

## Sécuriser son réseau et son infrastructure TCP/IP

Référence	Niveau	Durée
AT-PI-206	1	2 jours

### Avis de l'expert

**La généralisation des infrastructures TCP/IP dans l'entreprise et l'utilisation intensive d'Internet poussent des individus malveillants à tenter de nuire aux entreprises quelque soit leur taille. Ce séminaire de 2 jours dresse un panorama des failles utilisées par les hackers pour s'introduire dans nos réseaux et des solutions techniques permettant de sécuriser son infrastructure**

### Bénéfices métier

- Identifier les failles de l'infrastructure TCP/IP qui peuvent introduire des risques pour l'entreprise.
- Avoir un aperçu exhaustif des solutions permettant de prévenir les risques et d'en limiter les conséquences.
- Avoir des conseils pratiques pour la mise en place d'une politique efficace de lutte contre les intrusions et les actes de malveillance.

### Parcours pédagogique

#### Introduction

- Rappel sur les principaux concepts de l'architecture TCP/IP
- Historique de la sécurité des SI
- Les principales normes et méthodes en vigueur permettant d'apprécier les risques

#### Présentation des menaces et des risques liés à l'usage de TCP/IP

- Les catégories de menaces
- Les catégories d'attaquants
- Les techniques utilisées par les hackers pour s'introduire dans nos réseaux TCP/IP

#### Présentation des principales attaques

- Les attaques au niveau des protocoles réseaux
  - L'attaque MAC Flooding
  - L'attaque ARP Spoofing
  - Les attaques ICMP
  - Les attaques VLAN Hopping et Double Tagging
  - Les Private VLANs
  - Les attaques STP
  - Les techniques BPDU Guard et BPDU Filtering
  - Les attaques de type Rerouting
  - Les attaques sur les protocoles de routage : RIP, OSPF et BGP

#### Les attaques au niveau des applications réseaux

- Les attaques DHCP
- Les attaques DNS.
- Les attaques Session Replay et Session Hijacking
- Les attaques SNMP

#### L'état de l'art de la sécurité des réseaux TCP/IP

- Les architectures de sécurité périmétrique.
- Les différents composants de sécurité (FW, VLAN, ...).
- La détection et la prévention des intrusions (IDS/IPS).
- Les contrôles d'accès au niveau du réseau (NAC).
- La lutte contre les codes malveillants (lutte anti-virale, lutte anti-malware, lutte anti-spams, ...).
- Les solutions de surveillance et de traçabilité

#### Conclusion

- Recommandations générales pour sécuriser son infrastructure TCP/IP
- Synthèse des techniques de protection

### Comment se déroule le stage ?

Cours théorique avec de nombreux exemples et retours d'expérience.  
Echanges interactifs entre les participants et le formateur

### Public concerné

- Directeur des systèmes d'information ou responsable informatique
- RSSI, Chefs de projet sécurité
- Architectes informatiques