Sécurisation de Windows

Les bonnes pratiques

Les services de sécurité

Restreindre les droits administrateur avec JEA

Just Enough Administration (JEA) est une technologie de sécurité qui permet une administration déléguée de tout ce qui peut être géré avec PowerShell.

- Réduire le nombre d'administrateurs sur vos ordinateurs
- Limiter les opérations réalisables par les utilisateurs
- Journalisation du travail des utilisateurs

En savoir plus https://learn.microsoft.com/fr-fr/powershell/scripting/learn/remoting/jea/using-jea?view=powershell-7.3

MIM

MIM 2016 est la solution de gestion des identités de Microsoft. Il s'agit plus d'un ensemble de produits que d'une solution unique :

- MIM 2016 Synchronization Service est le composant historique de cette solution.
- MIM 2016 Service est un moteur de synchronisation, un portail web et un moteur de workflow (extensible avec MIMWALL).
- BHOLD est le composant de MIM 2016 qui permet de faire de l'attestation, de la certification et du SOD. Ce composant a été très peu déployé en entreprise.
- Le moteur de rapport de MIM 2016 s'appuie sur le produit Microsoft System Center Service Manager (SCSM).
- Le composant MIM 2016 Certificate Management (anciennement appelée Certificate Lifecycle Manager – CLM) est une solution de gestion de certificats et de cartes à puces virtuelles.

- Le composant Privilege Access Management (PAM) permet de gérer les groupes à fort privilèges avec la possibilité de définir des accès temporaires à ces groupes.

En savoir plus < https://docs.microsoft.com/fr-fr/microsoft-identity-manager/microsoft-identity-manager-2016>

Contrôle d'application avec Windows Defender

Aujourd'hui, les méthodes traditionnelles de détection basée sur les signatures des solutions antivirus, offrent une protection insuffisante contre les nouvelles attaques.

Le contrôle de l'application est une ligne essentielle de défense pour se protéger menaces actuelles. Le contrôle de l'application n'utilise pas le modèle d'approbation classique où toutes les applications sont supposées êtres dignes de confiance.

Windows Defender Application Control (WDAC) est une solution visant à réduire ces types de menaces, en limitant les applications que les utilisateurs sont autorisés à exécuter et en limitant le code qui s'exécute dans le noyau du système. Les stratégies WDAC bloquent également les scripts non signés, les MSI et Windows PowerShell s'exécute en Mode Limité.

NB : Les stratégies WDAC peuvent être créés uniquement sur les ordinateurs exécutant Windows 10 entreprise ou Windows Server 2016.

Guide de conception WDAC https://docs.microsoft.com/fr-fr/windows/security/threat-protection/windows-defender-application-control/windows-defender-application-control-design-guide>
Guide de déploiement de WDAC < https://docs.microsoft.com/fr-fr/windows/security/threat-protection/windows-defender-application-control/windows-defender-application-control-deployment-guide

Device Guard

C'est un ensemble de fonctionnalités de sécurité matérielle et logicielle.

- **Hyper-V Code Integrity (HVCI)**, l'un des services de la sécurité basée sur la virtualisation. Il permet de s'assurer que seuls les drivers, exécutables et DLLs respectant la stratégie d'entreprise sont autorisés à se lancer.
- **Code Integrity** va permettre l'exécution dans le kernel du code de confiance et des programmes approuvés dans l'environnement utilisateur. Pour cela, il s'appuie sur une

stratégie nommée "**Code Integrity Policy**" qui est un fichier déployé sur les postes de travail référençant les signataires de code de confiance.

NB. *Pour bloquer des applications au cas par cas, il convient de se tourner vers AppLocker et de créer les règles spécifiques.*

En savoir plus https://technet.microsoft.com/fr-fr/library/mt463091(v=vs.85).aspx

Advanced Threat Analytics

Permet de gérer la sécurité du réseau de l'entreprise en identifiant des comportements anormaux. Il tente de détecter la présence de logiciels malveillants dans un réseau et verrouille les applications pour empêcher que les données sensibles ne soient copiées dans un appareil. ATA scrute de façon continuelle le réseau de l'entreprise et utilise des techniques d'apprentissage de base pour pouvoir identifier les comportements suspects de dispositifs et d'utilisateurs puis lance une alarme si nécessaire.

