

200-201: Cisco Certified Cybersecurity Associate

Build practical SOC analyst skills in monitoring, analysis and response, aligned to the Cisco 200-201 exam.

DURATION

5 days · 40 hours

LEVEL

Intermediate

CURRICULUM

14 modules · 6 labs

DELIVERY

Live online, Onsite,
Corporate

Course overview

Security operations centres need analysts who can look at alerts, logs and packet captures and quickly decide what is real, what matters and what to do next. Cisco's associate-level cybersecurity certification, based on the 200-201 exam, targets exactly this role. This five-day course prepares you for the exam while building the analytical habits of a junior SOC analyst.

Day one covers security concepts: the CIA triad, security deployments, access control models, threat intelligence, and the vocabulary of risk, vulnerability and exploit. Day two focuses on security monitoring: the data types a SOC collects, how encryption and tunnelling affect visibility, common attack types and how they appear in logs and traffic. Day three is about host-based analysis, including endpoint technologies, operating system artefacts, malware analysis concepts and evidence handling. Day four covers network intrusion analysis: reading packet captures, interpreting IDS alerts and NetFlow, and extracting indicators. Day five turns to security policies and procedures, incident handling models, SOC metrics and profiling, followed by exam preparation.

Labs give you hands-on experience with packet analysis in Wireshark, log investigation in a SIEM-style interface, interpreting IDS alerts, examining host artefacts, and working through a mock incident from detection to report.

This course is aligned to the Cisco 200-201 exam. Cisco has renamed this certification from CyberOps Associate, so confirm the current name, exam topics and pricing with Cisco before booking.

Highlights

- 40 hours of live, trainer-led sessions
- Covers all five 200-201 exam topic areas
- Packet capture, log and alert analysis labs
- Incident handling using recognised frameworks
- Mock exam with detailed review

What's included

- Trainer with security operations experience
- Plan aligned to the five 200-201 topic areas
- Packet capture and log analysis labs
- IDS alert and NetFlow interpretation
- Mock incident from detection to report
- Mock exam with review
- Course completion certificate from Ace Skills Consulting

Who this course is for

Who should attend

- Aspiring and junior SOC analysts
- Network and system administrators moving into security
- IT support engineers interested in cybersecurity
- Graduates targeting security operations roles

Prerequisites

- Basic networking knowledge, such as TCP/IP and common protocols
- Familiarity with Windows and Linux operating systems

Detailed curriculum — 5 days, 40 hours, 14 modules, 6 hands-on labs

Day 1 Security Concepts

8 hours

1.1 Foundations

- CIA triad
- Agentless and agent-based protection
- Security deployments: network, endpoint, application
- SIEM and SOAR concepts

1.2 Risk and access

- Threat, vulnerability, exploit and risk
- Threat intelligence and threat hunting
- Access control models

1.3 Frameworks

- Attack frameworks and kill chains
- Security metrics
- CVSS terminology

LAB Map an attack scenario to a framework · 35 min

Day 2 Security Monitoring

8 hours

2.1 Data and visibility

- Data types: full packet, session, transaction, statistical, alert
- Network telemetry
- Impact of encryption, NAT and tunnelling

2.2 Attack types

- Network attacks
- Social engineering
- Web application attacks
- Evasion and obfuscation techniques

2.3 Log analysis

- Log sources and formats
- Correlating events

LAB Investigate suspicious activity in SIEM-style logs · 60 min

Day 3 Host-Based Analysis

8 hours

3.1 Endpoint technologies

- Host firewalls and antimalware
- Application allow-listing and sandboxing
- HIDS and EDR

3.2 Operating system artefacts

- Windows processes, registry and event logs
- Interpreting host evidence
- Linux processes and logs

LAB Examine host artefacts after a compromise · 50 min

3.3 Evidence and malware

- Evidence types and chain of custody
- Indicators of compromise
- Malware analysis tool output

Day 4 Network Intrusion Analysis

8 hours

4.1 Packet analysis

- Protocol headers
- Extracting files and indicators
- Reading PCAP files

LAB Analyse a packet capture to reconstruct an attack · 60 min

4.2 Alerts and flows

- IDS/IPS alerts and true and false positives
- Regular expressions for searching
- NetFlow analysis

LAB Triage IDS alerts and classify them · 40 min

Day 5 Security Policies, Procedures and Exam Readiness

8 hours

5.1 Incident handling

- Incident response life cycle
- Evidence and reporting
- Roles in a SOC

LAB Work a mock incident from detection to report · 60 min

5.2 Profiling and metrics

- Network and server profiling
- SOC metrics
- Data classification

5.3 Exam readiness

- Domain review
- Mock exam and review

Skills and tools

Skills you will build

Security monitoring

Log analysis

SIEM concepts

Packet analysis

Intrusion analysis

IDS alert triage

NetFlow

Host forensics basics

Indicators of compromise

Incident response

Threat intelligence

Attack frameworks

Tools used in class

Wireshark

Security Onion

Linux command line

Windows Event Viewer

Sysinternals tools

Certification exam

This course is aligned to the exam below and prepares you for it. The exam itself is booked and taken with the vendor.

Exam	Cisco Certified Cybersecurity Associate
Exam code	200-201
Official page	https://www.cisco.com/site/us/en/learn/training-certifications/index.html

Exam skill areas covered

Security Operations
Network Security
Incident Response

Exam details are pending verification. Confirm the current exam code, format and fee on the official vendor page before booking.

Frequently asked questions

Is this the same as the old CyberOps Associate?

It is based on the same 200-201 exam, which Cisco has rebranded. Confirm the current certification name with Cisco before booking.

Do I need CCNA first?

No. Basic networking knowledge is enough, and we review key concepts where needed.

Is the exam fee included?

Only when the batch shows the "Exam voucher included" badge. Otherwise you book directly with Cisco through Pearson VUE.

What roles does this prepare me for?

It suits junior SOC analyst, security monitoring and incident response support roles.

Book a batch or talk to an advisor

Course page: aceskillsconsulting.com/course/200-201-cisco-certified-cybersecurity-associate · Email: info@aceskillsconsulting.com

Chennai office

Guindy, Chennai, Tamil Nadu

Delhi office

B-95, Old Post Office Street, Shakarpur
New Delhi 110092
Office: 98180 12523

Cisco, CCNA and CCNP are trademarks of Cisco Systems, Inc. All product names, logos, brands, trademarks and registered trademarks are the property of their respective owners. Ace Skills Consulting is an independent training provider; unless explicitly stated, it is not affiliated with, endorsed by or sponsored by any vendor mentioned on this site. Exam details are provided for guidance and may change — always confirm on the vendor's official website. Curriculum generated on 23 Oct 2026; topics and order may be adjusted by the trainer to suit each batch.