



### Durée

- ▶ **10 heures** : 8 heures en collectif, 1 heure de travail individuel et 1 heure d'accompagnement personnalisé.



### Moyens pédagogiques

- ▶ Sessions collectives et individuelles,
- ▶ Formation à distance,
- ▶ Exercices d'application en séance et intersession.



### Appréciation des résultats

- ▶ Session individuelle,
- ▶ Evaluation à chaud et à froid.

## Contenu et Programme de la formation

- ▶ **Présentation de l'action, de l'intervenant**  
PC, serveurs, tablettes ...) : Windows defender, Malwarebytes, Kaspersky, Bitlocker, Veracrypt, ...
- ▶ **Attentes des participants**
  - Protection du courriel (Vadeseure, Fortinet, Spamassasin ...)
- ▶ **Comprendre les enjeux de la cybersécurité**
  - Revue de presse
  - Description de cas modèles et de leurs impacts
- ▶ **Comprendre qui peut être la cible d'une cyberattaque**
- ▶ **Connaître les cyberattaques les plus répandues (mises en situation)**
  - Phishing
  - Fraude au président / au faux ordre de virement
  - Rançongiciel
- ▶ **Connaître les solutions techniques**
  - Protection périmétrique (Fortinet, pfSense, Serenicity ...)
  - Protection des équipements finaux (Smartphones,
- ▶ **Et surtout les solutions humaines ...**
  - Sensibilisation
  - Formation
- ▶ **Détecter les risques informatiques dans mon entreprise**
  - Auto-diagnostic
- En individuel**
- ▶ **Définir son plan d'actions :**
  - Les participants réalisent leur propre diagnostic
  - Ils établissent leur propre plan d'actions
- ▶ **Information et orientation vers les dispositifs existants**