

## Formation Sécurité Internet Intranet



Au travers de deux jours de formation nous traiterons des différentes problématiques liés à la sécurité d'un système d'information diffusé sur Internet ou un réseau Intranet. Nous traiterons notamment de l'importance d'une bonne architecture et aborderons la sécurité d'un point de vue organisationnel, fonctionnel et juridique.

Cette formation permet d'obtenir une vue d'ensemble sur les différentes techniques permettant l'évaluation de la sécurité du système d'information

### Objectifs

---

- Comprendre comment fonctionne la sécurité d'un système basé sur les technologies Internet
- Acquérir la maîtrise globale de la sécurisation d'un réseau privé utilisant les technologies Internet / Intranet
- Sécuriser l'interconnexion réseau privé / réseaux extérieurs

### Public concerné

---

- Responsable sécurité
- Chef de projets
- Acteur d'un projet sécurité

### Pré requis

---

- Connaissance des réseaux Internet / Intranet

### Une formation de 2 jours

---

#### Caractéristiques

**Tarif : 1200 € HT par personne**

**Numéro de formateur : 11753687675**

**Nombre d'heures : 14**

**Référence : SINI**

**Contact : Loic LE FUR**

**Telephone : 01.41.16.83.70**

**Email : [formation@alterway.fr](mailto:formation@alterway.fr)**

## Description des modules

num	Module
<b>1</b>	<b>Introduction</b>
<b>Détails</b>	<ul style="list-style-type: none"><li>- Le contexte, les concepts fondamentaux de la sécurité, les objectifs</li><li>- Rappels techniques sur les protocoles (TCP/IP, TCP, IP, UDP, ICMP)</li></ul>
<b>2</b>	<b>Architecture</b>
<b>Détails</b>	<ul style="list-style-type: none"><li>- Rôle, principes et structure d'une architecture sécurisée</li><li>- Eléments d'une architecture basiques : routeur filtrant, machine relais</li><li>- Eléments d'une architecture complètes : routeur, serveur de relaying</li><li>- Eléments d'une architecture multistrates : DMZ, routeur, objectifs</li><li>- Cloisonnement physique : DMZ</li><li>- Cloisonnement par authentification des utilisateurs : relaying http</li><li>- Cloisonnement par tunnels</li></ul>
<b>3</b>	<b>Le filtrage IP</b>
<b>Détails</b>	<ul style="list-style-type: none"><li>- Rôle, principe et structure du filtrage IP (en bout, en traversée, double sécurité)</li><li>- Différents types de filtrage (statique, à états, dynamique)</li><li>- Eléments de filtrage (traduction d'adresses, construction d'un filtre, fonctionnement d'un filtre)</li><li>- Les limites du filtrage</li></ul>
<b>4</b>	<b>Le relaying applicatif</b>
<b>Détails</b>	<ul style="list-style-type: none"><li>- Objectifs, enjeux et rôle du relaying applicatif</li><li>- Concepts et caractéristiques du relaying applicatif</li><li>- Les services relayages</li><li>- Les limites du relaying applicatif</li></ul>
<b>5</b>	<b>Critères de choix d'une solution de sécurité Internet</b>
<b>Détails</b>	<ul style="list-style-type: none"><li>- Le marketing et le vocabulaire</li><li>- Boîtes noires et boîtes blanches</li><li>- Maîtrise technique, disponibilité des sources, architecture de la solution</li><li>- Capacité de filtrage IP et de relaying</li><li>- La sécurité dans le temps</li><li>- Les produits du marché</li></ul>
<b>6</b>	<b>Mise en place de l'exploitation d'une passerelle de sécurité Internet</b>
<b>Détails</b>	<ul style="list-style-type: none"><li>- Organisation et formalisation de l'exploitation</li><li>- Plan de secours</li><li>- Responsabilisation des utilisateurs</li><li>- Journalisation (Outils, centralisation et gestion, exemple avec IPFC)</li><li>- Veille technologique en vulnérabilités</li><li>- Réagir en cas d'attaque / d'incident</li></ul>
<b>7</b>	<b>Analyses, audits et tests d'intrusions</b>
<b>Détails</b>	<ul style="list-style-type: none"><li>- Introduction définitions et comparatifs</li><li>- Analyse de risque et ISO17799</li><li>- Audits (différents types, objectif d'un audit et exemples)</li><li>- Tests d'intrusion (types, objectifs, limites)</li></ul>
<b>8</b>	<b>Infogérance de sa sécurité Internet/Intranet</b>
<b>Détails</b>	<ul style="list-style-type: none"><li>- Intérêt et besoin des MSSP</li><li>- Méthodologie pour infogérer sa sécurité</li><li>- Les questions à poser</li></ul>
<b>9</b>	<b>Les ASP de tests de vulnérabilité</b>
<b>Détails</b>	<ul style="list-style-type: none"><li>- Outils, objectif et acteurs du marché</li></ul>

- Caractéristiques, limites
- Tests de vulnérabilités assistés

### 10 Aspects juridiques

- Détails**
- Respect de la vie privée / CNIL
  - Responsabilités des dirigeants
  - Plainte pour piratage
  - Chiffrement et journaux