En savoir plus https://docs.microsoft.com/fr-fr/advanced-threat-analytics/what-is-ata

Chiffrement et BitLocker

BitLocker est une technique de chiffrement de lecteur qui est utilisée pour sécuriser vos données par mot de passe. Les données sont chiffrées à l'aide d'un algorithme de chiffrement fort ce qui vous confère une sécurité maximale. Il peut être utilisé pour un disque dur interne ou externe et une clé USB.

En savoir plus https://technet.microsoft.com/fr-fr/library/mt404680(v=vs.85).aspx

FSRM

Il intègre une fonctionnalité qui permet de filtrer les fichiers, l'objectif sera alors de bloquer certaines extensions (et fichiers) propres au comportement d'un ransomware, et d'en avertir l'administrateur par e-mail et/ou par une entrée dans l'observateur d'événements.

En savoir plus https://docs.microsoft.com/fr-fr/windows-server/storage/fsrm/fsrm-overview

ADRMS

Cette technologie permet la protection des informations numériques, utilisant le chiffrement des données (via des clés) et une restriction sur les droits d'accès sur les documents sensibles (mails, documents confidentiels).
L'avantage est que la protection des données est inscrite dans le document lui-même, ce qui permet de garder sa protection à l'intérieur et à l'extérieur du réseau, mais aussi en ligne et hors ligne.

En savoir plus <https://msdn.microsoft.com/fr-fr/library/hh831364(v=ws.11).aspx

WSUS

Service permettant de distribuer les mises à jour (Windows Update) pour Windows et d'autres applications Microsoft sur les différents ordinateurs fonctionnant sous Windows au sein d'un parc informatique.

En savoir plus https://msdn.microsoft.com/fr-fr/library/hh852340(v=ws.11).aspx

Le firewall

Permet de protéger localement un serveur ou une station de travail. Il existe la possibilité de créer ses propres règles dans la partie configuration avancée (voir tuto).

Serveur NPS

Network Policy server, gère l'authentification et les autorisations selon les différents modes de connexion (locale, VPN…). Il intègre RADIUS et NAP.

RADIUS

Le serveur NPS centralise l'authentification, l'autorisation et la gestion de comptes pour les connexions sans fil, les connexions à commutateur d'authentification, et les connexions d'accès à distance et de réseau privé virtuel (VPN).

Serveur de stratégie NAP

Le serveur NPS évalue les déclarations d'intégrité envoyées par les ordinateurs clients compatibles avec la protection d'accès réseau (NAP) qui tentent de se connecter au réseau. Les systèmes ne correspondant pas aux critères définis ne seront pas capables d'exploiter le réseau avec les systèmes dits sains, seul un accès restreint est alors autorisé.

Il s'appuie sur des règles telles que :

- un logiciel anti-virus mis à jour ;
- un pare-feu activé
- existence de serveurs de réseaux privés virtuels (VPN)
- présence de serveurs mandataires (proxy)

https://docs.microsoft.com/fr-fr/windows-server/networking/technologies/nps/nps-top

Docker

Solution de virtualisation applicative, ce qui veut dire que l'on isole l'application du système d'exploitation afin qu'elle puisse être transportée d'une machine à une autre en gardant les configurations effectuées. Cela permet d'effectuer un déploiement de masse rapide et cohérent. De plus, cela permet d'exécuter plusieurs instances de cette application sans risque de conflit.

