Implementing an Integrated Threat Defense Solution (SECUR201)

Duration: 2 days

Course Overview

Implementing an Integrated Threat Defense Solution (SECUR201) is an instructor-led, lab-based, hands-on course offered by Cisco®Learning Services. This course is part of a series of Cisco security solutions courses designed to help businesses implement and operate their Cisco Integrated Threat Defense solution.

This lab-intensive course introduces you to Cisco's Integrated Threat Defense solution with a focus on product integration. The skills you will learn include:

1. **Integration of solution components with existing network services**
2. **Integration of solution components with the pxGrid framework**
3. **Integration of network-and endpoint-based malware protection**
4. **Observation of security data flow after introduction of malware**

The course begins with an analysis of the current cybersecurity landscape and includes details on why networks today need an integrated threat defense architecture. You will integrate and verify proper operation of the key Cisco Integrated Threat Defense products, including Cisco Identity Services Engine (ISE), Cisco Stealth watch®, Cisco Firepower® NGFW, and Cisco AMP for Endpoints. Verification includes the introduction of malware into the network to ensure proper identification, analysis, and quarantine. This course combines lecture materials and hands-on labs that give you practice in configuring the solution integrations.

Who should attend?

This course is designed for technical professionals who need to know how to deploy a Cisco Integrated Threat Defense solution in their network environment. The primary audience for this course includes:

1. **Systems and network engineers**
2. **Technical architects**
3. **Technical support personnel**
4. **Channel partners and resellers**

Prerequisites

Cisco recommends that you have the following knowledge and skills before taking this course:

1. **Technical understanding of TCP/IP networking and network architecture**
2. **Technical understanding of security concepts and protocols**
3. **Familiarity with Cisco ISE, Stealth watch, Firepower, and AMP is an advantage**

Course Objectives

After completing this course, you should be able to:

1. **Describe the current network security landscape and the Cisco Integrated Threat Defense (ITD) solution**
2. **Describe the key components of the ITD solution and their use in the network**
3. **Configure the ISE for a baseline of operation in the ITD solution**
4. **Configure the integration between the Stealthwatch and ISE platforms**
5. **Configure the integration between the Cisco Firepower and ISE platforms**
6. **Configure the integration between Cisco Firepower and AMP for Endpoints**

Course Content

1. **Module 1: Integrated Threat Defense Introduction**
2. **Module 2: ITD Products**
3. **Module 3: Identity Services Engine Setup**
4. **Module 4: Integration of Stealth watch with Identity Services Engine**
5. **Module 5: Integration of Firepower with Identity Services Engine**
6. **Module 6: Integration of Firepower with AMP for Endpoints**