

# SECURITE INFRASTRUCTURE

## Stratégie et outils

Référence : IESSECINFR

PLAN DE COURS

<b>Objectifs</b> : Évaluer les risques internes et externes liés à l'utilisation d'Internet ; Comprendre comment garantir la fiabilité et la confidentialité des données grâce aux différentes solutions sécurisantes.	
<b>Prérequis</b> : Il est nécessaire d'avoir une bonne connaissance des réseaux Windows ou Unix ou du protocole TCP/IP	
<b>Public</b> : Techniciens, Webmasters	
<b>Niveau</b> : Débutant	<b>Durée standard préconisée</b> : 2 jours
<b>Pédagogie</b> : alternance d'apports théoriques et nombreux exercices de mise en pratique	
<b>Moyens pédagogiques</b> : un ordinateur multimédia par apprenant, ordinateur et vidéoprojecteur pour l'animateur	<b>Évaluation des acquis</b> : Mise en pratique à l'aide d'exercices en autonomie puis corrigés individuellement et collectivement
<b>Suivi après formation</b> : • Certificat de stage • Bilan de formation rempli par le formateur	• Évaluation de satisfaction à chaud remplie par l'apprenant • Un ouvrage de référence (remis en formation)

### Détail des objectifs

	Cocher les OBJECTIFS	
	définis lors du tour de table	traités durant la formation
<b>Développer la politique de sécurité</b> .....	<input type="checkbox"/>	<input type="checkbox"/>
Gérer la sécurité et la continuité .....	<input type="checkbox"/>	<input type="checkbox"/>
Gérer les applications et les outils disponibles .....	<input type="checkbox"/>	<input type="checkbox"/>
<b>Gérer la sécurité des systèmes Unix et Windows</b> .....	<input type="checkbox"/>	<input type="checkbox"/>
Gérer l'authentification.....	<input type="checkbox"/>	<input type="checkbox"/>
Gérer les services réseau .....	<input type="checkbox"/>	<input type="checkbox"/>
<b>Gérer la sécurité client</b> .....	<input type="checkbox"/>	<input type="checkbox"/>
Gérer les certificats clients.....	<input type="checkbox"/>	<input type="checkbox"/>
Gérer les options de sécurité des navigateurs.....	<input type="checkbox"/>	<input type="checkbox"/>
<b>Gérer la sécurité serveur</b> .....	<input type="checkbox"/>	<input type="checkbox"/>
Gérer l'authentification des utilisateurs .....	<input type="checkbox"/>	<input type="checkbox"/>
Protéger l'accès au serveur .....	<input type="checkbox"/>	<input type="checkbox"/>
<b>Mettre en place l'Intranet via le réseau public</b> .....	<input type="checkbox"/>	<input type="checkbox"/>
Déployer un réseau privé virtuel (VPN) .....	<input type="checkbox"/>	<input type="checkbox"/>
Utiliser les méthodes d'authentification (PAP, CHAP) .....	<input type="checkbox"/>	<input type="checkbox"/>
<b>Mettre en place des certificats</b> .....	<input type="checkbox"/>	<input type="checkbox"/>
Gérer les serveurs de certificats .....	<input type="checkbox"/>	<input type="checkbox"/>
Gérer les certificats numériques.....	<input type="checkbox"/>	<input type="checkbox"/>
<b>Intégrer les serveurs proxy</b> .....	<input type="checkbox"/>	<input type="checkbox"/>
Définir l'architecture d'un proxy .....	<input type="checkbox"/>	<input type="checkbox"/>
Gérer les proxys avec des firewalls .....	<input type="checkbox"/>	<input type="checkbox"/>
<b>Détecter et surveiller les faiblesses</b> .....	<input type="checkbox"/>	<input type="checkbox"/>
Définir les informations à surveiller .....	<input type="checkbox"/>	<input type="checkbox"/>
Analyser le trafic réseau.....	<input type="checkbox"/>	<input type="checkbox"/>
<b>Mettre en place la sécurité des données de l'entreprise</b> .....	<input type="checkbox"/>	<input type="checkbox"/>
Évaluer les besoins de l'entreprise.....	<input type="checkbox"/>	<input type="checkbox"/>
Définir les règles de la mise en place d'un plan de sécurité .....	<input type="checkbox"/>	<input type="checkbox"/>

Compléments : .....

.....

.....