L'avantage est qu'il n'est pas nécessaire d'embarquer un OS complet pour chaque application virtualisée.

https://docs.microsoft.com/fr-fr/virtualization/windowscontainers/quick-start/quick-start-windows-server

Les GPO

Modifier le répertoire de création de nouveaux ordinateurs

Lorsque vous ajoutez un nouvel ordinateur dans votre domaine Active Directory, s'il n'a pas été créé au préalable, le compte ordinateur est automatiquement créé dans le conteneur Computers qui malheureusement ne peut pas recevoir de stratégie de groupe spécifique.

Il est possible de modifier l'emplacement par défaut de création de comptes ordinateur.

Commencez par créer une nouvelle Unité d'organisation nommée **Ordinateurs.**

Puis, lancez une invite de commande et entrez la commande :
redircmp « OU=Ordinateurs, DC=NomDuDC, DC=NomDuDC »
Par exemple, « OU=Ordinateurs, DC=societe, DC=local »

Lors des prochaines jonctions, les comptes ordinateur seront créés dans la nouvelle unité d'organisation, avec la possibilité de mettre en place des GPO.

Protéger l'accès anonyme

Sous Windows 2012 R2, on doit configurer les 4 paramètres de stratégies de groupe pour se protéger des accès anonymes. Deux choix soit en jouant sur stratégies locales (un serveur) soit via les GPO (toutes les serveurs)

Configuration ordinateur > Stratégies > Paramètres Windows > Paramètres de sécurité > Options de sécurité

- Accès réseau – **Permet la traduction de noms/SID anonymes**
  Permet à un anonyme de retrouver le nom d'un utilisateur à partir de son SID. Il faut donc désactiver ce paramètre.
- Accès réseau – **Ne pas autoriser l'énumération anonyme des comptes SAM**
  Le système remplace l'autorisation "Tout le monde" par "Utilisateurs authentifiés" concernant la lecture de cette ressource. Il faut donc activer ce paramètre.
  NB : Ce paramètre n'aura aucun impact sur un serveur contrôleur de domaine, car sa base SAM est inactive comme il joue le rôle d'annuaire.
- Accès réseau : **ne pas autoriser l'énumération anonyme des comptes et partages SAM**
  Même chose que le paramètre précédent, mais cette fois-ci pour les partages situés sur la machine. Il faut activer ce paramètre.
- Accès réseau : **les autorisations Tout le monde s'appliquent aux utilisateurs anonymes**
  Implique que les utilisateurs anonymes peuvent accéder à toutes les ressources pour lesquelles le groupe "Tout le monde" dispose d'autorisations. Il est nécessaire de s'assurer que ce paramètre est bien désactivé.

Gestion des applications via AppLocker

Cette fonctionnalité permet de créer des règles pour autoriser ou refuser l'exécution d'applications qu'un utilisateur pourrait lancer. Elle contrôle les fichiers exécutables, les scripts , les fichiers Windows Installer et les fichiers DLL.

Les stratégies AppLocker peuvent être implémentées par unité d'organisation à l'aide d'une stratégie de groupe.

La configuration de cette stratégie de groupe se trouve dans Configuration de l'ordinateur/Stratégie/Paramètres Windows/Paramètres de Sécurité/Stratégie de contrôle de l'application/AppLocker.

Générer les règles par défaut : Faire un clic droit sur règles de l'exécutable ou pour règles de script et cliquer sur "Créer des règles par défaut"

Configurer les règles de l'exécutable ou de script : clic droit sur règles de l'exécutable/script pour empêcher l'exécution , puis sur "Créer une règle". Dans la rubrique Autorisation, sélectionner "Refuser" et poursuivre les instructions.

Configuration de l'identité de l'application : Sélectionner Services système dans le Paramètre de sécurité, doubler cliquer sur Identité de l'application. Cocher "Définir ce paramètre de stratégie et le mode de démarrage de service Automatique".

La configuration de mise en application des règles : Sélectionner AppLocker, cliquer sur le lien Configurer la mise en application des règles. Cocher Configurer pour appliquer les règles dans les rubriques Régles de l'exécutable et règles de script.

