FIREFLY

CONTACT US

Implementing Cisco Threat Control Solutions

DURATION: 5 DAYS COURSE CODE: SITCS FORMAT: LECTURE/LAB

COURSE DESCRIPTION

Implementing Cisco Threat Control Solutions (SITCS) v1.5 is an updated five-day instructor-led training course, which 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 Cisco's Email Security (ESA); Web Security (CWS, WSA); advanced Malware Protection (AMP); and Next Generation Intrusion Prevention Systems (NGIPS).

The goal of the course is to provide students with foundational knowledge and the capabilities to implement and manage security threat controls by leveraging the capabilities of Cisco's FirePOWER NGIPS, AMP, WSA, WS, and ESA products and solutions.

Students will gain hands-on experience with configuring various advanced Cisco security solutions to mitigate outside threats, and to secure traffic traversing the network and security systems. This course can provide a valuable learning experience for students studying to pass the SITCS Exam #300-210.

WHO SHOULD ATTEND

Job Roles for SITCS v1.5 remain the same as they were for SITCS v1.0 –only the technology has evolved o include "SourceFIRE" based technologies, and older, EOL'ed products have been removed from the labs.

Typical Job Roles for the CCNP Security candidate include "Network Security Engineer", among others.

PREREQUISITES

This section lists the skill, knowledge, and attitudes that learners must possess to benefit fully from the course. It includes recommended Cisco learning offerings that the learner may complete to benefit fully from this course.

CCNA Security or valid CCSP or any CCIE certification can act as a prerequisite

LEARNING OBJECTIVES

Describe and implement Cisco Web Security Appliance (WSA)

Describe and implement Cisco Cloud WebSecurity (CWS)

Describe and implement Cisco Email Security Appliance (ESA)

Describe and implement Advanced Malware Protection (AMP)

Describe and implement Cisco FirePOWER Next-Generation IPS

Describe and implement Cisco ASA FirePOWER Services Module

COURSE OUTLINE

1. Cisco Web Security Appliance

- Describing the Cisco Web Security Appliance Solutions
- Integrating the Cisco Web Security Appliance
- Configuring Cisco Web Security Appliance Identities and User Authentication Controls
- Configuring Cisco Web Security Appliance Acceptable Use Controls
- Configuring Cisco Web Security Appliance Anti-Malware
- Controls Configuring Cisco Web Security Appliance Decryption
- Configuring Cisco Web Security Appliance Data Security Controls

2. Cisco Cloud Web Security

- Describing the Cisco Cloud Web Security Solutions
- Configuring Cisco Cloud Web Security Connectors
- Describing the Web Filtering Policy in Cisco ScanCenter

3. Cisco Email Security Appliance

- Describing the Cisco Email Security Solutions
- Describing the Cisco Email Security Appliance Basic Setup Components
- Configuring Cisco Email Security Appliance Basic Incoming and Outgoing Mail Policies

4. Advanced Malware Protection for Endpoints

- AMP for Endpoints Overview and Architecture
- Customizing Detection and AMP Policy
- IOCs and IOC Scanning
- Deploying AMP Connectors
- AMP Analysis Tools

5. Cisco FirePOWER Next-Generation IPS

- Describing the Cisco FireSIGHT System
- Configuring and Managing Cisco FirePOWER Devices
- Implementing an Access Control Policy
- Understanding Discovery Technology
- Configuring File-Type and Network Malware Detection
- Managing SSL Traffic with Cisco FireSIGHT
- Describing IPS Policy and Configuration Concepts
- Describing the Network Analysis Policy
- Creating Reports
- Describing Correlation Rules and Policies
- Understanding Basic Rule Syntax and Usage

6. Cisco ASA FirePOWER Services Module

- Installing Cisco ASA 5500-X Series FirePOWER Services (SFR) Module

DISCOVERY LABS

1: Configure Cisco Web Security Appliance Explicit Proxy and User Authentication
2: Configure Cisco Web Security Appliance Acceptable Use Controls
3: Configure Cisco Email Security Appliance Basic Policies
4: Configure Cisco Email Security Appliance Basic Policies
5: Customizing Detection and AMP Policy
6: IOCs and IOC Scanning
7: Deploying AMP Connectors
8: AMP Analysis Tools
9: Configure Inline Interfaces and Create Objects
10: Create Access Control Policy Rules
11: Configure Network Discovery Detection
12: Create a File Policy
13: Create an Intrusion Policy
14: Create a Network Analysis Policy
15: Compare Trends
16: Create Correlation Policies