

# Sécurité Linux

## INFORMATIONS GÉNÉRALES

**Type de formation :** Formation continue

**Éligible au CPF :** Non

**Domaine :** Développement

**Action collective :** Non

**Filière :** Open Source - LAMP : Linux Apache PHP

**Rubrique :** Linux - Apache

**Code de formation :** AS913

## PRÉSENTATION

### Objectifs & compétences

Disposer de l'ensemble des fondamentaux nécessaires à la sécurisation de ses réseaux grâce à Linux : firewall, filtrage, ...

### Public visé

Architectes réseaux, administrateurs système et réseaux, responsables de parcs informatiques.

### Pré-requis

Il est nécessaire de posséder une première expérience d'administration de Linux ou d'avoir suivi le stage "Linux : Administration"

### € Tarifs

**Prix public :** 2500 €

### Tarif & financement :

Nous vous accompagnons pour trouver la meilleure solution de financement parmi les suivantes :

**Le plan de développement des compétences de votre entreprise :** rapprochez-vous de votre service RH.

**Le dispositif FNE-Formation.**

**L'OPCO** (opérateurs de compétences) de votre entreprise.

**France Travail:** sous réserve de l'acceptation de votre dossier par votre conseiller Pôle Emploi.

**CPF** -MonCompteFormation

Contactez nous pour plus d'information : [contact@aston-institut.com](mailto:contact@aston-institut.com)

## PROGRAMME

### 1. Sensibilisation à la Sécurité

- Enjeux de la sécurité des réseaux et des données
- Politique de sécurité
- Typologie des attaques
- Sécurité au niveau du noyau
- Services essentiels (DNS, WEB, Mail, FTP)
- Sécurité des autres logiciels (ICP, IE, etc.)
- Sécurité des postes clients

### 2. Sécurisation d'un Serveur

- Sécurité du système d'exploitation
- Sécurité des services
- Audit SSH
- Enjeux de SSH
- Algorithmes de chiffrement (RSA1, RSA2, DSA)
- Solutions existantes pour clients et serveurs SSH
- Mise en place du client et du serveur SSH
- Transferts de fichiers sécurisés
- Utilisation avancée (intégration de script ssh\_agent)
- Les faiblesses de SSH

### 3. Proxy

- Définition et fonctionnalités des proxies

### 4. Squid

- Filtrage avec SquidGuard

### 5. Firewall

### 📍 Lieux & Horaires

**Durée :** 35 heures

**Délai d'accès :** Jusqu'à 8 jours avant le début de la formation, sous condition d'un dossier d'inscription complet

### 📅 Prochaines sessions

Consultez-nous pour les prochaines sessions.

- Enjeux d'un pare-feu
- Les protocoles de communication
- Solutions existantes de pare-feu
- Cas pratique : Configuration de pare-feu avec iptables
- Outils d'assistance à la configuration du pare-feu : FWBuilder, GuardDog
- Audit : Vérification des solutions de sécurité mises en place

## MODALITÉS

### Modalités

**Modalités :** en présentiel, distanciel ou mixte . Toutes les formations sont en présentiel par défaut mais les salles sont équipées pour faire de l'hybride. – Horaires de 9H à 12H30 et de 14H à 17H30 soit 7H – Intra et Inter entreprise.

**Pédagogie :** essentiellement participative et ludique, centrée sur l'expérience, l'immersion et la mise en pratique. Alternance d'apports théoriques et d'outils pratiques.

**Ressources techniques et pédagogiques :** Support de formation au format PDF ou PPT Ordinateur, vidéoprojecteur, Tableau blanc, Visioconférence : Cisco Webex / Teams / Zoom.

**Pendant la formation :** mises en situation, autodiagnostic, travail individuel ou en sous-groupe sur des cas réels.

### Méthode

**Fin de formation :** entretien individuel.

**Satisfaction des participants :** questionnaire de satisfaction réalisé en fin de formation.

**Assiduité :** certificat de réalisation.

**Validations des acquis :** grille d'évaluation des acquis établie par le formateur en fin de formation.