Cisco Certified CyberOps Associate

Price	Duration	Delivery Methods
$1,795.00	5 Daytime Classes Or 10 Evening Classes	Virtual, In-Person, Private Group,

CAREER SKILLS+™

This foundational course equips learners with the essential knowledge and skills needed for roles in cybersecurity operations centers. Focusing on the basics of cybersecurity, the course covers network infrastructure, security principles, and an introduction to the protocols necessary for securing a network. Students will gain insights into the security posture of networks and devices, and how to respond to and recover from incidents. This course lays the groundwork necessary for the Cisco Certified CyberOps Associate certification.

Who Should Attend

This course is designed for individuals seeking to begin a career in cybersecurity, specifically in roles within security operations centers as cybersecurity analysts.

Course Objectives

Cybersecurity Foundations: Understand the key concepts of

cybersecurity and the roles and responsibilities of a cybersecurity professional.
Network Security Basics: Learn the basics of network security, including different types of cyberattacks and defensive mechanisms.
Security Monitoring: Introduction to security monitoring tools and techniques used to detect and respond to threats.
Incident Response: Learn the fundamentals of incident response, including preparation, detection, containment, eradication, and recovery.
Threat Intelligence: Understand the basics of threat intelligence to identify and mitigate potential threats.
Security Policies: Learn about the creation and implementation of security policies that help protect an organization from cyber threats.

Course Prerequisites

Recommended Knowledge: Basic understanding of computer networks and operating systems.
Technical Familiarity: Familiarity with the concepts of networking and basic security principles is advantageous but not required.

Agenda

1. Lessons

- Introduction to Cybersecurity Operations
- Network Security Fundamentals
- Security Monitoring: Tools and Techniques
- Cybersecurity Threats and Attack Vectors
- Fundamentals of Incident Response
- Introduction to Security Information and Event Management (SIEM) Systems
- Cybersecurity Best Practices and Policies
- Basic Cryptography and its Applications in Cybersecurity
- Working in a Security Operations Center
- Legal and Compliance Issues in Cybersecurity

2. Lab Outline

- Setting Up a Security Monitoring Environment
- Basic Network Security Configurations
- Using SIEM Tools for Threat Detection
- Simulating Cyber Attacks and Incident Response
- Implementing Basic Cryptographic Systems
- Analyzing Real-Time Security Alerts

Creating and Managing Security Documentation
Conducting Basic Forensic Analysis