



Cisco Certified CyberOps Associate

The Cisco Certified CyberOps Associate certification program validates the day-to-day, tactical knowledge and skills that Security Operations Center (SOC) teams need to detect and respond to cybersecurity threats.

The Cisco CyberOps training course, Understanding Cisco Cybersecurity Operations Fundamentals, covers knowledge and skills related to security concepts, security monitoring, host-based analysis, network intrusion analysis, and security policies and procedures.

Cisco CyberOps is compliant with ISO 17024 standards and approved by the US DoD to meet directive 8140/8570.01-M requirements.

Our unique model follows a streamlined approach to workforce development and skills attainment

Assess: Assess each student to determine existing skill sets

Educate: Deliver goal-specific training utilizing all delivery modalities

Mentor: Expose students to instructors and mentors with front-line IT and cybersecurity experience

Certify: Certify students with the requisite hands-on skills to perform the tasks related to their functional roles

Validate: Validate student abilities through performance analytics and real-world exercises hosted on a cyber range

Exam Objectives: 200-201 CBROPS

Cisco Certified CyberOps Associate

Security Concepts	20%
Security Monitoring	25%
Host-Based Analysis	20%
Network Intrusion Analysis	20%
Security Policies and Procedures	15%

Course Outline:

Chapter 1: Cybersecurity Fundamentals

Chapter 2: Introduction to Cloud Computing and Cloud Security

Chapter 3: Access Control Models

Chapter 4: Types of Attacks and Vulnerabilities

Chapter 5: Fundamentals of Cryptography and Public Key Infrastructure (PKI)

Chapter 6: Introduction to Virtual Private Networks (VPNs)

Chapter 7: Introduction to Security Operations Management

Chapter 8: Fundamentals of Intrusion Analysis

Chapter 9: Introduction to Digital Forensics

Chapter 10: Network Infrastructure Device Telemetry and Analysis

Chapter 11: Endpoint Telemetry and Analysis

Chapter 12: Challenges in the Security Operations Center (SOC)

Chapter 13: The Art of Data and Event Analysis

Chapter 14: Classifying Intrusion Events into Categories

Chapter 15: Introduction to Threat Hunting

Included

40 hours of instructor-led training sessions

Cisco authorized textbook and class materials

Practice questions and exam study tips