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

Nous contacter :
04 67 13 45 45
www.ait.fr
contact@ait.fr

Référence	**4-SE-SERV**
Durée	**4 jours (28 heures)**
Éligible CPF	**NON**
Mise à jour	**27/11/2023**

Sécuriser mes serveurs Microsoft et mon SI

Objectifs pédagogiques

- Réduire l'exposition aux risques
- Gérer et administrer selon les meilleures pratiques
- Protéger et défendre son système d'information et ses serveurs concrètement sur le terrain

Public concerné

Cette formation s'adresse aux administrateurs, aux techniciens et aux responsables de parc informatique en environnement Microsoft.

Prérequis

Une réelle connaissance informatique est nécessaire

Moyens pédagogiques

- 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

Modalités d'évaluation

- 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 présentiel

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

Accessibilité

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

Formateur expert du domaine.

Leur expérience de terrain et leurs qualités pédagogiques constituent un gage de qualité.

Certification possible

Aucune

Sécuriser mes serveurs Microsoft et mon SI

Mon réseau est-il fiable ?
- ☐ Comment analyser sa propre situation ?
- ☐ Quelques méthodes concrètes d'analyse du risque.
- ☐ Évaluer les priorités
- ☐ Mettre en perspectives les actions à mener sur le terrain par les IT

Sécurisation de l'OS du serveur :

Quel OS Microsoft pour quel usage ?
- ☐ Quel OS Microsoft pour quel usage ?
- ☐ Version Core / Nano / Conteneur / Version avec ou sans interface graphique ? Standard ou Datacenter ?

Et la haute disponibilité dans tout ça ?
- ☐ Rappel des technologies disponibles pour l'environnement Microsoft Serveur
- ☐ Virtualisation / Cluster...

Les outils de sécurisation à ma disposition :
- ☐ Modèles d'administration
- ☐ Modèles de sécurité : SCM / SCT
- ☐ GPO
- ☐ Device Guard et Credential Guard
- ☐ Bonnes pratiques
- ☐ Normes et règles : Microsoft / Anssi
- ☐ Sources d'informations sur le Web

Maintenir son OS à jour :
- ☐ Comment obtenir et déployer les MaJ de l'OS : conseils, bonnes pratiques et outils disponibles...

Administration "Juste à temps"
- ☐ Comment utiliser l'administration "juste à temps" sur mon parc ?
- ☐ Mise en oeuvre

Forêt Bastion

PowerShell et la sécurité
- ☐ PowerShell et la sécurité

Sécuriser son Active Directory... bien sûr, mais comment ?
- ☐ Sécuriser son Active Directory... bien sûr, mais comment ?

Analyse des risques et des attaques spécifiques au SI et à l'AD...
- ☐ Analyse des risques et des attaques spécifiques au SI et à l'AD...

Sécuriser le contrôleur de domaine
- ☐ Sécuriser le contrôleur de domaine
- ☐ Sauvegarde et restauration
- ☐ RODC
- ☐ AD LDS

Réduction de la surface d'attaque de l'annuaire
- ☐ Normes et bonnes pratiques : Microsoft / Anssi
- ☐ Gestion des privilèges
- ☐ Délégation et administration avec privilèges minimum
- ☐ Authentification robuste et sécurisation d'accès au contrôleur de domaine
- ☐ Gestion des "droits d'utilisateurs et des services"
- ☐ Gestion des comptes d'ordinateurs et de services
- ☐ Gestion des groupes pour une meilleure sécurité

Surveillance de l'AD à la recherche d'attaques

- ☐ Les outils disponibles dans Windows : audit / powershell...
- ☐ Être alerté d'un danger potentiel
- ☐ Des outils tiers possibles

Plan de reprise ou de continuité de service en cas de compromission

- ☐ C'est arrivé ! Il me faut du temps pour réparer... Quelle est ma stratégie pendant cette période ?

Microsoft Azure et la synchronisation de l'annuaire avec le nuage

- ☐ Scénario de synchronisation AD avec Azure
- ☐ Gestion des groupes et des comptes utilisateurs
- ☐ Approche sécuritaire

Sources d'information pour la sécurisation de l'AD : normes et bonnes pratiques

- ☐ Articles Microsoft
- ☐ Articles de l'Anssi

Gestion des certificats dans Windows

- ☐ Tour d'horizon des certificats les plus utilisés : authentification / cryptage... / Rds / Exchange...
- ☐ Installation et administration de l'autorité de certification Microsoft
- ☐ Mise en œuvre concrètes des certificats

Sécurisation d'un serveur applicatif

- ☐ Applocker
- ☐ WDAC
- ☐ Le cas de messagerie Exchange
- ☐ Le cas de l'environnement RDS

Sécurisation des services réseaux

- ☐ Durcissement des protocoles utiles : Smb, Rdp, ...
- ☐ Cryptage de trafic réseau : IPSEC / SMB...
- ☐ Sécurisation du DHCP
- ☐ Sécurisation du DNS
- ☐ Pare-feu
- ☐ Serveur Radius et NPS / Contrôle d'accès réseau

Sécurisation du serveur de fichiers

- ☐ Filtrage - Quotas - Gestionnaire de rapports
- ☐ Classification de données et tâches de gestion de fichiers
- ☐ Chiffrement : EFS / BitLocker / Partage de fichiers chiffrés
- ☐ Surveillance de l'accès aux fichiers et alertes
- ☐ Gestion des permissions
- ☐ Bonnes pratiques d'administration
- ☐ Haute disponibilité : Cluster / DFS / ...

Sécurisation de la virtualisation

- ☐ Machines virtuelles blindées
- ☐ Host Guardian Service

Synthèse sur la protection de notre SI