

# Sécurisation des accès et des services

Sécurisation des services exposés (web, base de données, accès distants), gestion des ports, tunnels VPN, firewall, authentification multifactorielle, segmentation réseau.

## Modalité

Formation en centre de formation sur Colmar

## Durée totale

14 heures (2 jours)

## Tarif

2020.00€ TTC / pers.

## Modalités Pédagogiques

- Méthodes : Expositive, démonstrative et active
- Moyens : Cas pratique, mise en situation
- Ressources : Support de cours et Programme de formation
- Moyens techniques : Teams

## Prérequis

Bonne maîtrise des systèmes et réseaux

## Public cible

Administrateurs sécurité, responsables IT, auditeurs internes

## Délai et Modalités d'accès

Délai d'accès 10 jours après la signature du contrat. Dates à convenir entre le client et l'organisme de formation.

## Objectifs

À l'issue de la formation, le stagiaire doit être capable de maîtriser les compétences suivantes :

- Réduire la surface d'exposition réseau d'un serveur ou d'un poste critique
- Assurer un accès distant fiable et difficile à compromettre
- Maîtriser la gestion des droits d'administration pour limiter les abus et erreurs
- Appliquer un durcissement de base sur un service web exposé

## Déroulé du parcours de formation

### Sécurisation des ports et services réseau

- Analyse des services actifs (netstat, ss, nmap)
- Configuration et renforcement des services exposés : HTTP, SSH, FTP, etc.
- Pare-feu applicatif : iptables, ufw, pare-feu Windows avancé
- Notions de segmentation réseau (zones DMZ)

### Mise en place d'un accès distant sécurisé (VPN, tunnels, MFA)

- Configuration d'un tunnel VPN simple (Wireguard, OpenVPN)
- Accès distant sécurisé via bastion ou rebond SSH
- Authentification forte : gestion des clés, TOTP/MFA
- Surveillance des connexions (audit SSH, RDP)

### Contrôle des accès utilisateurs et droits d'administration

- Gestion des comptes à privilèges
- Application du principe de moindre privilège
- Utilisation des groupes, ACL, sudoers (Linux), UAC et GPO (Windows)
- Journalisation des actions administratives

### Sécurisation d'un service Web exposé

- Configuration SSL/TLS avec certificat (Let's Encrypt ou auto-signé)
- Protection contre les attaques courantes (XSS, brute-force, directory listing)
- Sécurisation via reverse proxy (Nginx, Apache)
- Test avec outils de scan de vulnérabilités (Nikto, OpenVAS)

### Évaluations formatives

Le suivi de la progression pédagogique est assuré par des quiz de validation des connaissances à la fin des modules et des exercices d'application pratiques (mises en situation).

### Modalités d'évaluation

Le formateur évalue la progression en cours de formation à l'aide de cas pratiques, mises en situation, QCM...  
Un test de positionnement sera complété en amont et en aval afin de valider les compétences acquises.

### Formateurs

Tous les formateurs de CE FORMATION sont des professionnels en activité, à leur compte ou salarié, ils conservent ainsi "les mains dans le cambouis".  
Ils ont chacun leur spécialité, mais également une vision globale du métier et sont dotés d'un niveau BAC+3 ou supérieur.  
Ils sont tous également formateurs dans d'autres centres de formation, depuis au minimum 2 ans, et sont connus et respectés pour leur engagement, leur pédagogie et leur humilité face au métier et à sa constante évolution.

### Contacts

CE FORMATION  
07.68.48.96.63  
[contact@ce-formation.com](mailto:contact@ce-formation.com)  
CE FORMATION

### Accessibilité aux PSH

Cette formation est accessible aux personnes en situation de handicap.  
Si la situation nécessite des aménagements spécifiques, le candidat peut contacter notre référent handicap :  
Christel EHRHART  
07.68.48.96.63  
[christel@ce-formation.com](mailto:christel@ce-formation.com)

### Indicateurs

Taux de satisfaction : *En cours*

Taux d'accomplissement : *En cours*