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

Updated on 05/13/2026

Sign up

Cisco CCNP Cybersecurity Certification Training: Concentration

5 days (35 hours)

Overview

Cisco CCNP Cybersecurity: Concentration is an advanced certification that validates specialized expertise in network forensics, incident response, and cyber threat investigation through the 300-215 CBRFIR exam.

Our Cisco CCNP Cybersecurity: Concentration certification training will help you master the skills required for the 300-215 CBRFIR exam.

You will learn to analyze security incidents, analyze logs, identify indicators of compromise, conduct network investigations, and structure an effective incident response.

You will be able to assess an alert, collect evidence, interpret technical traces, reconstruct an attack timeline, and propose containment and remediation measures.

Through a hands-on approach focused on real-world cases, forensic analysis, log analysis, and practical workshops, this training will prepare you for the operational demands of SOC and Incident Response environments.

Upon completion of the course, you will be ready to take the 300-215 CBRFIR exam, which covers cybersecurity, forensics, and incident response.

Like all our courses, this one will introduce you to **the latest stable version** of the technology and its new features.

Objectives

- Prepare for the 300-215 CBRFIR exam.
- Master the fundamentals of network forensics.
- Analyze security incidents and indicators of compromise.
- Structure an incident response process.
- Analyze logs, network traces, and digital evidence.

Target Audience

- SOC analysts
- Cybersecurity engineers
- Network security administrators
- Incident response consultants
- Professionals preparing for the CCNP Cybersecurity Concentration certification

Prerequisites

- Solid knowledge of TCP/IP networks
- Basic understanding of operational cybersecurity
- Experience with security log and event analysis
- Basic knowledge of incident response and investigation

Technical requirements

- Laptop with at least 8 GB of RAM and administrator privileges.
- Stable internet connection to access Cisco labs and resources.
- Recent web browser: Chrome, Firefox, or Edge.
- SSH client and PDF reader installed.

Cisco CCNP Cybersecurity Certification Training Program: Concentration

[Day 1 - Morning]

Introduction to CCNP Cybersecurity Specializations

- Understanding the CCNP Cybersecurity track and concentration exams
- Identify the specializations: Firepower, ISE, VPN, SOC, Automation
- Analyzing the technical objectives of Cisco exams
- Positioning the skills required in SOC and network security environments
- Understanding advanced Cisco Security architectures
- Hands-on workshop: Mapping a Cisco Security architecture.

[Day 1 - Afternoon]

Zero Trust architecture and advanced segmentation

- Understanding Zero Trust principles
- Implementing Advanced Network Segmentation
- Controlling East-West and North-South Traffic
- Analyzing Risks Associated with Lateral Access
- Applying Microsegmentation Policies
- Hands-on Workshop: Creating a Zero Trust Policy.

Access security and identity control

- Understanding AAA and NAC mechanisms
- Configuring identity-based access policies
- Analyzing secure authentication flows
- Implementing dynamic access control
- Understanding Cisco ISE Use Cases
- Hands-on workshop: Building a network access policy.

[Day 2 - Morning]

Next-Generation Firewall and Advanced Inspection

- Understanding how NGFWs work
- Analyzing application inspection policies
- Configuring IPS mechanisms and advanced filtering
- Monitoring security logs and events
- Optimizing Cisco security policies
- Hands-on workshop: Analyzing and optimizing a firewall policy.

[Day 2 - Afternoon]

Advanced VPNs and secure connectivity

- Implementing secure VPN architectures
- Understanding IPsec and SSL VPN mechanisms
- Diagnosing tunneling incidents
- Securing remote user access
- Optimize VPN performance and high availability
- Hands-on workshop: Troubleshooting a VPN infrastructure.

Web security and content protection

- Identifying web and application threats
- Implementing URL filtering policies

- Analyze suspicious behavior in HTTP/HTTPS traffic
- Understand sandboxing mechanisms
- Blocking malicious content and data exfiltration
- Hands-on workshop: Advanced web incident analysis.

[Day 3 - Morning]

Email security and combating phishing

- Understanding modern email attacks
- Implementing SPF, DKIM, and DMARC protections
- Analyzing phishing and spear phishing campaigns
- Configuring quarantine policies
- Identifying suspicious behavior in emails
- Hands-on workshop: Investigating a malicious email.

[Day 3 - Afternoon]

Threat detection and SOC analysis

- Understanding SOC workflows
- Analyzing security logs and events
- Correlating alerts in a SIEM environment
- Identifying indicators of compromise
- Prioritizing and qualifying incidents
- Hands-on workshop: SOC investigation of network logs.

Endpoint protection and EDR

- Understanding EDR and Endpoint Security mechanisms
- Analyzing suspicious behavior on client workstations
- Detecting malicious activity and ransomware
- Responding to critical endpoint alerts
- Implement containment strategies
- Hands-on workshop: Analysis of an endpoint compromise.

[Day 4 - Morning]

Cloud Security and Hybrid Environments

- Understanding cloud security challenges
- Identifying risks associated with hybrid environments
- Securing connections between data centers and the cloud
- Implementing cloud visibility policies
- Analyzing shared responsibility models

- Hands-on workshop: Analyzing a secure cloud architecture.

[Day 4 - Afternoon]

Cisco Security Automation and APIs

- Understanding the principles of security automation
- Leveraging Cisco APIs for security operations
- Automating controls and checks
- Creating security orchestration workflows
- Identifying risks associated with API access
- Hands-on workshop: Automating a Cisco security task.

Incident response and network forensics

- Understanding incident response methodologies
- Collect and preserve digital evidence
- Analyzing network traces and system logs
- Implement containment measures
- Documenting and formalizing a security incident
- Hands-on workshop: Simplified forensic investigation.

[Day 5 - Morning]

Hardening, compliance, and security governance

- Applying hardening best practices
- Understanding security compliance frameworks
- Implementing governance policies
- Analyzing compliance gaps and risks
- Develop security recommendations
- Hands-on workshop: Security compliance audit.

[Day 5 - Afternoon]

Performance optimization and security troubleshooting

- Diagnosing complex security incidents
- Analyzing security-related network performance issues
- Identifying common configuration errors
- Implement troubleshooting methodologies
- Optimizing Cisco Security policies and equipment
- Hands-on workshop: Multi-technology incident resolution.

Final preparation for the Cisco CCNP Cybersecurity Concentration certification

- Review key technical areas of the selected exam
- Analyze Cisco’s expectations for advanced scenarios
- Identify common certification pitfalls
- Optimize time management during the exam
- Consolidate knowledge through practical case studies and quizzes
- Hands-on workshop: Take a practice exam + review.

Target Audience

This training is designed 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 methods.

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 running of the training session.

Teaching Methods

Practical Course: 60% Practical, 40% Theory. Training materials distributed in digital format to all participants.

Organization

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

Certification

At the end of the session, a multiple-choice quiz is used 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.