Learning@Cisco

Integrated Threat Defense Investigation and Mitigation (SECUR202)

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.

Duration

Instructor-Led Training (ILT): 2 days

Virtual Instructor-Led Training (VILT): 2 days

Target 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

Course 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

Course prerequisites

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

- 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 is an advantage

Course outline

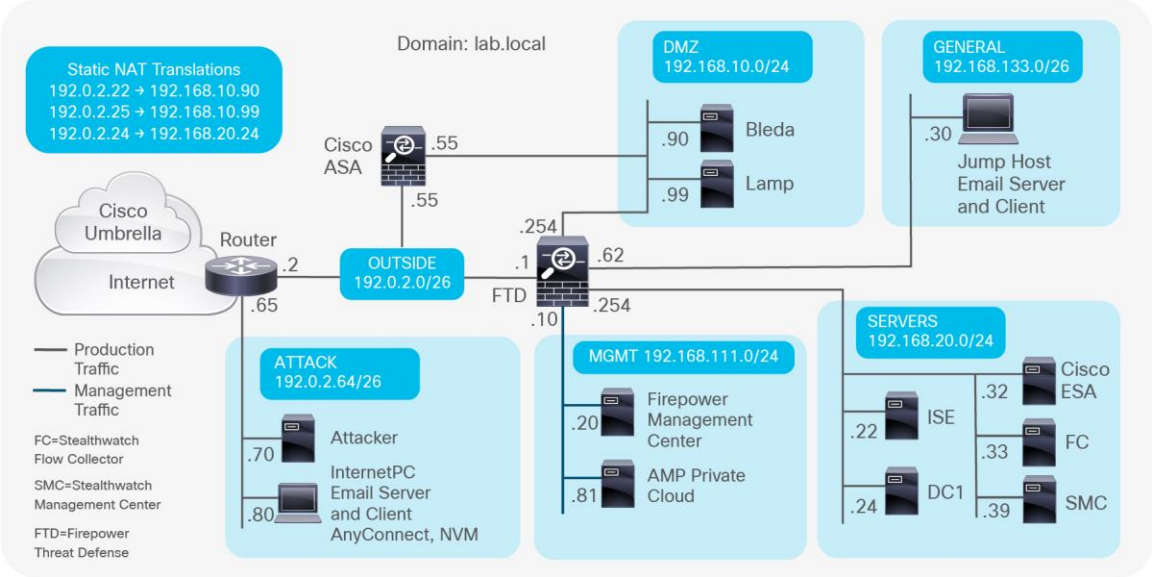
- Module 1: Network Threat Investigation Introduction
  - Network Attack Introduction
  - Hunting Network Threats in the Enterprise
- Module 2: Investigation and Mitigation of Email Malware Threats
  - Examining Email Malware Threats
  - Investigating and Verifying Email Malware Threat Mitigation
- Module 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

Lab outline

- 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

Lab topology



Registration email

For more information about schedules and registration for this course, contact aeskt_registration@cisco.com.

Cisco Capital financing helps you achieve your objectives

Cisco Capital® financing can help you acquire the technology you need to achieve your objectives and stay competitive.

We can help you reduce Capital Expenditures (CapEx), accelerate your growth, and optimize your investment dollars and ROI. Cisco Capital financing gives you flexibility in acquiring hardware, software, services, and complementary third-party equipment. And there's just one predictable payment. Cisco Capital financing is available in more than 100 countries. Learn more.

Website addresses for more information

For more information, visit the following websites:

- Cisco Learning Services for Cisco products and technologies: https://www.cisco.com/go/cls
- Security training: https://www.cisco.com/c/en/us/training-events/resources/learning-services/technology/security.html
- Data center training: https://www.cisco.com/c/en/us/training-events/resources/learning-services/technology/data-center.html
- Network management training: https://www.cisco.com/c/en/us/training-events/resources/learning-services/technology/network-management.html

- Optical networking training: https://www.cisco.com/c/en/us/training-events/resources/learning-services/technology/optical.html
- Service provider mobility training: https://www.cisco.com/c/en/us/training-events/resources/learning-services/technology/mobile.html
- Routing training for service providers: https://www.cisco.com/c/en/us/training-events/resources/learning-services/technology/service-provider-routing.html
- Broadband video training for service providers: https://www.cisco.com/c/en/us/training-events/resources/learning-services/technology/service-provider-video.html

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **https://www.cisco.com/go/offices**.

Printed in USA **Course version: SECUR202_1-0** C78-740025-00 01/18