コースコード：CI-SCOR
税抜価格：600,000円
日数：5日間

前提条件

To fully benefit from this course, you should have the following knowledge and skills: Skills and knowledge equivalent to those learned in Implementing and Administering Cisco Solutions (CCNA®) v1.0 course Familiarity with Ethernet and TCP/IP networking Working knowledge of the Windows operating system Working knowledge of Cisco IOS networking and concepts Familiarity with basics of networking security concepts These Cisco courses are recommended to help you meet these prerequisites: Implementing and Administering Cisco Solutions (CCNA) v1.0

受講対象者

Security engineer
Network engineer
Network designer
Network administrator
Systems engineer
Consulting systems engineer
Technical solutions architect
Network manager
Cisco integrators and partners

コース概要

The Implementing and Operating Cisco Security Core Technologies (SCOR) v1.0 course helps you prepare for the Cisco® CCNP® Security and CCIE® Security certifications and for senior-level security roles. In this course, you will master the skills and technologies you need to implement core Cisco security solutions to provide advanced threat protection against cybersecurity attacks. You will learn security for networks, cloud and content, endpoint protection, secure network access, visibility, and enforcements. You will get extensive hands-on experience deploying Cisco Firepower® Next-Generation Firewall and Cisco Adaptive Security Appliance (ASA)

Firewall; configuring access control policies, mail policies, and 802.1X Authentication; and more. You will get introductory practice on Cisco Stealthwatch® Enterprise and Cisco Stealthwatch Cloud threat detection features.

This course, including the self-paced material, helps prepare you to take the exam, Implementing and Operating Cisco Security Core Technologies (350-701 SCOR), which leads to the new CCNP Security, CCIE Security, and the Cisco Certified Specialist - Security Core certifications.

目的

このトレーニングを修了すると次のことができるようになります

・ネットワークにおける情報セキュリティのコンセプトと戦略を説明できる
・一般的なTCP/IP、ネットワークアプリケーションと端末に対する攻撃を説明できる
・攻撃に対して防御するために、どのようにネットワークセキュリティ技術が協調して動作するか説明できる
・Cisco ASAアプライアンスとCisco Firepower次世代ファイアウォールにおいてアクセス制御を実装できる
・Cisco Emailセキュリティ アプライアンスによって提供される基本的なemailセキュリティ機能を説明し実装できる
・Cisco Webセキュリティ アプライアンスによって提供されるWebコンテンツセキュリティ機能を説明し実装できる
・Cisco Umbrellaセキュリティ機能と配置モデル、ポリシー管理、捜査コンソールについて説明できる
・VPNを導入し、暗号化ソリューションとアルゴリズムを説明できる
・Ciscoのセキュアなサイト間接続ソリューションである、Cisco IOS VTIベース ポイントツーポイント IPsec VPN、およびCisco ASAとCisco Firepower次世代ファイアウォールにおけるポイントツーポイント IPsec VPNをどのように展開するか説明できる
・Ciscoのセキュアなリモートアクセス接続ソリューションを説明、展開し、802.1XとEAP認証を説明できる
・エンドポイント セキュリティの基本的な理解と、Advanced Malware

Protection(AMP) for
Endpointsのアーキテクチャおよび基本的な機能を説明できる
・制御プレーンおよび管理プレーンを保護するCiscoデバイスで、様々な防御を評価できる
・Cisco IOSソフトウェアのL2/L3データプレーンの制御を設定し確認できる
・Cisco Stealthwatch EnterpriseとStealthwatch
Cloudソリューションを説明できる
・クラウドコンピューティングの基本、一般的なクラウドへの攻撃とクラウド環境をどのようにセキュアにするかを説明できる

アウトライン

Describing Information Security Concepts*
Information Security Overview
Assets, Vulnerabilities, and Countermeasures
Managing Risk
Vulnerability Assessment
Understanding Common Vulnerability Scoring System (CVSS)
Describing Common TCP/IP Attacks*
Legacy TCP/IP Vulnerabilities
IP Vulnerabilities
Internet Control Message Protocol (ICMP) Vulnerabilities
TCP Vulnerabilities
User Datagram Protocol (UDP) Vulnerabilities
Attack Surface and Attack Vectors
Reconnaissance Attacks
Access Attacks
Man-in-the-Middle Attacks
Denial of Service and Distributed Denial of Service Attacks
Reflection and Amplification Attacks
Spoofing Attacks
Dynamic Host Configuration Protocol (DHCP) Attacks
Describing Common Network Application Attacks*
Password Attacks
Domain Name System (DNS)-Based Attacks
DNS Tunneling

