Maîtriser SELinux et Gérer les Politiques de Sécurité Linux

DURÉE
3 jours (21h)

RÉFÉRENCE
SEC310

CATÉGORIE
Sécurité des Systèmes, Sécurité des Serveurs

OBJECTIFS DE LA FORMATION

À l'issue de cette formation, vous serez capable de :

- Comprendre les principes fondamentaux du contrôle d’accès obligatoire (MAC) et le rôle de SELinux dans la sécurité des systèmes Linux
- Identifier et diagnostiquer les causes des blocages ou alertes générées par SELinux
- Configurer, ajuster et administrer efficacement les contextes et booléens de sécurité
- Concevoir et déployer des politiques de sécurité personnalisées adaptées à l’environnement de production
- Renforcer la posture de sécurité globale d’un système Linux à l’aide des outils et bonnes pratiques SELinux

POUR QUI ?

- Administrateurs systèmes Linux confirmés souhaitant approfondir leurs compétences en sécurité
- Ingénieurs systèmes et responsables infrastructure
- Responsables sécurité (RSSI, responsables cybersécurité) souhaitant intégrer SELinux dans la stratégie de durcissement
- Auditeurs techniques ou membres d’équipes de réponse à incident (CSIRT, SOC)

Programme détaillé

1/ INTRODUCTION À LA SÉCURITÉ MANDATAIRE ET À SELINUX

- Différences entre DAC et MAC
- Objectifs et architecture de SELinux
- Les politiques de sécurité : targeted, minimum, mls
- Les modes de fonctionnement : enforcing, permissive, disabled

2/ EXPLORATION DES CONTEXTES DE SÉCURITÉ

- Structure et signification d'un contexte SELinux (user, role, type, level)
- Identifier et interpréter les contextes avec les options `-Z` et `ls -Z`
- Comprendre les transitions de contexte et leurs impacts sur la sécurité

3/ OUTILS DE GESTION DE BASE

- Utilisation des commandes `sestatus`, `getenforce`, `setenforce`, `selinuxenabled`
- Gestion des journaux SELinux (`/var/log/audit/audit.log`)
- Introduction à `ausearch` et `sealert` pour l'analyse des incidents

4/ PREMIERS CAS PRATIQUES

- Identification et résolution de blocages courants
- Manipulation des fichiers et répertoires protégés
- Exercices guidés sur le diagnostic et la correction d'erreurs SELinux

5/ GESTION DES BOOLÉENS ET DES CONTEXTES

- Découverte des booléens SELinux (`getsebool`, `setsebool`)
- Configuration persistante et temporaire des booléens
- Réétiquetage et restauration des contextes (`restorecon`, `fixfiles`, `setfiles`)

- Modification ciblée des contextes (`chcon`) et bonnes pratiques

6/ ADMINISTRATION DES POLITIQUES AVEC `semanage`

- Introduction à la commande `semanage` et ses sous-modules (fcontext, port, login, boolean)
- Configuration fine des accès réseau et des ports
- Création de règles personnalisées et gestion des exceptions

7/ ANALYSE ET DÉBOGAGE AVANCÉS

- Lecture et interprétation des logs d'audit
- Utilisation des outils `audit2why` et `audit2allow` pour générer des règles adaptées
- Comprendre les risques liés à la génération automatique de règles
- Étude de cas : durcissement d'un service web (Apache/Nginx) sous SELinux

8/ CONCEPTION DE MODULES DE POLITIQUE PERSONNALISÉS

- Structure d'un module de politique SELinux
- Création et compilation d'un module (`checkmodule`, `semodule_package`, `semodule`)
- Gestion du cycle de vie d'un module (ajout, suppression, mise à jour)
- Exemple complet : autoriser un processus personnalisé à accéder à une ressource spécifique

9/ OUTILS D'ANALYSE ET D'ADMINISTRATION AVANCÉE

- Utilisation des outils `seinfo`, `sesearch`, et `apol` pour explorer les politiques
- Interprétation des rôles et types dans une politique
- Techniques de traçage et de vérification de cohérence

10/ INTÉGRATION ET BONNES PRATIQUES DE MISE EN ŒUVRE

- Déploiement d'une configuration SELinux dans un environnement de production
- Méthodologie de test et validation avant mise en service
- Sauvegarde, export et documentation des politiques

- Audit de conformité et alignement avec les référentiels de sécurité (CIS, ANSSI)

Approche pédagogique

- Support Ecrit et Projection
- Exposés Interactifs, Podcasts et Vidéos
- Brainstorming et Jeux de Rôle
- Cas Pratiques et Labs inclus pour leur impact opérationnel
- Test de Validation des Acquis des Connaissances

Prochaines dates programmées

22 au 24 Juil. 2026	Casablanca - Maroc
16 au 18 Sep. 2026	Casablanca - Maroc
11 au 13 Nov. 2026	Casablanca - Maroc

Autres dates possibles sur demande. Contactez-nous pour organiser une session intra-entreprise.

Réservation & Renseignements

Téléphone : +212 522 247 210
Email : contact@innov-systems.com
Web : https//www.innov-systems.com

Scannez pour accéder à la fiche en ligne