# Implementing Cisco Threat Control Solutions (CS-SITCS) 1.0

**Modality: Virtual Classroom**

**Duration: 2 Days**

**CLC: 25 Units**

## About this course:

Implementing Cisco Threat Control Solutions (SITCS) v1.0 is a newly created 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 Next Generation Firewall (NGFW) as well as Web Security, Email Security and Cloud Web Security. The goal of the course is to provide students with foundational knowledge and the capabilities to implement and managed security on Cisco ASA firewalls utilizing Cisco Next Generation product solution which integrates Cisco Prime Security Manager for managing identity policies. The student will gain hands-on experience with configuring various advance Cisco security solutions for mitigating outside threats and securing traffic traversing the firewall. At the end of the course, students will be able to reduce the risk to their IT infrastructures and applications using Cisco's Next Generation Firewall security appliance feature and provide operational support for Intrusion Prevention Systems, Email Security, and Web based security appliances. This course also prepares the students for Cisco: 300-210 SITCS exam.

The Implementing Cisco Threat Control Solutions (SITCS) V1.0 is a freshly introduced instructor-led training course, that lasts five days. It is a section of the curriculum path that leads to the achievement of the Cisco Certified Network Professional Security (CCNP Security) certification. The course has been designed to help the engineers prepare for Cisco’s Next Generation Firewall, Email Security, Web Security, and Cloud Web Security, through hands-on lecture and theoretical knowledge.

The aim of the course is to supply the candidates with fundamental information and skills that will allow them to apply and conserve security on Cisco ASA firewalls through the use of Cisco Next Generation product solution which will include the Cisco Prime Security Manager to supervise identity policies. The students will receive practical experience when it comes to setting up of several Cisco advanced level security solutions to lessen external threats while make sure that the traffic crossing the firewall is secure. By the end of the course the students will be enables to appease the risks posed to their applications and IT infrastructures through the use of Cisco’s Next Generation Firewall Security appliance feature and also supply functional assistance for the Intrusion Preventions Systems, Web based security appliances, and email security.

Furthermore, with the help of this course the students will be able to prepare for the Cisco: 300-21 SITCS exam.

This course is part of the following Boot Camps:

- CS-CCNP-Sec - 14-Day Official CCNP Security + CCNA Security Dual-Certification Boot

Camp.

The average salary for Cisco Systems Network Security Engineer is **$91,175** per year.

## Course Objectives:

- Cisco ASA NGFW
- Deploy and configure Cisco Web Security Appliance
- Setup and employ Cisco Web Security Appliance
- Configure Cisco Cloud Web Security Connectors
- Cisco Email Security solution
- Configure Cisco Email Appliance incoming and outgoing policies
- Cisco IPS Threat Control
- Configure and Implement Cisco IPS Sensor into a network

## Audience:

- Network security engineers

## Prerequisites:

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

## Suggested prerequisite courses:

- CS-CCNA-Sec CCNA Security Boot Camp: Implementing Cisco IOS Network Security (IINS) (CS-CCNA-Sec)
- Implementing Cisco Secure Access Solutions (SISAS)

## 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