+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 CCNP Cybersecurity Certification Training

5 days (35 hours)

Overview

The Cisco CCNP Cybersecurity certification validates advanced skills in cybersecurity operations, threat analysis, threat hunting, and defense against attacks in complex environments.

Our Cisco CCNP Cybersecurity training course prepares you for the 350-201 CBRCOR and 300-220 CBRTHD exams in your chosen certification path. It will help you develop the skills needed to analyze risks, detect malicious activity, and conduct advanced investigations.

You will learn to leverage threat intelligence, model threats using MITRE ATT&CK, and identify the tactics, techniques, and procedures used by attackers. You will also be able to formulate threat hunting hypotheses and search for signs of compromise in network data, endpoints, applications, and cloud environments.

The training also covers incident response playbooks, advanced attack analysis, detection gaps, and the automation of security operations. You will learn how to transform the results of your investigations into new detection capabilities and appropriate remediation measures.

Upon completion of this training, you will be able to conduct an advanced SOC investigation, standardize your threat hunting processes, and improve your organization’s defense posture. You will also have the knowledge needed to prepare for the 350-201 CBRCOR and 300-220 CBRTHD exams, which lead to Cisco CCNP Cybersecurity certification in your chosen track.

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

Objectives

- Prepare for the 350-201 CBRCOR and 300-220 CBRTHD exams
- Master advanced cybersecurity operations and incident response processes
- Use threat intelligence and threat models to analyze adversarial behavior
- Conduct threat hunting campaigns on endpoints, networks, applications, and cloud environments
- Identify detection gaps and strengthen monitoring and defense capabilities
- Automate and standardize investigation, detection, and remediation processes

Target Audience

- Experienced SOC analysts
- Cybersecurity analysts
- Threat Hunters
- Security engineers
- Cybersecurity consultants
- Professionals preparing for the Cisco CCNP Cybersecurity certification

Prerequisites

- Strong grasp of the fundamentals of cybersecurity and TCP/IP networks
- Hands-on experience analyzing security logs, events, and alerts
- Knowledge of incident detection and response processes
- Knowledge of Windows and Linux systems and the main sources of security telemetry
- Basic knowledge of Python or PowerShell is recommended for automation and threat hunting
- Experience in a SOC or skills equivalent to the CCNA Cybersecurity certification are recommended

Technical prerequisites

- Laptop with at least 8 GB of RAM and administrator privileges
- Stable internet connection to access the labs and resources required for the training
- A modern web browser: Chrome, Firefox, or Edge
- An environment that allows you to use the network analysis tools, log analysis tools, and scripts required for the exercises
- SSH client and tools provided or specified by the instructor for the hands-on exercises

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

Curriculum for our Cisco CCNP Cybersecurity Certification Training

[Day 1 - Morning]

Mastering Cybersecurity Operations and Risk Management

- Understanding the exam topics for the 350-201 CBRCOR and 300-220 CBRTHD exams
- Analyzing the relationships between assets, vulnerabilities, threats, impacts, and risks
- Understand the roles and responsibilities of SOC teams and cybersecurity analysts
- Assess the security posture of a system or infrastructure and identify configuration discrepancies
- Understand the policies, standards, and risk management mechanisms applied to security operations
- Hands-on workshop: Analyze a compromise scenario and develop a risk assessment and associated security measures.

[Day 1 - Afternoon]

Develop playbooks and manage incident response

- Understanding the structure and components of a security playbook
- Apply the various steps of the incident response process
- Define the actions for qualification, containment, eradication, recovery, and escalation
- Implement the principles of hardening, segmentation, and reducing the attack surface
- Use incident response metrics to measure and improve operational effectiveness
- Hands-on workshop: Build and execute an incident response playbook, then define the necessary hardening actions.

