Integrated Threat Defense Investigation and Mitigation (SECUR202) v1.0

What you'll learn in this course

The **Cisco Integrated Threat Defense Investigation and Mitigation** (SECUR202) v1.0 course shows you how to identify, isolate, and mitigate network threats using the Cisco® Integrated Threat Defense solution platform. Through expert instruction and lab-based scenarios, you will be introduced to network threat investigation, and learn how to identify relationships between Cisco products and the stages of the attack lifecycle. This course is the second in a pair of courses (SECUR201) covering the Cisco Integrated Threat Defense (ITD) solution.

Course duration

- Instructor-led training: 2 days in the classroom with hands-on lab practice
- Virtual instructor-led training: 2 days of web-based classes with hands-on lab practice
- E-learning: Equivalent of 2 days of instruction with videos and practice

How you'll benefit

This course will help you:

- Gain hands-on practice with Cisco's Integrated Threat Defense solutions
- Gain leading-edge career skills for high-demand job roles and responsibilities focused on enterprise security

Who should enroll

- Network analysts
- Network investigators
- Cisco integrators and partners

How to enroll

- For instructor-led training, visit the Cisco Learning Locator.
- For private group training, visit Cisco Private Group Training.
- For digital library access visit Cisco Platinum Learning Library.
- For e-learning volume discounts, ask_cpll@cisco.com.

Technology areas

- Security

Course details

Objectives

After taking this course, you should be able to:

- Describe the stages of the network attack lifecycle and identify ITD solution platform placement based on a given stage
- Detail how to locate and mitigate email malware attacks
- Describe email phishing attacks and the steps taken to locate and mitigate them on the network
- Identify and mitigate data exfiltration threats on the network
- Identify malware threats on the network and mitigate those threats after investigation

Prerequisites

To fully benefit from this course, you should have the following knowledge:

- Technical understanding of TCP/IP networking and network architecture
- Technical understanding of security concepts and protocols
- Familiarity with Cisco Identity Services Engine, Cisco Stealthwatch®, Cisco Firepower®, and Cisco Advanced Malware Protection (AMP) for Endpoints is an advantage

Outline

- Network Threat Investigation Introduction
  - Network Attack Introduction
  - Hunting Network Threats in the Enterprise
- Investigation and Mitigation of Email Malware Threats
  - Examining Email Malware Threats
  - Investigating and Verifying Email Malware Threat Mitigation
- Investigation and Mitigation of Email Phishing Threats
  - Examining Email Phishing Attacks
  - Configuring Cisco Email Security Appliance (ESA) for URL and Content Filtering
  - Investigating and Verifying Email Phishing Threat Mitigation
- Investigation and Mitigation of Data Exfiltration Threats
  - Exploiting Vulnerable Network Servers
  - Investigating Data Exfiltration Threats
  - Mitigating and Verifying Data Exfiltration Threats
- Investigation and Mitigation of Malware Threats
  - Examining Endpoint Malware Protection
  - Investigating and Mitigating Endpoint Malware Threats

Lab outline

- Connecting to the Lab Environment
- Threat Scenario 1—Email Malware Attachments
- Threat Scenario 2—Email-Based Phishing
- Threat Scenario 3—Targeted Network Server Threats and Data Exfiltration
- Threat Scenario 4—Endpoint Malware Investigation and Mitigation