Web-Based Attacks

HTTP 302 Cushioning

Command Injections

SQL Injections

Cross-Site Scripting and Request Forgery

Email-Based Attacks

Describing Common Endpoint Attacks*

Buffer Overflow

Malware

Reconnaissance Attack

Gaining Access and Control

Gaining Access via Social Engineering

Gaining Access via Web-Based Attacks

Exploit Kits and Rootkits

Privilege Escalation

Post-Exploitation Phase

Angler Exploit Kit

Describing Network Security Technologies

Defense-in-Depth Strategy

Defending Across the Attack Continuum

Network Segmentation and Virtualization Overview

Stateful Firewall Overview

Security Intelligence Overview

Threat Information Standardization

Network-Based Malware Protection Overview

Intrusion Prevention System (IPS) Overview

Next Generation Firewall Overview

Email Content Security Overview

Web Content Security Overview

Threat Analytic Systems Overview

DNS Security Overview

Authentication, Authorization, and Accounting Overview

Identity and Access Management Overview

Virtual Private Network Technology Overview

Network Security Device Form Factors Overview

Deploying Cisco ASA Firewall

Cisco ASA Deployment Types

Cisco ASA Interface Security Levels

Cisco ASA Objects and Object Groups

Network Address Translation

Cisco ASA Interface Access Control Lists (ACLs)

Cisco ASA Global ACLs

Cisco ASA Advanced Access Policies

Cisco ASA High Availability Overview

Deploying Cisco Firepower Next-Generation Firewall

Cisco Firepower NGFW Deployments

Cisco Firepower NGFW Packet Processing and Policies

Cisco Firepower NGFW Objects

Cisco Firepower NGFW Network Address Translation (NAT)

Cisco Firepower NGFW Prefilter Policies

Cisco Firepower NGFW Access Control Policies

Cisco Firepower NGFW Security Intelligence

Cisco Firepower NGFW Discovery Policies

Cisco Firepower NGFW IPS Policies

Cisco Firepower NGFW Malware and File Policies

Deploying Email Content Security

Cisco Email Content Security Overview

Simple Mail Transfer Protocol (SMTP) Overview

Email Pipeline Overview

Public and Private Listeners

Host Access Table Overview

Recipient Access Table Overview

Mail Policies Overview

Protection Against Spam and Graymail

Anti-virus and Anti-malware Protection

Outbreak Filters

Content Filters

Data Loss Prevention

Email Encryption

Deploying Web Content Security

Cisco Web Security Appliance (WSA) Overview

Deployment Options

Network Users Authentication
Secure HTTP (HTTPS) Traffic Decryption
Access Policies and Identification Profiles
Acceptable Use Controls Settings
Anti-Malware Protection
Deploying Cisco Umbrella*
Cisco Umbrella Architecture
Deploying Cisco Umbrella
Cisco Umbrella Roaming Client
Managing Cisco Umbrella
Cisco Umbrella Investigate Overview and Concepts
Explaining VPN Technologies and Cryptography
VPN Definition
VPN Types
Secure Communication and Cryptographic Services
Keys in Cryptography
Public Key Infrastructure
Introducing Cisco Secure Site-to-Site VPN Solutions
Site-to-Site VPN Topologies
IPsec VPN Overview
IPsec Static Crypto Maps
IPsec Static Virtual Tunnel Interface
Dynamic Multipoint VPN
Cisco IOS FlexVPN
Deploying Cisco IOS VTI-Based Point-to-Point IPsec VPNs
Cisco IOS VTIs
Static VTI Point-to-Point IPsec Internet Key Exchange (IKE) v2 VPN Configuration
Deploying Point-to-Point IPsec VPNs on the Cisco ASA and Cisco Firepower NGFW
Point-to-Point VPNs on the Cisco ASA and Cisco Firepower NGFW
Cisco ASA Point-to-Point VPN Configuration
Cisco Firepower NGFW Point-to-Point VPN Configuration
Introducing Cisco Secure Remote Access VPN Solutions
Remote Access VPN Components
Remote Access VPN Technologies

Secure Sockets Layer (SSL) Overview

Deploying Remote Access SSL VPNs on the Cisco ASA and Cisco Firepower NGFW

Remote Access Configuration Concepts

Connection Profiles

Group Policies

Cisco ASA Remote Access VPN Configuration

Cisco Firepower NGFW Remote Access VPN Configuration

Explaining Cisco Secure Network Access Solutions

Cisco Secure Network Access

Cisco Secure Network Access Components

AAA Role in Cisco Secure Network Access Solution

Cisco Identity Services Engine

Cisco TrustSec

Describing 802.1X Authentication

802.1X and Extensible Authentication Protocol (EAP)

EAP Methods

Role of Remote Authentication Dial-in User Service (RADIUS) in 802.1X Communications

