Check Point Security Engineering R81.10

Référence : **CHS-CCSER81** Durée : **3 jours** Certification : **156-215.81**

CONNAISSANCES PREALABLES

• 1-Être certifié CCSA R81 ou avoir suivi la formation "Check Point Security Administration (CCSA) R81.10". • 2-Il est fortement recommandé d'avoir des compétences sur TCP/IP, la mise en réseau, internet et la gestion des systèmes Unix et Windows. • 3-Avoir des connaissances de base en langue anglaise car le support de cours est en langue anglaise.

PROFIL DES STAGIAIRES

• 1-Utilisateurs experts devant effectuer des configurations de déploiement avancées des lames logicielles Check Point. • 2-Toutes personnes visant la certification CCSE.

OBJECTIFS

• Fournir un aperçu du service de mise à niveau et des options disponibles. • Expliquer comment effectuer la mise à niveau et la migration de la gestion. • Articuler le processus à l'aide des fonctions CPUSE. • Articuler le but et la fonction de Management High Disponibilité. • Expliquer Primaire vs Secondaire, Actif vs Veille et Synchronisation. • Expliquer les étapes de reprise après sinistre au cas où la gestion principale serveur devient indisponible. • Fournir une vue d'ensemble du déploiement central dans SmartConsole. • Articuler une compréhension de la mise à niveau du cluster Security Gateway methodes. • Expliquer les mises à niveau de Multi Version Cluster (MVC). • Discuter des Commandes Gaia et comment elles sont utilisées. • Expliquer les principaux processus sur s et s. • Décrire comment travailler avec des scripts et des SmartTasks pour configurer des gestes automatiques. • Expliquer la séparation des plans de données de gestion (MDPS). • Expliquer les opérations du noyau et le flux de trafic. • Articuler des objets dynamiques et actualisables dans les passerelles de sécurité. • Expliquer le flux d'installation de la politique et les fichiers utilisés. • Décrire l'utilisation de l'historique d'installation des politiques. • Expliquer la politique d'installation simultanée et accélérée. • Décrire un aperçu des API et des façons de les utiliser et de s'authentifier. • Expliquer comment apporter des changements dans GAIA et la gestion de la configuration. • Expliquer comment installer la stratégie à l'aide de l'API. • Expliquer comment déterminer si la configuration est conforme aux les meilleures pratiques. • Expliquer comment définir les éléments d'action pour respecter la conformité. • Discuter du fonctionnement de SmartEvent pour identifier la sécurité critique des problèmes. • Expliquer comment la technologie d'accélération SecureXL améliore et optimise les performances de Security Gateway. • Décrire comment la technologie d'accélération CoreXL améliore et améliore les performances de Security Gateway. • Expliquer comment l'utilisation de plusieurs files d'attente de trafic peut rendre le trafic manipulation plus efficace. • Discuter des bases, du déploiement et des communautés de Site-to-Site VPN. • Décrire comment analyser et interpréter le trafic du tunnel VPN. • Expliquer les options de sélection de lien et de redondance ISP. • Expliquer les fonctionnalités de gestion des tunnels. • Discuter des solutions d'accès à distance Check Point et de leurs différences de chacun d'eux. • Décrire comment la sécurité du client peut être fournie par l'accès à distance. • Expliquer les méthodes d'authentification, y compris l'authentification machine. • Expliquer le point d'entrée multiple (MEP). • Discuter de la lame logicielle d'accès mobile et de la façon dont elle sécurise la communication et l'échange de données lors de connexions à distance. • Discuter des diverses fonctionnalités de Mobile Access telles que les portails, les liens la traduction, l'exécution d'applications natives, proxy inverse et plus encore. • Expliquer les concepts de base de Clustering et ClusterXL. • Expliquer le protocole de contrôle de cluster (CCP) et la synchronisation. • Décrire les fonctions et modes avancés de ClusterXL comme le partage de charge, Mode actif-actif, VMAC, etc. • Discuter de la couche de correction de cluster (CCL) pour fournir une connexion collante. • Journaux et surveillance avancés. • Décrire les composants de SmartEvent et leur déploiement d'option. • Discuter de la manière dont SmartEvent peut aider à signaler les menaces de sécurité. • Expliquer comment personnaliser les définitions d'événements et définir une politique d'événement.

CERTIFICATION PREPAREE

Cette formation prépare au test 156-215.81 et entre en jeu dans le cursus de certification : Check Point Certified Security Expert (CCSE)

METHODES PEDAGOGIQUES

- Mise à disposition d'un poste de travail par stagiaire
- Remise d'une documentation pédagogique papier ou numérique pendant le stage
- La formation est constituée d'apports théoriques, d'exercices pratiques, de réflexions et de retours d'expérience
- Le suivi de cette formation donne lieu à la signature d'une feuille d'émargement

FORMATEUR

Consultant-Formateur expert CheckPoint

METHODE D'EVALUATION DES ACQUIS

- Auto-évaluation des acquis par le stagiaire via un questionnaire
- Attestation de fin de stage adressée avec la facture

CONTENU DU COURS

Préparer une mise à niveau de Security Management Server

Mettre à niveau le serveur de gestion de la sécurité

Déployer un serveur de gestion de sécurité secondaire

Configurer un serveur de journaux distribué

Mettre à niveau une passerelle de sécurité à partir de SmartConsole

Travailler avec la ligne de commande

Utiliser des scripts et des SmartTask

Configurer des objets dynamiques

Surveiller le trafic

Vérifier l'installation et l'état de la stratégie

Travailler avec Gaia et les API de gestion

Travailler avec les fonctionnalités d'accélération

Configurer un site géré localement vers Site VPN

Configurer un VPN de site à site avec un appareil interopérable

Configurer le VPN d'accès à distance

Configurer le VPN d'accès mobile

Configurer un cluster à haute disponibilité

Travailler avec ClusterXL

Configurer la conformité aux stratégies

Déployer SmartEvent