Cisco 200-201 CyberOps Associate Prep (2026)

Cisco 200-201 CBROPS 2026. Threat analysis, security monitoring, incident response, and SOC operations.

IT Certifications Instructor: Brian Mitchell • 5 sections • 45 lessons • 14.75h total

View this course online Browse all courses

About this course

Preparing for the Cisco 200-201 exam can feel overwhelming with its mix of security concepts, monitoring tools, and incident response procedures. This course cuts through the noise by focusing on the practical skills you need to pass the CBROPS exam and handle real security operations center (SOC) tasks. We will walk through the key exam topics using clear explanations and hands-on scenarios.

You will learn how to interpret security alerts, analyze logs from various sources, and apply incident response steps in a structured way. The course includes real case studies from network traffic and malware analysis, plus practical walkthroughs of tools like Wireshark and security monitoring platforms. Each lesson prepares you for both the exam questions and your first day in a SOC.

Course curriculum

Foundations and Exam Overview

- Understanding the Cisco 200-201 CBROPS Exam Structure (12m)
  Get a clear breakdown of the 200-201 exam domains for 2026, question types, and how to plan your study schedule effectively.
- Key Security Concepts for SOC Analysts (18m)
  Learn the core principles like CIA triad, vulnerabilities, threats, and risks with real-world examples from security operations.
- Network Protocols and Ports Deep Dive (25m)
  Step-by-step guide to TCP/IP, common ports, and protocol interactions to build a solid foundation for traffic analysis.
- Types of Network Attacks and How to Spot Them (22m)
  Explore DDoS, man-in-the-middle, and ransomware attacks using case studies to recognize signs in logs and alerts.
- Endpoint Security Fundamentals (15m)
  We'll show you how antivirus, EDR, and host-based firewalls protect endpoints, with downloadable comparison templates.
- Security Monitoring Principles and Tools (20m)
  Understand SIEM, IDS/IPS, and NetFlow basics, including how to configure simple monitoring rules for exam prep.
- Data Privacy and Compliance in Security Operations (14m)
  Cover GDPR, HIPAA, and PCI-DSS impacts on SOC work, with practical tips for handling sensitive data during incidents.

Core Concepts in Security Monitoring

- How Network Intrusion Detection Systems (IDS) Work (28m)
  Real case study analysis of signature-based vs. anomaly-based IDS to interpret alerts accurately.
- Analyzing Firewall Logs for Security Events (16m)
  Hands-on walkthrough of Cisco ASA and next-gen firewall logs to identify blocked traffic and policy violations.
- Using NetFlow and IPFIX for Traffic Monitoring (24m)
  Learn to collect and analyze flow data to detect unusual network patterns, with a downloadable NetFlow query template.
- Endpoint Detection and Response (EDR) in Action (19m)
  Problem-solving session on EDR alerts, including how to triage suspicious processes on Windows and Linux hosts.
- Email Security and Phishing Detection Techniques (21m)
  Break down SPF, DKIM, and DMARC records using real phishing email headers to spot malicious intent.

- Web Proxy Logs and URL Filtering Analysis (17m)
  Step-by-step guide to parsing proxy logs for C2 communication and data exfiltration attempts.
- Wireless Security Monitoring Essentials (13m)
  Cover rogue AP detection and WPA2/WPA3 issues, with examples from common wireless IDS tools.
- Cloud Security Monitoring Basics (AWS/Azure) (26m)
  We'll show you how to monitor cloud logs for unauthorized access, including a sample CloudTrail query.
- Correlating Events Across Multiple Data Sources (30m)
  Practical case study using SIEM to link endpoint, network, and application logs for a full attack timeline.

