SITCS (IMPLEMENTING CISCO THREAT CONTROL SOLUTIONS)

Objetivo

Implementing Cisco Threat Control Solutions (SITCS) versão 1.5 é um treinamento que faz parte da grade de certificação CCNP Security. Este curso visa preparar os engenheiros em segurança de rede com o conhecimento e as habilidades que eles precisam para que possam implantar o Cisco ASA Next Generation Firewall (NGFW) e o Cisco Prime Security Manager, prover segurança com Cisco WSA (Web Security Appliance) e Cisco ESA (Email Security Appliance) e a integração do ASA com o serviço Cisco Cloud Web Security. O aluno vai ganhar experiência hands-on com a configuração de várias soluções de segurança avançada Cisco para mitigar ameaças externas e proteger o tráfego que atravessa o firewall. No final do curso, os alunos serão capazes de reduzir o risco de suas infraestruturas de TI e aplicações usando os recursos do Cisco ASA NGFW, NGIPS, do Cisco WSA e do Cisco ESA. Depois de concluir este curso, os alunos serão capazes de: • Entender o Cisco ASA Next-Generation Firewall (NGFW); • Implantar o Cisco Web Security Appliance para mitigar malwares; • Configurar o Cisco Web Security Appliance para controles de acesso a Web; • Configurar e integrar o ASA com serviço Cisco Cloud Web Security; • Descrever a solução para Email da Cisco (ESA); • Configurar o Cisco ESA (Email Appliance) com Políticas de inspeção na entrada e saída de Email; • Descrever o IPS e suas funcionalidades; • Configurar e Implantar o Cisco IPS em uma rede.

Público Alvo

• O público principal deste curso são os responsáveis em projetar, implantar e fornecer suporte em segurança utilizando o conjunto de soluções da Cisco. Esse curso faz parte dos cursos preparatórios para a certificação CCNP Security.

Pré-Requisitos

Para aproveitar ao máximo este curso, é recomendável que os alunos possuam as seguintes habilidades e conhecimentos: • Ter participado no curso ICND 1 ou possuir conhecimentos equivalentes; • Ter participado no curso IINS ou possuir conhecimentos equivalentes; • Conhecimento do sistema operacional Microsoft Windows

Carga Horária

40 horas (5 dias).

Conteúdo Programático

Course Introduction

Cisco Web Security Appliance
• Describe how to implement the Cisco Web Security Appliance.

- Describing the Cisco Web Security Appliance Solutions
- Describe the Cisco Web Security Appliance main features

Cisco Modular Network Architecture and Cisco WSA
- Cisco WSA Overview
- Cisco WSA Architecture
- Cisco WSA Malware Detection and Protection
- Cisco Web-Based Reputation Score
- Cisco WSA Acceptable Use Policy Enforcement
- Cisco WSA GUI Management
- Cisco WSA Committing the Configuration Changes
- Cisco WSA Policy Types Overview
- Cisco WSA Access Policies
- Cisco WSA Identity: To Whom Does This Policy Apply?
- Cisco WSA Identity Example
- Cisco WSA Policy Assignment Using Identity
- Cisco WSA Identity and Authentication
- Cisco WSA Policy Trace Tool

Integrating the Cisco Web Security Appliance
- Explicit vs. Transparent Proxy Mode
- Explicit Proxy Mode
- PAC Files
- PAC File Deployment Options
- PAC File Hosting on Cisco WSA
- Traffic Redirection In Transparent Mode
- Connecting the Cisco WSA to a WCCP Router
- Verifying WCCP

Configuring Cisco Web Security Appliance Identities and User Authentication Controls
- Configure Identities to Group Client Transactions
- Configure Policy Groups
- The Need for User Authentication
- Authentication Protocols and Schemes
- Basic Authentication in Explicit Proxy and Transparent Proxy Mode
- Configure Realms and Realm Sequences
- Configure NTLM Realm for Active Directory
- Join Cisco WSA to Active Directory
- Configure Global Authentication Settings
- Configure an Identity to Require Authentication (Basic or NTLMSSP)
- Configure an Identity to Require Transparent User Identification
- Configure LDAP Realm for LDAP Servers
- Define How User Information Is Stored in LDAP
- Bind Cisco WSA to the LDAP Directory
- LDAP Group Authorization
- Allowing Guest Access to Users Who Fail Authentication
- Testing Authentication Settings
- Authenticated Users in Reports

• Guided Lab 1: Configure Cisco Web Security Appliance Explicit Proxy and User Authentication Web-related connectivity.

