Développez vos talents
Certifiez vos compétences

Cisco - Offre officielle certifiante

Cisco Security Core Technologies - Implementing and operating

5 jours (35h00) | ★★★★½ 4,6/5 | SCOR | Certification 350-701 (non incluse) | Évaluation qualitative de fin de stage | Formation délivrée en présentiel ou distanciel [1]

Formations Informatique › Réseaux et Télécoms › Cisco - Offre officielle certifiante

À l'issue de ce stage vous serez capable de :

- Décrire les concepts et les stratégies de sécurité de l'information au sein du réseau
- Aborder les attaques courantes de TCP/IP, d'applications réseau et de points d'extrémité
- Savoir 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 Cisco Firepower Next-Generation Firewall (NGFW)
- Connaître et mettre en oeuvre les fonctions de base de la sécurité du contenu du courrier électronique fournies par l'application Cisco Email Security Appliance
- Décrire et mettre en oeuvre les caractéristiques et les fonctions de sécurité du contenu Web fournies par le Cisco Web Security Appliance
- Aborder 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 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
- 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
- Connaître les solutions Stealthwatch Enterprise et Stealthwatch Cloud de Cisco
- Décrire les principes de base de l'informatique en Cloud, les attaques courantes dans le Cloud, ainsi que la manière de sécuriser l'environnement Cloud.

(1) Modalité et moyens pédagogique :

Formation délivrée en présentiel ou distanciel * (e-learning, classe virtuelle, présentiel à distance). Le formateur alterne entre méthodes ** démonstrative, interrogative et active (via des travaux pratiques et/ou des mises en situation). La validation des acquis peut se faire via des études de cas, des quiz et/ou une certification.

Les moyens pédagogiques mis en oeuvre (variables suivant les formations) sont : ordinateurs Mac ou PC (sauf pour les cours de l'offre Management), connexion internet fibre, tableau blanc ou paperboard, vidéoprojecteur ou écran tactile interactif (pour le distanciel). Environnements de formation installés sur les postes de travail ou en ligne. Supports de cours et exercices.

* Nous consulter pour la faisabilité en distanciel. ** Ratio variable selon le cours suivi.

Niveau requis

Etre familiarisé avec Ethernet et les réseaux TCP/IP. Avoir des connaissances pratiques du système d'exploitation Windows, des réseaux et des concepts de Cisco IOS. Avoir des notions de base de la sécurité des réseaux. De plus, il est recommandé d'avoir suivi la formation CCNA "Cisco Solutions - Implementing and administering".

Public concerné

Ingénieurs sécurité et/ou réseaux, concepteurs réseaux, administrateurs réseaux, ingénieurs systèmes, ingénieurs conseil systèmes, architectes des solutions techniques, intégrateurs / partenaires Cisco, gestionnaires de réseau.

Cette formation :

- Est animée par un consultant-formateur dont les compétences techniques, professionnelles et pédagogiques ont été validées par des diplômes et/ou testées et approuvées par l'éditeur et/ou par M2i Formation
- Bénéficie d'un suivi de son exécution par une feuille de présence émargée par demi-journée par les stagiaires et le formateur.

Programme

Concepts de sécurité de l'information*

Les attaques TCP/IP les plus courantes*

Les attaques des applications de réseau les plus communes*

Les attaques de points finaux les plus fréquentes*

Technologies de sécurité des réseaux

Déploiement du pare-feu Cisco ASA

Déploiement du pare-feu de Cisco Firepower Next-Generation

Déploiement de la sécurité du contenu des courriels

Déploiement de la sécurité du contenu Web

Déploiement de Cisco Umbrella*

Les technologies VPN et la cryptographie

Solutions VPN sécurisées de site à site de Cisco

Déploiement de l'IOS Cisco basé sur le VTI point à point

Déploiement de VPN IPsec point à point sur le Cisco ASA et le Cisco Firepower NGFW

Solutions VPN d'accès distant sécurisé de Cisco

Déploiement de VPN SSL d'accès à distance sur le Cisco ASA et le Cisco Firepower NGFW

Solutions d'accès sécurisé au réseau Cisco

Description de l'authentification 802.1X

Configuration de l'authentification 802.1X

Technologies de sécurité des points d'accès*

Déploiement de l'AMP Cisco pour les points d'extrémité*

Introduction à la protection des infrastructures de réseau*

Déploiement des contrôles de sécurité dans les plans de contrôle*

Déploiement des contrôles de sécurité du plan de données de la couche 2*

Déploiement des contrôles de sécurité du plan de données de la couche 3*

Certification (en option)

- Prévoir l'achat de la certification en supplément
- Le passage de l'examen se fera (ultérieurement) dans un centre agréé Pearson Vue

– L'examen (en anglais) s'effectue en ligne, et durera en moyenne 2h00

* Module en auto-apprentissage (e-learning en autonomie)

Modalités d'évaluation des acquis

L'évaluation des acquis se fait :

– En cours de formation, par des études de cas ou des travaux pratiques
– Et, en fin de formation, par un questionnaire d'auto-évaluation ou une certification (M2i ou éditeur)

Les + de la formation

Ce cours comprend des modules en présentiel et d'autres à suivre en e-learning de manière autonome (modules accessibles durant 90 jours, dès le début de la formation).

Le support de cours et les labs sont en anglais.