+33 (0)1 48 10 09 46
formation@ambient-it.net
140 Avenue Jean Lolive 93500 Pantin - France

Updated on 09/22/2026

Sign Up

Cisco CCNA Cybersecurity Certification Training

5 days (35 hours)

Overview

The Cisco CCNA Cybersecurity certification validates the skills needed to monitor systems, analyze threats, and participate in incident detection and response within a Security Operations Center (SOC).

This Cisco CCNA Cybersecurity training will help you develop the practical skills expected of a cybersecurity analyst. You'll learn to identify key threats, analyze Windows and Linux systems, and leverage network and endpoint data to detect signs of a compromise.

You will be able to analyze logs, NetFlow streams, network captures, and security alerts; correlate different telemetry sources; and use MITRE ATT&CK to understand the techniques employed by attackers.

The training also covers SIEM, SOAR, and XDR technologies, network intrusion analysis, threat hunting, and the development of SOC playbooks. You will learn how to triage alerts, reduce false positives, and reconstruct the timeline of an incident based on available data.

Upon completion of this training, you will be able to participate in a SOC investigation, lead the initial stages of an incident response, and apply the policies and procedures necessary for security operations. You will also have the knowledge needed to prepare for the CCNACBR 200-201 exam to earn the Cisco CCNA Cybersecurity certification.

Like all our training courses, this one will introduce you to **the latest stable version** of CyberOps Associate technology (1.2) and its new features.

Objectives

- Understand the fundamentals of cybersecurity and how a SOC operates
- Analyze systems, logs, network traffic, and events to identify signs of a compromise
- Master the principles of network security monitoring and intrusion analysis
- Use SIEM, SOAR, and XDR technologies to correlate events and facilitate investigations
- Implement the principles of incident response, threat hunting, and SOC playbooks
- Prepare for the CCNACBR 200-201 exam for the Cisco CCNA Cybersecurity certification

Target Audience

- Junior cybersecurity analysts
- Level 1/Level 2 SOC analysts
- Security technicians
- System and network administrators looking to transition into cybersecurity
- Professionals looking to develop skills in security operations

Prerequisites

- Basic knowledge of TCP/IP networks, ports, and common protocols
- General understanding of cybersecurity and major IT threats
- Basic knowledge of Windows and Linux systems is recommended
- No prior Cisco certifications are required

Note: Ambient IT does not own Cisco certifications. These certifications are the property of Cisco Systems, Inc.

Curriculum for our Cisco CCNA Cybersecurity (200-201 CCNACBR) Certification Training

[Day 1 - Morning]

Understanding the Fundamentals of Cybersecurity

- Understanding the concepts of threats, vulnerabilities, exploits, and risk
- Identifying the main threat actors and their motivations
- Understanding the principles of confidentiality, integrity, and availability in the CIA model
- Applying the principles of defense in depth and access control
- Understand the role of a cybersecurity analyst and the structure of a SOC
- Hands-on workshop: Analyze a compromise scenario and identify the associated threats, vulnerabilities, and security controls.

[Day 1 - Afternoon]

Analyzing Networks and Protocols for Cybersecurity

- Review the OSI and TCP/IP models, ports, and key network services
- Analyzing Ethernet, IP, TCP, and UDP protocols in a security context
- Understand how DNS, DHCP, HTTP/HTTPS, and SMTP work
- Identify the role of routing, VLANs, NAT, and network segmentation
- Understand the 5-tuple and its use in identifying and correlating network communications
- Hands-on workshop: Examine a network capture with Wireshark and identify protocols, traffic flows, and suspicious behavior.

Master cryptography and security controls

- Compare symmetric and asymmetric encryption and their main use cases
- Understand hash functions, digital signatures, and integrity mechanisms
- Understand how certificates, PKI, and TLS work
- Identify the role of firewalls, IDS/IPS, proxies, and endpoint protection solutions
- Understand authentication, authorization, and access control mechanisms
- Hands-on workshop: Analyze a TLS communication and interpret the information in a digital certificate.

[Day 2 - Morning]

Analyzing System and Endpoint Security

- Identify the main security components and mechanisms of Windows and Linux systems
- Analyze an endpoint’s processes, services, users, files, and network connections
- Understand logging mechanisms and events useful for investigations
- Identify signs of compromise and abnormal behavior on a system
- Understand the role of antivirus, EDR, and endpoint security solutions
- Hands-on workshop: Analyze events and processes on an endpoint to identify traces of a simulated compromise.

[Day 2 - Afternoon]

Understand threats and attacker behavior

- Identify the main categories of malware and their infection and persistence mechanisms
- Understanding phishing, social engineering, and attacks powered by generative AI
- Identify the characteristics of Advanced Persistent Threats (APTs)
- Use indicators of compromise: IP addresses, domains, URLs, hashes, and artifacts
- Map attacker behavior using MITRE ATT&CK and attack cycle models
- Hands-on workshop: Analyze an attack scenario and map the observed techniques using MITRE ATT&CK.

Collect and analyze security data

- Understanding the principles of Network Security Monitoring (NSM)
- Identify the main sources of telemetry: logs, events, alerts, network captures, and flows
- Understanding and analyzing NetFlow data to analyze communications
- Collect and interpret system, application, network, and security logs
- Understand data collection, normalization, enrichment, and retention in a SOC
- Hands-on workshop: leveraging multiple telemetry sources to identify abnormal network activity abnormal activity.

