

## LA VEILLE INFORMATIQUE

### OBJECTIF :

Le Web est la plus formidable base de données pour les entreprises : informations sur les concurrents, marchés nouveaux, tendances et analyses macro-économiques, études et sondages ....

Au-delà des techniques de base de la recherche sur Internet, les participants apprendront :

- ✓ Exploiter des fonctionnalités avancées de recherche
- ✓ Mettre en place une veille personnelle d'informations
- ✓ Identifier les outils de surveillance de pages, de sites et de recherches
- ✓ Détecter les "signaux faibles"
- ✓ Recourir aux assistants et agents les plus adaptés
- ✓ Evaluer l'information trouvée sur Internet
- ✓ Vérifier et analyser les résultats de l'activité de veille

### DESTINATAIRES :

Formation destinée aux utilisateurs avertis d'Internet qui souhaitent un approfondissement dans la maîtrise des outils et des méthodes de recherche d'informations.

DUREE : 1 jour

### PROGRAMME :

1. Rappels et approfondissements  
La recherche d'informations sur Internet :  
Outils et méthodes  
Le rôle des agents intelligents:  
Que peuvent-ils apporter à vos recherches quotidiennes?
2. Définitions et enjeux de la veille
3. Les particularités de la veille sur Internet  
Qui peut utiliser cette information ?  
Pourquoi faire de la veille sur Internet ?
4. Méthodologie spécifique à la veille sur Internet : stratégie et outils
5. Veille d'informations - organisation d'une veille personnelle d'information adaptée aux participants
6. Les problèmes posés par l'information sur Internet
7. Mener une étude sur Internet
8. Organiser une revue de presse à partir du web
9. Les outils de capture sur le web
10. Répertoire Internet sur la veille  
Cabinets spécialisés  
Ressources gouvernementales  
Logiciels de veille  
Formations  
Livres  
Documentation en ligne  
Producteurs et serveurs de banques de données

## SECURITE INFORMATIQUE ET PROTECTION DES DONNEES

### OBJECTIF :

Ce cours apporte les connaissances fondamentales dont vous avez besoin pour analyser les risques qui pèsent sur votre système et de créer une politique de sécurité réaliste qui protégera vos ressources des intrusions, destructions ou vols.

### DESTINATAIRES :

Formation destinée aux utilisateurs avertis d'Internet qui souhaitent un approfondissement dans la maîtrise des outils et des méthodes de recherche d'informations. Administrateurs de réseaux/systèmes, managers, équipes de support technique.

DUREE : 1 jour

### PROGRAMME :

1. Sécurité informatique  
La gestion du mot de passe  
Hacker, Cracker et Phreaker  
Script Kiddies , Zombie  
Les précautions/Les conséquences  
Bris de sécurité/Infiltrations  
Social engineering" - arnaques  
Vandalisme de sites /Vol de sites
2. Les virus  
Qu'est-ce qu'un virus ?  
Les types de virus/Les précautions  
Les faux virus (hoax)/Références
3. Interconnexion de réseaux : un point vulnérable majeur  
Concepts de base des systèmes d'exploitation et de TCP/IP Améliorations de la sécurité
4. Développer votre politique de sécurité  
Les démarches à faire dès maintenant  
Répondre aux attaques
5. Pourquoi sécuriser ? parlons technique  
Les enjeux Protection physique  
La vulnérabilité des systèmes Les données  
Les dommages Se protéger de l'extérieur  
Les solutions de sécurité du marché  
Ce qu'un "firewall" peut et ne peut pas faire  
Le "firewall" comme outil pour mettre en œuvre votre politique de sécurité
6. Qui nous menace ? questions réponses  
D'où vient le risque Echange et discussion  
Les différents types d'attaques  
Profils des attaquants, leurs enjeux  
Techniques de défense
7. Parlons technique  
Les enjeux Protection physique  
Evaluation et analyse des risques Contrôle des accès et audit  
La vulnérabilité des systèmes/ Les données  
Les dommages : se protéger de l'extérieur  
La sécurité passive  
Les solutions de sécurité du marché