Implementing Cisco Threat Control Solutions (SITCS) 1.5

Course Overview:

Implementing Cisco Threat Control Solutions (SITCS) v1.5 is a 5-day instructor led course that provides network professional with the knowledge to implement Cisco FirePOWER NGIPS (Next-Generation Intrusion Prevention System) and Cisco AMP (Advanced Malware Protection), as well as Web Security, Email Security and Cloud Web Security. You will gain hands-on experience configuring various advance Cisco security solutions for mitigating outside threats and securing traffic traversing the firewall.

Who Should Attend:

- Network Security Engineers

Prerequisites:

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

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

Course Objectives:

Upon completing this course, the learner will be able to meet these overall objectives:

- Describe and implement Cisco Web Security Appliance
- Describe and implement Cloud Web Security
- Describe and implement Cisco Email Security Appliance
- Describe and implement Advanced Malware Protection
- Describe and implement Cisco FirePOWER Next-Generation IPS
- Describe and implement Cisco ASA FirePOWER Services Module

Course Outline:

Module 1: Cisco Web Security Appliance

- Lesson 1: Describing the Cisco Web Security Appliance 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 Controls
- 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

Module 2: Cisco Cloud Web Security

- Lesson 1: Describing the Cisco Cloud Web Security Solutions
- Lesson 2: Configuring Cisco Cloud Web Security Connectors
- Lesson 3: Describing the Web Filtering Policy in Cisco ScanCenter

Module 3: Cisco Email Security Appliance

- Lesson 1: Describing the Cisco Email Security Solutions
- Lesson 2: Describing the Cisco Email Security Appliance Basic Setup Components
- Lesson 3: Configuring Cisco Email Security Appliance Basic Incoming and Outgoing Mail Policies

Module 4: Advanced Malware Protection for Endpoints

- Lesson 1: AMP for Endpoints Overview and Architecture
- Lesson 2: Customizing Detection and AMP Policy
- Lesson 3: IOCs and IOC Scanning
- Lesson 4: Deploying AMP Connectors
- Lesson 5: AMP Analysis Tools

Module 5: Cisco FirePOWER Next-Generation IPS

- Lesson 1: Describing the Cisco FireSIGHT System
- Lesson 2: Configuring and Managing Cisco FIrePOWER Devices
- Lesson 3: Implementing an Access Control Policy
- Lesson 4: Understanding Discovery Technology
- Lesson 5: Configuring File-Type and Network Malware Detection
- Lesson 6: Managing SSL Traffic with Cisco FireSIGHT
- Lesson 7: Describing IPS Policy and Configuration Concepts
- Lesson 8: Describing the Network Analysis Policy
- Lesson 9: Creating Reports
- Lesson 10: Describing Correlation Rules and Policies

- Lesson 11: Understanding Basic Rule Syntax and Usage

Module 6: Cisco ASA FirePOWER Services Module

- Lesson 1: Installing Cisco ASA 5500-X Series FirePOWER Services (SFR) Module

Lab Outline:

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