

## Etat de l'art de la sécurité de l'information

### De la mise en place de la politique de sécurité à la maîtrise des risques

Référence	Niveau	Durée
AT-PI-202	1	3 jours

#### Avis de l'expert

Pour faire face à la montée en puissance des menaces qui pèsent sur nos systèmes d'information, le monde de la sécurité doit s'adapter, et est de fait en perpétuelle évolution aussi bien sur le plan des technologies que des méthodes et modèles conceptuels sous-jacents.

Ce séminaire de 3 jours dresse un état de l'art complet des outils organisationnels et techniques de maîtrise du risque informatique.

#### Bénéfices métier

- Identifier les différents domaines de la sécurité et de la maîtrise des risques liés aux informations
- Disposer d'information sur les tendances actuelles, que ce soit dans les menaces ou dans les solutions à notre disposition
- Connaître les principaux outils et acteurs du marché (y compris logiciels libres), avec à chaque une présentation des forces et des faiblesses des solutions existantes

#### Itinéraire pédagogique

##### Les solutions du marché seront présentées pour chaque thème

- Introduction – objectif de la formation

##### 1 – Tendances des menaces et les risques

- Statistiques sur la sécurité
- Tendances dans l'évolution des menaces
- Profil des attaquants
- Architecture générale SSI

##### SECURITE DES RESEAUX ET DES SYSTEMES

##### 2 – Sécurité périmétrique

- Fonctionnalités proposées
- Logiciels, appliances et UTM
- Mise en cluster, scalabilité

##### 3 – Solutions antivirusales

- Tendances du risque viral
- Protection des postes et serveurs
- Sécurité des flux et protection des passerelles

##### 4 – Solutions antispam

- Evolution du spamming (chiffres et technologies)
- Solutions de lutte anti-spam

##### 5 – Détection et prévention d'intrusion

- Principes et concepts
- Différence entre IDS et IPS, avantages comparés

##### 6 – Network Access Control

- Concept de NAC
- Limites des technologies

##### 7 – Sécurité des contenus

- Principes et concepts
- Sécurité des flux applicatifs (messagerie, messagerie instantanée, VoIP...)

##### 8 – Qualité de service et supervision

- Principes et concepts
- Security Information Management

##### 9 – Haute disponibilité

- Haute disponibilité des réseaux et des liens
- Equilibrage, routage dynamique
- Haute disponibilité des systèmes, clusters, virtualisation
- Haute disponibilité des données, SAN et sauvegardes

##### NOMADISME

##### 10 – Sécurité des postes nomades

- Problèmes de sécurité liés au nomadisme
- Protection d'un poste vs. solutions spécifiques
- Mise en quarantaine

##### 11 – Accès distants, VPN SSL

- Concept et standards de VPN sécurisé
- Intérêts du VPN SSL
- Contrôle du point d'accès

##### GESTION DES IDENTITES ET DES ACCES

##### 12 – Gestion des identités

- Gestion du cycle de vie des utilisateurs
- Problématique organisationnelle
- Problématique technique
- Gestion des identités vs. SSO

##### 13 – Authentification forte

- Systèmes cryptographiques
- Tokens
- Systèmes biométriques

##### 14 – Authentification LDAP et SSO

- Urbanisation de l'authentification
- Architectures à base d'annuaire LDAP
- SSO

##### 15 – Fédération d'identités

- Enjeux de la fédération d'identités
- Concepts et normes

##### 16 – Infrastructures de clés publiques

- Cryptographie à clé publique, certificats de clés
- Autorités de certification et d'enregistrement
- Révocation et gestion des urgences

##### Produits et services du marché SECURITE APPLICATIVE

##### 17 - Applications web et web services

- Architecture des applications web
- Normes et standards de sécurité des web services

##### 18 - Développement sécurisé

- Principes de développement sécurisé
- Tests et analyse de code
- Méthodes et outils

##### RISK MANAGEMENT, NORMES

##### 19 – Méthodes d'audit et d'analyse des risques

- Normes et méthodes d'audit
- Etat des méthodes d'analyse des risques informatique

##### 20 – Normes de sécurité

- ISO27000 : système de management de la sécurité de l'information
- BS25999 : continuité des activités
- Autres normes internationales de sécurité des SI

##### 21 – Outils d'audit et de test de sécurité

- Typologie des audits et outils d'audit
- Typologie des tests de sécurité

#### Comment se déroule le stage ?

Les échanges entre participants et l'expérience du formateur facilitent les retours d'expérience.

#### Public concerné

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