Integrated Threat Defense Investigation and Mitigation (SECUR202)

Duration: 2 days

Course Overview

The Cisco Integrated Threat Defense Investigation and Mitigation (SECUR202) course is an instructor-led, lab-based, hands-on course offered by Cisco® Learning Services. The overall course goal is to enable students to identify, isolate, and mitigate network threats using the Cisco Integrated Threat Defense solution platforms. This course is the second in a pair of courses covering the Cisco Integrated Threat Defense solution.

This course will introduce students to network threat investigation and then reinforce student learning through a series of lab scenarios designed to identify relationships between the Cisco products and the stages of the attack lifecycle.

Who should attend?

This course is designed for technical professionals who need to know how to use a deployed Integrated Threat Defense (ITD) network solution to identify, isolate, and mitigate network threats. The primary audience for this course includes:

1. Network analysts
2. Network investigators

Prerequisites

The knowledge and skills that a student must have before attending this course are as follows:

1. Technical understanding of TCP/IP networking and network architecture
2. Technical understanding of security concepts and protocols
3. Familiarity with Cisco Identity Services Engine, Cisco Stealthwatch®, Cisco Firepower®, and Cisco AMP for Endpoints is an advantage

Course Objectives

Upon completion of this course, you should be able to:

1. Describe the stages of the network attack lifecycle and identify ITD solution platform placement based on a given stage
2. Detail how to locate and mitigate email malware attacks
3. Describe email phishing attacks and the steps taken to locate and mitigate them on the network
4. Identify and mitigate data exfiltration threats on the network

5. **Identify malware threats on the network and mitigate those threats after investigation**

Course Content

Module 1: Network Threat Investigation Introduction

Network Attack Introduction
Hunting Network Threats in the Enterprise

Module 2: Investigation and Mitigation of Email Malware Threats

Examining Email Malware Threats
Investigating and Verifying Email Malware Threat Mitigation

Module 3: Investigation and Mitigation of Email Phishing Threats

Examining Email Phishing Attacks
Configuring Cisco ESA for URL and Content Filtering
Investigating and Verifying Email Phishing Threat Mitigation

Module 4: Investigation and Mitigation of Data Exfiltration Threats

Exploiting Vulnerable Network Servers
Investigating Data Exfiltration Threats
Mitigating and Verifying Data Exfiltration Threats

Module 5: Investigation and Mitigation of Malware Threats

Examining Endpoint Malware Protection
Investigating and Mitigating Endpoint Malware Threats