Formation Mettre en œuvre et gérer les solutions de sécurité Cisco

Description de la formation Cisco Sécurité

Cette **formation Mettre en œuvre et gérer les solutions de sécurité Cisco** vous apprend à implémenter les principales solutions de sécurité Cisco afin d'assurer une protection avancée contre les attaques de cybersécurité.

Vous apprenez à mettre en œuvre la sécurité des réseaux, du cloud et du contenu, la protection des points d'extrémité, l'accès sécurisé au réseau, la visibilité et les mesures d'application. La formation vous permet d'acquérir une vaste expérience pratique du déploiement du pare-feu Cisco Firepower de nouvelle génération et du pare-feu Cisco ASA, de la configuration des politiques de contrôle d'accès, des politiques de messagerie et de l'authentification 802.1X, etc.

Enfin, vous bénéficiez d'une introduction aux fonctionnalités de détection des menaces de Cisco Stealthwatch Enterprise et Cisco Stealthwatch Cloud.

Objectifs

À l'issue de cette **formation Cisco Sécurité**, vous aurez acquis les connaissances et compétences nécessaires pour :

- Décrire les concepts et les stratégies de sécurité de l'information au sein du réseau
- Décrire les attaques TCP/IP courantes, les applications réseau et les points d'extrémité
- Décrire comment les différentes technologies de sécurité des réseaux fonctionnent ensemble pour se protéger contre les attaques
- Mettre en place un contrôle d'accès sur l'appliance Cisco ASA et le pare-feu Cisco Firepower de nouvelle génération
- Décrire et mettre en œuvre les fonctions de base de la sécurité du contenu du courrier électronique fournies par l'application Cisco Email Security Appliance

- Décrire et mettre en œuvre les caractéristiques et les fonctions de sécurité du contenu web fournis par le Cisco Web Security Appliance
- Décrire les capacités de sécurité de Cisco Umbrella, les modèles de déploiement, la gestion des politiques et la console Investigate
- Introduire les VPN et décrire les solutions et les algorithmes de cryptographie
- Décrire les solutions de connectivité sécurisée de site à site de Cisco et expliquer comment déployer des VPN IPsec point à point basés sur le système IOS VTI de Cisco, et des VPN IPsec point à point sur le Cisco ASA et le Cisco FirePower NGFW
- Décrire et déployer les solutions de connectivité d'accès à distance sécurisé Cisco et décrire comment configurer l'authentification 802.1X et EAP
- Fournir une compréhension de base de la sécurité des points d'accès et décrire l'architecture et les caractéristiques de base de l'AMP pour les points d'accès
- Examiner les différentes défenses des dispositifs Cisco qui protègent le plan de contrôle et de gestion
- Configurer et vérifier les contrôles des plans de données de la couche 2 et de la couche 3 du logiciel Cisco IOS
- Décrire les solutions Stealthwatch Enterprise et Stealthwatch Cloud de Cisco
- Décrire les principes de base de l'informatique dans le cloud et les attaques courantes dans le cloud, ainsi que la manière de sécuriser l'environnement du cloud

À qui s'adresse cette formation ?

Public :

Ce cours Cisco Sécurité s'adresse aux personnes chargées de la sécurité qui doivent être en mesure de mettre en œuvre et d'exploiter les principales technologies de sécurité, notamment la sécurité des réseaux, la sécurité dans le cloud, la sécurité des contenus, la protection et la détection des points d'extrémité, l'accès sécurisé aux réseaux, la visibilité et la mise en application.

Prérequis :

Pour assister à cette formation Cisco Security, vous devez connaître les réseaux Ethernet et TCP/IP, avoir une expérience pratique du système d'exploitation Windows, des réseaux et des concepts de Cisco IOS, et posséder les notions de base de la sécurité des réseaux.

