Durcissement Sécurité Linux

Lien : https://innov-systems.com/formation/durcissement-securite-linux

DURÉE	RÉFÉRENCE	CATÉGORIE
5 jours (35h)	**SEC113**	**Sécurité des Systèmes et Serveurs**

OBJECTIFS DE LA FORMATION

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

- Comprendre l’intérêt des techniques de durcissement systèmes et réseau
- Maîtriser les différentes techniques de durcissement des systèmes Linux

POUR QUI ?

- Administrateurs
- Architectes
- Experts en sécurité
- Responsables sécurité

Innov Systems

Programme détaillé

1 / Présentation du système Linux

- Familles
- Fonctionnement
- Évolutions

2 / Introduction à la sécurité

- Menaces et attaques sur l'environnement Linux
- La sécurité de l'environnement Linux
- Les tests d'exposition (Shodan)

3 / Les politiques de sécurités

- Les politiques de sécurité
- Caractéristiques d'une PSSI
- Types de politiques de sécurité
- Normes et standards de sécurité

4 / Déploiement du système Linux : Bonnes pratiques

- Matériel
- Démarrage
- Configuration du noyau
- Paquetages logiciels
- Partitionnement des disques durs
- Les scripts de démarrage
- Réseau
- Ecrire des procédures Shell sécurisées (script)

Innov Systems

5 / Identification et authentification

- Définitions
- Politique de mots de passe
- Gestion des comptes utilisateurs
- Présentation de PAM (Pluggable Authentication Modules)
- Les niveaux de sécurité PAM
- Les OTP (Sécurité Hardware et Software)

6 / Protection des fichiers

- Droits standards des systèmes de fichiers Unix
- Les listes de contrôle d'accès
- Les attributs étendus
- Vérification de l'intégrité d'un système de fichiers
- Le chiffrement des fichiers
- Le ACL (Access Control List)

7 / Sécurisation du Noyau

- Compilation du noyau
- SELinux
- GrSecurity
- Sysctl
- Kernel auditing

8 / Les malwares sous Linux

- Les types de malwares sous Linux
- Simulation d'attaque
- Les rootkits
- Solutions anti-malwares

Innov Systems

9 / La sécurité du réseau

- Panorama des attaques
- Sécurité au niveau de la couche physique
- Sécurité au niveau de la couche liaison
- Sécurité au niveau de la couche réseau
- Daemons et serveurs
- VPN

10 / La sécurité par la surveillance du système

- L'utilitaire de consignation
- Outils d'analyse des logs
- Le dispositif d'accounting system
- Application de patchs
- Mise à jour du système

11 / Le patch management

- Mise en place d'une politique et solution de patch management

12 / Les sondes de détection d'intrusions

- Les IDS (Intrusion Detection System)
- Les IPS (Intrusion Prevention System)
- Les HIDS (Host-based Intrusion Detection System)
- Les HIPS (Host-based Intrusion Prevention System)
- Modèle de déploiement
- OSSEC et Tripwire
- OSSIM
- Les EDR (Endpoint Detection and Response)

13 / Durcissement complémentaire

Inov Systems

- Durcissement des serveurs Web
- Durcissement des serveurs mail
- Durcissement des serveurs FTP
- Durcissement Applicatif
- Durcissement des hyperviseurs
- Durcissement des VM
- Durcissement IPv6
- Sécurité des données (RGPD)
- Les plans DLP (Data Loss Prevention)

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

12 au 18 Jan. 2027	Présentiel - Casablanca
08 au 12 Mars 2027	Présentiel - Casablanca
03 au 07 Mai 2027	Présentiel - Casablanca
28 Juin au 02 Juil. 2027	Présentiel - Casablanca
23 au 27 Août 2027	Présentiel - Casablanca

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

Innov Systems

Réservation & Renseignements

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

Innov Systems — Tous droits réservés

Innov Systems