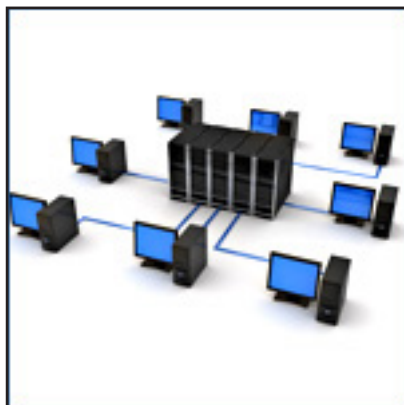


## SECURITE DES SYSTEMES INFORMATIQUES



### Objectifs

Acquérir une vision globale de la sécurité d'un système d'information. Comprendre les enjeux actuels en matière de sécurité et analyser les risques, la sécurité des systèmes informatiques (postes et serveurs).

Apprendre les méthodes et moyens de sécuriser le système d'information. Et enfin connaître les méthodes pour évaluer la sécurité mise en place.

Une formation concrète avec de nombreux cas pratiques..

► **Type de cours : Stage pratique**

► **Référence : SSI**

► **Durée: 3 jours - 21h de formation**

► **Lieu : Paris en inter ou en intra**

**Formation éligible au CPF - Code : 146867**  
**Passage de la certification SECURITE DES TI**



### Méthodes pédagogiques

- Un poste de travail par stagiaire
- Accès Internet
- Exercices individuels sur PC
- Supports de cours
- Mises en application des logiciels
- Evaluation en fin de stage

**ATTESTATION DE FORMATION  
DELIVRÉE EN FIN DE STAGE**

#### Pré-requis :

Notions de réseaux informatiques et d'internet.

#### Public visé :

Responsables sécurité informatique, Administrateurs sécurité, Gérants d'entreprise, Managers

# Programme du stage

## **Analyse du risque et du coût**

Que veut t'on protéger ? Pourquoi ?  
Return On security Investment (ROSI)  
Définition correct des accès suivant les utilisateurs  
Qui accède à quoi ?  
Qualification de la typologie des utilisateurs  
Gestion de la politique de mot de passe

## **Sécurité des réseaux**

Principaux types d'attaques référencés  
Firewall  
Proxy  
IPS  
VPN  
Wi-Fi

## **Sécurité postes et serveurs**

GPO  
Antivirus  
Chiffrement

## **Sauvegarde et mise à jour**

Politique de sauvegarde des équipements  
Politique de mise à jour  
Redondance des infrastructures

## **Supervision et analyse**

Centralisation des logs  
Indicateur de suivi  
Rapport régulier sur les accès (Type, nombre, évolution)  
Réglementation

## **Continuité de service**

Définition d'un PRA  
Définition d'un PSI  
Recensement des métiers et des postes clés

## **Sensibilisation des utilisateurs**

Formation  
Affichage  
Mailing  
Anticipation des erreurs courantes

## **Benchmark**

Méthodes pour tester la sécurité de son SI

## **Veille technologique**

Adaptation et ajustements  
Évolution du SI et des infrastructures