Développez vos talents
Certifiez vos compétences

Offre éditeurs

Red Hat Security - Linux in Physical, Virtual, and Cloud (RH415) + examen (EX415)

5,5 jours (30h15) | ★★★★½ 4,6/5 | RH416 | Certification EX415 (incluse) | Évaluation qualitative de fin de stage | Formation délivrée en présentiel ou distanciel [1]

Formations Informatique › Cybersécurité › Offre éditeurs

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

- Analyser et corriger des problèmes de conformité du système à l'aide d'OpenSCAP et de SCAP Workbench
- Utiliser et adapter le contenu de politiques de référence fourni avec Red Hat Enterprise Linux
- Gérer les activités en lien avec la sécurité sur vos systèmes à l'aide de l'infrastructure d'audit du noyau
- Mettre en oeuvre des techniques SELinux avancées pour restreindre l'accès au niveau des utilisateurs, des processus et des machines virtuelles
- Déterminer l'intégrité des fichiers et de leurs permissions avec l'utilitaire AIDE
- Bloquer l'utilisation de périphériques USB non autorisés à l'aide d'USBGuard
- Protéger des données au repos avec déchiffrement automatique sécurisé dès le démarrage avec NBDE
- Identifier des risques et des erreurs de configuration de façon proactive sur les systèmes et correction à l'aide de Red Hat Insights
- Analyser l'état de conformité et corriger à grande échelle à l'aide d'OpenSCAP, de Red Hat Insights, de Red Hat Satellite et de Red Hat Ansible Tower.

Niveau requis

Etre titulaire de la certification RHCE (Ingénieur Certifié Red Hat), ou avoir des connaissances et/ou expérience(s) équivalentes de l'utilisation de Red Hat Enterprise Linux.

(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.

Public concerné

Administrateurs système, administrateurs de sécurité informatique, ingénieurs de sécurité informatique et autres professionnels chargés de la conception, de la mise en oeuvre, du maintien et de la gestion de la sécurité de systèmes Red Hat Enterprise Linux conformément aux politiques de sécurité en vigueur dans l'entreprise.

Partenaire / Éditeur

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

Gestion de la sécurité et des risques

- Définir des stratégies pour gérer la sécurité sur des serveurs Red Hat Enterprise Linux

Automatisation de la configuration et de la correction avec Ansible

- Corriger les problèmes de configuration et de sécurité à l'aide de playbooks Ansible

Protection des données avec LUKS et NBDE

- Chiffrer les données sur des périphériques de stockage avec LUKS
- Utiliser NBDE pour gérer le déchiffrement automatique lorsque les serveurs sont démarrés

Restriction de l'accès des périphériques USB

- Protéger le système contre l'accès des périphériques USB non autorisés grâce à USBGuard

Contrôle de l'authentification à l'aide de modules PAM (Pluggable Authentication Modules)

- Gérer les contrôles d'authentification, d'autorisation, de paramètres de session et de mots de passe en configurant des modules PAM

Enregistrement des évènements système dans le système d'audit

- Enregistrer et analyser les évènements système touchant à la sécurité à l'aide du sous-système d'audit du noyau Linux et d'outils complémentaires

Surveillance des changements au sein des systèmes de fichiers

- Détecter et analyser les modifications apportées aux systèmes de fichiers d'un serveur et à leur contenu avec l'utilitaire AIDE

Réduction des risques avec SELinux

- Renforcer la sécurité et le confinement des processus à l'aide de SELinux et de ses techniques et analyses avancées

Gestion de la conformité avec OpenSCAP

- Evaluer et corriger la conformité d'un serveur à l'aide de politiques de sécurité en utilisant OpenSCAP

Automatisation de la conformité avec Red Hat Satellite

- Automatiser et faire évoluer votre capacité d'effectuer des vérifications OpenSCAP
- Corriger les problèmes de conformité avec Red Hat Satellite

Analyse et correction des problèmes avec Red Hat Insights

- Détecter, identifier et corriger des problèmes et vulnérabilités courants sur des systèmes Red Hat Enterprise Linux avec Red Hat Insights

Révision approfondie

- Réviser le contenu de ce cours au travers d'exercices pratiques

Passage de l'examen

- Le prix et le passage de l'examen sont inclus dans la formation si elle est réalisée en présentiel (si formation en distanciel, certification passée à froid, en Kiosk)
- L'examen (en anglais) a lieu le dernier jour, à l'issue de la formation et s'effectue en ligne, pour une durée moyenne de 4h00

Modalités d'évaluation des acquis

- 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

En distanciel, ce cours est dispensé sur 30h15, soit 5,5 jours, de 9h à 15h (avec une pause déjeuner de 45 minutes). Cette durée inclut le passage de l'examen en Kiosk (à froid), d'une durée de 4h.

En présentiel, ce cours est dispensé sur 4,5 jours (de 9h à 17h) dont la dernière demi-journée est dédiée au passage de l'examen, d'une durée de 4h.

Le support de cours et les labs sont en anglais.