

Understanding Cisco Cybersecurity Operations Fundamentals (CCNACBR)

Description

The **Understanding Cisco Cybersecurity Operations Fundamentals (CCNACBR)** 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 30 Continuing Education (CE) credits toward recertification.

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 30 CE credits toward recertification

Who should enroll

- Associate-Level Cybersecurity Analysts

Technology areas

- Cybersecurity

Objectives

- 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
- 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 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
- 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
- Differentiate between various cloud deployment and service models and explain the shared responsibility for security in cloud environments
- Identify and describe various cloud security frameworks and their role in achieving compliance
- Identify and explain key regulatory compliance requirements relevant to cloud environments
- Apply Identity and Access Management (IAM) principles and best practices to secure cloud-based identities and access controls
- Explain the principles of DevSecOps and how security is integrated throughout the software development lifecycle
- 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
- Identify and describe common hacking tools and techniques used in offensive security operations

- 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
- 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
- Explain the benefits and challenges of integrating XDR, SIEM, and SOAR platforms for enhanced SOC efficiency
- Explain the role of AI and Machine Learning (ML) in security operations and identify their applications in threat detection
- 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

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

These skills can be found in the following Cisco Learning Offering:

- [Implementing and Administering Cisco Solutions \(CCNA\)](#)

Outline

- Security Operations
- Security Principles
- Access Control Models
- Windows OS Basics
- Linux OS Basics

-
- CLIs in Security
 - Cryptography for Security Operations
 - Network Protocols
 - Network Security Controls
 - IDS and IPS
 - Endpoint Security
 - Cloud Security Models
 - Cloud Security Frameworks
 - Cloud Regulatory Compliance
 - Identity and Access Management (IAM) in Cloud
 - Secure Development Lifecycle (DevSecOps)
 - Threat Actors
 - Cyber Kill Chain Model
 - MITRE Attack Framework
 - Social Engineering Attacks
 - Network Attack Fundamentals
 - Hacking Tools & Techniques
 - Advanced Threat Landscape
 - Network Security Monitoring (NSM) Data
 - Log Data Sources
 - NetFlow for Security Monitoring
 - Web Application Attacks
 - Advanced Log Analysis
 - Packet Capture & Forensics
 - Malware & Threat Intelligence
 - Security Information and Event Management (SIEM)
 - Security Orchestration, Automation, and Response (SOAR)
 - Extended Detection and Response (XDR)
 - Integrating Security Operations Platforms
 - AI & Machine Learning in Security Operations
 - Incident Response Planning
 - CSIRT Roles and Operations
 - Security Monitoring Playbooks
 - Threat Hunting Methodologies

Lab Outline

- Explore the Windows Operating System
- Explore the Linux Operating System
- Explore Cryptographic Technologies
- Explore Endpoint Security
- Investigate Hacker Methodology
- Explore TCP/IP Attacks
- Investigate Advanced Persistent Threats
- Use NSM Tools to Analyze Data Categories

-
- Explore Security Data for Analysis
 - Analyze Suspicious DNS Activity
 - Investigate Browser-based Attacks
 - Investigate Suspicious Activity Using Security Onion
 - Correlate Event Logs, PCAPs, and Alerts of an Attack
 - Cisco XDR to Splunk Enterprise Integration Simulation
 - Explore SOC Playbooks
 - Hunt Malicious Traffic

What to expect on the exam

Understanding Cisco Cybersecurity Operations Fundamentals (200-201 CCNACBR) v1.2 is a 120-minute exam associated with the CCNA Cybersecurity certification.

This exam demonstrates your readiness for a cybersecurity operations analyst role, covering:

- Security concepts
- Security monitoring
- Host-based analysis
- Network intrusion analysis
- Security policies and procedures

Links

- [Cisco U. Learning Path](#)
- [Cisco Learning Locator](#)