[Day 3 - Morning]

Analyze intrusions and network traffic

- Identifying the main TCP/IP attacks and their traces in network traffic
- Analyze suspicious behavior on DNS, HTTP/HTTPS, and other application protocols
- Understand how IDS/IPS alerts work and how to use them
- Interpret timestamps, sessions, and metadata from a network capture
- Use network forensics techniques to reconstruct malicious activity
- Hands-on workshop: Reconstruct the various stages of an intrusion using a PCAP capture.

[Day 3 - Afternoon]

Detecting Web Attacks and Malicious Activities

- Understand how web applications work and the main attack vectors
- Identify traces of attacks against HTTP, DNS, and browsers
- Recognize Command & Control (C2) communications and beaconing behavior
- Identify signs of data exfiltration, lateral movement, and privilege escalation
- Correlate network and endpoint data to characterize malicious activity
- Hands-on workshop: Analyze network and endpoint traces to identify the scenario of a web attack followed by a compromise.

Leveraging SIEM, SOAR, and XDR in a SOC

- Understand the architecture and role of a SIEM in security operations
- Create and interpret correlation rules and security alerts
- Understand the role of SOAR in orchestrating and automating responses
- Using Run Book Automation principles to standardize SOC operations
- Understand the role of an XDR platform and the positioning of Cisco XDR in investigations
- Hands-on workshop: Correlate multiple events in a SIEM and trigger an automated response scenario.

[Day 4 - Morning]

Correlating events and conducting an investigation

- Build an incident timeline using logs, PCAPs, alerts, and endpoint data
- Identify relationships between events and distinguish between cause, effect, and operational noise
- Assess an alert and determine its severity and potential impact
- Reduce false positives and improve the relevance of investigations
- Document the evidence, hypotheses, and conclusions of a SOC investigation
- Hands-on workshop: Correlate multiple data sources to reconstruct the complete timeline of an incident.

[Day 4 - Afternoon]

Manage incident response and CSIRT activities

- Understand the incident response lifecycle and the recommendations of NIST SP 800-61 Rev. 3
- Identify the roles and responsibilities of a CSIRT and the various stakeholders
- Implement the detection, analysis, containment, eradication, and recovery phases
- Preserve the evidence necessary for incident investigations and traceability
- Organize communication, escalation, and reporting during a security incident
- Hands-on workshop: Leading an incident response from alert qualification through the recovery plan.

Build and use SOC playbooks

- Understand the role of playbooks and runbooks in standardizing security operations
- Define the steps for qualification, investigation, escalation, and response based on the type of incident
- Identify the data sources and tools required for each procedure
- Define escalation criteria and the responsibilities of the various SOC levels
- Measuring the effectiveness of procedures and organizing their continuous improvement
- Hands-on workshop: Build a SOC playbook to address a compromise scenario and define the associated escalation actions.

[Day 5 - Morning]

Implement a threat hunting approach

- Understand the objectives and principles of threat hunting
- Develop a research hypothesis based on indicators, behaviors, or threat intelligence
- Leverage network, endpoint, and SIEM data to search for signs of compromise
- Use MITRE ATT&CK to guide and structure investigations
- Transform the results of a threat hunt into new detection rules and capabilities
- Hands-on Workshop: Conduct a threat hunting session based on a compromise hypothesis and document the results.

[Day 5 - Afternoon]

Apply security policies, procedures, and best practices

- Understand the role of policies, standards, procedures, and guidelines in cybersecurity operations
- Identify responsibilities related to governance, risk, and compliance
- Understand vulnerability management and the prioritization of remediation measures
- Apply the principles of the NIST Cybersecurity Framework to security operations
- Document incidents, investigations, and actions to improve SOC processes
- Hands-on workshop: Analyze an incident and develop security recommendations and related procedural updates.

Prepare for the Cisco CCNA Cybersecurity certification

- Review the five domains of the 200-201 CCNACBR v1.2 exam syllabus
- Review the concepts of Security Concepts, Security Monitoring, and Host-Based Analysis
- Review skills in Network Intrusion Analysis and Security Policies and Procedures
- Identify areas requiring further review before taking the exam
- Apply a time-management strategy tailored to the 120-minute exam
- Hands-on workshop: Take a CCNACBR practice exam, analyze the results, and develop a personalized study plan.

Target Audience

This training is intended for both individuals and companies—large or small—seeking to train their teams in new, advanced IT technologies or to acquire specific industry knowledge or modern methodologies.

Entry-Level Assessment

The pre-training assessment complies with Qualiopi quality standards. Upon final registration, the learner receives a self-assessment questionnaire that allows us to evaluate their estimated proficiency level across various types of technologies, as well as their expectations and personal goals for the upcoming training, within the limits imposed by the selected format. This questionnaire also allows us to anticipate certain connection or internal security issues within the company (intra-company or virtual classroom) that could pose challenges for monitoring and ensuring the smooth running of the training session.

Teaching Methods

Hands-On Training: 60% Practical, 40% Theoretical. Training materials distributed in digital format to all participants.

Organization

The course alternates between theoretical input from the instructor—supported by examples and reflection sessions—and group work.

Assessment

At the end of the session, a multiple-choice quiz is administered to verify that participants have successfully acquired

of the skills.

Certification

A certificate will be issued to each trainee who has completed the entire training program.