RADIUS Change of Authorization

Configuring 802.1X Authentication

Cisco Catalyst® Switch 802.1X Configuration

Cisco Wireless LAN Controller (WLC) 802.1X Configuration

Cisco Identity Services Engine (ISE) 802.1X Configuration

Supplicant 802.1x Configuration

Cisco Central Web Authentication

Describing Endpoint Security Technologies*

Host-Based Personal Firewall

Host-Based Anti-Virus

Host-Based Intrusion Prevention System

Application Whitelists and Blacklists

Host-Based Malware Protection

Sandboxing Overview

File Integrity Checking

Deploying Cisco Advanced Malware Protection (AMP) for Endpoints*

Cisco AMP for Endpoints Architecture
Cisco AMP for Endpoints Engines
Retrospective Security with Cisco AMP
Cisco AMP Device and File Trajectory
Managing Cisco AMP for Endpoints
Introducing Network Infrastructure Protection*
Identifying Network Device Planes
Control Plane Security Controls
Management Plane Security Controls
Network Telemetry
Layer 2 Data Plane Security Controls
Layer 3 Data Plane Security Controls
Deploying Control Plane Security Controls*
Infrastructure ACLs
Control Plane Policing
Control Plane Protection
Routing Protocol Security
Deploying Layer 2 Data Plane Security Controls*
Overview of Layer 2 Data Plane Security Controls
Virtual LAN (VLAN)-Based Attacks Mitigation
Spanning Tree Protocol (STP) Attacks Mitigation
Port Security
Private VLANs
Dynamic Host Configuration Protocol (DHCP) Snooping
Address Resolution Protocol (ARP) Inspection
Storm Control
MACsec Encryption
Deploying Layer 3 Data Plane Security Controls*
Infrastructure Antispoofing ACLs
Unicast Reverse Path Forwarding
IP Source Guard
Deploying Management Plane Security Controls*
Cisco Secure Management Access
Simple Network Management Protocol Version 3
Secure Access to Cisco Devices
AAA for Management Access

Deploying Traffic Telemetry Methods*
Network Time Protocol
Device and Network Events Logging and Export
Network Traffic Monitoring Using NetFlow
Deploying Cisco Stealthwatch Enterprise*
Cisco Stealthwatch Offerings Overview
Cisco Stealthwatch Enterprise Required Components
Flow Stitching and Deduplication
Stealthwatch Enterprise Optional Components
Stealthwatch Enterprise and ISE Integration
Cisco Stealthwatch with Cognitive Analytics
Cisco Encrypted Traffic Analytics
Host Groups
Security Events and Alarms
Host, Role, and Default Policies
Describing Cloud and Common Cloud Attacks*
Evolution of Cloud Computing
Cloud Service Models
Security Responsibilities in Cloud
Cloud Deployment Models
Common Security Threats in Cloud
Patch Management in the Cloud
Security Assessment in the Cloud
Securing the Cloud*
Cisco Threat-Centric Approach to Network Security
Cloud Physical Environment Security
Application and Workload Security
Cloud Management and API Security
Network Function Virtualization (NFV) and Virtual Network Functions (VNF)
Cisco NFV Examples
Reporting and Threat Visibility in Cloud
Cloud Access Security Broker
Cisco CloudLock®
OAuth and OAuth Attacks
Deploying Cisco Stealthwatch Cloud*

Cisco Stealthwatch Cloud for Public Cloud Monitoring
Cisco Stealthwatch Cloud for Private Network Monitoring
Cisco Stealthwatch Cloud Operations
Describing Software-Defined Networking (SDN*)
Software-Defined Networking Concepts
Network Programmability and Automation
Cisco Platforms and APIs
Basic Python Scripts for Automation

*のついている章は自己学習していただく部分になります。コース内では説明の時間を設けません。

Lab outline
Configure Network Settings and NAT on Cisco ASA
Configure Cisco ASA Access Control Policies
Configure Cisco Firepower NGFW NAT
Configure Cisco Firepower NGFW Access Control Policy
Configure Cisco Firepower NGFW Discovery and IPS Policy
Configure Cisco NGFW Malware and File Policy
Configure Listener, Host Access Table (HAT), and Recipient Access Table (RAT) on Cisco Email Security Appliance (ESA)
Configure Mail Policies
Configure Proxy Services, Authentication, and HTTPS Decryption
Enforce Acceptable Use Control and Malware Protection
Examine the Umbrella Dashboard
Examine Cisco Umbrella Investigate
Explore DNS Ransomware Protection by Cisco Umbrella
Configure Static VTI Point-to-Point IPsec IKEv2 Tunnel
Configure Point-to-Point VPN between the Cisco ASA and Cisco Firepower NGFW
Configure Remote Access VPN on the Cisco Firepower NGFW
Explore Cisco AMP for Endpoints
Perform Endpoint Analysis Using AMP for Endpoints Console
Explore File Ransomware Protection by Cisco AMP for Endpoints Console
Explore Cisco Stealthwatch Enterprise v6.9.3

Explore Cognitive Threat Analytics (CTA) in Stealthwatch Enterprise v7.0

Explore the Cisco Cloudlock Dashboard and User Security

Explore Cisco Cloudlock Application and Data Security

Explore Cisco Stealthwatch Cloud

Explore Stealthwatch Cloud Alert Settings, Watchlists, and Sensors