



# C2POINTS

La passion de l'informatique

MI34

## Sécurité des systèmes d'information

---

- **Objectif**

Donner les compétences nécessaires aux stagiaires pour connaître les risques introduits dans les systèmes d'information

A l'issue de cette formation, ils comprendront la terminologie des réseaux, ils connaîtront les diverses technologies et solutions de la sécurité des réseaux.

- **Public**

Responsables informatiques ayant la gestion d'un réseau et souhaitant le sécuriser.

- **Niveau requis**

Expérience pratique des environnements réseau TCP/IP et des systèmes d'exploitation.

- **Durée**

4 Jours

- **Technicité**

@ @ @

---

- **MODULE 1**

### INTRODUCTION SUR LA SECURITE

#### Sécurité des systèmes d'exploitation et applications

Sensibilisation aux correctifs

Patchs applicatifs

Les virus informatique

Les programmes espions

#### Sécurité des réseaux

Sécurité de la pile de protocoles TCP/IP

Rappels sur TCP/IP

Descriptions des attaques liées à cette pile de protocoles

- **MODULE 2**

### METHODOLOGIE : LES DIFFERENTES APPROCHES

#### Impacts des violations de la sécurité.

#### Discipline de gestion des risques de sécurité

Evaluation des risques

Développement et implémentation de solution

Exploitation

#### Modèle de défense en profondeur

Couche Sensibilisation et procédures

Couche Sécurité physique

Couche Périmètre

Couche Réseau interne

Couche Hôtes

Couche Applications

Couche Données

- **MODULE 3**

## **LES MENACES ET TYPES D'ATTAQUES**

### **Identification du type de menaces et d'attaques**

Les refus de services (DoS et DDos)

L'usurpation d'identité (Ingénierie sociale, attaque MITM, spoofing)

Attaques des services réseau (Web, bases de données)

Dépassement de buffers (Buffers Overflow)

### **Outils de détection**

Les pare-feu

La détection et prévention d'intrusion

Les freewares

- **MODULE 4**

## **LES OUTILS DE SECURITE**

### **Réponse aux incidents**

Liste des contrôles de réponse

Méthodes conseillées

### **Solutions anti-virus**

#### **Solutions pare-feu client**

#### **Solutions anti spywares**

#### **Solutions Microsoft SUS et WSUS pour la gestion des correctifs**

#### **Sites Internet des Editeurs**

#### **Impacts des délais d'application des correctifs**

- **MODULE 5**

## **SECURISATION DES SYSTEMES D'INFORMATION**

### **Sécurité des serveurs**

Introduction à la sécurité des serveurs – Sécurité de base

Sécurité des domaines

Renforcement de la sécurité des serveurs membres

Renforcement de la sécurité des contrôleurs de domaines

Renforcement de la sécurité des serveurs à rôle spécifique

Renforcement de la sécurité des serveurs autonomes

### **Sécurité des postes de travail**

Composants de la sécurité des ordinateurs clients

Mises à jour de logiciels

Considérations sur les mots de passes

Protection des données

Sécurité des applications

Protection des canaux d'information

Pare-feu et anti-virus

Informatique mobile

Réduction de période d'indisponibilité

- **MODULE 6**

## **SECURISATION DES RESEAUX LOCAUX (LAN) ET ETENDUS (WAN)**

### **LAN : Protocol IPSec**

Notions de certificats

Cryptage de l'authentification

Cryptage des transferts de données

### **Technologies de sécurisation des réseaux Wifi**

Authentification Wep, WPA, 802.1x

Filtrage des adresses MAC

Clé de cryptages

### **WAN : Utilisation des VPN**

Protocol de « tunneling » PPTP, L2TP et MPLS

### **Sécurisation des accès réseau à distance**

- **ATELIER**

**Simuler une attaque virale...**