



Cisco Certified CyberOps Associate Prep Course (On-Site Live/Blended Learning)

Course Dates: 2021 Offerings TBD

Enrollment opens 60 prior to course start. Enrollment closes 10 business days before course start date.

Location for On-Site Training: 100 Grace Hopper Lane, Augusta GA 30901

Course Costs

Included in Course	Cost
Cisco Exam Voucher	\$300
On site instruction (6 days)	\$1,195
6 months DL content access	\$50
40+ hours custom recorded video lecture	\$200
Total Course Price	\$1,995

- Price includes shipping, tax, credit card processing and any applicable administrative fees.

General Information

Description

Cisco Certified CyberOps Associate exam tests core knowledge required to in the tasks, duties, and responsibilities of an associate-level Security Analyst working in a Security Operations Center (SOC). The Cisco CyberOps Certification is compliant with ISO 17024 standards and approved by the US DoD to meet directive 8140/8570.01-M requirements for CSSP Analyst, and Incident Responder roles.

Course Material Details

Material Included

The following materials are included with the cost of the course and provided directly to the student.

- Cisco Exam Voucher
- 1 week live instruction, review and tutoring by training expert on curriculum
- 6 months access to Distance Learning Portal
 - ✓ Custom Instructor Recorded Lecture (40+ hours)
 - ✓ Rich multimedia content, including interactive activities, videos, games, and quizzes
 - ✓ Virtual Machine Images required to perform all practical labs and exercises

Link for Enrollment

Links will be released when classes are scheduled, check back for 2021 class dates in October 2020 at:

<https://gacybercenter.pdx.catalog.canvaslms.com/>



Expectations and Goals

This course prepares the learner over a course of 2 weeks to pass the Cisco Certified CyberOps Associate Exam. Access for up to 6 months to all the online content allow individuals that need to continue to review the material ample time to prepare for the certification exam. This course will prepare students to perform the following tasks:

- Install virtual machines to create a safe environment for implementing and analyzing cybersecurity threat events.
- Explain the role of the Cybersecurity Operations Analyst in the enterprise.
- Explain the Windows OS features and characteristics needed to support cybersecurity analyses.
- Explain the features and characteristics of the Linux Operating System.
- Analyze the operation of network protocols and services.
- Explain the operation of the network infrastructure.
- Classify the various types of network attacks.
- Use network monitoring tools to identify attacks against network protocols and services.
- Use various methods to prevent malicious access to computer networks, hosts, and data.
- Explain the impacts of cryptography on network security monitoring.
- Explain how to investigate endpoint vulnerabilities and attacks.
- Evaluate network security alerts.
- Analyze network intrusion data to identify compromised hosts and vulnerabilities.
- Apply incident response models to manage network security incidents.



Course Schedule

Online/Recorded Lecture and Labs/activities

Chapter 1: Cybersecurity and the Security Operations Center

Chapter 2: Windows Operating System

Chapter 3: Linux Overview

Chapter 4: Network Protocols and Services

Chapter 5: Network Infrastructure

Chapter 6: Principles of Network Security

Chapter 7: Network Attacks

On-site/In-person Training conducted at Georgia Cyber Center

Day 5: Online Content Review

Chapter 8: Protecting the Network

Day 6: Chapter 9: Cryptography and Public Key Infrastructure

Day 7: Chapter 11: Security Monitoring

Day 8: Chapter 12: Intrusion Data Analysis

Day 9: Chapter 10: Endpoint Security and Analysis (lecture) (first half)

Day 10: Chapter 10: Endpoint Security and Analysis (lecture) (last half)

Chapter 13: Incident Response and Handling

Skills Based Assessment/Online Final