CYBERSÉCURITÉ

Check Point - Certified Security Engineer R80.40

3 jours (21h00) | CS00013 | Num form : form-256 | Perfectionnement / Avancé

INFORMATIQUE / SÉCURITÉ IT / CYBERSÉCURITÉ

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

- Identifier les commandes CLI avancées
- Distinguer les procédures de gestion du système, notamment comment effectuer des mises à niveau du système et appliquer des patches et des hotfixes
- Décrire l'infrastructure de Check Point Firewall
- Lister les méthodes avancées de collecte de données importantes sur les passerelles à l'aide de CPView et CPInfo
- Reconnaître comment l'architecture API flexible de Check Point prend en charge l'automatisation et l'orchestration
- Présenter les fonctions avancées de ClusterXL
- Décrire les avantages de la redondance du réseau VRRP
- Expliquer comment la technologie d'accélération SecureXL est utilisée pour renforcer et améliorer les performances
- Décrire comment la technologie d'accélération CoreXL est utilisée pour renforcer et améliorer les performances
- Identifier les composants SmartEvent qui stockent les logs d'activité du réseau et identifient les événements
- Présenter le processus SmartEvent qui détermine quelles activités du réseau peuvent conduire à des problèmes de sécurité
- Expliquer comment SmartEvent peut aider à détecter, corriger et prévenir les menaces de sécurité
- Décrire le logiciel Mobile Access Blace et la manière dont il sécurise les communications et les données
- Identifier les options de déploiement de Mobile Access
- Reconnaître les solutions Check Point Remote Access
- Présenter les composants de Check Point Capsule et la manière dont ils protègent les appareils mobiles et les documents professionnels
- Enumérer les différentes solutions Check Point pour les attaques telles que zero-day et Advanced Persistent Threats
- Expliquer comment SandBlast, Threat Emulation et Threat Extraction préviennent les incidents de sécurité
- Identifier comment Check Point Mobile Threat Prevention peut aider à protéger les données

accessibles sur les smartphones et tablettes de l'entreprise.

Niveau requis :

Avoir suivi la formation CHK80-N1 "Check Point - Certified Security Administrator R80.40" ou être certifié CCSA. De plus, il est fortement recommandé d'avoir des connaissances pratiques de Windows, UNIX, la mise en réseau, TCP/IP et Internet.

Public concerné :

Utilisateurs experts et/ou revendeurs ayant besoin d'effectuer des configurations de déploiement avancées de Check Point Software Blades.

Programme :

- **Gestion des systèmes**
- **Automatisation et orchestration**
- **Redondance**
- **Accélération**

SmartEvent

- **Accès mobile et distant**
- **Prévention des menaces**