APPLIED TECHNOLOGY ACADEMY

800.674.3550
Info@AppliedTechAc.com
AppliedTechnologyAcademy.com

Understanding Cisco Cybersecurity Operations Fundamentals (CCNACBR) Training

Award Winning Training · Applied Technology Academy

Understanding Cisco Cybersecurity Operations Fundamentals (CCNACBR, course v2.0) prepares associate-level analysts to work in a threat-centric security operations center. Cisco renamed this course from CBROPS in February 2026; the certification is now CCNA Cybersecurity and the exam remains 200-201.

LEVEL	DURATION	EXPERIENCE	EXAM	CERTIFICATION
Associate	**5 Days**	**None (TCP/IP, Windows & Linux basics recommended)**	**200-201 CCNACBR (v1.2)**	**CCNA Cybersecurity**

Course Overview

You will learn security concepts, security monitoring, host-based analysis, network intrusion analysis, and security policies and procedures — the five domains of the 200-201 CCNACBR exam — and practice them across 13 hands-on labs.

Course Outline

- 1. Security Operations
- 2. Security Principles
- 3. Access Control Models
- 4. Cloud Security Models
- 5. Cryptography for Security Operations
- 6. Windows OS Basics
- 7. Linux OS Basics
- 8. CLIs in Security
- 9. Network Protocols
- 10. Network Security Controls
- 11. IDS and IPS
- 12. Endpoint Security
- 13. Threat Actors
- 14. Cyber Kill Chain Model
- 15. MITRE ATT&CK Framework
- 16. Social Engineering Attacks

800.674.3550
Info@AppliedTechAc.com
AppliedTechnologyAcademy.com

- 17. Network Attack Fundamentals
- 18. Advanced Threat Landscape
- 19. Network Security Monitoring (NSM) Data
- 20. Log Data Sources
- 21. NetFlow for Security Monitoring
- 22. Web Application Attacks
- 23. Advanced Log Analysis
- 24. Packet Capture and Forensics
- 25. Malware and Threat Intelligence
- 26. Security Information and Event Management (SIEM)
- 27. Security Orchestration, Automation, and Response (SOAR)
- 28. Extended Detection and Response (XDR)
- 29. Incident Response Planning
- 30. CSIRT Roles and Operations
- 31. Security Monitoring Playbooks
- 32. Threat Hunting Methodologies

Intended Audience

Associate-level cybersecurity analysts working in security operations centres, and students or professionals moving into SOC analyst, incident responder and security operations roles.

Prerequisites

There are no formal prerequisites. Cisco recommends familiarity with Ethernet and TCP/IP networking, working knowledge of the Windows and Linux operating systems, and familiarity with basic networking security concepts.

Lab Outline

- 1. Explore Cryptographic Technologies
- 2. Explore the Windows Operating System
- 3. Explore the Linux Operating System
- 4. Explore Endpoint Security
- 5. Investigate Hacker Methodology
- 6. Explore TCP/IP Attacks
- 7. Investigate Advanced Persistent Threats
- 8. Use NSM Tools to Analyze Data Categories
- 9. Analyze Suspicious DNS Activity

- 10. Investigate Browser-based Attacks
- 11. Correlate Event Logs, PCAPs, and Alerts of an Attack
- 12. Explore SOC Playbooks
- 13. Hunt Malicious Traffic

Ready to enroll? Call 800.674.3550 or email Info@AppliedTechAc.com — private team cohorts, GSA MAS purchasing, military credentialing funding, VA GI Bill and VR&E and student financing available.