Implementing an Integrated Threat Defense Solution (SECUR201) v1.0

What you'll learn in this course

The **Implementing an Integrated Threat Defense Solution** (SECUR201) v1.0 course shows you how to deploy and integrate Cisco®'s Integrated Threat Defense solutions. This hands-on course provides you with the knowledge and skills to implement and integrate solution components with existing network services, integrate solution components with the pxGrid (Platform Exchange Grid) framework, integrate network and endpoint-based malware protection, and observation of security dataflow after the introduction of malware.

Course duration

- Instructor-led training: 2 days in the classroom with hands-on lab practice
- Virtual instructor-led training: 2.5 days of web-based classes with hands-on lab practice
- E-learning: Equivalent of 2.5 days of instruction with videos and practice

How you'll benefit

This course will help you:

- Gain hands-on practice integrating 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

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

- Systems and network engineers
- Technical architects
- Technical support personnel
- 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 to SECUR201 v1.0, 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 current network security landscape and the Cisco Integrated Threat Defense (ITD) solution
- Describe the key components of the ITD solution and their use in the network
- Configure the Cisco Identity Services Engine (ISE) for a baseline of operation in the ITD solution
- Configure the integration between the Cisco Stealthwatch® and Cisco ISE platforms
- Configure the integration between the Cisco Firepower® and ISE platforms
- Configure the integration between Cisco Firepower and Cisco Advanced Malware Protection (AMP) for Endpoints

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 ISE, Stealthwatch, Firepower, and AMP

Outline

- Integrated Threat Defense Introduction
- ITD Products
- Identity Services Engine Setup
- Integration of Stealthwatch with Identity Services Engine
- Integration of Firepower with Identity Services Engine
- Integration of Firepower with AMP for Endpoints

Lab outline

- Connecting to the Lab Environment
- Integrating ISE and Active Directory
- Integrating ISE and Cisco Adaptive Security Appliance (ASA)
- Configuring pxGrid and Client Certificates
- Integrating Stealthwatch with Identity Services Engine
- Integrating Network Visibility Module (NVM) with AnyConnect
- Integrating Firepower with Identity Services Engine
- Integrating AMP for Endpoints with Firepower