Implémentation et exploitation des technologies Cisco Security Core

Code : CC05 **Durée** : 5 jours **Classe** : Présentiel / à distance

Public

- Ingénieur sécurité
- Ingénieur réseau
- Concepteur réseau
- Administrateur réseau
- Ingénieur système
- Ingénieur en systèmes de conseil
- Architecte des solutions techniques
- Intégrateurs/partenaires
- Cisco Gestionnaire de réseau I
- ntégrateurs et partenaires de Cisco

Prérequis

- Familiarité avec Ethernet et les réseaux TCP/IP
- Connaissance pratique du système d'exploitation Windows, des réseaux et des concepts de Cisco IOS
- Familiarité avec les notions de base de la sécurité des réseaux

Objectifs

- La formation Cisco SCOR est idéale pour les professionnels de la cybersécurité cherchant à optimiser leurs compétences en sécurité réseau et à se préparer à la certification CCNP Security . Elle offre une approche complète des technologies Cisco, abordant les firewalls, VPN, cryptographie et détection des menaces avancées . Animée par des formateurs certifiés, cette formation permet de maîtriser les outils et stratégies de sécurisation réseau, répondant aux exigences croissantes de protection des infrastructures IT. Cette formation prépare à la certification CCNP Security et Cisco Certified Specialist - Security Core

Programme détaillé

1- Modules d'auto-formation

- Décrire les concepts de sécurité de l'information
- Description des attaques TCP/IP courantes
- Description des attaques d'applications réseau courantes
- Description des attaques courantes des terminaux

2- Description des technologies de sécurité réseau

- Stratégie de défense en profondeur
- Défense à travers le continuum d'attaque
- Présentation de la segmentation et de la virtualisation du réseau
- Vue d'ensemble du pare-feu avec état
- Présentation du renseignement de sécurité
- Standardisation des informations sur les menaces
- Présentation de la protection contre les logiciels malveillants basée sur le réseau
- Présentation du système de prévention des intrusions (IPS)
- Présentation du pare-feu de nouvelle génération
- Présentation de la sécurité du contenu des e-mails
- Présentation de la sécurité du contenu Web
- Présentation des systèmes d'analyse des menaces
- Présentation de la sécurité DNS
- Présentation de l'authentification, de l'autorisation et de la comptabilité
- Présentation de la gestion des identités et des accès
- Présentation de la technologie de réseau privé virtuel
- Présentation des facteurs de forme des dispositifs de sécurité réseau

Implémentation et exploitation des technologies Cisco Security Core

Code : CC05 **Durée** : 5 jours **Classe** : Présentiel / à distance

3- Déploiement du pare-feu Cisco ASA
- Types de déploiement de Cisco ASA
- Niveaux de sécurité de l'interface Cisco ASA
- Objets et groupes d'objets Cisco ASA
- Traduction d'adresses réseau
- Listes de contrôle d'accès à l'interface Cisco ASA (ACL)
- ACL globales Cisco ASA
- Politiques d'accès avancé Cisco ASA
- Présentation de la haute disponibilité Cisco ASA

4- Déploiement du pare-feu de nouvelle génération Cisco Firepower
- Déploiements Cisco Firepower NGFW
- Traitement et politiques des paquets Cisco Firepower NGFW
- Objets Cisco Firepower NGFW
- Traduction d'adresses réseau (NAT) Cisco Firepower NGFW
- Politiques de préfiltre Cisco Firepower NGFW
- Politiques de contrôle d'accès Cisco Firepower NGFW
- Cisco Firepower NGFW Security Intelligence
- Politiques de découverte Cisco Firepower NGFW
- Politiques IPS de Cisco Firepower NGFW
- Politiques relatives aux logiciels malveillants et aux fichiers Cisco Firepower NGFW

