Cisco Certified CyberOps Associate

As of July 2018, The United States Department of Defense (DoD) has approved the Cisco CCNA Cyber Ops Certification (now called Cisco Certified CyberOps Associate certification) for the DoD 8570.01-M for the CSSP Analyst and CCSP Incident Responder categories. more details

SecureNinja's Cisco Certified CyberOps Associate training and certification boot camp will grant students foundational knowledge and skills needed for advanced job roles in cybersecurity. Students will also gain a basic understanding of how a SOC team detects and responds to security incidents, and how they protect their organization's information from modern-day cyber-attacks. The CyberOps Associate certification boot camp provides practical, relevant, and job-ready certification curricula which are aligned closely with specific tasks expected from in-demand professionals. The CyberOps Associate is an instructor-led course that is designed to help students learn about best practices and grant a hands-on experience on what it is like to work in the cybersecurity field. This course is specific to the best practices of network security administrators, engineers, and experts using the latest equipment, devices, and appliances. This course is also valuable to anyone who is looking to build confidence in their ability to identify or react to security threats or reinforce their skills.

The Cisco Certified CyberOps Associate program provides solid and professional knowledge that is required for any career in cybersecurity. It also enhances skills by providing a realistic and modern-day approach to different real-life scenarios. This course is also approved by the Department of Defense (DoD) for the DoD 8570.01-M and it is a 5-day course led by our certified ninja instructors.

Why Choose Cisco Certfied CyberOps Associate?

This program provides the necessary knowledge needed to start/boost a career in the growing cybersecurity field. This course provides different practices and methods that are used to detect, respond, and defeat cyber threats that could potentially harm an organization. This course is a highly essential program for anyone who is looking to start a career in the cybersecurity field, or for anyone who is working in the cybersecurity field.

Topics Covered

A Cisco Certified CyberOps Associate certification will cover the following topics:

- Security Concepts
- Security Monitoring
- Host-based analysis
- Network intrusion analysis
- Security policies and procedures
- Digital assets
- Malware analysis and interpretation
- Identifying protecting data

- Understanding key SOC metrics to expedite detection and containment of breaches

CyberOps Training Course Outline

- Defining the Security Operations Center
- Understanding Network Infrastructure and Network Security Monitoring Tools
- Exploring Data Type Categories
- Understanding Basic Cryptography Concepts
- Understanding Common TCP/IP Attacks
- Understanding Endpoint Security Technologies
- Understanding Incident Analysis in a Threat-Centric SOC
- Identifying Resources for Hunting Cyber Threats
- Understanding Event Correlation and Normalization
- Identifying Common Attack Vectors
- Identifying Malicious Activity
- Identifying Patterns of Suspicious Behavior
- Conducting Security Incident Investigations
- Using a Playbook Model to Organize Security Monitoring
- Understanding SOC Metrics
- Understanding SOC Workflow and Automation
- Describing Incident Response
- Understanding the Use of VERIS
- Understanding Windows Operating System Basics
- Understanding Linux Operating System Basics

CyberOps Lab outline

- Use NSM Tools to Analyze Data Categories
- Explore Cryptographic Technologies
- Explore TCP/IP Attacks
- Explore Endpoint Security
- Investigate Hacker Methodology
- Hunt Malicious Traffic
- Correlate Event Logs, Packet Captures (PCAPs), and Alerts of an Attack
- Investigate Browser-Based Attacks
- Analyze Suspicious Domain Name System (DNS) Activity
- Explore Security Data for Analysis
- Investigate Suspicious Activity Using Security Onion
- Investigate Advanced Persistent Threats
- Explore SOC Playbooks
- Explore the Windows Operating System
- Explore the Linux Operating System

Who is it for?

This program is designed for anyone who is looking to start a career in the cybersecurity field as someone who can detect, react, and eliminate different cyber threats. Students who take this course will also gain skills developed from different hands-on experiences that are inspired by real-life scenarios in the cybersecurity workplace.

Who Would Benefit?

- Security practitioners, engineers, analysts, specialist, architects, and managers
- Network security administrators
- Network security engineers
- Systems Administrator
- Program Manager
- SOC Professionals
- Incident Response Team Members
- Individuals who want to enrich or gain skills in the field of cybersecurity

Pre-requisites

There are no pre-requisites required to take the CyberOps Associate course; however, basic knowledge of computer operating systems, such as Windows and Linux is recommended.

Exam Information

The required exam for this certification is 200-201 CBROPS.

200-201 CBROPS

- Number of Questions: 95-105
- Duration: 120 minutes

Course Length

The Cisco Certified CyberOps Associate certification boot camp is a 5-day program consisting of 40 hours of instructor-led training.

Course Outline

The Cisco Certified CyberOps Associate training will be composed of 6 main subjects.

1. Network Concepts
2. Security Concepts
3. Cryptography
4. Host-Based Analysis
5. Security Monitoring
6. Attack Methods

Courseware

Cisco Certified CyberOps Associate CBROPS #200-201 Official Cert Guide

Cisco Certified CyberOps Associate (CBROPS #200-201) Official Cert Guide Library