

Certifiante

Formation Red Hat Security: Linux in Physical, Virtual, and Cloud (RH415)

Réf. SF34640

Sécuriser un parc Red Hat Enterprise Linux ne s'improvise pas : il faut l'outiller, l'automatiser et prouver sa conformité. Cette formation de 4 jours vous transmet les méthodes et les outils pour durcir vos serveurs, qu'ils tournent sur matériel physique, en machine virtuelle ou dans le cloud.

4 j
Durée

3 800 € HT
Inter / participant

0
Sessions à venir

Objectifs pédagogiques

- ✓ Superviser les activités sensibles à la sécurité grâce à l'infrastructure d'audit du noyau Linux
- ✓ Mettre en œuvre des techniques avancées de confinement des processus avec SELinux
- ✓ Vérifier l'intégrité des fichiers système à l'aide d'AIDE
- ✓ Bloquer les périphériques USB non autorisés avec USBGuard
- ✓ Chiffrer les données au repos et automatiser leur déverrouillage au démarrage avec LUKS et NBDE
- ✓ Détecter les risques de manière proactive grâce à Red Hat Insights
- ✓ Se préparer à l'examen de certification Red Hat Certified Specialist in Security: Linux Exam (EX415)

Public visé & prérequis

Public visé Administrateurs systèmes et réseaux

Prérequis Disposer de la certification Red Hat Certified Engineer (RHCE) ou justifier d'une maîtrise équivalente de l'administration de Red Hat Enterprise Linux acquise par l'expérience.

Programme détaillé

Stratégie de sécurité et gestion des risques

Démarche de sécurisation : définition d'une stratégie de gestion de la sécurité et des risques adaptée aux serveurs Red Hat Enterprise Linux.

Automatisation de la configuration et de la remédiation avec Ansible

– Remédiation automatisée : correction des défauts de configuration et des failles de sécurité à l'aide de playbooks Ansible.

Activités pratiques :

Écriture de playbooks Ansible pour appliquer et corriger des paramètres de sécurité.

Chiffrement des données avec LUKS et NBDE

– Données au repos : protection des supports de stockage par chiffrement LUKS et déverrouillage automatique au démarrage grâce au mécanisme NBDE (Network-Bound Disk Encryption).

Activités pratiques :

Chiffrement d'un volume avec LUKS, configuration du déchiffrement automatique via NBDE.

Maîtrise des accès aux périphériques USB

– Contrôle des périphériques : protection des systèmes contre les périphériques USB non autorisés à l'aide d'USBGuard.

Activités pratiques :

Définition de règles USBGuard pour autoriser ou bloquer des périphériques.

Contrôle de l'authentification avec PAM

– Sécurisation des accès : gestion de l'authentification, des autorisations, des paramètres de session et des contrôles de mots de passe via la configuration des modules PAM (Pluggable Authentication Modules).

Activités pratiques :

Configuration de modules PAM pour renforcer les règles de mots de passe et de session.

Journalisation des événements système avec Audit

– Traçabilité de sécurité : enregistrement et analyse des événements système sensibles à l'aide du sous-système d'audit du noyau Linux et de ses outils associés.

Activités pratiques :

Mise en place de règles d'audit et exploitation des journaux d'événements.

Surveillance de l'intégrité des systèmes de fichiers avec AIDE

– Détection des modifications : identification et analyse des changements apportés aux systèmes de fichiers et à leur contenu grâce à AIDE.

Activités pratiques :

Création d'une base de référence AIDE et détection des écarts d'intégrité.

Réduction des risques avec SELinux

– Confinement des processus : renforcement de la sécurité et de l'isolation entre processus grâce à SELinux et à ses techniques d'analyse avancées.

Activités pratiques :

Diagnostic et résolution de refus SELinux, ajustement de politiques de confinement.

Gestion de la conformité avec OpenSCAP

– Audit de conformité : évaluation et remédiation de la conformité d'un serveur aux politiques de sécurité à l'aide d'OpenSCAP.

Activités pratiques :

Analyse d'un serveur avec OpenSCAP et SCAP Workbench, correction des écarts détectés.

Industrialisation de la conformité avec Red Hat Satellite

– Conformité à l'échelle : automatisation et passage à l'échelle des contrôles OpenSCAP et de la remédiation des écarts via Red Hat Satellite.

Activités pratiques :

Planification de scans de conformité sur un parc de serveurs depuis Red Hat Satellite.

Analyse et remédiation proactives avec Red Hat Insights

– Sécurité prédictive : identification, détection et correction des problèmes courants et des vulnérabilités des systèmes Red Hat Enterprise Linux à l'aide de Red Hat Insights.

Activités pratiques :

Exploitation des recommandations Red Hat Insights pour prioriser et corriger les risques.

Synthèse et mise en pratique globale

Consolidation des acquis : révision de l'ensemble des notions du parcours à travers des exercices pratiques de synthèse.

Pourquoi choisir Sparks Formation ?

20 ans d'expertise IT, des formateurs experts et des sessions garanties contre l'annulation.

20 ans
d'expertise

1 068+
formations

11 178
apprenants formés/an

+67
Net Promoter Score

Avis des participants

Note moyenne des participants de la filière Administration Systèmes Unix/Linux : 4,9/5 — 28 avis

Alexander A. — Globalement, j'ai trouvé cette formation très intéressante et enrichissante. Le contenu était pertinent et m'a permis de mieux comprendre plusieurs notions de Linux. Le formateur était disponible et...

Alexander A. — Formation LPIC-101 très enrichissante. Le formateur est clair, compétent et possède une grande expérience terrain. J'ai beaucoup appris tout au long de la formation. C'était vraiment agréable de...

Ils nous font confiance

Cette année notre filière Administration Systèmes Unix/Linux a accompagné plus de 51 entreprises dont :

SOPRA STERIA I2S SOPRA STERIA GROUP CIMPA SAS CS GROUP FRANCE ADISTA ECONOCOM SERVICES & SOLUTION ECONOCOM
WORKPLACE INFRA INNOVATION SULLY GROUP ARPEGE CEGEDIM ACTIV +41 autres

Financement & certifications

Cette formation est éligible aux financements OPCO et FNE-Formation. Nos équipes vous accompagnent dans le montage de votre dossier.



Réservez votre place dès maintenant

20 ans d'expertise · 1 000+ formations · NPS +67 · réponse sous 24h ouvrées

0 805 950 800

demande@sparks-formation.com