Understanding Cisco Cybersecurity Fundamentals (SECFND) 1.0

Course Overview:

The Understanding Cisco Cybersecurity Fundamentals (SECFND) v1.0 course provides you with an understanding of network infrastructure devices, operations and vulnerabilities of the TCP/IP protocol suite, basic information security concepts, common network application operations and attacks, the Windows and Linux operating systems, and the types of data that are used to investigate security incidents.

After completing this course, you will have basic knowledge that is required to perform the job role of an entry-level cybersecurity analyst in a threat-centric security operations center.

Who Should Attend:

- Security Operations Center – Security Analyst
- Computer/Network Defense Analysts
- 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

Prerequisites:

Basic technical competency (must possess one or more of the following):

- Cisco certification (Cisco CCENT certification or higher)
- Relevant industry certification [(ISC)2, CompTIA Security+, EC-Council, GIAC, ISACA]
- Cisco Networking Academy letter of completion (CCNA 1 and CCNA 2)
- Windows expertise: Microsoft (Microsoft Specialist, MCSA, MCSE), CompTIA (A+, Network+, Server+)
- Linux expertise: CompTIA (Linux+), Linux Professional Institute (LPI) certification, Linux Foundation (LFCS, LFCE), Red Hat (RHCSA, RHCE, RHCA), Oracle Linux (OCA, OCP)

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

- Skills and knowledge equivalent to those learned in ICND1 - Interconnecting Cisco Networking Devices, Part 1.

Course Objectives:

Upon completing this course, the learner will gain the following knowledge:

- 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 attack methods, security weaknesses, evasion methods, and remote versus local exploits

Course Outline:

Module 1: TCP/IP and Cryptography Concepts

- Lesson 1: Understanding the TCP/IP Protocol Suite
- Lesson 2: Understanding the Network Infrastructure
- Lesson 3: Understanding Common TCP/IP Attacks
- Lesson 4: Understanding Basic Cryptography Concepts

Module 2: Network Applications and Endpoint Security

- Lesson 1: Describing Information Security Concepts
- Lesson 2: Understanding Network Applications
- Lesson 3: Understanding Common Network Application Attacks
- Lesson 4: Understanding Windows Operating System Basics
- Lesson 5: Understanding Linus Operating System Basics
- Lesson 6: Understanding Common Endpoint Attacks
- Lesson 7: Understanding Network Security Technologies

- Lesson 8: Understanding Endpoint Security Technologies

Module 3: Security Monitoring and Analysis

- Lesson 1: Describing Security Data Collection
- Lesson 2: Describing Security Event Analysis

LABS:

- Lab 1: Explore the TCP/IP Protocol Suite
- Lab 2: Explore the Network Infrastructure
- Lab 3: Explore TCP/IP Attacks
- Lab 4: Explore Cryptographic Technologies
- Lab 5: Explore Network Applications
- Lab 6: Explore Network Application Attacks
- Lab 7: Explore the Windows Operating System
- Lab 8: Explore the Linux Operating System
- Lab 9: Explore Endpoint Attacks
- Lab 10: Explore Network Security Technologies
- Lab 11: Explore Endpoint Security
- Lab 12: Explore Security Data for Analysis