Contenu du cours Cisco Sécurité

Décrire les concepts de sécurité de l'information (auto-apprentissage)

Aperçu de la sécurité de l'information
Gérer les risques
Évaluation de la vulnérabilité
Comprendre le CVSS

Description des attaques TCP/IP courantes (auto-apprentissage)

Vulnérabilités héritées de TCP/IP
Vulnérabilités de IP
Vulnérabilités de ICMP
Vulnérabilités de TCP
Vulnérabilités d'UDP
Surface d'attaque et vecteurs d'attaque
Attaques de reconnaissance
Attaques à l'accès
Attaques Man in the middle
Déni de service et attaques distribuées de déni de service
Réflexion et amplification des attaques
Attaques par usurpation d'identité
Attaques DHCP

Décrire les attaques des applications de réseau communes (auto-apprentissage)

Attaques de mots de passe
Attaques basées sur le DNS

Tunneling DNS

Attaques sur le web

HTTP 302 Amortissement

Injections de commandes

Injections SQL

Scripts intersites et falsification de demandes

Attaques par courrier électronique

Décrire les attaques de points terminaux communs (auto-apprentissage)

Débordement de la mémoire tampon

Malware

Attaque de reconnaissance

Obtenir l'accès et le contrôle

Obtenir l'accès par l'ingénierie sociale

Obtenir l'accès par le biais d'attaques basées sur le Web

Kits d'exploitation et Rootkits

Escalade des privilèges

Phase de post-exploitation

Angler Exploit Kit

Décrire les technologies de sécurité des réseaux

Stratégie de défense en profondeur

Défendre à travers le continuum des attaques

Vue d'ensemble de la segmentation des réseaux et de la virtualisation

Présentation du pare-feu Stateful

Aperçu du Security Intelligence

Normalisation de l'information sur les menaces

Aperçu de la protection contre les logiciels malveillants sur les réseaux

Aperçu des IPS

Pare-feu Next Generation

Aperçu de la sécurité du contenu du courrier électronique

Aperçu de la sécurité du contenu Web

Aperçu des systèmes d'analyse des menaces

Aperçu de la sécurité du DNS

Authentification, autorisation et comptabilité

Aperçu de la gestion des identités et des accès

Aperçu de la technologie des réseaux privés virtuels

Déploiement du pare-feu Cisco ASA

Types de déploiement

Niveaux de sécurité de l'interface

Objets et groupes d'objets

Translation d'adresse réseau

Gestion des ACL

Global ACL

Politiques d'accès avancé

Aperçu de la haute disponibilité

Déploiement du pare-feu Next Generation Cisco Firepower

Traitement des paquets et politiques de Cisco Firepower

Objets Cisco Firepower NGFW

Gestion du NAT sur le Cisco Firepower NGFW

Politiques du filtrage

Politiques de contrôle d'accès

Security Intelligence

Politiques IPS

Malware Cisco Firepower NGFW et politiques de fichiers

Déploiement de la sécurité du contenu des courriels

Aperçu de la sécurité du contenu des courriers électroniques Cisco

Aperçu du SMTP

Vue d'ensemble de l'acheminement du courrier électronique

Auditeurs publics et privés

Aperçu des politiques en matière de courrier

Protection contre le spam et le courrier gris (Graymail)

Protection antivirus et anti-malware

Filtres d'épidémie (outbreak)

Filtres de contenu

Prévention des pertes de données

Cryptage des courriers électroniques

Déployer la sécurité du contenu Web

Vue d'ensemble de Cisco WSA

Options de déploiement

Authentification des utilisateurs du réseau

Décryptage du trafic HTTPS

Politiques d'accès et profils d'identification

Paramètres des contrôles d'utilisation acceptables

Protection contre les logiciels malveillants

Déployer Cisco Umbrella (auto-apprentissage)

Architecture Cisco Umbrella

Déploiement Cisco Umbrella

Cisco Umbrella Roaming Client

Management de Cisco Umbrella

Introduction à Cisco Umbrella Investigate

Explorer les technologies VPN et la cryptographie

Définition des VPN

Types deVPN

Communications sSecurisées et services de cryptages

Clés de cryptage

Infrastructure de clés publiques

Introduire les solutions de VPN Site-to-Site Cisco

Topologies de VPN Site-to-Site

Introduction au VPN IPsec

IPsec Static Crypto Maps

IPsec Static Virtual Tunnel Interface

Dynamic Multipoint VPN

Cisco IOS FlexVPN

Déployer VTI-Based Point-to-Point

Cisco IOS VTIs

Configuration de VTI Point-to-Point IPsec statique

Déployer des VPNs IPSEC Point-to-Point sur les Cisco ASA et Cisco Firepower NGFW

VPN Point-to-Point VPNs sur les Cisco ASA et Cisco Firepower NGFW

Configuration sur le Cisco ASA

Configuration sur les Cisco Firepower NGFW

Introduire les solutions d'accès distantes sécurisées VPN Cisco

Composants d'un VPN d'accès distant

Technologiesd'un VPN d'accès distant

Présentation du SSL

Déployer les solutions d'accès distantes sécurisées sur les Cisco ASA et Cisco Firepower NGFW

