Understanding Cisco Cybersecurity Fundamentals (SECFND) v1.0

What you'll learn in this course

The **Understanding Cisco Cybersecurity Fundamentals (SECFND)** course gives you foundation-level knowledge of common security concepts, basic security techniques, and the fundamentals of applications, operating systems, and networking used in a Security Operations Center (SOC). This course helps you learn to find threats within a real-life network infrastructure using a variety of popular security tools. Through expert instruction and hands-on experience using enterprise-grade security tools, you will learn the basics of network and security concepts, endpoint attacks, cryptography, analysis, and monitoring. This course provides introductory knowledge for those interested in entering the field of cybersecurity and prepares you for the 210-250 SECFND exam, one of the two exams for the current Cisco Certified CyberOps Associate* certification.

Today's cybersecurity professionals need to detect, investigate, and respond to a wide variety of security events. This course will help you gain the skills to play a role in your organization's SOC detecting and responding to security events.

The United States Department of Defense recognizes Cisco CCNA CyberOps certification (now called Cisco Certified CyberOps Associate) as an approved baseline certification in the Information Assurance (IA) Workforce CCSP Incident Responder and CCSP Analyst job categories. Please see Cisco CCNA Cyber Ops and the DoD Approved 8570 Baseline Certifications for more information.

What to expect

- Instructor-led training: 5 days in the classroom with hands-on lab practice
- Virtual instructor-led training: 5 days of web-based classes with hands-on lab practice
- E-learning: Equivalent of 5 days of instruction with hands-on lab practice, videos, and challenges

How you'll benefit

This course will help you:

- Learn fundamental principles of cryptography, applications, operating systems, and networking
- Learn foundational knowledge for detecting and responding to cybersecurity incidents, including monitoring, analysis, and understanding common attacks
- Prepare for the Cisco Certified CyberOps Associate certification with hands-on practice using real-life security analysis tools, such as those found in a Linux distribution
- Start your career in the high-demand area of cybersecurity

Who should enroll

- IT professionals
- Any learner interested in entering associate-level cybersecurity roles such as:
  - SOC cybersecurity analysts
  - Computer or network defense analysts
  - Computer network defense infrastructure support personnel

- Future incident responders and SOC personnel
- Cisco integrators or partners

How to enroll

- For instructor-led training, visit the Cisco Learning Locator.
- For private group training, visit Cisco Private Group Training.

Technology areas

- Security
- Cybersecurity operations

Course details

Objectives

After taking this course, you should be able to:

- Describe network operations and attacks, basic cryptography concepts, and network infrastructure device operations
- Describe basic Windows and Linux OS operations, common network applications and attacks, endpoint attacks, and network and endpoint security solutions
- Describe security data collection and monitoring, and the common threat models that security operations organizations can reference when performing cybersecurity analysis

Prerequisites

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

Outline

TCP/IP and Cryptography Concepts

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

Network Applications and Endpoint Security

- 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

Security Monitoring and Analysis

- Describing Security Data Collection
- Describing Security Event Analysis

Lab outline

- Explore the TCP/IP Protocol Suite
- Explore the Network Infrastructure
- Explore TCP/IP Attacks
- Explore Cryptographic Technologies
- Explore Network Applications
- Explore Network Application Attacks
- Explore the Windows Operating System
- Explore the Linux Operating System
- Explore Endpoint Attacks
- Explore Network Security Technologies
- Explore Endpoint Security
- Explore Security Data for Analysis

* Cisco CCNA Cyber Ops has been renamed to Cisco Certified CyberOps Associate