

# Red Hat Security: Linux in Physical, Virtual, and Cloud («RH415»)

Ce cours s'adresse aux administrateurs système qui ont besoin de gérer l'exploitation sécurisée de serveurs exécutant Red Hat® Enterprise Linux® sur du matériel physique, sur une machine virtuelle ou dans une instance cloud.

**Durée:** 4 jours

**Prix:** 3'700.– excl. 8.1% TVA

## Contenu

Assurer la sécurité de systèmes informatiques consiste à gérer les risques en mettant en œuvre des processus et des normes basés sur des technologies et des outils. Dans ce cours, vous découvrirez les ressources que vous pouvez utiliser pour mettre en œuvre et respecter vos exigences de sécurité.

### Programme du cours

#### 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 et 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

- 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 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

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

- Automatiser et faire évoluer votre capacité d'effectuer des vérifications OpenSCAP et 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

**Remarque :** le programme du cours est susceptible d'être modifié au vu des avancées technologiques et de l'évolution de la nature du travail sous-jacent.

## Objectifs

- 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 prévention des problèmes de sécurité et de conformité
- Adaptation de la gestion d'OpenSCAP et de Red Hat Insights à l'aide de Red Hat Satellite et de Red Hat Ansible Tower

## Public cible

Administrateurs système, administrateurs de sécurité informatique, ingénieurs de sécurité informatique et autres professionnels chargés de la conception, de la mise en œuvre, 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.

## Avez-vous une question ou souhaitez-vous organiser un cours en entreprise ?

Nous vous conseillons volontiers au +41 22 738 80 80 ou [romandie@digicomp.ch](mailto:romandie@digicomp.ch). Retrouvez toutes les informations détaillées concernant les dates sur [www.digicomp.ch/formations-it-providers/red-hat/red-hat-enterprise-linux/cours-red-hat-security-linux-in-physical-virtual-and-cloud](http://www.digicomp.ch/formations-it-providers/red-hat/red-hat-enterprise-linux/cours-red-hat-security-linux-in-physical-virtual-and-cloud)