email : techcenter@trainocate.com.my
contact : +603-2281-1111

SECUR201: Implementing an Integrated Threat Defense Solution

Course Code: SECUR201
Duration: 2 days
Instructor-led Training (ILT) | Virtual Instructor-led Training (VILT)

OVERVIEW

The Implementing an Integrated Threat Defense Solution (SECUR201) v1.2 course provides an analysis of the cybersecurity landscape with an emphasis on the importance of an integrated threat defense architecture. Through a combination of lessons and hands-on practice, you will learn to deploy and integrate Cisco®'s Integrated Threat Defense solutions which include: Cisco Identity Services Engine (ISE), Cisco Stealthwatch, Cisco Firepower NGFW, and Cisco AMP for Endpoints. This 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.

SKILLS COVERED

After taking this course, you should be able to:

- Understand the network security landscape and the Cisco Integrated Threat Defense (ITD) solutions
- 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

WHO SHOULD ATTEND?

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

- Cisco integrators and partners
- Systems and network engineers
- Technical architects
- Technical support personnel

PRE-REQUISITES

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

- Technical understanding of TCP/IP networking and network architecture including DNS, SSH, FTP, SNMP, HTTP, and HTTPS
- Technical understanding of security concepts and protocols
- Familiarity with Cisco ISE, Stealthwatch, Firepower, and AMP

The following course can help you meet these prerequisites:

- Implementing and Administering Cisco Solutions (CCNA)

MODULES

Content

- 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

END OF PAGE