Check Point Certified Security Administrator (CCSA)

Durée: 3 Jours Réf de cours: CCSA Version: R81.2 Méthodes d'apprentissage: Classe à distance

Résumé:

Cette formation permet d'acquérir les concepts de base et développer les compétences nécessaires à la gestion des activités liées à la sécurité informatique, comme configurer les passerelles de sécurité CheckPoint et le logiciel de management des blades.
Pendant cette formation, les participants configureront une politique de sécurité et apprendront à gérer et à surveiller un réseau sécurisé, à mettre à niveau et à configurer une passerelle de sécurité et à mettre en œuvre un réseau privé virtuel.
Version étudiée R81.20
Mise à jour : 17/03/2025

Classe à Distance - site Client

Cette formation peut être suivie à distance en synchrone depuis n'importe quel site pourvu d'une connexion internet (2 Mb/s en symétrique recommandés). Le programme (théorie et pratique) suit le même déroulé pédagogique qu'en présentiel. La solution technologique adoptée permet aux apprenants à distance de suivre les présentations faites au tableau, de voir et d'entendre l'instructeur et les participants en temps réel, mais également d'échanger avec eux.

Public visé:

Cette formation s'adresse aux informaticiens qui effectuent le support technique, installent, déploient ou administrent les solutions Check Point, ainsi qu'à toute personne souhaitant obtenir la certification CCSA.

Objectifs:

- A l'issue de la formation, les participants seront capables de :
- Décrire les principaux composants d'une architecture Check Point à trois niveaux et expliquer comment ils fonctionnent ensemble dans un environnement Check Point.
- Expliquer comment la communication est sécurisée et comment le trafic est acheminé dans l'environnement Check Point.
- Décrire les fonctions de base du système d'exploitation Gaia.
- Identifier le workflowow de base pour installer Security Management Server et Security Gateway pour une solution à domaine unique.
- Créer des objets SmartConsole correspondant à la topologie de l'organisation pour les utiliser dans les politiques et les règles.
- Identifier les outils disponibles pour gérer les licences et les contrats Check Point, y compris leur objectif et leur utilisation.
- Identifier les fonctionnalités et les capacités qui améliorent la configuration et la gestion de la politique de sécurité.
- Expliquer comment les niveaux de politique influencent l'inspection du trafic.
- Expliquer comment la traduction d'adresses réseau influe sur le trafic
- Décrire comment configurer la traduction d'adresses réseau (NAT Network Address Translation) manuelle et automatique.
- Démontrer une compréhension des fonctionnalités de contrôle des applications, de filtrage d'URL et de Prévention Autonome des Menaces et comment configurer ces solutions pour répondre aux exigences de sécurité d'une entreprise.
- Expliquer comment les clés pré-partagées et les certificats peuvent être configurés pour pour s'authentifier auprès de passerelles VPN tierces et gérées en externe.
- Décrire comment analyser et interpréter le trafic des tunnels VPN.
- Configurer les paramètres de logging.
- Utiliser des requêtes prédéfinies et personnalisées pour filtrer les résultats des logs.
- Identifier comment surveiller le fonctionnement du matériel supporté par Check Point via le portail Gaia et la ligne de commande.
- Décrire les différentes méthodes pour sauvegarder les informations du système Check Point et discuter des meilleures pratiques et des recommandations
- pour chaque méthode.

Pré-requis:

Avoir une connaissance pratique des concepts de réseau, de Windows Server et/ou d'UNIX, et une expérience de TCP/IP et d'Internet.

Test et certification

Cette formation prépare les participants à l'examen Check Point Certified Security Administrator R81.2

Cours suivant(s):

eck Point Certified Security Expert (CCSE) R81.20

Contenu:

Introduction à la technologie Check Point

Gestion des politiques de sécurité

Couches de politiques

Solutions de sécurité Check Point et licences

Visibilité du trafic

Concepts de base du VPN

Gestion de l'accès des utilisateurs

Travailler avec ClusterXL

Mise en œuvre des tâches de l'administrateur

Ateliers

- Travailler avec le portail Gaia
- Modifier une politique de sécurité existante
- Configurer Hide et Static NAT
- Gérer l'accès de l'administrateur
- Installation et gestion d'une passerelle de sécurité à distance
- Gestion des sauvegardes
- Définition des couches de politiques de contrôle d'accès
- Définition et partage des couches de politiques de sécurité
- Travailler avec des licences et des contrats
- Travailler avec les journaux de Check Point
- Maintenir les journaux de Check Point
- Configurer un VPN site à site
- Fournir un accès utilisateur
- Travailler avec Cluster XL
- Vérifier la conformité du réseau
- Travailler avec CP View

Autre(s) Information(s):

Les participants réalisent un test d'évaluation des connaissances en amont et en aval de la formation pour valider les connaissances acquises pendant la formation.
Support de cours officiel remis aux participants

Plus d'informations:

• Compétence du formateur : Les experts qui animent la formation sont des spécialistes des matières abordées et ont au minimum cinq ans d'expérience d'animation. Nos équipes ont validé à la fois leurs connaissances techniques (certifications le cas échéant) ainsi que leur compétence pédagogique.
• Suivi d'exécution : Une feuille d'émargement par demi-journée de présence est signée par tous les participants et le formateur.
• En fin de formation, le participant est invité à s'auto-évaluer sur l'atteinte des objectifs énoncés, et à répondre à un questionnaire de satisfaction qui sera ensuite étudié par nos équipes pédagogiques en vue de maintenir et d'améliorer la qualité de nos prestations.

Délais d'inscription :

• Vous pouvez vous inscrire sur l'une de nos sessions planifiées en inter-entreprises jusqu'à 5 jours ouvrés avant le début de la formation sous réserve de disponibilité de places et de labs le cas échéant.
• Votre place sera confirmée à la réception d'un devis ou """"booking form""""" signé. Vous recevrez ensuite la convocation et les modalités