Configuring Cisco Web Security Appliance Acceptable Use Controls
• Acceptable Use Controls
• URL Categorizing Process
• Application Visibility and Control Overview
• Streaming Media Bandwidth Control Overview
• Enable Acceptable Use Controls
• Using the Policies Table
• Configure URL Filtering
• Enable Safe Search and Site Content Ratings
• Configure Custom URL Categories
• URL Category Reports
• Configuring AVC
• Configure Media Bandwidth Limits
• AVC Reports

Configuring Cisco Web Security Appliance Anti-Malware Controls
• Dynamic Vectoring and Streaming Engine Overview
• Contrast Webroot with Sophos or McAfee Malware Scanning
• Adaptive Scanning Overview
• Web Reputation Filtering Overview
• Enable Web Reputation Filtering, Adaptive Scanning and Malware Scanning
• Scanning Engines
• Configure Inbound Web Reputation Filtering and Malware Scanning
• Configure Outbound Malware Scanning
• Malware Reports

Configuring Cisco Web Security Appliance Decryption
• HTTPS Proxy Operations Overview
• Enable HTTPS Proxy
• Invalid Destination Web Server Certificate Handling
• Configure Decryption Policies
• Guided Lab 2: Configure Cisco Web Security Appliance Acceptable Use Controls

Configuring Cisco Web Security Appliance Data Security Controls
• Cisco WSA Data Security Overview
• Data Security Policies
• Control Uploaded Content
• External Data Loss Prevention
• Add an ICAP Server

Cisco Cloud Web Security
• Describing the Cisco Cloud Web Security Solutions
• Cisco Modular Network Architecture and Cisco Cloud Web Security (CWS)
• Cisco Cloud Web Security Overview
• Cisco Cloud Web Security Traffic Flow Overview

• Cisco Cloud Web Security URL Filtering, AVC, and Reporting Features Overview
• Cisco Cloud Web Security Scanning Processes and Day Zero Outbreak Intelligence Overview
• Cisco ScanCenter Overview

Configuring Cisco Cloud Web Security Connectors
• Describe traffic redirection to Cloud Web Security through connectors, how to configure them on Cisco ASA, Cisco WSA and Cisco IOS, and how to configure AnyConnect web security module
• Cisco Cloud Web Security Traffic Redirection Overview
• Cisco Cloud Web Security Authentication Key
• Authentication Key Generation from the Cisco ScanCenter
• Verifying Traffic Redirection to CWS Using Special URL
• Cisco ASA Cloud Web Security Overview
• Cisco ASA Cloud Web Security Basic Configuration Using ASDM
• Cisco ASA Cloud Web Security Basic Configuration Using the CLI
• Cisco ASA Cloud Web Security Configuration with the Whitelist and Identity Options Using the CLI
• Verifying Cisco ASA Cloud Web Security Operations Using the Cisco ASDM
• Verifying Cisco ASA Cloud Web Security Operations Using the CLI
• Cisco AnyConnect Web Security Module Overview
• Cisco AnyConnect Web Security Module for Standalone Use Overview
• • Configure Cisco AnyConnect Web Security Module for Standalone Use
• Configure Cisco ASA to Download the Web Security Module to the Client Machine
• Verifying Cisco AnyConnect Web Security Module Operations
• Cisco ISR G2 Cloud Web Security Overview
• Cisco ISR G2 Cloud Web Security Configuration
• Cisco ISR G2 Cloud Web Security Verification
• Cisco WSA Cloud Web Security Overview

Describing the Web Filtering Policy in Cisco ScanCenter
• ScanCenter Web Filtering Policy Overview
• ScanCenter Web Filtering Policy Configuration
• HTTPS Inspection Configuration Overview
• ScanCenter Web Filtering Verification
• ScanCenter Web Filtering Reporting

Cisco Email Security Appliance
• Describe basics of email security deployment and configurations using the Cisco Email Security
• Appliance.
• Describing the Cisco Email Security Solutions
• Cisco Modular Network Architecture and Cisco ESA
• Cisco Hybrid Email Security Solution Overview
• SMTP Terminologies
• SMTP Flow
• SMTP Conversation
• Cisco ESA Services Overview
• Cisco ESA GUI Management
• Cisco ESA Committing the Configuration Changes
• Cisco ESA Licensing
• Incoming Mail Processing Overview

- Outgoing Mail Processing Overview
- Cisco ESA LDAP Integration Overview
- Cisco Registered Envelope Service (CRES) Overview