5- Déploiement de la sécurité du contenu des e-mails
- Présentation de la sécurité du contenu de messagerie Cisco
- Présentation du protocole SMTP (Simple Mail Transfer Protocol)
- Présentation du pipeline de courrier électronique
- Auditeurs publics et privés
- Présentation de la table d'accès aux hôtes
- Vue d'ensemble du tableau d'accès des destinataires
- Présentation des politiques de messagerie
- Protection contre le spam et la messagerie Graymail
- Protection antivirus et anti-malware
- Filtres d'épidémie
- Filtres de contenu
- Prévention de la perte de données
- Chiffrement des e-mails

6- Déploiement de la sécurité du contenu Web
- Présentation de l'appliance de sécurité Web Cisco (WSA)
- Options de déploiement
- Authentification des utilisateurs du réseau
- Décryptage du trafic HTTP sécurisé (HTTPS)
- Politiques d'accès et profils d'identification
- Paramètres de contrôle d'utilisation acceptable
- Protection anti-malware

7- Module d'auto-formation
- Déploiement de Cisco Umbrella

Implémentation et exploitation des technologies Cisco Security Core

Code : CC05 **Durée** : 5 jours **Classe** : Présentiel / à distance

8- Présentation des technologies VPN et de la cryptographie
- Définition VPN
- Types de VPN
- Communication sécurisée et services cryptographiques
- Clés en cryptographie
- Infrastructure à clé publique

9- Présentation des solutions VPN sécurisées de site à site Cisco
- Topologies VPN de site à site
- Présentation du VPN IPsec
- Cartes cryptographiques statiques IPsec
- Interface de tunnel virtuel statique IPsec
- VPN multipoint dynamique
- Cisco IOS FlexVPN

10- Déploiement de l'IOS Cisco basé sur Cisco VTI point à point
- VTI Cisco IOS
- Configuration VPN statique VTI point à point IPsec Internet Key Exchange (IKE) v2

11- Déploiement de VPN IPsec point à point sur Cisco ASA et Cisco Firepower NGFW
- VPN point à point sur Cisco ASA et Cisco Firepower NGFW
- Configuration VPN point à point Cisco ASA
- Configuration VPN point à point Cisco Firepower NGFW

12- Présentation des solutions VPN d'accès distant sécurisé Cisco
- Composants VPN d'accès à distance
- Technologies VPN d'accès à distance
- Présentation de Secure Sockets Layer (SSL)

13- Déploiement de VPN SSL d'accès à distance sur Cisco ASA et Cisco Firepower NGFW
- Concepts de configuration d'accès à distance
- Profils de connexion
- Politiques de groupe
- Configuration VPN d'accès à distance Cisco ASA
- Configuration VPN d'accès à distance Cisco Firepower NGFW

14- Présentation des solutions d'accès sécurisé au réseau Cisco
- Accès réseau sécurisé Cisco
- Composants d'accès au réseau sécurisé Cisco
- Rôle AAA dans la solution Cisco Secure Network Access
- Moteur de services d'identité Cisco
- Cisco TrustSec

15- Description de l'authentification 802.1X
- 802.1X et protocole d'authentification extensible (EAP)
- Méthodes EAP
- Rôle du service utilisateur distant d'authentification à distance (RADIUS) dans les communications 802.1X
- Changement d'autorisation RADIUS

Implémentation et exploitation des technologies Cisco Security Core

Code : CC05 **Durée** : 5 jours **Classe** : Présentiel / à distance

16- Configuration de l'authentification 802.1X

- Configuration du commutateur Cisco Catalyst® 802.1X
- Configuration 802.1X du contrôleur LAN sans-fil Cisco (WLC)
- Configuration 802.1X de Cisco Identity Services Engine (ISE)
- Configuration du supplicant 802.1x
- Authentification Web centrale de Cisco

17- Modules d'auto-formation

- Description des technologies de sécurité des points d'accès
- Déploiement de l'AMP Cisco pour les terminaux
- Introduction à la protection des infrastructures réseau
- Déploiement des contrôles de sécurité dans les plans de contrôle
- Déploiement des contrôles de sécurité du plan de données de couche 2
- Déploiement des contrôles de sécurité du plan de données de couche 3