Groupes restreints

Les groupes restreints permettent à l'administrateur de rendre un utilisateur du domaine administrateur local des postes de travail, par exemple pour rendre les techniciens du support technique administrateurs de tous les postes sans qu'ils soient affectés au groupe administrateurs du domaine.

- Dans la console éditeur de gestion des Stratégies de groupe, développer Configuration de l'ordinateur/Stratégies/Paramètres Windows/Paramètres de Sécurité, clic droit sur "Groupes restreints", puis "Ajouter groupe". Rechercher le groupe contenant les techniciens (créé au préalable).
- Ajouter les groupes d'utilisateurs à ce groupe restreint.

- Ensuite, cliquer sur “Ajouter” au niveau de “Ce groupe est membre de” indiquer “Administrateurs” sans passer par “Parcourir” (on ne fait pas référence à un groupe Active Directory).
- Forcer l’application de la stratégie de groupe par la commande gpupdate/force.

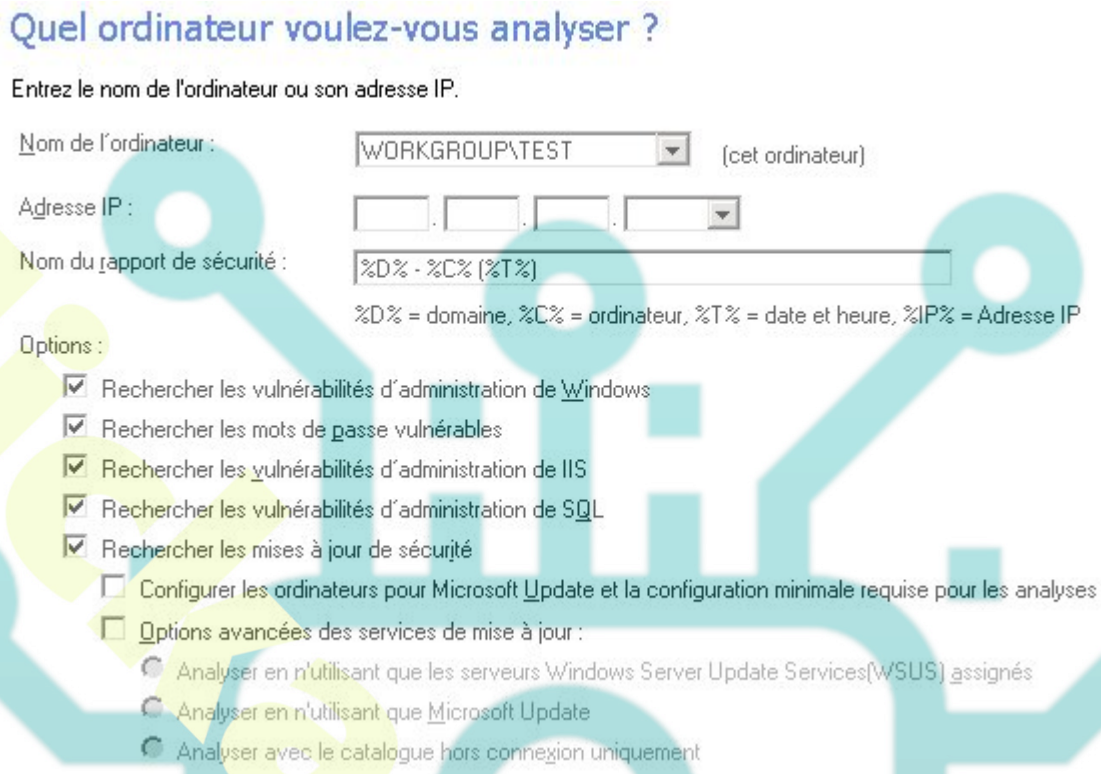
Les outils

Analyser les risques pour définir une stratégie de sécurité

Microsoft a mis à votre disposition **MBSA** (Microsoft Baseline Security Analyzer), un outil gratuit, pour aider à sécuriser les systèmes d’exploitation.
Il permet de détecter les erreurs de configuration de sécurité courantes et les mises à jour de sécurité manquantes. Il vous met à disposition les correctifs adéquats.