Describing the Cisco Email Security Appliance Basic Setup Components
- Cisco ESA Listener Overview
- Cisco ESA Listener Type: Private and Public
- Cisco ESA One Interface/One Listener Deployment Example
- Cisco ESA Two Interfaces/Two Listeners Deployment Example
- Cisco ESA Listener Major Components: HAT and RAT
- Cisco ESA One Listener Deployment Scenario
- One Listener Deployment Scenario: Interfaces and Listener
- One Listener Deployment Scenario: LDAP Accept Query non existing users
- One Listener Deployment Scenario: HAT
- One Listener Deployment Scenario: HAT > Sender Group
- One Listener Deployment Scenario: HAT > Sender Group SBRS
- One Listener Deployment Scenario: HAT > BLACKLIST Sender Group
- One Listener Deployment Scenario: HAT > RELAYLIST Sender Group
- One Listener Deployment Scenario: HAT > Add Sender Group
- One Listener Deployment Scenario: HAT > Mail Flow Policy
- One Listener Deployment Scenario: HAT > Mail Flow Policy > Anti-Spam and Anti-Virus
- One Listener Deployment Scenario: HAT > Mail Flow Policies Summary
- One Listener Deployment Scenario: RAT
- One Listener Deployment Scenario: SMTP Routes
- One Listener Deployment Scenario: Email Relaying on Internal Mail Server

Configuring Cisco Email Security Appliance Basic Incoming and Outgoing Mail Policies
- Explain how to configure the different features within the incoming and outgoing mail policies (anti-spam, anti-virus, content filters, outbreak filters, data loss prevention).
- Cisco ESA Incoming and Outgoing Mail Policies Overview
- Cisco ESA Mail Policies Matching
- Anti-Spam Overview
- Anti-Spam Configuration
- Spam Quarantine Configuration

Policy, Virus, Outbreak Quarantines Configuration
- Anti-Virus Overview
- Anti-Virus Configuration
- Content Filters Overview
- Content Filters Configuration
- Outbreak Filters Overview
- Outbreak Filters Configuration
- Data Loss Prevention Overview
- Data Loss Prevention Configuration
- Reporting Overview
- Message Tracking
- Trace
- Guided Lab 3: Configure Cisco Email Security Appliance Basic Policies

Advanced Malware Protection for Endpoints
• Provide a general overview of AMP for Endpoints, its major components, and the products available in the AMP product line up.
• AMP for Endpoints Overview and Architecture
• Modern Malware
• Why Defenses Fail
• Introduction to AMP for Endpoints
• AMP for Endpoints Architecture
• AMP Connector Architecture
• Installation Components
• How AMP Connector Components Interact
• The Role of the AMP Cloud
• Transaction Processing
• Additional Transaction Processing
• Real-time Data Mining
• Private Cloud Architecture
• Private Cloud Modes
• Cloud Proxy Mode Communications
• Air Gap Mode
• Guided Lab 4: Accessing the AMP Public Cloud Console

Customizing Detection and AMP Policy
• Describe how to customize detection and AMP policy
• Detection, Application Control, DFC Options, and IOCs
• Endpoint Policy
• Policy Modes
• Simple Custom Detections
• Creating A Simple Custom Detection
• Application Blocking
• Advanced Custom Signatures
• Whitelisting
• Android Custom Detections
• DFC IP Blacklists and Whitelists
• DFC IP Blacklists
• DFC IP Whitelists
• Configuring Exclusions
• Custom Exclusion Sets
• Guided Lab 5: Customizing Detection and AMP Policy

IOCs and IOC Scanning
• Describe Indicators of Compromise (IOC) and IOC scanning
• Indications of Compromise (IOCs)
• IOC Scanning
• Customizing IOCs
• Guided Lab 6: IOCs and IOC Scanning

Deploying AMP Connectors
• Groups

- Creating Groups
- Deploying Windows Connectors
- Direct Download Deployment
- Creating the Installer (Public Cloud)
- Email Deployment
- Microsoft Windows Installation and Interface
- Connectivity Considerations
- Command-Line Installation
- Guided Lab 7: Deploying AMP Connectors

AMP Analysis Tools
- Review the various malware analysis features available in the AMP for Endpoints console.
- Event View Filters
- Events List
- Event Detail: File Detection
- Event Detail: Connector Info
- Event Detail: Comments
- File Analysis
- The File Analysis Page
- File Analysis Results
- File Repository
- Trajectory
- File Trajectory Page
- Device Trajectory
- Device Trajectory Filters and Search
- Prevalence
- Vulnerable Software
- Reporting
- Creating a Report
- Guided Lab 8: AMP Analysis Tools

