Understanding Cisco Cybersecurity Fundamentals (SECFND) 1.0

Length: 5 Days

Summary: The course helps to prepare students for beginning and associate level roles in cybersecurity operations. The course focuses on security principles and technologies, using Cisco security products to provide hands-on examples. Using instructor-led discussions, extensive hands-on lab exercises, and supplemental materials, this course allows learners to understand common security concepts, and start to learn the basic security techniques used in a Security Operations Center (SOC) to find threats on a network using a variety of popular security tools within a real-life network infrastructure.

Course Objectives: Upon completion of this course, 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

Prerequisites: It is recommended, but not required, that students have the following knowledge and skills

- Working knowledge of the Windows operating system
- Working knowledge of the Linux operating system
- Basic IPv4 and IPv6 addressing knowledge

Who Should Attend

- Security Operations Center Security Analyst
- Computer/Network Defense Analyst
- Computer Network Defense Infrastructure Support Personnel
- Future Incident Responders and Security Operations Center (SOC) personnel
- Students beginning a career, entering the cybersecurity field
- Cisco Channel Partners

COURSE CONTENT

Module 1: Network Concepts

Module 2: Security Concepts

Module 3: Cryptography /IP

Module 4: Host-Based Analysis

Module 5: Security Monitoring

Module 6: Attack Methods