

---

# Programme de Formation

---

## Sécurité Informatique : les bases

---

### Organisation

---

**Durée** : 14 heures

**Mode d'organisation** : Mixte

**Nombre de participants** : 10

**Lieu de la formation** :

### Contenu pédagogique

---



#### **Public visé**

Toute personne soucieuse de renforcer sa compréhension des enjeux posés par la sécurité informatique et leur impact sur les activités professionnelles.



#### **Prérequis**

Aucun



#### **Admission** (Délais d'accès)

Après avoir complété le formulaire d'entrée, un calendrier des sessions vous sera proposé.

En fonction du mode de financement prévu et de la validation du dossier, compter un délai de 15 jours pour accéder à la session de formation choisie.



Une fois la date sélectionnée et les formalités d'accès validées, une confirmation de votre participation vous sera transmise par courriel.

#### **Accessibilité**

Nos locaux sont certifiés ERP PMR.

Nous pouvons adapter nos formations à certains handicaps déclarés.

Dans le cas contraire, nous serons en mesure de vous rediriger.

Merci de nous faire part des adaptations qui, selon vous, seraient nécessaires.

Notre référent handicap : [ref.handicap@ls-in.com](mailto:ref.handicap@ls-in.com). / + 33 6 78 50 00 31

Pour toutes informations complémentaires, vous pouvez contacter notre [équipe LS](#).



#### **Objectifs de la formation / Critères de réussite**

- Ordonner les concepts, les technologies et les solutions de sécurité des réseaux informatiques (coopération avec les spécialistes et pilotage des prestataires)
- Intégrer la vision globale de la sécurité
- Reconnaître les rôles des intervenants du secteur et leurs métiers
- Identifier les nouveaux enjeux associés à la sécurité informatique



#### **Intervenant**

Intervenants spécialisés dans le domaine de la cybersécurité.



#### **Description / Contenu**

##### **Jour 1**

1. Principes généraux de la sécurité informatique
2. Comprendre les différents types de vulnérabilités et d'attaques
3. Connaître le fonctionnement des équipements de protection dédiés

4. Exploiter les plates-formes spécialisées de sécurité

#### **Jour 2**

1. Utiliser la combinaison des équipements pour sécuriser
2. Mesurer les impacts de la mise en place de la sécurité sur la performance du système global et l'architecture du SI
3. Les référentiels pour gérer la sécurité informatique
4. Les grandes tendances



### **Modalités pédagogiques**

Groupe de 3 à 8 personnes maximum.

Approche résolument interactive privilégiant la mise en pratique des acquis tout au long du module. Pendant le parcours, l'intervenant implique les stagiaires dans leur propre formation, par l'emploi de techniques actives et motivantes (mise en situation du stagiaire, jeux de rôle, simulations), adaptées à chaque cas et mesurant les écarts éventuels entre les attendus et les acquis observés, afin de mettre en place dès que possible des actions correctives.

L'assiduité et la participation active seront les garants de la réussite de l'apprentissage.



### **Moyens et supports pédagogiques**

Présentation théorique, à distance via "Dendreo Live", test analytiques et mises en situation.

Participation à la [Communauté de pratiques](#).



### **Modalités d'évaluation et de suivi**

Chaque stagiaire reçoit en amont de la formation un questionnaire permettant de mesurer ses compétences, connaître son profil et ses attentes. Tout au long de la formation, les participants sont évalués au moyen de différentes méthodes (quizz, ateliers, exercices et/ou de travaux pratiques, etc.) permettant de vérifier l'atteinte des objectifs. Un questionnaire d'évaluation à chaud est soumis en fin de formation pour s'assurer de l'adéquation des acquis de la formation avec les attentes des bénéficiaires. Un questionnaire d'évaluation à froid est adressé 2 mois plus tard.

Une attestation de réalisation de la formation est remise en fin de formation.