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-DEF2**
Durée	**2 jours (14 heures)**
Éligible CPF	**NON**
Mise à jour	**06/09/2023**

Bonnes pratiques pour défendre son système informatique des menaces en ligne et sur site – 2 jours

Objectifs pedagogiques

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

Public concerne

- Responsable de services informatiques et intervenants techniques (service IT)

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

- Aucune

Bonnes pratiques pour défendre son système informatique des menaces en ligne et sur site – 2 jours

Accueil et introduction

- ☐ 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
- ☐ Cryptage de fichiers
- ☐ Mises à jour régulières des logiciels
- ☐ Sensibilisation à l'email et aux pièces jointes suspectes
- ☐ Sensibilisation aux bonnes pratiques : usb, échanges de documents, gestion des comptes…
- ☐ Travail à distance et prestataires extérieurs
- ☐ Accès au réseau en inter, Wi-Fi…

Comment securiser mon environnement

- ☐ Le poste de travail
- ☐ Outils et conseils pour sécuriser le poste utilisateur (Windows 10/11…)

Suite de la securisation du poste client

- ☐ Rappels des technologies disponibles dans Windows : Antivirus, boot sécurisé…
- ☐ Sécurisation par GPO
- ☐ Cryptage de postes et des fichiers
- ☐ Gestion des certificats

Comment securiser le domaine et Active Directory ?

- ☐ Comment bien organiser Active Directory et les GPO
- ☐ Renforcer la gestion des comptes et des groupes pour éviter les failles

Comment surveiller Active Directory

- ☐ Comment surveiller son SI à la recherche d'anomalies
- ☐ Bonnes pratiques et sources d'informations pour aller plus loin…

Comment securiser mon serveur de fichiers ?

- ☐ Bonnes pratiques pour gérer le serveur et les permissions sur les fichiers
- ☐ Outils pour sécuriser le serveur de fichiers
- ☐ Gestionnaire de ressources, sysinternals…
- ☐ Comment surveiller les accès aux fichiers ?

Securiser les services reseaux du quotidien

- ☐ Service DHCP et Serveur DNS : quels risques et quelles solutions ?
- ☐ Gestion des accès depuis l'extérieur : VPN, Web, Rds…
- ☐ Gestion du Wifi : accès privé / accès public

Gestion des mises a jour serveurs et postes clients

- ☐ Mise à jour manuelle ou automatisée
- ☐ Mise à jour des postes clients : obligatoire / falcultative
- ☐ Mise à jour des serveurs : bonnes pratiques ?

Serveurs d'impressions et serveurs applicatifs

- ☐ Comment augmenter la sécurité de l'impression
- ☐ Bonnes pratiques pour les serveurs applicatifs

PREVOIR UN PLAN DE REPRISE ET DE CONTINUITE EN CAS D'ATTAQUES OU DE PANNE

- ☐ Evaluer les risques
- ☐ Définir les priorités
- ☐ Assurer la continuité