 Days

Course Price
$4,395.00
44 CLCs

Methods of Delivery
In-Person ILT
Virtual ILT
Onsite ILT

About this Class

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

Understanding Cisco Cybersecurity Operations Fundamentals (CCNACBR)

Why Attend with Current Technologies CLC

- Our Instructors are 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 job roles best suited to the material in this course are:

- 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

How You'll Benefit

This training 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

Understanding Cisco Cybersecurity Operations Fundamentals (CCNACBR)

Objectives

After taking this course, you should be able to:

- Explain the foundational aspects of SOCs, including their types, key roles, and essential metrics for measuring effectiveness
- Apply foundational security principles and risk management concepts to assess and protect organizational assets
- Compare and apply various access control models to secure network resources and enforce organizational policies
- Differentiate between various cloud deployment and service models and explain the shared responsibility for security in cloud environments
- Explain the fundamental concepts of cryptography, differentiate between various cryptographic algorithms, and explain how cryptographic principles are applied in real-world protocols and systems, including key exchange, digital signatures, and SSL/TLS
- Identify and describe the fundamental components and operational aspects of the Windows operating system for security analysis
- Identify and describe the fundamental components and operational aspects of the Linux operating system for security analysis
- Utilize Command Line Interfaces (CLIs) for basic system interaction, file management, and security-related tasks in both Windows and Linux environments
- Explain the operations and identify the security implications of foundational network protocols
- Describe and differentiate various network security controls and their application in protecting network infrastructure
- Differentiate between various Intrusion Detection and Prevention Systems (IDS/IPS) and interpret their output for security monitoring
- Describe and compare various endpoint security solutions and their effectiveness against common threats

Understanding Cisco Cybersecurity Operations Fundamentals (CCNACBR)

Objectives

After taking this course, you should be able to:

- Identify and categorize various cyber threat actors based on their motivations, capabilities, and common tactics
- Explain the phases of the Classic Cyber Kill Chain model and identify adversary actions within each phase
- Apply the MITRE ATT&CK Framework to analyze and map cyber threats, explain its structure and application, and leverage it to enhance threat detection, incident response, and communication within a security operations environment
- Identify and describe various social engineering attack vectors, including those enhanced by generative AI
- Describe fundamental network attack techniques that exploit protocol vulnerabilities
- Describe advanced attack vectors and emerging threats in the current cybersecurity landscape
- Identify and explain various types of Network Security Monitoring (NSM) data and their role in incident investigation
- Identify and interpret various log data sources from operating systems, network devices, and security tools
- Explain NetFlow operations and its application as a security tool for network monitoring and anomaly detection
- Describe common web application attacks and their exploitation methods
- Apply advanced log analysis techniques to interpret security data and identify patterns of suspicious behavior

Understanding Cisco Cybersecurity Operations Fundamentals (CCNACBR)

Objectives

After taking this course, you should be able to:

- Perform packet capture analysis and apply digital forensics processes to investigate security incidents. Focus on the 5-tuple and timestamps to correlate with other logs, as this is your primary tool for network forensics
- Explain malware analysis outputs and apply threat intelligence frameworks for security investigations
- Explain the architecture, core functions, and best practices for implementing SIEM solutions for effective security monitoring
- Explain the features and common use cases of SOAR platforms for automating and streamlining incident response
- Explain the Cisco XDR platform, its core functions, features, and components for unified threat detection and response
- Differentiate between the legacy and modern NIST incident response guidance (NIST SP 800-61 Rev 2 and NIST SP 800-61 Rev 3 special publications), describe core IR components aligned with the NIST CSF 2.0 framework, and identify how these practices satisfy CMMC requirements for the Defense Industrial Base (DIB)
- Describe the roles, categories, and operational services of Computer Security Incident Response Teams (CSIRTs)
- Explain the concept of security monitoring playbooks and their components for standardizing incident response
- Apply various threat hunting methodologies to proactively identify and mitigate hidden threats within a network

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

Understanding Cisco Cybersecurity Operations Fundamentals (CCNACBR)

Course 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

Understanding Cisco Cybersecurity Operations Fundamentals (CCNACBR)

Course Outline

Module 23: 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