Deep Dive into Threat Analysis

- Malware Analysis Workflow for Beginners (23m)
  Learn static and dynamic analysis steps, including using sandbox tools to examine a sample malware file safely.
- Interpreting Packet Captures with Wireshark (32m)
  Hands-on guide to filtering and analyzing TCP streams, HTTP requests, and suspicious payloads in PCAP files.
- Identifying Command and Control (C2) Traffic Patterns (18m)
  Real-world examples of beaconing and DNS tunneling, with tips to spot them in NetFlow and proxy logs.
- Analyzing Suspicious DNS Queries and Responses (15m)
  Problem-solving session on NXDOMAIN, DGA domains, and DNS exfiltration using live query logs.
- Threat Intelligence Feeds and IOC Integration (20m)
  How to use STIX/TAXII feeds to enrich alerts, with a downloadable IOC matching checklist.
- Behavioral Analysis for Zero-Day Threats (27m)
  Step-by-step breakdown of baselining normal behavior and detecting anomalies in user and machine activity.
- Ransomware Indicators in Network and Endpoint Logs (22m)
  Case study analysis of a simulated ransomware attack, focusing on encryption and lateral movement signs.

Advanced Incident Response Techniques

- Incident Response Lifecycle: Preparation to Recovery (19m)
  NIST framework overview with practical steps for building your IR playbook, including a template download.
- Triage and Prioritization of Security Alerts (14m)
  Real case study on ranking alerts by severity and impact to avoid alert fatigue in the SOC.
- Containment Strategies for Network Breaches (25m)
  Hands-on guide to isolating affected hosts, blocking IPs, and segmenting networks during an active incident.

- Eradication and Root Cause Analysis (29m)
  Step-by-step process for removing malware and identifying how the attacker entered, with log correlation examples.
- Post-Incident Reporting and Lessons Learned (16m)
  We'll show you how to write clear IR reports for management, including metrics and remediation recommendations.
- Forensic Data Collection from Endpoints (21m)
  Practical walkthrough of memory dumps and disk imaging using free tools, preserving evidence chain of custody.
- Handling Insider Threats and Data Leaks (18m)
  Problem-solving session on detecting unauthorized data access, with examples from DLP and SIEM alerts.
- Automating Incident Response with SOAR Tools (31m)
  Introduction to SOAR playbooks for automated containment, including a simple workflow example.
- Legal and Ethical Considerations in IR (12m)
  Cover evidence handling, reporting obligations, and working with law enforcement during major incidents.
- Simulated Full Incident Response Exercise (35m)
  Capstone problem-solving session walking through a multi-stage attack from detection to recovery.

Implementation & Exam Success Strategies

- Hands-On Lab Setup for 200-201 Practice (11m)
  Step-by-step guide to building a virtual lab with Security Onion, Wireshark, and Cisco tools for exam simulations.
- Practice Exam: Security Monitoring Domain (20m)
  Timed quiz with explanations for each question to reinforce monitoring concepts and identify weak areas.
- Practice Exam: Threat Analysis Domain (22m)
  Realistic scenario-based questions on malware and traffic analysis, with detailed answer breakdowns.
- Practice Exam: Incident Response Domain (18m)
  Focus on IR procedures and prioritization, including tips for answering scenario questions efficiently.
- Time Management for the 200-201 Exam (9m)
  Proven strategies to pace yourself, flag questions, and review answers without rushing.
- Common Pitfalls and How to Avoid Them (13m)
  We'll highlight frequent mistakes like misinterpreting logs or overthinking scenarios, with corrective examples.
- Final Review: Key Exam Topics Checklist (16m)
  Downloadable checklist covering all exam objectives to ensure you're ready for test day.
- Career Paths After CyberOps Associate Certification (10m)
  Practical advice on SOC roles, resume tips, and next certifications like CCNA or CySA+.
- Staying Current: 2026 Security Trends (17m)
  Overview of emerging threats like AI-driven attacks and zero trust, to keep your skills relevant post-cert.

- Q&A: Common Exam Questions Answered (15m)
  Problem-solving session addressing student-submitted questions on tricky 200-201 topics.
- Building Your First SOC Workflow (24m)
  Hands-on guide to creating a daily monitoring routine, integrating tools and best practices from the course.
- Next Steps: Lab Challenges and Community Resources (8m)
  Action plan for ongoing practice, including challenge ideas and where to find study groups or forums.

Discover our blog

Learn more with free articles written by our professors and guest experts.

Latest article: **Flight Attendant Preparation: What to Study Before You Apply**

Visit the blog All courses This course