Cisco 350-201 Exam Prep 2026

Cisco 350-201 2026. Cybersecurity operations, threat analysis, and security operations frameworks.

IT Certifications Instructor: Brian Mitchell • 5 sections • 45 lessons • 13.25h total

View this course online Browse all courses

About this course

Preparing for the Cisco 350-201 exam can feel overwhelming with its focus on implementing cybersecurity operations. This course breaks down the key concepts into manageable lessons, using real cases to make the material stick. We cover everything from core security principles to advanced threat analysis.

You will learn how to apply security operations frameworks, analyze threats using practical tools, and navigate exam-specific scenarios. The course includes video lessons, walkthroughs, downloadable study guides, and practice quizzes. It is designed for professionals who want a straightforward path to certification.

Course curriculum

Section 1: Foundations and Exam Overview

- Understanding the 350-201 Exam Structure (12m)
  Learn the exam format, domains, and scoring so you know exactly what to expect on test day.
- Key Cybersecurity Operations Concepts (18m)
  We'll break down the core principles of security operations that the exam focuses on.
- Setting Up Your Study Environment (8m)
  A step-by-step guide to organizing your study materials and schedule for efficient learning.
- Common Exam Pitfalls to Avoid (15m)
  Real case analysis of mistakes candidates make and how to sidestep them.
- Creating a Personalized Study Plan (10m)
  Downloadable template to map out your study timeline based on your current knowledge.
- Essential Tools for Security Analysis (22m)
  Introduction to the tools and software you'll need for both the exam and real-world work.
- Review of Networking Basics for Security (25m)
  A refresher on networking fundamentals that underpin security operations.

Section 2: Core Security Operations

- Implementing Security Monitoring (14m)
  How to set up and interpret security alerts using common frameworks.
- Analyzing Network Traffic for Threats (28m)
  Practical walkthrough of using Wireshark and other tools to spot malicious activity.
- Understanding SIEM Systems (19m)
  Learn how Security Information and Event Management tools work in a SOC environment.
- Incident Response Fundamentals (16m)
  Step-by-step guide to the incident response lifecycle with a real case study.
- Threat Intelligence Integration (21m)
  How to use threat feeds and data to enhance your security posture.
- Vulnerability Management Basics (17m)
  Practical steps for identifying and prioritizing vulnerabilities in your network.
- Log Analysis Techniques (23m)
  Problem-solving session on parsing logs to uncover security events.
- Endpoint Security Monitoring (12m)
  How to monitor and protect endpoints from threats, with tool examples.
- Cloud Security Operations (20m)
  Applying security operations in cloud environments like AWS and Azure.

Section 3: Advanced Threat Analysis

- Malware Analysis Fundamentals (24m)
  Learn to dissect malware samples using safe, practical methods.

- Detecting Advanced Persistent Threats (30m)
  Case study analysis of APT campaigns and how to spot them early.
- Network Forensics Techniques (26m)
  Step-by-step guide to investigating network breaches and gathering evidence.
- Behavioral Analysis for Threat Detection (18m)
  How to use user and entity behavior analytics (UEBA) in your operations.
- Email Security and Phishing Defense (15m)
  Practical strategies for analyzing and blocking phishing attempts.
- Ransomware Response Strategies (22m)
  Real-world playbook for dealing with ransomware incidents.
- IoT and OT Security Challenges (19m)
  Overview of securing Internet of Things and Operational Technology systems.

Section 4: Exam-Focused Scenarios and Practice

- Navigating Multiple-Choice Questions (11m)
  Tips and tricks for tackling the exam's multiple-choice format effectively.
- Simulating Security Operations Tasks (27m)
  Hands-on lab exercises that mirror real exam scenarios.
- Time Management During the Exam (9m)
  A problem-solving session on pacing yourself to complete all questions.
- Analyzing Exam Case Studies (32m)
  Deep dive into sample case studies with detailed explanations.
- Practice Quiz: Security Monitoring (13m)
  Test your knowledge with questions focused on monitoring domains.
- Practice Quiz: Incident Response (14m)
  Another set of questions to gauge your incident response skills.
- Practice Quiz: Threat Analysis (16m)
  Challenge yourself with advanced threat analysis questions.
- Reviewing Incorrect Answers (12m)
  How to learn from mistakes and improve your weak areas.
- Final Mock Exam Walkthrough (35m)
  Complete mock exam with detailed video explanations for each answer.
- Adjusting Your Study Based on Practice Results (10m)
  Downloadable template to refine your study plan after practice tests.

Section 5: Implementation and Certification Path

- Applying 350-201 Knowledge on the Job (20m)
  Real-world examples of how to use exam concepts in your daily security work.
- Building a Security Operations Portfolio (18m)
  Step-by-step guide to showcasing your skills for career advancement.
- Next Certifications After 350-201 (15m)
  Overview of advanced Cisco certs and how they build on this exam.

- Staying Current with Security Trends (22m)
  Resources and habits to keep your knowledge up-to-date post-certification.
- Networking with Security Professionals (12m)
  Tips for joining communities and learning from peers in the field.
- Preparing for the Certification Renewal (16m)
  What you need to know about maintaining your Cisco certification.
- Troubleshooting Common Exam Issues (14m)
  A problem-solving session for technical and logistical exam-day problems.
- Creating a Long-Term Learning Plan (19m)
  Downloadable template for continuous professional development in cybersecurity.
- Case Study: Full Security Operations Cycle (28m)
  Walk through a comprehensive case from detection to resolution.
- Final Tips for Exam Day Success (8m)
  Quick checklist and mindset advice to boost your confidence.
- Course Wrap-Up and Next Steps (7m)
  Summary of key takeaways and how to proceed with your certification journey.
- Accessing Additional Resources (5m)
  Links to practice questions, study groups, and official Cisco materials.