

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



CERTIFICATION POSSIBLE

- ICDL

Sécuriser mes Serveurs Microsoft et mon SI

MON RÉSEAU EST-IL FIABLE ?

- Comment analyser sa propre situation ?
- Quelques méthodes concrètes d'analyse du risque.
- Evaluer 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 ?

- 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 œuvre

FORÊT BASTION

POWERSHELL ET LA SÉCURITÉ

SÉCURISER SON ACTIVE DIRECTORY...BIEN SÛR, MAIS COMMENT ?

ANALYSE DES RISQUES ET DES ATTAQUES SPÉCIFIQUES AU SI ET À L'AD...

SÉCURISER LE CONTRÔLEUR DE DOMAINE

- Sauvegarde et Restauration
- RODC
- AD LDS

RÉDUCTION DE LA SURFACE D'ATTAQUE DE L'ANNUAIRE AD

- 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 des 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 – Gestionnaires 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