Sécurité Red Hat : Linux dans des environnements physiques, virtuels et cloud

Durée: 5 Jours **Réf de cours: RH415** **Méthodes d'apprentissage: Classe à distance**

Résumé:

Pour assurer la sécurité des systèmes informatiques, il faut gérer les risques en mettant en œuvre des processus et des normes basés sur des technologies et des outils.
Ce cours s'adresse au personnel chargé de l'administration des systèmes et de la sécurité qui gère le fonctionnement sécurisé des serveurs exécutant Red Hat Enterprise Linux, que ce soit sur du matériel physique, sous forme de machine virtuelle ou d'instance cloud.
Vous découvrirez les technologies et les outils qui peuvent vous aider à appliquer et à respecter vos exigences de sécurité, notamment le sous-système d'audit du noyau, AIDE, SELinux, OpenSCAP et SCAP Workbench, USBGuard, l'authentification PAM et le NBDE (Network-Based Device Encryption).
Vous apprendrez à surveiller la conformité ainsi qu'à identifier, hiérarchiser et résoudre les problèmes de manière proactive à l'aide des solutions OpenSCAP, Red Hat Insights, Red Hat Satellite et Red Hat Ansible Automation Platform.
Vous découvrirez comment la solution Red Hat Ansible Automation Platform automatise le déploiement de la correction des systèmes à l'aide de playbooks Ansible depuis OpenSCAP ou Red Hat Insights.
Ce cours repose sur RHEL 9.2, Ansible Core 2.14, Red Hat Ansible Automation Platform 2.4, Satellite 6.14 et OpenSCAP 1.3.7.
À la fin de ce cours, vous continuerez de bénéficier d'un accès à des travaux pratiques pendant 45 jours
Mise à jour 05 08 2024

Public visé:

Administrateurs système : responsables de la prise en charge de l'infrastructure, des systèmes et des serveurs physiques et virtuels de l'entrepriseSpécialistes de la sécurité informatique, responsables de la conformité et auditeurs : personnel chargé de veiller à ce que l'environnement technologique soit protégé contre les attaques et conforme aux règles et réglementations en matière de sécurité/confidentialitéArchitectes en automatisation : ingénieurs ou architectes responsables du développement de l'automatisation et de l'optimisation des outils et de l'infrastructure cloud pour atteindre les objectifs d'automatisation

Objectifs pédagogiques:

- A l'issue de la formation, les participants auront étudié les points suivants :
- Gestion de la conformité avec OpenSCAP
- Activation de SELinux sur un serveur à partir d'un état désactivé, analyse simple de la politique système et réduction des risques à l'aide de techniques SELinux avancées
- Identification proactive et résolution des problèmes à l'aide de Red Hat Insights
- Surveillance de l'activité et des modifications sur un serveur à l'aide des utilitaires Linux Audit et AIDE
- Protection des données contre les intrusions à l'aide d'USBGuard et du chiffrement du stockage
- Gestion des contrôles d'authentification à l'aide de modules PAM
- Application manuelle des playbooks Ansible fournis pour automatiser la réduction des problèmes de sécurité et de conformité
- Adaptation de la gestion d'OpenSCAP et de Red Hat Insights à l'aide des solutions Red Hat Satellite et de Red Hat Ansible Automation Platform

Pré-requis:

Les participants doivent remplir les conditions préalables suivantes :

- Être titulaire de la certification RHCE (Ingénieur certifié Red Hat) ou justifier de connaissances et d'une expérience équivalentes de l'utilisation de Red Hat Enterprise Linux

Test et certification

Examen Spécialiste certifié Red Hat en sécurité : Linux (EX415)

Contenu:

Gestion de la sécurité et des risques

- Définir et mettre en œuvre des stratégies pour gérer la sécurité sur les systèmes Red Hat Enterprise Linux

Automatisation de la configuration et de la correction avec Ansible

- Corriger automatiquement les problèmes de configuration et de sécurité avec des playbooks Ansible

Protection des données avec LUKS et NBDE

- Chiffrer les données sur des périphériques de stockage avec LUKS et utiliser NBDE pour gérer le déchiffrement automatique au démarrage des serveurs

Restriction de l'accès des périphériques USB

- Protéger les systèmes contre les périphériques USB non autorisés grâce à USBGuard

Contrôle de l'authentification à l'aide de modules PAM

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

Enregistrement des événements système dans le système d'audit

- Enregistrer et analyser les événements système qui concernent la sécurité à l'aide du 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

- Évaluer la conformité d'un serveur et apporter les corrections nécessaires à l'aide de politiques de sécurité en utilisant OpenSCAP

Analyse et correction des problèmes avec Red Hat Insights

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

Automatisation de la conformité avec Red Hat Satellite

- Automatiser et mettre à l'échelle les contrôles de conformité OpenSCAP avec Red Hat Satellite

Révision approfondie

- Réviser les sujets du cours Sécurité Red Hat : Linux dans des environnements physiques, virtuels et cloud

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