Cisco® Implementing Cisco® Threat Control Solutions v1.5 (SITCS1)

Course Overview

Implementing Cisco Threat Control Solutions (SITCS) v1.5 is part of the curriculum path leading to the Cisco Certified Network Professional Security (CCNP Security) certification. Additionally, it is designed to prepare security engineers with the knowledge and hands-on experience so that they can deploy Ciscos Next Generation Firewall (NGFW) as well as Web Security, Email Security and Cloud Web Security.

Who Should Attend

Network Security Engineers

Course Objectives

Understand Cisco ASA Next-Generation Firewall (NGFW). Deploy Cisco Web Security appliance to mitigate malware. Configure Web Security appliance for acceptable use controls. Configure Cisco Cloud Web Security Connectors. Describe Cisco Email Security Solution. Configure Cisco Email Appliance Incoming and Outgoing Policies. Describe IPS Threat Controls. Configure and Implement Cisco IPS Sensor into a Network.

Other Prerequisites

Cisco Certified Network Associate (CCNA) certification
Cisco Certified Network Associate (CCNA) Security certification
Knowledge of Microsoft Windows operating system

Course Outline

1 Course Introduction

2 Cisco ASA (CX) NGFW

Lesson 1: Describing the Cisco Modular Network Architecture
Lesson 2: Describing the Cisco ASA (CX) NGFW Management Architecture
Lesson 3: Configure Cisco ASA (CX) NGFW Policy Objects
Lesson 4: Monitoring Cisco ASA (CX) NGFW Operations
Lesson 5: Configuring Cisco ASA (CX) NGFW Access Policies
Lesson 6: Configuring Cisco ASA (CX) NGFW Identity Policies
Lesson 7: Configuring Cisco ASA (CX) NGFW Access Decryption Policies
Lesson 8: Module Summary

This is a 5-day class

800.683.NHLS (6457)
nhls.com

Cisco® Implementing Cisco® Threat Control Solutions v1.5 (SITCS1)

3   Cisco Web Security Appliance

Lesson 1: Describing The Cisco Web Security Appliance (WSA) Solutions
Lesson 2: Integrating the Cisco Web Security Appliance
Lesson 3: Configuring Cisco Web Security Appliance Identities and User Authentication Controls
Lesson 4: Configuring Cisco Web Security Appliance Acceptable Use Control
Lesson 5: Configuring Cisco Web Security Appliance Anti-Malware Controls
Lesson 6: Configuring Cisco Web Security Appliance Decryption
Lesson 7: Configuring Cisco Web Security Appliance Data Security Controls
Lesson 8: Module Summary

4   Cisco Cloud Web Security

Lesson 1: Describing the Cisco Cloud Web Security Solution
Lesson 2: Configuring Cisco Cloud Web Security Connectors
Lesson 3: Describing the Web Filtering Policy in Cisco ScanCenter
Lesson 4: Module Summary

5   Cisco Email Security Appliance

Lesson 1: Describe the Cisco Email Security Solutions
Lesson 2: Describing the Cisco Email Security Appliance Basic Configuration
Lesson 3: Deploying Cisco ASA Application Inspection Policies
Lesson 4: Summary

6   Cisco Intrusion Prevention Systems - Lab Guide

Lesson 1: Describing IPS Threat Controls
Lesson 2: Integrating Cisco IPS Sensor into a Network
Lesson 3: Configuring Basic Cisco IPS Settings
Lesson 4: Tuning Cisco IPS Signatures
Lesson 5: Configuring Custom Cisco IPS Signatures
Lesson 6: Configuring Cisco IPS Anomaly-Detection
Lesson 7: Configuring Cisco IPS Reputation-Based Features
Lesson 8: Summary