Présentation des concepts

Connection Profiles

Group Policies

Configuration sur les Cisco ASA

Configuration sur les Cisco Firepower NGFW

Explorer les solutions Cisco Secure Network Access

Cisco Secure Network Access

Composants di Cisco Secure Network Access

Utilisation du AAA

Cisco Identity Services Engine

Cisco TrustSec

Décrire l'authentification 802.1X

802.1X et EAP

Méthodes EAP

Rôle du RADIUS dans les communications 802.1X

Changements des autorisations sur une serveur RADIUS

Configurer l'authentification 802.1X

Configuration d'un Cisco Catalyst Switch

Configuration sur un Cisco WLC

Configuration sur un Cisco ISE

Configuration d'un supplicant

Cisco Central Web Authentication

Décrire les solutions sécurisées sur les endpoints (auto-apprentissage)

Pare-feux

Anti-Virus

Intrusion Prevention System

Gestion des listes blanches et listes noires

Protection contre les malwares

Présentation du bac à sable (Sandboxing)

Vérification de l'intégraité des fichiers

Déployer Cisco AMP pour les terminaux (auto-apprentissage)

Architecture du Cisco AMP

Cisco AMP for Endpoints Engines

Cisco AMP Device and File Trajectory

Manager Cisco AMP for Endpoints

Introduction de la protection des infrastructures de réseau (auto-apprentissage)

Identification du data plane réseau

Sécurisation du control plane

Sécurisation du dataplane

Télémétrie en réseau

Contrôle du control plane de la couche 2

Contrôle du control plane de la couche 2

Déploiement de la sécurité du control Plane (auto-apprentissage)

Infrastructure des ACLs

Control Plane Policing

Protection du Control Plane

Sécurisation des protocoles de routage

Déploiement de la sécurité de couche 2 du control Plane (auto-apprentissage)

Présentation

Gestion des attaques basées sur les VLAN

Gestion des attaques basées sur le STP

Port Security

Private VLANs

DHCP Snooping

ARP Inspection

Storm Control

MACsec Encryption

Déploiement de la sécurité de couche 3 du control Plane (auto-apprentissage)

Antispoofing ACLs

Unicast Reverse Path Forwarding

IP Source Guard

Travaux Pratiques

De très nombreux pratiques émaillent cette formation. Ces derniers vous inviteront à :

- Configurer les paramètres réseaux et le NAT sur les Cisco ASA
- Configurer les polices de contrôle d'accès sur les Cisco ASA
- Configurer le NAT sur les Cisco Firepower NGFW
- Configurer les polices de contrôle d'accès sur les Cisco Firepower NGFW
- Configurer les policies IPS sur les Cisco Firepower NGFW
- Configurer les policies contre les malwares Cisco NGFW
- Configurer Listener, HAT, et RAT sur les Cisco ESA
- Configurer les Mail Policies
- Configurer les Proxy Services, Authentication, et HTTPS Decryption
- Configurer les politiques de courrier
- Configurer les services de proxy, l'authentification et le décryptage HTTPS
- Faire respecter le contrôle de l'utilisation acceptable et la protection contre les logiciels malveillants
- Examiner le tableau de bord général
- Examiner l'enquête sur Cisco Umbrella
- Explorer la protection des DNS contre les rançons par Cisco Umbrella
- Configurer le tunnel IKEv2 statique VTI point à point IPsec
- Configurer le VPN point à point entre le Cisco ASA et le Cisco Firepower NGFW
- Configurer le VPN d'accès à distance sur le Cisco Firepower NGFW
- Explorer l'AMP Cisco pour les terminaux
- Effectuer une analyse des points finaux en utilisant la console AMP for Endpoints
- Explorer la protection des fichiers contre les rançons par Cisco AMP for Endpoints Console
- Explorer Cisco Stealthwatch Enterprise v6.9.3
- Explorer le CTA dans Stealthwatch Enterprise v7.0

- Explorer le tableau de bord du cloudlock Cisco et la sécurité des utilisateurs
- Découvrir l'application Cisco Cloudlock et la sécurité des données
- Explorer le nuage Cisco Stealthwatch
- Découvrir les paramètres, les listes de surveillance et les capteurs de l'alerte au nuage Stealthwatch