

# CYBERSÉCURITÉ

## INTRODUCTION



**Durée : 2 heures**

**Moyens pédagogiques :**

- Formation en distanciel
- Démonstration

**Attestation officielle : oui**

**Compétences acquises à l'issue de la formation :**

- Compréhension des types courants de cybermenaces, notamment les logiciels malveillants, les attaques de phishing, les logiciels espions et les violations de données
- Acquérir des compétences pratiques pour se protéger et protéger son organisation contre les cybermenaces
- Apprendre à identifier les données sensibles et à mettre en place des mesures pour garantir leur sécurité

### DESCRIPTION :

De la compréhension des principales cybermenaces à la mise en œuvre de mesures de défense efficaces, cette formation vous permet de protéger au mieux vos données sensibles.

Cette formation propose des stratégies clés pour atténuer le risque de cyberattaques et sécuriser vos informations. Explorez avec nous le monde fascinant et complexe de la cybersécurité et faites de votre environnement numérique un lieu sûr.

*Proposé en partenariat avec Millenium Micro Académie*

### PROGRAMME :

#### Module 1 : Identifier et comprendre les cybermenaces courantes

Les participants seront en mesure d'identifier les différentes formes de cybermenaces, comme les logiciels malveillants, les logiciels espions, les attaques par hameçonnage et les attaques par rançongiciel, et de comprendre comment elles fonctionnent.

#### Module 2 : Mettre en œuvre des pratiques de sécurité efficaces

Ils apprendront à appliquer des stratégies de cybersécurité, telles que l'utilisation de mots de passe forts, la mise à jour régulière des logiciels et des systèmes, la navigation sécurisée sur Internet, et l'installation et l'utilisation d'outils de sécurité informatique.

#### Module 3 : Protéger les données personnelles et sensibles

Les participants seront en mesure d'identifier les types de données qui nécessitent une protection spéciale, de comprendre les lois et réglementations pertinentes, et de mettre en œuvre des pratiques pour garantir la sécurité de ces données, comme le cryptage et l'authentification à deux facteurs.

(suite page suivante)



### Module 4 : Réagir de manière appropriée aux incidents de cybersécurité

Ils acquerront des compétences pour détecter les signes d'une violation de sécurité potentielle, pour signaler correctement les incidents de sécurité et pour participer à la réponse à l'incident

### Module 5 : Maintenir une culture de sécurité dans leur environnement

Les participants seront en mesure d'évaluer régulièrement leurs pratiques de sécurité, de se tenir au courant des dernières menaces et tendances en matière de cybersécurité, et de promouvoir une culture de sécurité parmi leurs collègues ou les membres de leur organisation.