[Day 2 - Morning]

Leverage threat intelligence and model threats

- Collect and analyze indicators of compromise from various sources
- Understand how a Threat Intelligence Platform (TIP) works and the intelligence lifecycle
- Interpret threat intelligence reports and identify tactics, techniques, and procedures
- Model threats using MITRE ATT&CK, MITRE CAPEC, TaHiTI, and PASTA
- Develop and prioritize threat hunting hypotheses based on available intelligence
- Hands-on workshop: Enrich indicators of compromise and then model an attack scenario using MITRE ATT&CK.

[Day 2 - Afternoon]

Analyze threat actors and attribute malicious activities

- Identify tactics, techniques, and procedures (TTPs) based on security data
- Analyze the characteristics of Advanced Persistent Threats and different categories of actors

- Distinguish between the behavior of a malicious actor and that of an authorized penetration tester
- Use the Pyramid of Pain to select artifacts useful for detection and investigation
- Correlate technical and contextual information to improve the attribution of suspicious activity
- Hands-on workshop: Analyze multiple compromise traces and determine the TTPs and of the actor involved.

[Day 3 - Morning]

Implement advanced threat hunting techniques

- Build a structured threat hunting approach based on a research hypothesis
- Use Python and PowerShell to enhance analysis and detection capabilities
- Search for undetected threats based on artifacts present on endpoints
- Identify Command & Control (C2) communications and suspicious network behavior
- Analyze logs, sessions, protocols, and network data to confirm or refute a hypothesis
- Hands-on workshop: Conduct a threat hunting campaign using endpoint and network data, then document the results.

[Day 3 - Afternoon]

Search for threats in the cloud, applications, and the IoT

- Conduct a threat hunting process in a cloud environment
- Identify the specific characteristics of cloud-native workloads and applications during investigations
- Analyze applications and code to identify exploitable behaviors or vulnerabilities
- Understand the methods used to analyze applications and systems on IoT devices
- Correlate cloud, application, endpoint, and network data to detect malicious activity
- Hands-on workshop: Searching for traces of malicious activity in a cloud environment and simulated application environment.

[Day 4 - Morning]

Analyze advanced attacks and enhance detection

- Understand the principles of in-memory attacks and identify actionable artifacts
- Interpret the results of specialized tools such as Volatility during an investigation
- Understand the principles of reverse engineering as applied to identifying a compromise
- Identify undetected threats, vulnerabilities, and configuration errors that cause detection gaps
- Build signatures and recommend new monitoring and detection capabilities

- Hands-on workshop: Analyze memory artifacts, identify indicators of an attack, and propose new detection rules.

[Day 4 - Afternoon]

Scaling and automating threat hunting operations

- Apply the Threat Hunting Maturity Model to assess and improve an organization’s capabilities
- Structuring the stages of collection, analysis, investigation, validation, and remediation in a hunting campaign
- Develop runbooks and playbooks to standardize SOC operations
- Automate the collection, enrichment, and qualification of security data
- Understand the uses of AI, machine learning, and SecDevOps in automating cybersecurity operations
- Hands-on workshop: Build an automated threat hunting workflow that integrates data enrichment, qualification, and human validation.

[Day 5 - Morning]

Conducting a SOC investigation and remediating threats

- Qualify an incident using logs, telemetry, endpoint data, and network traffic
- Build a timeline and identify the different stages of a compromise
- Identify TTPs, detection gaps, and elements useful for attributing the attack
- Define appropriate containment measures, countermeasures, and remediation actions
- Translate investigation findings into recommendations for detection and improving the defense posture
- Hands-on workshop: Conduct a comprehensive SOC investigation from initial detection through to the
creation of a prioritized remediation plan.

[Day 5 - Afternoon]

Prepare for the CBRCOR and CBRTHD exams

- Review the domains of the 350-201 CBRCOR v1.1 standard
- Review the domains of the 300-220 CBRTHD v1.0 standard
- Identify the differences between the Core competencies and the Threat Hunting and Defending specialization
- Review the methods, models, tools, and processes expected on both exams
- Develop a time-management strategy for the 120-minute and 90-minute exams
- Hands-on workshop: Take a practice exam covering CBRCOR and CBRTHD, 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 in 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 operation 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 instruction 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 the skills have been properly acquired.

Certification

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