



Check Point EndPoint Security Full Disk Encryption

Objectif Endpoint Security de Check Point est une approche unifiée permettant de protéger les postes de travail des accès non autorisés et illicites. Ce cours vous apprend à configurer et à gérer un système protégé par Endpoint Security Full Disk Encryption en utilisant la console de gestion FDE. Vous apprendrez les détails du chiffrement de disque dur et comment déployer au mieux Endpoint Security FDE dans votre organisation

Pré requis Pour suivre ce stage, il est nécessaire d'avoir les compétences sur TCP/IP et sur le système Windows. Experience du chiffrement symétrique (AES)....

Durée 1 jour

Contenu

Module 1 : Aperçu de Full Disk Encryption

- Technologie de chiffrement de données de Full Disk Encryption
- Chiffrement de fichier et de disque
- Protection/authentification du boot
- Le modèle de sécurité totale de Check Point
- Fonctionnalités de sécurité de Full Disk Encryption
- Langages supportés dans Full Disk Encryption
- Gestion de Full Disk Encryption
- Méthodes d'authentification
- Récupération
- Niveau d'autorité de Full Disk Encryption
- Enregistrement automatique des logs et audit centralisé
- Aide à distance
- Licensing de Full Disk Encryption
- Composants de Full Disk Encryption
- Base de données de Full Disk Encryption
- Authentification au boot de Full Disk Encryption
- Console de gestion de Full Disk Encryption
- Génération de la clé de chiffrement de Full Disk Encryption
- Services et processus.
- Prérequis systèmes
- Systèmes d'exploitation supportés
- Prérequis/limitations des systèmes d'exploitation
- Systèmes de fichiers / Volumes / Mises à jour de l'OS
- Incompatibilités logicielles
- Limitations connues

Module 2 : la console de gestion de Full Disk Encryption

- Aperçu de la console de gestion de Full Disk Encryption
- Authentification sur la console de gestion
- Boîte de dialogue FDEMC
- Le dossier Local
- Edition des paramètres
- Le dossier Distant
- Ensembles de configuration
- Travailler avec des Profils
- Niveaux de Groupes d'Autorités (GAL)
- GAL et permissions

- GAL et aide à distance

Module 3 : gestion de Full Disk Encryption

- Astuces pour le déploiement
- Liste de vérifications pour le déploiement
- Travailler avec des profils de mise à jour
- Création d'un profil de mise à jour
- Effacer un utilisateur à travers le système de mise à jour de profil
- Mise à jour spécifique à une machine
- Envoi des profils de mise à jour aux ordinateurs
- Mise à jour de Full Disk Encryption
- Mise à jour depuis les versions 4.x et 5.x
- Aide à distance
- Types d'aide à distance
- Vérification de l'utilisateur
- Propriétés de l'aide à distance
- Utilisation d'un compte de démarrage de service
- Prérequis génériques
- Exemple de mise en place

Module 4 : gestion des logs de Full Disk Encryption

- Audit Pointsec.
- Log de Full Disk Encryption
- Transfer manuel du fichier de log au fichier de log central
- Timestamp et le gestionnaire d'évènement de Windows
- Affichage des événements Windows
- Visualiser un fichier de log local
- Structure des logs.
- Export des logs d'audit

Module 5 : Désinstallation, récupération et résolution des problèmes

- Types de désinstallation
- Créer et déployer un profil de désinstallation
- Ajout/suppression de programmes sous Windows
- Récupération
- Récupération selon la version de Full Disk Encryption sur le poste client
- Méthodes de récupération
- Désinstallation par un média de récupération
- Booter depuis un média alternatif
- Menu de personnalisation du préboot



- Personnalisation et paramétrage de Full Disk Encryption
- Résolution des problèmes d'une installation ayant échoué
- Utilisation de Reco_img.exe

Module 6 SmartCenter pour Pointsec – webRH.

- SmartCenter pour Pointsec – Aperçu de WebRH
- SmartCenter pour Pointsec – Installation de WebRH
- Prérequis concernant l'utilisateur.
- Prérequis système
- Prérequis Full Disk Encryption.
- Prérequis du navigateur
- Installation de Smartcenter pour Pointsec – webRH
- Smartcenter pour Pointsec – webRH Installation de la base de données SQL
- Smartcenter pour Pointsec – Application Web webRH
- Smartcenter pour Pointsec – Administration de webRH
- Gérer les unités organisationnelles.
- Démarrer en utilisant SmartCenter pour Pointsec – webRH
- Gestion des groupes OU (unités organisationnelles)
- Gestion des comptes utilisateurs
- Gestion des tokens d'authentification
- Configuration des paramètres de mots de passe
- Complèxité du mot de passe
- Désactivation des mots de passe fixes
- Utilisation de l'aide à distance
- Fichiers de logs dans SmartCenter pour Pointsec – webRH