Vous pouvez télécharger là **https://www.microsoft.com/fr-fr/download/details.aspx?id=19892**

Une fois installé, vous pouvez analyser un réseau ou bien une machine.
Il suffit de rentrer son IP et de faire OK. L’analyse prendre une minute environ.



Une fois l'analyse terminée, il informe des erreurs détectées dans des rapports classés en différentes rubriques. Par exemple: Analyse de SQL Server, Analyse de MSSQL, Vulnérabilité d'administration, d'Internet Explorer, IIS, etc…

On peut voir la criticité de l'alerte. Et ainsi savoir qu'une mise à jour doit être installée pour tel produit avec le KB correspondant.

Choisir « Comment corriger le problème » et suivre les instructions de Microsoft qui redirigera vers les bulletins de sécurité à appliquer.

Microsoft met à votre disposition un **bulletin de sécurité** **https://technet.microsoft.com/fr-fr/security/bulletin/dn602597.aspx** Windows qui recense les informations détaillées sur tous les composants affectés par des vulnérabilités.

Les outils Sysinternals

Microsoft fournit une suite d'utilitaires pour mieux gérer et dépanner Windows

Interface

- **BgInfo**
  Affichage des informations système sur le fond du bureau
- **Autoruns**
  Interface graphique pour configurer les programmes lancés au démarrage de Windows.

Resources pour la sécurité du système

- **AccessChk**
  Montre quels genre d'accès sont réalisés sur les ressources (fichiers etc.).
- **AccessEnum**
  Indique qui a accès aux répertoires et contenu du registre.
- **RootkitRevealer**
  Détecte les virus dans le registre.
- **SDelete**
  Efface les fichiers de telle sorte qu'on ne puisse ni les récupérer ni voir leur contenu en analysant le disque dur.

Informations sur le système et les fichiers

- **Diskmon**
  Affiche l'activité des disque durs.
- **DiskView**
  Affiche graphiquement l'implantation des fichiers sur un disque dur.
- **DU**
  Affiche pour un répertoire donné, le nombre de fichiers et l'espace occupé.
- **Handle**
  Indique quels fichiers sont utilisés par tel programme, quels processus sont ouverts.
- **NtfsInfo**
  Informations sur un volume NTFS, notamment ou se trouve la table de fichiers et sous quelle forme elle est stockée.
- **ProcessExplorer**
  Interface graphique élaborée pour afficher les processus en cours et l'activité du système.
- **ProcessMonitor**
  Affiche les processus et les logiciels en cours et aide à traquer une activité malveillante.

Il permet d'éditer le registre et remplace regmon.

- **ProcFeatures**
  Affiche le nom et les caractéristiques du processeur, comme par exemple le support 3D Now, SSE…
- **VolumeId**
  Change l'ID d'un volume FAT ou NTFS.
- **WinObj**
  Gestion des objets, pour les administrateurs.
- **Strings**
  Convertit les fichiers contenant des codes unicode illisibles pour les éditeurs de texte.
- **Sync**
  Vide les mémoires tampons et termine les fichiers en cours d'écriture pour pouvoir retirer une unité amovible en toute sécurité.

Gestion du système et du réseau local

- **Portmon**
  Gestion des ports série et parallèle.
- **PsExec**
  RemplacemeTelnet afin d'exécuter des procédures sur une machine distante.
- **PsFile**
  Montre les fichiers distants ouverts et permet de les clôturer.
- **PsInfo**
  Fournit des informations sur un système Windows local ou distant.
- **PsPasswd**
  Changer un mot de passe.
- **PsShutdown**
  Éteint l'ordinateur ou le redémarre.
- **ShareEnum**
  Détecte les domaines utilisateurs pour les fichiers partagés.
- **TcpView**
  Montre les connexions en cours et permet de les fermer.
- **WhoIs**
  Affiche le whois pour un nom de domaine DNS ou une adresse IP.