Cisco FirePOWER Next-Generation IPS
- Provide general information about the Cisco FirePOWER Next-Generation IPS (NGIPS) solution.
- Describing the Cisco FireSIGHT System
- Provide an overview of the Cisco FireSIGHT System.
- Cisco FireSIGHT System Overview
- Cisco FirePOWER NGIPS and NGFW
- Cisco FireSIGHT System Detection and Architecture
- Cisco FireSIGHT System Components
- Cisco FireSIGHT System Device Configuration
- Traffic Flows

Configuring and Managing Cisco FirePOWER Devices
- Explore the process for registering devices to the FireSIGHT Management Center.
- Introduction to Device Management
- Interfaces Tab
- Virtual Device Configuration
- Static Route Configuration

• Object Management
• Guided Lab 9: Configure Inline Interfaces and Create Objects

Implementing an Access Control Policy
• Explore the elements that make up an access control policy.
• Access Control Policy Overview
• Access Control Policy Configuration
• Default Action
• Targets Tab
• Security Intelligence
• HTTP Responses
• Advanced Tab
• Access Control Policy Rules
• Rule Constraints Overview
• Save and Apply the Access Control Policy
• Guided Lab 10: Create Access Control Policy Rules

Understanding Discovery Technology
• Describe the Cisco FirePOWER collection of technologies that provide the contextual information behind the FirePOWER NGFW and NGIPS solutions.
• Introduction to Host Discovery
• Network Discovery Policy
• Discovery Overview
• Guided Lab 11: Configure Network Discovery Detection

Configuring File-Type and Network Malware Detection
• Describe file-type and network malware detection.
• Introduction to Network-Based Malware Detection
• Network-Based Malware Detection Overview
• File Dispositions
• Important Network-Based Malware Detection Concepts
• Retrospective Event Overview
• Cisco FireSIGHT File-Type Detection Architecture
• Cisco FireSIGHT Malware Detection Architecture
• File Disposition Caching
• File Lists
• File Policy
• Guided Lab 12: Create a File Policy

Managing SSL Traffic with Cisco FireSIGHT
• Describe the architecture of onboard SSL decryption on Cisco FirePOWER devices.
• SSL Traffic Management Overview
• SSL Inspection Architecture
• Cisco FireSIGHT SSL Inspection
• SSL Policy

Describing IPS Policy and Configuration Concepts
• Describe the IPS detection policy and the elements that make up the policy.

- Introduction to IPS Policy
- Policy Layering Model
- Rule Management
- Cisco FireSIGHT Rule Recommendations
- IPS Policy Layering
- Guided Lab 13: Create an Intrusion Policy

Describing the Network Analysis Policy
- Describe the network analysis policy.
- Network Analysis Policy Introduction
- Network Analysis Policy Customization
- Preprocessors
- Network Analysis Policy Configuration
- Network Analysis Policy Creation
- Preprocessor Configuration
- Guided Lab 14: Create a Network Analysis Policy

Creating Reports
- Discuss the reporting features in the Cisco FireSIGHT System.
- Reporting System Overview
- Report Templates
- Report Sections
- Advanced Settings
- Guided Lab 15: Compare Trends

Correlation Rules and Policies
- Describe various features that leverage event data to allow for enhanced alerting and reacting to
- conditions surfaced by the Cisco FireSIGHT System.
- Correlation Policies Overview
- Correlation Policy ResponsesRemediations Configuration
- Remediation Module Configuration
- Correlation Policy Rules
- Correlation Policies Overview
- Correlation Events
- Whitelists Overview
- Whitelist Events and Violations
- Traffic Profiles Overview
- Traffic Profiles in Correlation Policies
- Guided Lab 16: Create Correlation Policies

Understanding Basic Rule Syntax and Usage
- Describe the fundamentals of Cisco Snort rules, including their structure, syntax, and options.
- Basic Snort Rule Structure
- Snort Rule Headers
- Snort Rule Bodies

Cisco ASA FirePOWER Services Module
- Describe how to install the ASA FirePOWER (SFR) module and how to manage the ASA FirePOWER (SFR) module

using the FireSIGHT Management Center (Defense Center).
• Installing Cisco ASA 5500-X Series FirePOWER Services (SFR) Module
• Describe the Cisco ASA FirePOWER Services Module.
• Cisco ASA FirePOWER Services (SFR) Module Overview
• Cisco FireSIGHT Management Center Overview FirePOWER Services Module.
• Cisco ASA FirePOWER Services Software Module Management Interface
• Cisco ASA FirePOWER Services Module Package Installation
• Cisco ASA FirePOWER Services Module Verification
• Redirect Traffic to Cisco ASA FirePOWER Services Module