**SARL ONEO**
1025 rue Henri Becquerel
Parc Club du Millénaire, Bât. 27
34000 MONTPELLIER
**N° organisme : 91 34 0570434**

**Nous contacter :**
**+33 (0)4 67 13 45 45**
**www.ait.fr**
**contact@ait.fr**

| | |
|---|---|
| Référence | **4-SE-DEF1** |
| Durée | **0,5 jour (3,5 heures)** |
| Éligible CPF | **NON** |
| Mise à jour | **06/09/2023** |

# Cybersécurité : les bonnes pratiques

## Objectifs pedagogiques

- Aider les responsables des TPE et PME à protéger leur entreprise des menaces informatiques

## Public concerne

- Responsable, technicien, correspondant informatique

## Prerequis

- Une réelle connaissance informatique est nécessaire

## Moyens pedagogiques

- Réflexion de groupe et apports théoriques du formateur
- Travail d'échange avec les participants sous forme de réunion-discussion
- Utilisation de cas concrets issus de l'expérience professionnelle
- Validation des acquis par des questionnaires, des tests d'évaluation, des mises en situation et des jeux pédagogiques
- Alternance entre apports théoriques et exercices pratiques (en moyenne 30 à 50%)
- Remise d'un support de cours.

## Modalites d'evaluation

- Feuille de présence signée en demi-journée,
- Evaluation des acquis tout au long de la formation,
- Questionnaire de satisfaction,
- Attestation de stage à chaque apprenant,
- Positionnement préalable oral ou écrit,
- Evaluation formative tout au long de la formation,
- Evaluation sommative faite par le formateur ou à l'aide des certifications disponibles

## Moyens techniques en presentiel

- Accueil des stagiaires dans une salle dédiée à la formation équipée à minima d'un vidéo projecteur et d'un tableau blanc et/ou paperboard.
- Pour les formations nécessitant un ordinateur, un PC est mis à disposition de chaque participant.

## Moyens techniques en distanciel

- A l'aide d'un logiciel (Teams, Zoom...), d'un micro et éventuellement d'une caméra les apprenants interagissent et communiquent entre eux et avec le formateur.
- Sessions organisées en inter comme en intra entreprise.
- L'accès à l'environnement d'apprentissage ainsi qu'aux preuves de suivi et d'assiduité (émargement, évaluation) est assuré.
- Pour toute question avant et pendant le parcours, assistance technique à disposition au 04 67 13 45 45.

## Organisation

- Délai d'accès : 5 jours ouvrés
(délai variable en fonction du financeur)
- Les cours ont lieu de 9h à 12h30 et de 13h30 à 17h

## Accessibilite

- Les personnes en situation d'handicap sont invitées à nous contacter directement, afin d'étudier ensemble les possibilités de suivre la formation.
- Pour tout renseignement, notre référent handicap reste à votre disposition : mteyssedou@ait.fr

## Profil formateur

- Nos formateur sont des experts dans leurs domaines d'intervention
- Leur expérience de terrain et leurs qualités pédagogiques constituent un gage de qualité.

## Certification possible

- PCIE

# Cybersécurité : les bonnes pratiques

## Accueil et introduction

- ☐ Accueil des participants
- ☐ Présentation de l'objectif du cours
- ☐ Brève introduction à la cybersécurité

## Les menaces en ligne pour les TPE et PME

- ☐ Les principales menaces en ligne : phishing, ransomware, malware, etc
- ☐ Les menaces venant de l'intérieur : virus, vol de données, destruction de données…
- ☐ Exemples de cas réels de cyberattaques contre les petites entreprises
- ☐ Les conséquences financières et de réputation des cyberattaques

## Bonnes pratiques en cybersecurite

- ☐ Utilisation de mots de passe forts et uniques
- ☐ Cryptages de fichiers
- ☐ Mises à jour régulières des logiciels
- ☐ Sensibilisation à l'email et aux pièces jointes suspectes
- ☐ Sensibilisation aux bonnes pratiques : échanges de documents, gestion des comptes…
- ☐ Travail à distance et prestataires extérieurs
- ☐ Accès au réseau en interne, Wi-Fi…

## Comment securiser mon environnement Windows et Microsoft ?

- ☐ Outils et conseils pour sécuriser le poste utilisateur (Windows 10/11…)
- ☐ Conseils pour sécuriser mon domaine et Active Directory
- ☐ Outils et conseils pour sécuriser mon serveur de fichiers
- ☐ Conseils pour la gestion du réseau et des serveurs applicatifs