Red Hat Security: Linux in Physical, Virtual, and Cloud

Durée: 5 Jours **Réf de cours: RH415** **Méthodes d'apprentissage: Virtual Learning**

Résumé:

Cette formation permet aux participats d'acquérir les compétences et connaissances nécessaires pour réduire les risques de sécurité et pour mettre en œuvre, gérer et remédier aux problèmes de conformité et de sécurité de manière efficace. Les outils et les techniques peuvent être utilisés pour s'assurer que les systèmes sont configurés et déployés de manière à répondre aux besoins de sécurité et de conformité, qu'ils continuent à répondre à ces exigences, et que tous les systèmes existants peuvent être audités et que les remédiations et les changements sont appliqués de manière cohérente au fur et à mesure que ces exigences sont révisées. Cette flexibilité peut aider l'entreprise à réduire efficacement le risque de failles de sécurité, qui ont un coût élevé en termes d'interruption d'activité, d'érosion de la marque, de perte de confiance des clients et des actionnaires, et de coûts financiers pour la remédiation après l'incident. En outre, l'organisation peut être en mesure d'utiliser les outils de cette formation pour aider à démontrer que les exigences de conformité fixées par les clients, les auditeurs ou d'autres parties prenantes ont été respectées.

Cette formation est basée sur Red Hat Enterprise Linux 7.5, Red Hat Satellite 6.3, Red Hat Ansible® Engine 2.5, Red Hat Ansible Tower 3.2, et Red Hat Insights.

Public visé:

Cette formation s'adresse aux administrateurs système, administrateurs de la sécurité informatique, ingénieurs de la sécurité informatique et autres professionnels responsables de la conception, de la mise en œuvre, de la maintenance et de la gestion de la sécurité des systèmes Red Hat Enterprise Linux et de leur conformité avec les politiques de sécurité de l'organisation.

Objectifs pédagogiques:

- A l'issue de la formation, les participants seront capables de :
- Analyser et remédier à la conformité du système en utilisant OpenSCAP et SCAP Workbench, en employant et en personnalisant le contenu de la politique de base fournie avec Red Hat Enterprise Linux.
- Surveiller les activités relatives à la sécurité sur vos systèmes avec l'infrastructure d'audit du noyau.
- Expliquer et mettre en œuvre des techniques SELinux avancées pour restreindre l'accès des utilisateurs, des processus et des machines virtuelles.
- Confirmer l'intégrité des fichiers et leurs permissions avec AIDE.
- Empêcher l'utilisation de périphériques USB non autorisés avec USBGuard.
- Protéger les données au repos mais fournir un décryptage automatique sécurisé au démarrage à l'aide de NBDE.
- Identifier de manière proactive les risques et les mauvaises configurations des systèmes et y remédier avec Red Hat Insights.
- Analyser et remédier à la conformité à l'échelle avec OpenSCAP, Red Hat Insights, Red Hat Satellite et Red Hat Ansible Tower.

Pré-requis:

Les participants doivent remplir les conditions préalables suivantes :

- Être un ingénieur certifié Red Hat RHCE® ou démontrer une connaissance et une expérience équivalentes de Red Hat Enterprise Linux.

Test et certification

Recommandée comme préparation aux examens suivants :

- EX415 - Red Hat Certified Specialist in Security : Linux

Contenu:

Gérer la sécurité et les risques

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

Automatiser la configuration et la remédiation avec Ansible

- Remédier aux problèmes de configuration et de sécurité avec les Playbooks Ansible.

Protéger les données avec LUKS et NBDE

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

Restreindre l'accès aux périphériques USB

- Protéger le système contre l'accès de périphériques USB malveillants avec USBGuard.

Contrôle de l'authentification avec PAM

- Gérer l'authentification, l'autorisation, les paramètres de session et les contrôles de mot de passe en configurant des modules d'authentification enfichables (PAM).

Enregistrement des événements système avec audit

- Enregistrer et inspecter les événements système pertinents pour la sécurité, en utilisant le sous-système d'audit du noyau Linux et les outils correspondants.

Surveiller les modifications du système de fichiers

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

Atténuer les risques avec SELinux

- Améliorer la sécurité et le confinement entre les processus en utilisant SELinux et les techniques et analyses SELinux avancées.

Gérer la conformité avec OpenSCAP

- Évaluez et remédiez à la conformité d'un serveur avec les politiques de sécurité en utilisant OpenSCAP.

Automatiser la conformité avec Red Hat Satellite

- Automatiser et augmenter votre capacité à effectuer des contrôles OpenSCAP et à remédier aux problèmes de conformité à l'aide de Red Hat Satellite.

Analyser et remédier aux problèmes avec Red Hat Insights

- Identifier, détecter et corriger les problèmes courants et les vulnérabilités de sécurité des systèmes Red Hat Enterprise Linux en utilisant Red Hat Insights.

Effectuer une révision complète

Réviser le contenu de ce cours en effectuant des exercices de révision pratiques.

Méthodes pédagogiques :

Support de cours officiel remis aux participants

Autres moyens pédagogiques et de suivi:

• 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 d'accès en présentiel ou distanciel.
• Attention, si cette formation est éligible au Compte Personnel de Formation, vous devrez respecter un délai minimum et non négociable fixé à 11 jours ouvrés avant le début de la session pour vous inscrire via moncompteformation.gouv.fr.

Accueil des bénéficiaires :

• En cas de handicap : plus d'info sur globalknowledge.fr/handicap
• Le Règlement intérieur est disponible sur globalknowledge.fr/reglement