

SECFND – Understanding Cisco Cybersecurity Fundamentals

Duration: 5 Days

Overview:

This is an Associate-level self-study technical course in the curriculum for the CCNA Cyber Ops certification. This course allows learners to understand cybersecurity's basic principles and foundational knowledge, as well as obtain the core skills needed to grasp the more advanced associate-level materials in the second required exam, "Implementing Cisco Cybersecurity Operations (SECOPS)". It focuses on cybersecurity operations principles and technologies, using hands-on examples in realistic scenarios, with real-life security products and equipment

Audience:

- IT Professionals
- Any learner interested in entering associate-level cybersecurity roles such as:
 - SOC cybersecurity analysts
 - Computer or network defense analysts
 - Computer networks defense infrastructure support personnel
 - Future incident responders and SOC personnel
 - Cisco integrators or partners

Module 1: TCP/IP and Cryptography Concepts

Lessons:

- Understanding the TCP/IP Protocol Suite
- Understanding the Network Infrastructure
- Understanding Common TCP/IP Attacks
- Understanding Basic Cryptography concepts

Module 2: Network Applications and Endpoint Security

Lessons:

- Describing Information Security Concepts
- Understanding Network Applications
- Understanding Common Network Application Attacks
- Understanding Windows Operating System Basics
- Understanding Linux Operating System Basics
- Understanding Common Endpoint attacks
- Understanding Network Security Technologies
- Understanding Endpoint Security Technologies

Module 3: Security Monitoring and Analysis

Lessons:

- Describing Security Data Collection
- Describing Security Event Analysis

Pre-requisites:

We recommend that you have knowledge of one or more of the following before attending this course:

- Familiarity with basic networking concepts
- Working knowledge of the Windows operating system
- Familiarity with the Linux operating system

Course Completion:

Upon completion you will be able to:

- Describe, compare and identify various network concepts
- Fundamentals of TCP/IP
- Describe and compare fundamental security concepts
- Describe network applications and the security challenges
- Understand basic cryptography principles
- Understand endpoint attacks, including interpreting log data to identify events in Windows and Linux
- Develop knowledge in security monitoring, including identifying sources and types of data and events
- Know various attacks methods, security weaknesses, evasion methods, and remote versus local exploits

On Demand:

This course is available On-Demand. With On-Demand you get access to:

- 365 days of unlimited access to interactive, Cisco authorised training
- Hands-on practice labs delivered through Discovery Labs
- Course content that is equivalent to classroom training
- Graded assessments at the end of every section to provide students with vital feedback