IMPLEMENTING CISCO THREAT CONTROL SYSTEMS

DURATION: 5 DAYS

COURSE OVERVIEW

Implementing Cisco Threat Control Solutions is designed to provide security engineers with the knowledge and hands-on experience required to deploy Cisco's Email Security (ESA); Web Security (CWS, WSA); Advanced Malware Protection (AMP); and Next Generation Intrusion Prevention Systems (NGIPS).

Students will learn how to implement and manage security threat controls by leveraging the capabilities of Cisco's Fire POWER NGIPS, AMP, WSA, CWS, and ESA products and solutions. The hands-on labs will provide experience in configuring advanced Cisco security solutions to mitigate outside threats, and to secure traffic traversing the network and security systems.

TARGET AUDIENCE

This course is aimed at engineers involved in the implementation and support of Cisco Security Solutions that include NGIPS and AMP, Web Security. Email Security and Cloud Web Security Appliances. This course is also required for engineers looking to achieve the Cisco Certified Network Professional Certification for Security.

COURSE OBJECTIVES

After completing this course you should be able to:

1. Describe and Implement Cisco Web Security Appliance (WSA)
2. Describe and Implement Cisco Web Security(CWS)
3. Describe and Implement Cisco Email Security Appliance(ESA)
4. Describe and Implement Advanced Malware Protection(AMP)
5. Describe and Implement Cisco Fire Power Next-Generation IPS
6. Describe and Implement Cisco ASA Fire Power Services Module

COURSE CONTENT

Cisco Web Security Appliance

1. Describing The Cisco Web Security Appliance (WSA) Solutions
2. Integrating the Cisco Web Security Appliance

3. Configuring Cisco Web Security Appliance Identities and User Authentication Controls
4. Configuring Cisco Web Security Appliance Acceptable Use Control
5. Configuring Cisco Web Security Appliance Anti-Malware Controls
6. Configuring Cisco Web Security Appliance Decryption
7. Configuring Cisco Web Security Appliance Data Security Controls

Cisco Cloud Web Security

1. Describing the Cisco Cloud Web Security Solutions
2. Configuring Cisco Cloud Web Security Connectors
3. Describing the Web Filtering Policy in Cisco Scan Center

Cisco Email Security Appliance

1. Describe the Cisco Email Security Solutions
2. Describing the Cisco Email Security Appliance Basic Setup Components
3. Configuring Cisco Email Security Appliance Basic Incoming and Outgoing Mail Policies

Advanced Malware Protection for Endpoints

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

Cisco Fire POWER Next-Generation IPS

1. Describing the Cisco Fire SIGHT System
2. Configuring and Managing Cisco Fire POWER Devices
3. Implementing an Access Control Policy
4. Understanding Discovery Technology
5. Configuring File-Type and Network Malware Detection
6. Managing SSL Traffic with Cisco Fire SIGHT
7. Describing IPS Policy and Configuration Concepts
8. Describing the Network Analysis Policy
9. Creating Reports
10. Describing Correlation Rules and Policies
11. Understanding Basic Rule Syntax and Usage

Cisco ASA Fire POWER Services Module

1. Installing Cisco ASA 5500-X Series Fire POWER Services (SFR) Module

Labs

Lab 1: Configure Cisco Web Security Appliance Explicit Proxy and User Authentication

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

COURSE PREREQUISITES

Attendees should meet the following prerequisites:

1. Cisco Certified Network Associate Certification **ICND1** and **ICND2** or **CCNABC**
2. Cisco Certified Network Associate Security Certification **ICND1** and **IINS**
3. Knowledge of Microsoft Windows operating system

TEST CERTIFICATION

Recommended Preparation for Exam(s):

300-210 - Implementing Cisco Threat Control Solutions Exam

FOLLOW ON COURSES

Delegates looking to achieve the Cisco Certified Network Professional Certification for Security should also attend the following courses.

1. **SENSS** - Implementing Cisco Edge Network Security Solutions
2. **SISAS** - Implementing Cisco Secure Access Solutions
3. **SIMOS** - Implementing Cisco Secure Mobility Solutions