Contact:
Info@silverlake.sg
+65 - 65882456

# Cisco Integrated Threat Defense Investigation and Mitigation

**Course#:SECUR202**
**Duration:2 Days**
**Price:0.00**

## Course Description

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. This course is the second in a pair of courses covering the Cisco Integrated Threat Defense (ITD) solution.

## Objectives

Upon completion of 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

## Audience

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:

- Network analysts
- Network investigators

## Prerequisites

The knowledge and skills that a student must have before attending this course include:

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 AMP for Endpoints

SECUR201 - Implementing an Integrated Threat Defense Solution

## Content

Virtual Classroom Live Outline

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

Virtual Classroom Live Labs

Lab 1: Connecting to the Lab Environment
Lab 2: Threat Scenario 1: Email Malware Attachments
Lab 3: Threat Scenario 2: Email-Based Phishing
Lab 4: Threat Scenario 3: Targeted Network Server Threats and Data Exfiltration
Lab 5: Threat Scenario 4: Endpoint Malware Investigation and Mitigation