Formation Implémenter et exploiter les technologies Cisco Security Core (SCOR)

N° ACTIVITÉ : 11 92 18558 92 | TÉLÉPHONE : 01 85 77 07 07 | E-MAIL : inscription@hubformation.com

Référence	CS130
Durée	5 jours (35h)
Tarif	4 090 €HT

PROCHAINES SESSIONS

Pour connaître les prochaines dates ou organiser un intra-entreprise, contactez-nous, nous vous répondrons sous 72 heures.

Objectifs

| mettre en place un contrôle d'accès sur l'appliance Cisco ASA et le pare-feu Cisco Firepower de nouvelle génération ainsi que les fonctions de base de la sécurité du contenu du courrier électronique fournies par l'application Cisco Email Security Appliance
| Introduire les VPN et décrire les solutions et les algorithmes de cryptographie
| Connaître les solutions de connectivité sécurisée de point à point Cisco et expliquer comment déployer les VPN IPsec point à point basés sur le système IOS VTI de Cisco et les VPN IPsec point à point sur le Cisco ASA et le Cisco FirePower NGFW
| déployer les solutions de connectivité d'accès à distance sécurisé Cisco et décrire comment configurer l'authentification 802.1X et EAP
| vérifier les contrôles des plans de données de la couche 2 et de la couche 3 du logiciel Cisco IOS

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

Prérequis

| Avoir suivi la formation Implémentation et administration des solutions Cisco (CCNA)
| 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

Programme de la formation

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

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

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

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
| 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

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

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

Module d'auto-formation
| Déploiement de Cisco Umbrella

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

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

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

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

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

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

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

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
| Changement d'autorisation RADIUS

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

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

Méthode pédagogique

Chaque participant travaille sur un poste informatique qui lui est dédié. Un support de cours lui est remis soit en début soit en fin de cours. La théorie est complétée par des cas pratiques ou exercices corrigés et discutés avec le formateur. Le formateur projette une

présentation pour animer la formation et reste disponible pour répondre à toutes les questions.

Méthode d'évaluation

Tout au long de la formation, les exercices et mises en situation permettent de valider et contrôler les acquis du stagiaire. En fin de formation, le stagiaire complète un QCM d'auto-évaluation.

Accessibilité

Les sessions de formation se déroulent sur des sites différents selon les villes ou les dates, merci de nous contacter pour vérifier l'accessibilité aux personnes à mobilité réduite.
Pour tout besoin spécifique (vue, audition...), veuillez nous contacter au 01 85 77 07 07.