

## Formation « Fondamentaux techniques de la cybersécurité »

**Réf : SECUCYBER**

Si le fait d'être sensibilisé à la sécurité est important quel que soit le poste occupé, comprendre les concepts de base de la SSI est une nécessité absolue pour le personnel technique de l'entreprise. En effet, la sécurité n'est pas seulement l'affaire du RSSI et de ses équipes : administrateurs système et réseau, architectes, développeurs ont tous leur rôle à jouer dans la protection de l'entreprise et de son patrimoine.

La formation SECUCYBER, en abordant sur 5 jours tous les aspects techniques de la sécurité informatique, vise à apporter à cette population les connaissances indispensables leur permettant de choisir, d'implémenter et de maintenir les mesures de sécurité propres à leur domaine de compétence.

### Objectifs

- Être en mesure dans tous les domaines techniques de la sécurité (système, réseau, applications, cryptographie...) de :
  - Maîtriser le vocabulaire et les concepts principaux du domaine
  - Connaître différentes techniques d'attaque
  - Choisir et appliquer les bonnes mesures de sécurité

### Durée & horaires

- 5 jours soit 35 heures
- Horaires : de 9h30 à 12h et de 13h30 à 18h00.

### Nombre de participant

- Minimum 6 participants – Maximum 24 participants

### Public visé

- Administrateurs système ou réseau
- Architectes
- Développeurs
- Personnel débutant ou souhaitant acquérir de bonnes bases techniques en SSI
- Prestataires référencés par [cybermalveillance.gouv.fr](https://cybermalveillance.gouv.fr) voulant le label "expert cyber"

### Pré-requis

- Bonnes connaissances en informatique

### Méthode pédagogique

- Cours magistral illustré par des travaux pratiques réguliers

### Supports

- Support de cours au format papier en français en présentiel et au format numérique en distanciel
- Ordinateur portable mis à disposition du stagiaire
- Cahier d'exercices et corrections des exercices
- Certificat attestant de la participation à la formation

## Modalité d'évaluation de la formation

- Fiche d'évaluation remise aux stagiaires à l'issue de la formation afin de recueillir leurs impressions et identifier d'éventuels axes d'amélioration
- Evaluation de pré-formation envoyée avant le début de la formation
- Evaluation de mi-formation effectuée en session par le formateur au moyen de QCM et de travaux pratiques
- Examen final à la fin de la formation (cf certification)  
Ces évaluations ont pour but de valider les compétences acquises.

## Certification

- A l'issue de cette formation, le stagiaire a la possibilité de passer un examen ayant pour but de valider les connaissances acquises. Cet examen de type QCM dure 1h30 et a lieu durant la dernière après-midi de formation. La réussite à l'examen donne droit à la certification SECUCYBER par HS2.

## Programme

### Module 1 : SSI - principes de bases

- Pourquoi la SSI ?
- Notion de risque
- Les règles de base
- Contrôle d'accès
  - AAA
  - Gestion des utilisateurs
  - Authentification
  - Gestion des privilèges

### Module 2 : Cryptographie

- Concepts fondamentaux
- Fonctions de base
  - Chiffrement
  - Hachage
  - Signature
- Protocoles
  - TLS
  - IPSec
  - SSH
- PKI / IGC

### Module 3 : Réseau

- Modèles théoriques : OSI, TCP/IP
- Attaques classiques
  - Découverte de ports
  - Man-in-the-Middle
- Contrôle d'accès réseau
- Segmentation
  - Qu'est qu'une bonne architecture ?
  - Comment segmenter son réseau
  - VLAN
  - Parefeu

- Proxy
- Réseaux sans fil
- Sécuriser le Cloud

### Module 4 : Applications

- Architecture n-tiers
- Protocoles
- Authentification et sessions
- Top 10 de l'OWASP
- Buffer Overflow
- Processus de développement

### Module 5 : Windows

- Installation
- Bitlocker
- Mesures Windows 10 :
  - Device Guard
  - Application Guard
  - Exploit Guard
- Gestion des administrateurs
- Éviter le Pass-The-Hash

### Module 6 : Linux

- Système de fichiers
- Minimisation
- Comptes utilisateurs
- Authentification
- SELinux
- AppArmor
- SSH
- Netfilter
- Journalisation

